



TECHDEFENCELABS

Your Trusted **Cyber Security** Partner

A CERT-In Empanelled Information Security Organisation

No:- 3(15)/2004-CERT-In



Document Authorization, Revision History, and Control

Document Preparation	
Document Title	Server, Endpoint, Switch Configuration Review Assessment Report
Evaluated Organization	LKP Securities Limited
Document ID	TDL-LSL-CR-04/26/0041
Report Version	v1.0
Assessment Approach	Configuration Review Assessment Audit Report
Type of Audit Report	First Audit Report
Primary Assessment Period	06-Jan-2026 to 10-Feb-2026
Re-Assessment Period	Follow Up Audit Not Performed
Report Prepared by	Kunal Patil
Reviewed by	Heet Kakadiya
Approved by	Rohit Soni
Released by	Pavan Saxena
Date of Release	21 Apr 2026

Document Change History		
Version	Date	Remarks / Reason of Change
v1.0	21 Apr 2026	First Audit Report

Document Distribution List			
Name	Organization	Designation	Email Id
Dhruv Chauhan	TechD Cybersecurity Limited	Enterprise Business – Manager	dhruv.chauhan@techdefence.com
Mr. Umair Patel	LKP Securities Ltd	Asst. Manager – Information Security	umair.patel@lkpsec.com

Confidentiality and Disclaimer

This report is prepared exclusively for the management of the Evaluated organization and is intended solely for internal use. TechD Cybersecurity Limited disclaims any liability to third parties for the unauthorized use or distribution of this document or its contents. The findings, information, data, advice, and recommendations are based on the cooperation of the Evaluated organization and the data provided during the assessment period. Any limitations due to environmental constraints, access restrictions, or insufficient information may have impacted the thoroughness of our analysis and could result in unidentified vulnerabilities.

The report assesses the initial security controls implemented by the Evaluated organization, specifically focusing on the security of the defined domain and systems in-scope. TechD Cybersecurity Limited highlights areas for potential improvement; however, the responsibility for implementing and maintaining robust security measures lies with the management of the Evaluated organization. The information provided in this document reflects the state of the security environment at the time of preparation and is not an exhaustive evaluation.

Note: *For the purpose of this report, the term “Evaluated organization” refers to the client organization for which this assessment was conducted.*

©TechD Cybersecurity Limited, 2026
9th Floor, Abhishree Adroit,
Near Mansi Circle, Vastrapur,
Ahmedabad-380015.

Table of Contents

Document Authorization, Revision History, and Control	2
Document Preparation	2
Document Change History	2
Document Distribution List	2
Confidentiality and Disclaimer	3
1. Assessment Details	5
1.1 Engagement Scope	5
1.2 Scope Exclusions	7
1.3 Project Team	7
1.4 Tools used during the assessment	7
2. Configuration Audit Methodology and Standards	8
2.1 Phases of the Assessment	8
2.2 Standards and Methodologies	8
3. Executive Summary	9
3.1 Visual Representation of Assessment Results	9
4. Detailed Observations	10
Annexure A - Engagement Limitations	289
Annexure B - Retesting Statement	289
Annexure C - Disclaimer and Precautions for Patch Implementation	290
Annexure D - CERT-In Reporting and Remediation Compliance	290

1. Assessment Details

The Evaluated organization engaged TechD Cybersecurity Limited to assess the Configuration of its infrastructure. The evaluation focused on identifying infrastructure Configuration-level vulnerabilities, testing security of its Configuration. The assessment followed industry standards, including Center for Internet Security (CIS) Benchmarks.

1.1 Engagement Scope

The following Infrastructure IPs provided by the Evaluated organization were identified as in scope for this Configuration review assessment, as defined during the engagement.

In Scope of Assessment			
Type of Infrastructure	IP Address	No. of Devices	Internal/External
Server	172.17.100.31	34	Internal
	172.17.100.32		
	172.17.100.33		
	172.17.100.60		
	172.17.100.120		
	172.17.100.83		
	172.17.100.112		
	172.17.100.20		
	192.168.10.20		
	172.17.100.56		
	172.17.100.59		
	172.17.100.35		
	172.17.100.73		
	172.17.100.66		
	172.17.100.151		
	172.17.100.177		
	172.17.100.152		
	172.17.100.53		
	172.17.100.81		
	172.17.100.68		
	172.17.100.54		
	172.17.100.145		
	172.17.100.146		
	172.17.100.147		
	172.17.100.148		
	172.17.100.38		

	172.17.100.232 172.17.100.233 172.17.100.234 172.17.100.235 172.17.100.236 172.17.100.237 172.17.100.141 172.17.100.140		
Endpoint	192.168.150.180 192.168.150.166 192.168.150.115 192.168.10.85 192.168.10.134 192.168.150.71 192.168.150.238 192.168.150.74 192.168.10.184 192.168.150.133 192.168.10.127 192.168.10.80 192.168.10.194 192.168.150.66 192.168.150.199 192.168.150.139 192.168.150.9 192.168.150.29 192.168.150.64 192.168.150.148	20	Internal
Switch	172.17.100.10 172.17.100.101	2	Internal

1.2 Scope Exclusions

1. The configuration review of any applications hosted on the scoped IP servers/devices fall outside the specified configuration review scope will not be considered.
2. Security testing and Vulnerability Assessment and Penetration Testing (VAPT) of the scoped IPs are outside the scope of the configuration review.
3. Any part of the IPs, management console, or configurations not provided by the evaluated organization will be considered out of scope.

1.3 Project Team

Below are the TechD Cybersecurity Limited Auditing team members who played a key role in this engagement:

Name	Designation	Email-ID	Qualifications/ Certifications	Listed in CERT-In Snapshot? (Yes/No)
Pavan Saxena	Team Lead - VAPT	pavan@techdefence.com	BCA OSCP, (ISC)2 - CC, AZ-900, CEHv12, eJPT-v2, CAP, CNSP, CAPen, KLCP, ISO-27001: Lead Auditor	Yes
Rushikesh Patil	Sr. Security Analyst	Rushikesh.patil@techdefence.com	CEH Master, ISO27001	No
Kunal Patil	Security Analyst	kunal.p@techdefence.com	BSc, CAP, CNSP	No

1.4 Tools used during the assessment

Sr. No	Name of Tool /Software used	Version of the tool /Software used	Open Source /Licensed
01	Nessus Professional	v10.11.3	Licensed

2. Configuration Audit Methodology and Standards

2.1 Phases of the Assessment

- **Pre-engagement Phase:** Define the scope, timeline, and rules of engagement for the review. Identify relevant CIS benchmarks to be followed for the configuration assessment.
- **Configuration Analysis:** Compare system configurations against CIS benchmarks using automated tools and manual techniques. Identify deviations, vulnerabilities, and misconfigurations.
- **Manual Analysis:** Manually inspect critical configurations that automated tools may miss, focusing on areas like user access controls and service settings to uncover complex risks.
- **Reporting and Recommendations:** Document configuration weaknesses and their potential impact. Provide prioritized, actionable recommendations to align systems with CIS best practices.
- **Remediation and Rescan:** After remediation, rescan systems to ensure vulnerabilities are fixed. Verify compliance with CIS benchmarks and ensure no new risks have been introduced.

2.2 Standards and Methodologies

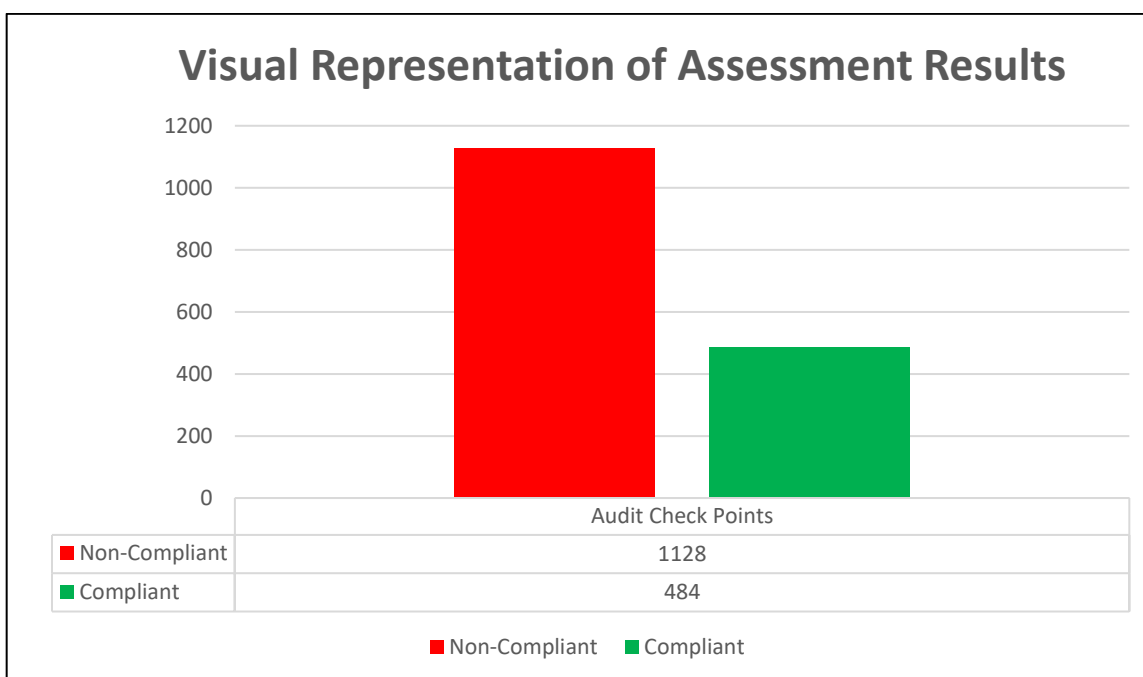
- **Center for Internet Security (CIS) Benchmarks:** The CIS Benchmarks are a set of globally recognized best practices designed to secure IT systems and data from cyber threats. Developed through a consensus-based process involving cybersecurity professionals, government agencies, and industry experts, these benchmarks provide comprehensive configuration guidelines. They cover a wide range of IT systems, including operating systems, server software, cloud computing environments, network devices, and mobile devices.

These benchmarks serve as a foundational standard for performing configuration reviews, ensuring that systems are securely configured and compliant with industry best practices. By following CIS Benchmarks, organizations can significantly enhance their security posture and reduce the risk of vulnerabilities in their systems.

3. Executive Summary

The following section provides an Executive Summary of the Configuration Review Audit, highlighting both compliant and non-compliant aspects identified during the audit. Detailed recommendations for each observation are outlined in Section 4 of this report.

3.1 Visual Representation of Assessment Results



4. Detailed Observations

#	Audit Check Name	IP Address	Infrastructure Type	Status
1	1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
2	1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
3	1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
4	1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
5	1.1.6 (L1) Ensure 'Relax minimum password length limits' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
6	1.2.2 (L1) Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
7	1.2.3 (L1) Ensure 'Allow Administrator account lockout' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
8	2.2.2 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
9	2.2.5 (L1) Ensure 'Allow log on locally' is set to 'Administrators, Users'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
10	2.2.7 (L1) Ensure 'Back up files and directories' is set to 'Administrators'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
11	2.2.16 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests'	192.168.10.85, 192.168.150.71,	Endpoint/ Server	Non-Compliant

		192.168.150.66, 172.17.100.151, 172.17.100.152,		
12	2.2.17 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
13	2.2.18 (L1) Ensure 'Deny log on as a service' to include 'Guests'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
14	2.2.19 (L1) Ensure 'Deny log on locally' to include 'Guests'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
15	2.2.20 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
16	2.2.23 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
17	2.2.24 (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
18	2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
19	2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators, Users'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
20	2.3.1.3 (L1) Configure 'Accounts: Rename administrator account'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
21	2.3.1.4 (L1) Configure 'Accounts: Rename guest account'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
22	2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151,	Endpoint/ Server	Non-Compliant

		172.17.100.152, 192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
23	2.3.7.1 (L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
24	2.3.7.2 (L1) Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
25	2.3.7.4 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
26	2.3.7.5 (L1) Configure 'Interactive logon: Message text for users attempting to log on'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
27	2.3.7.6 (L1) Configure 'Interactive logon: Message title for users attempting to log on'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
28	2.3.7.8 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
29	2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
30	2.3.9.1 (L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
31	2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
32	2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
33	2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
34	2.3.10.3 (L1) Ensure 'Network access: Do not allow	192.168.10.85,	Endpoint/	Non-Compliant

	anonymous enumeration of SAM accounts and shares' is set to 'Enabled'	192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Server	
35	2.3.10.4 (L1) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
36	2.3.10.10 (L1) Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
37	2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
38	2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
39	2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
40	2.3.11.4 (L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
41	2.3.11.6 (L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
42	2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
43	2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
44	2.3.11.11 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
45	2.3.11.12 (L1) Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts'	192.168.10.85, 192.168.150.71, 192.168.150.66,	Endpoint/ Server	Non-Compliant

		172.17.100.151, 172.17.100.152, 192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,		
46	2.3.11.13 (L1) Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher	172.17.100.151, 192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
47	2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
48	2.3.17.2 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' or higher	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
49	2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
50	5.19 (L1) Ensure 'Remote Procedure Call (RPC) Locator (RpcLocator)' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
51	5.26 (L1) Ensure 'SSDP Discovery (SSDPsrv)' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
52	5.27 (L1) Ensure 'UPnP Device Host (upnphost)' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
53	5.31 (L1) Ensure 'Windows Media Player Network Sharing Service (WMPNetworkSvc)' is set to 'Disabled' or 'Not Installed'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
54	5.32 (L1) Ensure 'Windows Mobile Hotspot Service (icssvc)' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
55	5.38 (L1) Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
56	5.39 (L1) Ensure 'Xbox Live Auth Manager (XblAuthManager)' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant

57	5.40 (L1) Ensure 'Xbox Live Game Save (XblGameSave)' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
58	5.41 (L1) Ensure 'Xbox Live Networking Service (XboxNetApiSvc)' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
59	9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
60	9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
61	9.2.3 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
62	9.2.4 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
63	9.2.5 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
64	9.2.6 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
65	9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
66	9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
67	9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
68	9.3.3 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No'	192.168.10.85, 192.168.150.71,	Endpoint/ Server	Non-Compliant

		192.168.150.66, 172.17.100.151, 172.17.100.152,		
69	9.3.4 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
70	9.3.5 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
71	9.3.6 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
72	9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
73	17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
74	17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
75	17.2.3 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
76	17.3.1 (L1) Ensure 'Audit PNP Activity' is set to include 'Success'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
77	17.3.2 (L1) Ensure 'Audit Process Creation' is set to include 'Success'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
78	17.5.1 (L1) Ensure 'Audit Account Lockout' is set to include 'Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
79	17.5.2 (L1) Ensure 'Audit Group Membership' is set to include 'Success'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151,	Endpoint/ Server	Non-Compliant

		172.17.100.152, 192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,		
80	17.5.5 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
81	17.6.1 (L1) Ensure 'Audit Detailed File Share' is set to include 'Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
82	17.6.2 (L1) Ensure 'Audit File Share' is set to 'Success and Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
83	17.6.3 (L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
84	17.6.4 (L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
85	17.7.3 (L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
86	17.7.4 (L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
87	17.7.5 (L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
88	17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
89	17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
90	17.9.4 (L1) Ensure 'Audit Security System Extension' is set to include 'Success'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
91	18.1.1.1 (L1) Ensure 'Prevent enabling lock screen camera'	192.168.10.85,	Endpoint/	Non-Compliant

	is set to 'Enabled'	192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Server	
92	18.1.1.2 (L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
93	18.1.2.2 (L1) Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
94	18.4.1 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
95	18.4.2 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
96	18.4.4 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
97	18.4.5 (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
98	18.4.6 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
99	18.5.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
100	18.5.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
101	18.5.5 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
102	18.5.7 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66,	Endpoint/ Server	Non-Compliant

		172.17.100.151, 172.17.100.152,		
103	18.5.9 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
104	18.5.10 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires' is set to 'Enabled: 5 or fewer seconds'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
105	18.5.13 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
106	18.6.4.1 (L1) Ensure 'Configure multicast DNS (mDNS) protocol' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
107	18.6.7.1 (L1) Ensure 'Audit client does not support encryption' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
108	18.6.7.2 (L1) Ensure 'Audit client does not support signing' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
109	18.6.7.3 (L1) Ensure 'Audit insecure guest logon' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
110	18.6.7.4 (L1) Ensure 'Enable authentication rate limiter' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
111	18.6.7.5 (L1) Ensure 'Enable remote mailslots' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
112	18.6.7.6 (L1) Ensure 'Mandate the minimum version of SMB' is set to 'Enabled: 3.1.1'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
113	18.6.7.7 (L1) Ensure 'Set authentication rate limiter delay (milliseconds)' is set to 'Enabled: 2000' or more	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant

114	18.6.8.1 (L1) Ensure 'Audit insecure guest logon' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
115	18.6.8.2 (L1) Ensure 'Audit server does not support encryption' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
116	18.6.8.3 (L1) Ensure 'Audit server does not support signing' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
117	18.6.8.4 (L1) Ensure 'Enable insecure guest logons' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
118	18.6.8.5 (L1) Ensure 'Enable remote mailslots' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
119	18.6.8.6 (L1) Ensure 'Mandate the minimum version of SMB' is set to 'Enabled: 3.1.1'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
120	18.6.8.7 (L1) Ensure 'Require Encryption' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
121	18.6.11.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
122	18.6.11.3 (L1) Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
123	18.6.14.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with 'Require Mutual Authentication', 'Require Integrity', and 'Require Privacy' set for all NETLOGON and SYSVOL shares'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
124	18.6.21.1 (L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 3 = Prevent Wi-Fi when on Ethernet'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
125	18.6.23.2.1 (L1) Ensure 'Allow Windows to automatically connect to suggested open hotspots, to networks shared	192.168.10.85, 192.168.150.71,	Endpoint/ Server	Non-Compliant

	by contacts, and to hotspots offering paid services' is set to 'Disabled'	192.168.150.66, 172.17.100.151, 172.17.100.152,		
126	18.7.1 (L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
127	18.7.2 (L1) Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
128	18.7.3 (L1) Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
129	18.7.4 (L1) Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
130	18.7.5 (L1) Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
131	18.7.6 (L1) Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections:' is set to 'Enabled: Negotiate' or higher	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
132	18.7.7 (L1) Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
133	18.7.8 (L1) Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
134	18.7.10 (L1) Ensure 'Limits print driver installation to Administrators' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
135	18.7.11 (L1) Ensure 'Manage processing of Queue-specific files' is set to 'Enabled: Limit Queue-specific files to Color profiles'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
136	18.7.12 (L1) Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151,	Endpoint/ Server	Non-Compliant

		172.17.100.152, 192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,		
137	18.7.13 (L1) Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
138	18.9.3.1 (L1) Ensure 'Include command line in process creation events' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
139	18.9.4.1 (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
140	18.9.4.2 (L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
141	18.9.5.1 (L1) Ensure 'Turn On Virtualization Based Security' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
142	18.9.5.2 (L1) Ensure 'Turn On Virtualization Based Security: Select Platform Security Level' is set to 'Secure Boot' or higher	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
143	18.9.5.3 (L1) Ensure 'Turn On Virtualization Based Security: Virtualization Based Protection of Code Integrity' is set to 'Enabled with UEFI lock'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
144	18.9.5.4 (L1) Ensure 'Turn On Virtualization Based Security: Require UEFI Memory Attributes Table' is set to 'True (checked)'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
145	18.9.5.5 (L1) Ensure 'Turn On Virtualization Based Security: Credential Guard Configuration' is set to 'Enabled with UEFI lock'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
146	18.9.5.6 (L1) Ensure 'Turn On Virtualization Based Security: Secure Launch Configuration' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
147	18.9.5.7 (L1) Ensure 'Turn On Virtualization Based Security: Kernel-mode Hardware-enforced Stack Protection' is set to 'Enabled: Enabled in enforcement mode'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
148	18.9.7.2 (L1) Ensure 'Prevent device metadata retrieval	192.168.10.85,	Endpoint/	Non-Compliant

	from the Internet' is set to 'Enabled'	192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Server	
149	18.9.13.1 (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
150	18.9.19.2 (L1) Ensure 'Continue experiences on this device' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
151	18.9.20.1.2 (L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
152	18.9.20.1.6 (L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
153	18.9.26.1 (L1) Ensure 'Allow Custom SSPs and APs to be loaded into LSASS' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
154	18.9.26.2 (L1) Ensure 'Configures LSASS to run as a protected process' is set to 'Enabled: Enabled with UEFI Lock'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
155	18.9.28.1 (L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
156	18.9.28.2 (L1) Ensure 'Do not display network selection UI' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
157	18.9.28.3 (L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
158	18.9.28.4 (L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
159	18.9.33.6.1 (L1) Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66,	Endpoint/ Server	Non-Compliant

		172.17.100.151, 172.17.100.152,		
160	18.9.33.6.2 (L1) Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
161	18.9.33.6.5 (L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
162	18.9.33.6.6 (L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
163	18.9.35.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
164	18.9.35.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
165	18.9.36.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
166	18.9.36.2 (L1) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
167	18.9.51.1.1 (L1) Ensure 'Enable Windows NTP Client' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
168	18.9.52 (L1) Ensure 'Configure the behavior of the sudo command' is set to 'Enabled: Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
169	18.10.4.2 (L1) Ensure 'Not allow per-user unsigned packages to install by default (requires explicitly allow per install)' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
170	18.10.4.3 (L1) Ensure 'Prevent non-admin users from installing packaged Windows apps' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant

171	18.10.5.1 (L1) Ensure 'Let Windows apps activate with voice while the system is locked' is set to 'Enabled: Force Deny'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
172	18.10.6.1 (L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
173	18.10.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
174	18.10.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
175	18.10.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
176	18.10.9.1.1 (L1) Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
177	18.10.13.1 (L1) Ensure 'Turn off cloud consumer account state content' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
178	18.10.13.3 (L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
179	18.10.14.1 (L1) Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
180	18.10.15.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
181	18.10.15.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
182	18.10.15.3 (L1) Ensure 'Prevent the use of security questions for local accounts' is set to 'Enabled'	192.168.10.85, 192.168.150.71,	Endpoint/ Server	Non-Compliant

		192.168.150.66, 172.17.100.151, 172.17.100.152,		
183	18.10.16.1 (L1) Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
184	18.10.16.3 (L1) Ensure 'Disable OneSettings Downloads' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
185	18.10.16.4 (L1) Ensure 'Do not show feedback notifications' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
186	18.10.16.5 (L1) Ensure 'Enable OneSettings Auditing' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
187	18.10.16.6 (L1) Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
188	18.10.16.7 (L1) Ensure 'Limit Dump Collection' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
189	18.10.17.1 (L1) Ensure 'Download Mode' is NOT set to 'Enabled: Internet'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
190	18.10.18.2 (L1) Ensure 'Enable App Installer Experimental Features' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
191	18.10.18.3 (L1) Ensure 'Enable App Installer Hash Override' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
192	18.10.18.4 (L1) Ensure 'Enable App Installer Local Archive Malware Scan Override' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
193	18.10.18.5 (L1) Ensure 'Enable App Installer Microsoft Store Source Certificate Validation Bypass' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151,	Endpoint/ Server	Non-Compliant

		172.17.100.152, 192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,		
194	18.10.18.6 (L1) Ensure 'Enable App Installer ms-appinstaller protocol' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
195	18.10.26.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
196	18.10.26.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
197	18.10.26.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
198	18.10.26.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
199	18.10.26.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
200	18.10.26.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
201	18.10.26.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
202	18.10.26.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
203	18.10.29.3 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
204	18.10.29.4 (L1) Ensure 'Do not apply the Mark of the Web tag to files copied from insecure sources' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
205	18.10.29.5 (L1) Ensure 'Turn off heap termination on	192.168.10.85,	Endpoint/	Non-Compliant

	corruption' is set to 'Disabled'	192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Server	
206	18.10.29.6 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
207	18.10.42.1 (L1) Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
208	18.10.43.4.1 (L1) Ensure 'Enable EDR in block mode' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
209	18.10.43.5.1 (L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
210	18.10.43.6.1.1 (L1) Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
211	18.10.43.6.1.2 (L1) Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
212	18.10.43.6.3.1 (L1) Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
213	18.10.43.7.1 (L1) Ensure 'Enable file hash computation feature' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
214	18.10.43.10.1 (L1) Ensure 'Configure real-time protection and Security Intelligence Updates during OOBE' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
215	18.10.43.10.2 (L1) Ensure 'Scan all downloaded files and attachments' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
216	18.10.43.10.3 (L1) Ensure 'Turn off real-time protection' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66,	Endpoint/ Server	Non-Compliant

		172.17.100.151, 172.17.100.152,		
217	18.10.43.10.4 (L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
218	18.10.43.10.5 (L1) Ensure 'Turn on script scanning' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
219	18.10.43.11.1.1.2 (L1) Ensure 'Configure Remote Encryption Protection Mode' is set to 'Enabled: Audit' or higher	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
220	18.10.43.13.1 (L1) Ensure 'Scan excluded files and directories during quick scans' is set to 'Enabled: 1'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
221	18.10.43.13.2 (L1) Ensure 'Scan packed executables' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
222	18.10.43.13.3 (L1) Ensure 'Scan removable drives' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
223	18.10.43.13.4 (L1) Ensure 'Trigger a quick scan after X days without any scans' is set to 'Enabled: 7'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
224	18.10.43.13.5 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
225	18.10.43.16 (L1) Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
226	18.10.43.17 (L1) Ensure 'Control whether exclusions are visible to local users' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
227	18.10.44.1 (L1) Ensure 'Allow auditing events in Microsoft Defender Application Guard' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant

228	18.10.44.2 (L1) Ensure 'Allow camera and microphone access in Microsoft Defender Application Guard' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
229	18.10.44.3 (L1) Ensure 'Allow data persistence for Microsoft Defender Application Guard' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
230	18.10.44.4 (L1) Ensure 'Allow files to download and save to the host operating system from Microsoft Defender Application Guard' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
231	18.10.44.5 (L1) Ensure 'Configure Microsoft Defender Application Guard clipboard settings: Clipboard behavior setting' is set to 'Enabled: Enable clipboard operation from an isolated session to the host'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
232	18.10.44.6 (L1) Ensure 'Turn on Microsoft Defender Application Guard in Managed Mode' is set to 'Enabled: 1'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
233	18.10.51.1 (L1) Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
234	18.10.57.2.3 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
235	18.10.57.3.3.3 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
236	18.10.57.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
237	18.10.57.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
238	18.10.57.3.9.3 (L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
239	18.10.57.3.9.4 (L1) Ensure 'Require user authentication for remote connections by using Network Level	192.168.10.85, 192.168.150.71,	Endpoint/ Server	Non-Compliant

	Authentication' is set to 'Enabled'	192.168.150.66, 172.17.100.151, 172.17.100.152,		
240	18.10.57.3.9.5 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
241	18.10.57.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
242	18.10.58.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
243	18.10.58.2 (L1) Ensure 'Turn on Basic feed authentication over HTTP' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
244	18.10.59.3 (L1) Ensure 'Allow Cortana' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
245	18.10.59.4 (L1) Ensure 'Allow Cortana above lock screen' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
246	18.10.59.5 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
247	18.10.59.6 (L1) Ensure 'Allow search and Cortana to use location' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
248	18.10.66.2 (L1) Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
249	18.10.66.3 (L1) Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
250	18.10.72.1 (L1) Ensure 'Allow widgets' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151,	Endpoint/ Server	Non-Compliant

		172.17.100.152, 192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,		
251	18.10.76.1.1 (L1) Ensure 'Automatic Data Collection' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
252	18.10.76.1.2 (L1) Ensure 'Notify Malicious' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
253	18.10.76.1.3 (L1) Ensure 'Notify Password Reuse' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
254	18.10.76.1.4 (L1) Ensure 'Notify Unsafe App' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
255	18.10.76.1.5 (L1) Ensure 'Service Enabled' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
256	18.10.76.2.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
257	18.10.78.1 (L1) Ensure 'Enables or disables Windows Game Recording and Broadcasting' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
258	18.10.79.1 (L1) Ensure 'Enable ESS with Supported Peripherals' is set to 'Enabled: 1'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
259	18.10.80.2 (L1) Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
260	18.10.81.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
261	18.10.81.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
262	18.10.82.1 (L1) Ensure 'Configure the transmission of the	192.168.10.85,	Endpoint/	Non-Compliant

	user's password in the content of MPR notifications sent by winlogon.' is set to 'Disabled'	192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Server	
263	18.10.82.2 (L1) Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
264	18.10.89.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
265	18.10.89.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
266	18.10.89.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
267	18.10.89.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
268	18.10.89.2.4 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
269	18.10.91.1 (L1) Ensure 'Allow clipboard sharing with Windows Sandbox' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
270	18.10.91.3 (L1) Ensure 'Allow networking in Windows Sandbox' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
271	18.10.92.2.1 (L1) Ensure 'Prevent users from modifying settings' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
272	18.10.93.1.1 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
273	18.10.93.2.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66,	Endpoint/ Server	Non-Compliant

		172.17.100.151, 172.17.100.152,		
274	18.10.93.2.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
275	18.10.93.2.3 (L1) Ensure 'Enable features introduced via servicing that are off by default' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
276	18.10.93.2.4 (L1) Ensure 'Remove access to 'Pause updates' feature' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
277	18.10.93.4.1 (L1) Ensure 'Manage preview builds' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
278	18.10.93.4.2 (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
279	18.10.93.4.3 (L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
280	18.10.93.4.4 (L1) Ensure 'Enable optional updates' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
281	19.5.1.1 (L1) Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
282	19.7.5.1 (L1) Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
283	19.7.5.2 (L1) Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
284	19.7.8.1 (L1) Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant

285	19.7.8.2 (L1) Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
286	19.7.8.5 (L1) Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
287	19.7.26.1 (L1) Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
288	19.7.40.1 (L1) Ensure 'Turn off Windows Copilot' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
289	19.7.44.1 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Non-Compliant
290	1.1.2 (L1) Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
291	1.1.7 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
292	1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
293	1.2.4 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
294	2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
295	2.2.3 (L1) Ensure 'Act as part of the operating system' is set to 'No One'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
296	2.2.4 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK'	192.168.10.85, 192.168.150.71,	Endpoint/ Server	Compliant

	SERVICE'	192.168.150.66, 172.17.100.151, 172.17.100.152,		
297	2.2.6 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
298	2.2.8 (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
299	2.2.9 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
300	2.2.10 (L1) Ensure 'Create a pagefile' is set to 'Administrators'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
301	2.2.11 (L1) Ensure 'Create a token object' is set to 'No One'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
302	2.2.12 (L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
303	2.2.13 (L1) Ensure 'Create permanent shared objects' is set to 'No One'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
304	2.2.14 (L1) Ensure 'Create symbolic links' is set to 'Administrators'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
305	2.2.15 (L1) Ensure 'Debug programs' is set to 'Administrators'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
306	2.2.21 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
307	2.2.22 (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151,	Endpoint/ Server	Compliant

		172.17.100.152, 192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
308	2.2.25 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
309	2.2.26 (L1) Ensure 'Load and unload device drivers' is set to 'Administrators'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
310	2.2.27 (L1) Ensure 'Lock pages in memory' is set to 'No One'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
311	2.2.30 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
312	2.2.31 (L1) Ensure 'Modify an object label' is set to 'No One'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
313	2.2.32 (L1) Ensure 'Modify firmware environment values' is set to 'Administrators'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
314	2.2.33 (L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
315	2.2.34 (L1) Ensure 'Profile single process' is set to 'Administrators'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
316	2.2.35 (L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
317	2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
318	2.2.39 (L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
319	2.3.1.1 (L1) Ensure 'Accounts: Guest account status' is set	192.168.10.85,	Endpoint/	Compliant

	to 'Disabled'	192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Server	
320	2.3.1.2 (L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
321	2.3.2.2 (L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
322	2.3.7.7 (L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
323	2.3.8.2 (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
324	2.3.8.3 (L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
325	2.3.9.4 (L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
326	2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
327	2.3.10.2 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
328	2.3.10.5 (L1) Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
329	2.3.10.6 (L1) Ensure 'Network access: Named Pipes that can be accessed anonymously' is set to 'None'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
330	2.3.10.7 (L1) Ensure 'Network access: Remotely accessible registry paths' is configured	192.168.10.85, 192.168.150.71, 192.168.150.66,	Endpoint/ Server	Compliant

		172.17.100.151, 172.17.100.152,		
331	2.3.10.8 (L1) Ensure 'Network access: Remotely accessible registry paths and sub-paths' is configured	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
332	2.3.10.9 (L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
333	2.3.10.11 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
334	2.3.10.12 (L1) Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
335	2.3.11.5 (L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
336	2.3.11.8 (L1) Ensure 'Network security: LDAP client encryption requirements' is set to 'Negotiate sealing' or higher	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
337	2.3.11.9 (L1) Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
338	2.3.15.1 (L1) Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
339	2.3.15.2 (L1) Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
340	2.3.17.4 (L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
341	2.3.17.5 (L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant

342	2.3.17.6 (L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
343	2.3.17.7 (L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
344	2.3.17.8 (L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
345	5.3 (L1) Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
346	5.7 (L1) Ensure 'IIS Admin Service (IISADMIN)' is set to 'Disabled' or 'Not Installed'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
347	5.8 (L1) Ensure 'Infrared monitor service (irmon)' is set to 'Disabled' or 'Not Installed'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
348	5.10 (L1) Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Disabled' or 'Not Installed'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
349	5.12 (L1) Ensure 'OpenSSH SSH Server (sshd)' is set to 'Disabled' or 'Not Installed'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
350	5.21 (L1) Ensure 'Routing and Remote Access (RemoteAccess)' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
351	5.23 (L1) Ensure 'Simple TCP/IP Services (simptcp)' is set to 'Disabled' or 'Not Installed'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
352	5.25 (L1) Ensure 'Special Administration Console Helper (sacsvr)' is set to 'Disabled' or 'Not Installed'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
353	5.28 (L1) Ensure 'Web Management Service (WMSvc)' is set to 'Disabled' or 'Not Installed'	192.168.10.85, 192.168.150.71,	Endpoint/ Server	Compliant

		192.168.150.66, 172.17.100.151, 172.17.100.152,		
354	5.37 (L1) Ensure 'World Wide Web Publishing Service (W3SVC)' is set to 'Disabled' or 'Not Installed'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
355	17.2.2 (L1) Ensure 'Audit Security Group Management' is set to include 'Success'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
356	17.5.3 (L1) Ensure 'Audit Logoff' is set to include 'Success'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
357	17.5.4 (L1) Ensure 'Audit Logon' is set to 'Success and Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
358	17.5.6 (L1) Ensure 'Audit Special Logon' is set to include 'Success'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
359	17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to include 'Success'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
360	17.7.2 (L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
361	17.9.2 (L1) Ensure 'Audit Other System Events' is set to 'Success and Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
362	17.9.3 (L1) Ensure 'Audit Security State Change' is set to include 'Success'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
363	17.9.5 (L1) Ensure 'Audit System Integrity' is set to 'Success and Failure'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
364	18.4.3 (L1) Ensure 'Enable Certificate Padding' is set to 'Enabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151,	Endpoint/ Server	Compliant

		172.17.100.152, 192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,		
365	18.5.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
366	18.10.89.2.3 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	192.168.10.85, 192.168.150.71, 192.168.150.66, 172.17.100.151, 172.17.100.152,	Endpoint/ Server	Compliant
367	1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
368	1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
369	1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194,	Endpoint/Server	Non-Compliant

		192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
370	1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
371	1.1.6 (L1) Ensure 'Relax minimum password length limits' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
372	1.2.2 (L1) Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29,	Endpoint/Server	Non-Compliant

		192.168.150.64, 192.168.150.148, 172.17.100.35,		
373	1.2.3 (L1) Ensure 'Allow Administrator account lockout' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
374	2.2.2 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
375	2.2.4 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
376	2.2.5 (L1) Ensure 'Allow log on locally' is set to	192.168.150.180,	Endpoint/Server	Non-Compliant

	'Administrators, Users'	192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
377	2.2.7 (L1) Ensure 'Back up files and directories' is set to 'Administrators'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
378	2.2.16 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
379	2.2.17 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238,	Endpoint/Server	Non-Compliant

		192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
380	2.2.18 (L1) Ensure 'Deny log on as a service' to include 'Guests'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
381	2.2.19 (L1) Ensure 'Deny log on locally' to include 'Guests'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
382	2.2.20 (L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127,	Endpoint/Server	Non-Compliant

		192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
383	2.2.23 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
384	2.2.24 (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
385	2.2.36 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139,	Endpoint/Server	Non-Compliant

		192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
386	2.2.37 (L1) Ensure 'Restore files and directories' is set to 'Administrators'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
387	2.2.38 (L1) Ensure 'Shut down the system' is set to 'Administrators, Users'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
388	2.3.1.1 (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148,	Endpoint/Server	Non-Compliant

		172.17.100.35, 192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
389	2.3.1.4 (L1) Configure 'Accounts: Rename administrator account'		Endpoint/Server	Non-Compliant
390	2.3.1.5 (L1) Configure 'Accounts: Rename guest account'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
391	2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
392	2.3.7.1 (L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115,	Endpoint/Server	Non-Compliant

		192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
393	2.3.7.2 (L1) Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
394	2.3.7.4 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
395	2.3.7.5 (L1) Configure 'Interactive logon: Message text for users attempting to log on'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184,	Endpoint/Server	Non-Compliant

		192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
396	2.3.7.6 (L1) Configure 'Interactive logon: Message title for users attempting to log on'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
397	2.3.7.8 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
398	2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194,	Endpoint/Server	Non-Compliant

		192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
399	2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
400	2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
401	2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29,	Endpoint/Server	Non-Compliant

		192.168.150.64, 192.168.150.148, 172.17.100.35,		
402	2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
403	2.3.10.4 (L1) Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
404	2.3.10.10 (L1) Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
405	2.3.11.1 (L1) Ensure 'Network security: Allow Local System	192.168.150.180,	Endpoint/Server	Non-Compliant

	to use computer identity for NTLM' is set to 'Enabled'	192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
406	2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
407	2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
408	2.3.11.4 (L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238,	Endpoint/Server	Non-Compliant

		192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
409	2.3.11.6 (L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
410	2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
411	2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127,	Endpoint/Server	Non-Compliant

		192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
412	2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
413	2.3.11.11 (L1) Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
414	2.3.11.12 (L1) Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139,	Endpoint/Server	Non-Compliant

		192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
415	2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
416	2.3.17.2 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' or higher	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
417	2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148,	Endpoint/Server	Non-Compliant

		172.17.100.35, 192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
418	5.7 (L1) Ensure 'IIS Admin Service (IISADMIN)' is set to 'Disabled' or 'Not Installed'		Endpoint/Server	Non-Compliant
419	5.9 (L1) Ensure 'Internet Connection Sharing (ICS) (SharedAccess)' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
420	5.25 (L1) Ensure 'Remote Procedure Call (RPC) Locator (RpcLocator)' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
421	5.32 (L1) Ensure 'SSDP Discovery (SSDPSRV)' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115,	Endpoint/Server	Non-Compliant

		192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
422	5.33 (L1) Ensure 'UPnP Device Host (upnphost)' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
423	5.37 (L1) Ensure 'Windows Media Player Network Sharing Service (WMPNetworkSvc)' is set to 'Disabled' or 'Not Installed'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
424	5.38 (L1) Ensure 'Windows Mobile Hotspot Service (icssvc)' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184,	Endpoint/Server	Non-Compliant

		192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
425	5.43 (L1) Ensure 'World Wide Web Publishing Service (W3SVC)' is set to 'Disabled' or 'Not Installed'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
426	5.44 (L1) Ensure 'Xbox Accessory Management Service (XboxGipSvc)' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
427	5.45 (L1) Ensure 'Xbox Live Auth Manager (XblAuthManager)' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194,	Endpoint/Server	Non-Compliant

		192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
428	5.46 (L1) Ensure 'Xbox Live Game Save (XblGameSave)' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
429	5.47 (L1) Ensure 'Xbox Live Networking Service (XboxNetApiSvc)' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
430	9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29,	Endpoint/Server	Non-Compliant

		192.168.150.64, 192.168.150.148, 172.17.100.35,		
431	9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
432	9.2.3 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
433	9.2.4 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
434	9.2.5 (L1) Ensure 'Windows Firewall: Private: Logging: Size	192.168.150.180,	Endpoint/Server	Non-Compliant

	limit (KB)' is set to '16,384 KB or greater'	192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
435	9.2.6 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
436	9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
437	9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238,	Endpoint/Server	Non-Compliant

		192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
438	9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
439	9.3.3 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
440	9.3.4 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127,	Endpoint/Server	Non-Compliant

		192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
441	9.3.5 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
442	9.3.6 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
443	9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139,	Endpoint/Server	Non-Compliant

		192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
444	17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
445	17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
446	17.2.3 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148,	Endpoint/Server	Non-Compliant

		172.17.100.35, 192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
447	17.3.1 (L1) Ensure 'Audit PNP Activity' is set to include 'Success'		Endpoint/Server	Non-Compliant
448	17.3.2 (L1) Ensure 'Audit Process Creation' is set to include 'Success'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
449	17.5.1 (L1) Ensure 'Audit Account Lockout' is set to include 'Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
450	17.5.2 (L1) Ensure 'Audit Group Membership' is set to include 'Success'	192.168.150.180, 192.168.150.166, 192.168.150.115,	Endpoint/Server	Non-Compliant

		192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
451	17.5.5 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
452	17.6.1 (L1) Ensure 'Audit Detailed File Share' is set to include 'Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
453	17.6.2 (L1) Ensure 'Audit File Share' is set to 'Success and Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184,	Endpoint/Server	Non-Compliant

		192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
454	17.6.3 (L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
455	17.6.4 (L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
456	17.7.3 (L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194,	Endpoint/Server	Non-Compliant

		192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
457	17.7.4 (L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
458	17.7.5 (L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
459	17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29,	Endpoint/Server	Non-Compliant

		192.168.150.64, 192.168.150.148, 172.17.100.35,		
460	17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
461	17.9.4 (L1) Ensure 'Audit Security System Extension' is set to include 'Success'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
462	18.1.1.1 (L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
463	18.1.1.2 (L1) Ensure 'Prevent enabling lock screen slide	192.168.150.180,	Endpoint/Server	Non-Compliant

	show' is set to 'Enabled'	192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
464	18.1.2.2 (L1) Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
465	18.4.1 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
466	18.4.2 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238,	Endpoint/Server	Non-Compliant

		192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
467	18.4.4 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
468	18.4.5 (L1) Ensure 'LSA Protection' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
469	18.4.6 (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127,	Endpoint/Server	Non-Compliant

		192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
470	18.4.7 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
471	18.5.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
472	18.5.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139,	Endpoint/Server	Non-Compliant

		192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
473	18.5.5 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
474	18.5.7 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
475	18.5.9 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148,	Endpoint/Server	Non-Compliant

		172.17.100.35, 192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
476	18.5.10 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires' is set to 'Enabled: 5 or fewer seconds'		Endpoint/Server	Non-Compliant
477	18.5.13 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
478	18.6.4.1 (L1) Ensure 'Configure multicast DNS (mDNS) protocol' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
479	18.6.8.1 (L1) Ensure 'Require Encryption' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115,	Endpoint/Server	Non-Compliant

		192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
480	18.6.11.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
481	18.6.11.3 (L1) Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
482	18.6.14.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with 'Require Mutual Authentication', 'Require Integrity', and 'Require Privacy' set for all NETLOGON and SYSVOL shares'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184,	Endpoint/Server	Non-Compliant

		192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
483	18.6.21.1 (L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 3 = Prevent Wi-Fi when on Ethernet'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
484	18.6.23.2.1 (L1) Ensure 'Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
485	18.7.1 (L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194,	Endpoint/Server	Non-Compliant

		192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
486	18.7.2 (L1) Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
487	18.7.3 (L1) Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
488	18.7.4 (L1) Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29,	Endpoint/Server	Non-Compliant

		192.168.150.64, 192.168.150.148, 172.17.100.35,		
489	18.7.5 (L1) Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
490	18.7.6 (L1) Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections:' is set to 'Enabled: Negotiate' or higher	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
491	18.7.7 (L1) Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
492	18.7.8 (L1) Ensure 'Configure RPC packet level privacy	192.168.150.180,	Endpoint/Server	Non-Compliant

	setting for incoming connections' is set to 'Enabled'	192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
493	18.7.9 (L1) Ensure 'Limits print driver installation to Administrators' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
494	18.7.10 (L1) Ensure 'Manage processing of Queue-specific files' is set to 'Enabled: Limit Queue-specific files to Color profiles'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
495	18.7.11 (L1) Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238,	Endpoint/Server	Non-Compliant

		192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
496	18.7.12 (L1) Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
497	18.9.3.1 (L1) Ensure 'Include command line in process creation events' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
498	18.9.4.1 (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127,	Endpoint/Server	Non-Compliant

		192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
499	18.9.4.2 (L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
500	18.9.7.2 (L1) Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
501	18.9.13.1 (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139,	Endpoint/Server	Non-Compliant

		192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
502	18.9.20.1.2 (L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
503	18.9.20.1.6 (L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
504	18.9.26.1 (L1) Ensure 'Allow Custom SSPs and APs to be loaded into LSASS' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148,	Endpoint/Server	Non-Compliant

		172.17.100.35, 192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
505	18.9.28.1 (L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'		Endpoint/Server	Non-Compliant
506	18.9.28.2 (L1) Ensure 'Do not display network selection UI' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
507	18.9.28.3 (L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
508	18.9.28.4 (L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115,	Endpoint/Server	Non-Compliant

		192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
509	18.9.33.6.1 (L1) Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
510	18.9.33.6.2 (L1) Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
511	18.9.33.6.5 (L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184,	Endpoint/Server	Non-Compliant

		192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
512	18.9.33.6.6 (L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
513	18.9.35.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
514	18.9.35.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194,	Endpoint/Server	Non-Compliant

		192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
515	18.9.36.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
516	18.9.36.2 (L1) Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
517	18.9.51.1.1 (L1) Ensure 'Enable Windows NTP Client' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29,	Endpoint/Server	Non-Compliant

		192.168.150.64, 192.168.150.148, 172.17.100.35,		
518	18.10.4.2 (L1) Ensure 'Not allow per-user unsigned packages to install by default (requires explicitly allow per install)' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
519	18.10.4.3 (L1) Ensure 'Prevent non-admin users from installing packaged Windows apps' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
520	18.10.5.1 (L1) Ensure 'Let Windows apps activate with voice while the system is locked' is set to 'Enabled: Force Deny'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
521	18.10.6.1 (L1) Ensure 'Allow Microsoft accounts to be	192.168.150.180,	Endpoint/Server	Non-Compliant

	optional' is set to 'Enabled'	192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
522	18.10.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
523	18.10.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
524	18.10.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238,	Endpoint/Server	Non-Compliant

		192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
525	18.10.9.1.1 (L1) Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
526	18.10.13.1 (L1) Ensure 'Turn off cloud consumer account state content' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
527	18.10.13.3 (L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127,	Endpoint/Server	Non-Compliant

		192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
528	18.10.14.1 (L1) Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
529	18.10.15.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
530	18.10.15.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139,	Endpoint/Server	Non-Compliant

		192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
531	18.10.15.3 (L1) Ensure 'Prevent the use of security questions for local accounts' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
532	18.10.16.1 (L1) Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
533	18.10.16.3 (L1) Ensure 'Disable OneSettings Downloads' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148,	Endpoint/Server	Non-Compliant

		172.17.100.35, 192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
534	18.10.16.4 (L1) Ensure 'Do not show feedback notifications' is set to 'Enabled'		Endpoint/Server	Non-Compliant
535	18.10.16.5 (L1) Ensure 'Enable OneSettings Auditing' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
536	18.10.16.6 (L1) Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
537	18.10.16.7 (L1) Ensure 'Limit Dump Collection' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115,	Endpoint/Server	Non-Compliant

		192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
538	18.10.16.8 (L1) Ensure 'Toggle user control over Insider builds' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
539	18.10.17.1 (L1) Ensure 'Download Mode' is NOT set to 'Enabled: Internet'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
540	18.10.18.2 (L1) Ensure 'Enable App Installer Experimental Features' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184,	Endpoint/Server	Non-Compliant

		192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
541	18.10.18.3 (L1) Ensure 'Enable App Installer Hash Override' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
542	18.10.18.4 (L1) Ensure 'Enable App Installer Local Archive Malware Scan Override' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
543	18.10.18.5 (L1) Ensure 'Enable App Installer Microsoft Store Source Certificate Validation Bypass' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194,	Endpoint/Server	Non-Compliant

		192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
544	18.10.18.6 (L1) Ensure 'Enable App Installer ms-appinstaller protocol' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
545	18.10.26.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
546	18.10.26.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29,	Endpoint/Server	Non-Compliant

		192.168.150.64, 192.168.150.148, 172.17.100.35,		
547	18.10.26.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
548	18.10.26.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
549	18.10.26.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
550	18.10.26.3.2 (L1) Ensure 'Setup: Specify the maximum log	192.168.150.180,	Endpoint/Server	Non-Compliant

	file size (KB)' is set to 'Enabled: 32,768 or greater'	192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
551	18.10.26.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
552	18.10.26.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
553	18.10.29.2 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238,	Endpoint/Server	Non-Compliant

		192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
554	18.10.29.3 (L1) Ensure 'Do not apply the Mark of the Web tag to files copied from insecure sources' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
555	18.10.29.4 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
556	18.10.29.5 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127,	Endpoint/Server	Non-Compliant

		192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
557	18.10.35.1 (L1) Ensure 'Disable Internet Explorer 11 as a standalone browser' is set to 'Enabled: Always'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
558	18.10.42.1 (L1) Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
559	18.10.43.4.1 (L1) Ensure 'Enable EDR in block mode' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139,	Endpoint/Server	Non-Compliant

		192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
560	18.10.43.5.1 (L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
561	18.10.43.6.1.1 (L1) Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
562	18.10.43.6.1.2 (L1) Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148,	Endpoint/Server	Non-Compliant

		172.17.100.35, 192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
563	18.10.43.6.3.1 (L1) Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block'		Endpoint/Server	Non-Compliant
564	18.10.43.7.1 (L1) Ensure 'Enable file hash computation feature' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
565	18.10.43.10.1 (L1) Ensure 'Configure real-time protection and Security Intelligence Updates during OOBE' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
566	18.10.43.10.2 (L1) Ensure 'Scan all downloaded files and attachments' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115,	Endpoint/Server	Non-Compliant

		192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
567	18.10.43.10.3 (L1) Ensure 'Turn off real-time protection' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
568	18.10.43.10.4 (L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
569	18.10.43.10.5 (L1) Ensure 'Turn on script scanning' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184,	Endpoint/Server	Non-Compliant

		192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
570	18.10.43.11.1.1.2 (L1) Ensure 'Configure Remote Encryption Protection Mode' is set to 'Enabled: Audit' or higher	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
571	18.10.43.13.1 (L1) Ensure 'Scan excluded files and directories during quick scans' is set to 'Enabled: 1'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
572	18.10.43.13.2 (L1) Ensure 'Scan packed executables' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194,	Endpoint/Server	Non-Compliant

		192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
573	18.10.43.13.3 (L1) Ensure 'Scan removable drives' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
574	18.10.43.13.4 (L1) Ensure 'Trigger a quick scan after X days without any scans' is set to 'Enabled: 7'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
575	18.10.43.13.5 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29,	Endpoint/Server	Non-Compliant

		192.168.150.64, 192.168.150.148, 172.17.100.35,		
576	18.10.43.16 (L1) Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
577	18.10.43.17 (L1) Ensure 'Control whether exclusions are visible to local users' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
578	18.10.51.1 (L1) Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
579	18.10.57.2.2 (L1) Ensure 'Do not allow passwords to be	192.168.150.180,	Endpoint/Server	Non-Compliant

	saved' is set to 'Enabled'	192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
580	18.10.57.3.3.3 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
581	18.10.57.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
582	18.10.57.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238,	Endpoint/Server	Non-Compliant

		192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
583	18.10.57.3.9.3 (L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
584	18.10.57.3.9.4 (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
585	18.10.57.3.9.5 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127,	Endpoint/Server	Non-Compliant

		192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
586	18.10.57.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
587	18.10.58.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
588	18.10.58.2 (L1) Ensure 'Turn on Basic feed authentication over HTTP' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139,	Endpoint/Server	Non-Compliant

		192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
589	18.10.59.3 (L1) Ensure 'Allow Cortana' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
590	18.10.59.4 (L1) Ensure 'Allow Cortana above lock screen' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
591	18.10.59.5 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148,	Endpoint/Server	Non-Compliant

		172.17.100.35, 192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
592	18.10.59.6 (L1) Ensure 'Allow search and Cortana to use location' is set to 'Disabled'		Endpoint/Server	Non-Compliant
593	18.10.66.2 (L1) Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
594	18.10.66.3 (L1) Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
595	18.10.72.1 (L1) Ensure 'Allow widgets' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115,	Endpoint/Server	Non-Compliant

		192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
596	18.10.76.2.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
597	18.10.78.1 (L1) Ensure 'Enables or disables Windows Game Recording and Broadcasting' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
598	18.10.80.2 (L1) Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184,	Endpoint/Server	Non-Compliant

		192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
599	18.10.81.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
600	18.10.81.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
601	18.10.82.1 (L1) Ensure 'Configure the transmission of the user's password in the content of MPR notifications sent by winlogon.' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194,	Endpoint/Server	Non-Compliant

		192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
602	18.10.82.2 (L1) Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
603	18.10.89.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
604	18.10.89.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29,	Endpoint/Server	Non-Compliant

		192.168.150.64, 192.168.150.148, 172.17.100.35,		
605	18.10.89.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
606	18.10.89.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
607	18.10.89.2.4 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
608	18.10.91.1 (L1) Ensure 'Allow clipboard sharing with	192.168.150.180,	Endpoint/Server	Non-Compliant

	Windows Sandbox' is set to 'Disabled'	192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
609	18.10.91.2 (L1) Ensure 'Allow networking in Windows Sandbox' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
610	18.10.92.2.1 (L1) Ensure 'Prevent users from modifying settings' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
611	18.10.93.1.1 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238,	Endpoint/Server	Non-Compliant

		192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
612	18.10.93.2.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
613	18.10.93.2.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
614	18.10.93.2.3 (L1) Ensure 'Remove access to 'Pause updates' feature' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127,	Endpoint/Server	Non-Compliant

		192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
615	18.10.93.4.1 (L1) Ensure 'Manage preview builds' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
616	18.10.93.4.2 (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
617	18.10.93.4.3 (L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139,	Endpoint/Server	Non-Compliant

		192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
618	19.5.1.1 (L1) Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
619	19.7.5.1 (L1) Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
620	19.7.5.2 (L1) Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148,	Endpoint/Server	Non-Compliant

		172.17.100.35, 192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
621	19.7.8.1 (L1) Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled'		Endpoint/Server	Non-Compliant
622	19.7.8.2 (L1) Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
623	19.7.8.5 (L1) Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
624	19.7.26.1 (L1) Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115,	Endpoint/Server	Non-Compliant

		192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
625	19.7.44.1 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Non-Compliant
626	1.1.2 (L1) Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
627	1.1.7 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184,	Endpoint/Server	Compliant

		192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
628	1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
629	1.2.4 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
630	2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194,	Endpoint/Server	Compliant

		192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
631	2.2.3 (L1) Ensure 'Act as part of the operating system' is set to 'No One'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
632	2.2.6 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
633	2.2.8 (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29,	Endpoint/Server	Compliant

		192.168.150.64, 192.168.150.148, 172.17.100.35,		
634	2.2.9 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
635	2.2.10 (L1) Ensure 'Create a pagefile' is set to 'Administrators'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
636	2.2.11 (L1) Ensure 'Create a token object' is set to 'No One'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
637	2.2.12 (L1) Ensure 'Create global objects' is set to	192.168.150.180,	Endpoint/Server	Compliant

	'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
638	2.2.13 (L1) Ensure 'Create permanent shared objects' is set to 'No One'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
639	2.2.14 (L1) Ensure 'Create symbolic links' is set to 'Administrators'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
640	2.2.15 (L1) Ensure 'Debug programs' is set to 'Administrators'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238,	Endpoint/Server	Compliant

		192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
641	2.2.21 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
642	2.2.22 (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
643	2.2.25 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127,	Endpoint/Server	Compliant

		192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
644	2.2.26 (L1) Ensure 'Load and unload device drivers' is set to 'Administrators'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
645	2.2.27 (L1) Ensure 'Lock pages in memory' is set to 'No One'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
646	2.2.30 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139,	Endpoint/Server	Compliant

		192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
647	2.2.31 (L1) Ensure 'Modify an object label' is set to 'No One'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
648	2.2.32 (L1) Ensure 'Modify firmware environment values' is set to 'Administrators'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
649	2.2.33 (L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148,	Endpoint/Server	Compliant

		172.17.100.35, 192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
650	2.2.34 (L1) Ensure 'Profile single process' is set to 'Administrators'		Endpoint/Server	Compliant
651	2.2.35 (L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
652	2.2.39 (L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
653	2.3.1.2 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115,	Endpoint/Server	Compliant

		192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
654	2.3.1.3 (L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
655	2.3.2.2 (L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
656	2.3.7.7 (L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184,	Endpoint/Server	Compliant

		192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
657	2.3.8.2 (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
658	2.3.8.3 (L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
659	2.3.9.1 (L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194,	Endpoint/Server	Compliant

		192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
660	2.3.9.4 (L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
661	2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
662	2.3.10.2 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29,	Endpoint/Server	Compliant

		192.168.150.64, 192.168.150.148, 172.17.100.35,		
663	2.3.10.5 (L1) Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
664	2.3.10.6 (L1) Ensure 'Network access: Named Pipes that can be accessed anonymously' is set to 'None'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
665	2.3.10.7 (L1) Ensure 'Network access: Remotely accessible registry paths' is configured	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
666	2.3.10.8 (L1) Ensure 'Network access: Remotely accessible	192.168.150.180,	Endpoint/Server	Compliant

	registry paths and sub-paths' is configured	192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
667	2.3.10.9 (L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
668	2.3.10.11 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
669	2.3.10.12 (L1) Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238,	Endpoint/Server	Compliant

		192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
670	2.3.11.5 (L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
671	2.3.11.8 (L1) Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
672	2.3.15.1 (L1) Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127,	Endpoint/Server	Compliant

		192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
673	2.3.15.2 (L1) Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
674	2.3.17.4 (L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
675	2.3.17.5 (L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139,	Endpoint/Server	Compliant

		192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
676	2.3.17.6 (L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
677	2.3.17.7 (L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
678	2.3.17.8 (L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148,	Endpoint/Server	Compliant

		172.17.100.35, 192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
679	5.3 (L1) Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed'		Endpoint/Server	Compliant
680	5.8 (L1) Ensure 'Infrared monitor service (irmon)' is set to 'Disabled' or 'Not Installed'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
681	5.11 (L1) Ensure 'LxssManager (LxssManager)' is set to 'Disabled' or 'Not Installed'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
682	5.12 (L1) Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Disabled' or 'Not Installed'	192.168.150.180, 192.168.150.166, 192.168.150.115,	Endpoint/Server	Compliant

		192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
683	5.14 (L1) Ensure 'OpenSSH SSH Server (sshd)' is set to 'Disabled' or 'Not Installed'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
684	5.27 (L1) Ensure 'Routing and Remote Access (RemoteAccess)' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
685	5.29 (L1) Ensure 'Simple TCP/IP Services (simptcp)' is set to 'Disabled' or 'Not Installed'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184,	Endpoint/Server	Compliant

		192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
686	5.31 (L1) Ensure 'Special Administration Console Helper (sacsvr)' is set to 'Disabled' or 'Not Installed'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
687	5.34 (L1) Ensure 'Web Management Service (WMSvc)' is set to 'Disabled' or 'Not Installed'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
688	17.2.2 (L1) Ensure 'Audit Security Group Management' is set to include 'Success'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194,	Endpoint/Server	Compliant

		192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
689	17.5.3 (L1) Ensure 'Audit Logoff' is set to include 'Success'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
690	17.5.4 (L1) Ensure 'Audit Logon' is set to 'Success and Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
691	17.5.6 (L1) Ensure 'Audit Special Logon' is set to include 'Success'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29,	Endpoint/Server	Compliant

		192.168.150.64, 192.168.150.148, 172.17.100.35,		
692	17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to include 'Success'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
693	17.7.2 (L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
694	17.9.2 (L1) Ensure 'Audit Other System Events' is set to 'Success and Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
695	17.9.3 (L1) Ensure 'Audit Security State Change' is set to	192.168.150.180,	Endpoint/Server	Compliant

	include 'Success'	192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
696	17.9.5 (L1) Ensure 'Audit System Integrity' is set to 'Success and Failure'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
697	18.4.3 (L1) Ensure 'Enable Certificate Padding' is set to 'Enabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
698	18.5.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238,	Endpoint/Server	Compliant

		192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,		
699	18.10.89.2.3 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	192.168.150.180, 192.168.150.166, 192.168.150.115, 192.168.10.134, 192.168.150.238, 192.168.150.74, 192.168.10.184, 192.168.150.133 192.168.10.127, 192.168.10.80, 192.168.10.194, 192.168.150.199, 192.168.150.139, 192.168.150.9, 192.168.150.29, 192.168.150.64, 192.168.150.148, 172.17.100.35,	Endpoint/Server	Compliant
700	1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
701	1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20,	Server	Non-Compliant

		192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
702	1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
703	1.2.2 (L1) Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
704	1.2.3 (L1) Ensure 'Allow Administrator account lockout' is	172.17.100.31,	Server	Non-Compliant

	set to 'Enabled' (MS only)	172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
705	2.2.3 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
706	2.2.6 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147,	Server	Non-Compliant

		172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
707	2.2.8 (L1) Ensure 'Allow log on locally' is set to 'Administrators' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
708	2.2.11 (L1) Ensure 'Back up files and directories' is set to 'Administrators'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
709	2.2.22 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53,	Server	Non-Compliant

		172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
710	2.2.23 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
711	2.2.24 (L1) Ensure 'Deny log on as a service' to include 'Guests'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
712	2.2.25 (L1) Ensure 'Deny log on locally' to include 'Guests'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20	Server	Non-Compliant

		172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
713	2.2.27 (L1) Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
714	2.2.31 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
715	2.2.45 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	172.17.100.31, 172.17.100.32,	Server	Non-Compliant

		172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
716	2.2.46 (L1) Ensure 'Restore files and directories' is set to 'Administrators'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
717	2.2.47 (L1) Ensure 'Shut down the system' is set to 'Administrators'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148,	Server	Non-Compliant

		172.17.100.38, 172.17.100.141, 172.17.100.140,		
718	2.3.1.4 (L1) Configure 'Accounts: Rename guest account'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
719	2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
720	2.3.7.2 (L1) Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81,	Server	Non-Compliant

		172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
721	2.3.7.3 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
722	2.3.7.4 (L1) Configure 'Interactive logon: Message text for users attempting to log on'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
723	2.3.7.5 (L1) Configure 'Interactive logon: Message title for users attempting to log on'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56,	Server	Non-Compliant

		172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
724	2.3.7.8 (L1) Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
725	2.3.7.9 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
726	2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33,	Server	Non-Compliant

		172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
727	2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
728	2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38,	Server	Non-Compliant

		172.17.100.141, 172.17.100.140,		
729	2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
730	2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
731	2.3.10.11 (L1) Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68,	Server	Non-Compliant

		172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
732	2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
733	2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
734	2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59,	Server	Non-Compliant

		172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
735	2.3.11.4 (L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
736	2.3.11.6 (L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
737	2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83,	Server	Non-Compliant

		172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
738	2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
739	2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141,	Server	Non-Compliant

		172.17.100.140, 172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
740	2.3.11.11 (L1) Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts'		Server	Non-Compliant
741	2.3.11.13 (L1) Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
742	2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145,	Server	Non-Compliant

		172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
743	2.3.17.2 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' or higher	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
744	2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
745	9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66,	Server	Non-Compliant

		172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
746	9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
747	9.1.3 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
748	9.1.4 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112,	Server	Non-Compliant

		172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
749	9.1.5 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
750	9.1.6 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant

751	9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
752	9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
753	9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146,	Server	Non-Compliant

		172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
754	9.2.3 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
755	9.2.4 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
756	9.2.5 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177,	Server	Non-Compliant

		172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
757	9.2.6 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
758	9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
759	9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20,	Server	Non-Compliant

		192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
760	9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
761	9.3.3 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
762	9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings:	172.17.100.31,	Server	Non-Compliant

	Apply local firewall rules' is set to 'No'	172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
763	9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
764	9.3.6 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147,	Server	Non-Compliant

		172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
765	9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
766	9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
767	9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53,	Server	Non-Compliant

		172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
768	17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
769	17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
770	17.2.6 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20	Server	Non-Compliant

		172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
771	17.3.1 (L1) Ensure 'Audit PNP Activity' is set to include 'Success'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
772	17.3.2 (L1) Ensure 'Audit Process Creation' is set to include 'Success'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
773	17.5.1 (L1) Ensure 'Audit Account Lockout' is set to include 'Failure'	172.17.100.31, 172.17.100.32,	Server	Non-Compliant

		172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
774	17.5.2 (L1) Ensure 'Audit Group Membership' is set to include 'Success'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
775	17.5.5 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148,	Server	Non-Compliant

		172.17.100.38, 172.17.100.141, 172.17.100.140,		
776	17.6.1 (L1) Ensure 'Audit Detailed File Share' is set to include 'Failure'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
777	17.6.2 (L1) Ensure 'Audit File Share' is set to 'Success and Failure'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
778	17.6.3 (L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81,	Server	Non-Compliant

		172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
779	17.6.4 (L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
780	17.7.3 (L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
781	17.7.4 (L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56,	Server	Non-Compliant

		172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
782	17.7.5 (L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
783	17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
784	17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'	172.17.100.31, 172.17.100.32, 172.17.100.33,	Server	Non-Compliant

		172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
785	17.9.4 (L1) Ensure 'Audit Security System Extension' is set to include 'Success'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
786	18.1.1.1 (L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38,	Server	Non-Compliant

		172.17.100.141, 172.17.100.140,		
787	18.1.1.2 (L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
788	18.1.2.2 (L1) Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
789	18.4.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68,	Server	Non-Compliant

		172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
790	18.4.2 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
791	18.4.3 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
792	18.4.4 (L1) Ensure 'Enable Certificate Padding' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59,	Server	Non-Compliant

		172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
793	18.4.6 (L1) Ensure 'LSA Protection' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
794	18.4.7 (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
795	18.4.8 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83,	Server	Non-Compliant

		172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
796	18.5.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
797	18.5.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141,	Server	Non-Compliant

		172.17.100.140, 172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
798	18.5.4 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'		Server	Non-Compliant
799	18.5.6 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
800	18.5.8 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145,	Server	Non-Compliant

		172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
801	18.5.9 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires' is set to 'Enabled: 5 or fewer seconds'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
802	18.5.12 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
803	18.6.4.1 (L1) Ensure 'Configure multicast DNS (mDNS) protocol' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66,	Server	Non-Compliant

		172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
804	18.6.4.2 (L1) Ensure 'Configure NetBIOS settings' is set to 'Enabled: Disable NetBIOS name resolution on public networks'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
805	18.6.4.4 (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
806	18.6.8.1 (L1) Ensure 'Enable insecure guest logons' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112,	Server	Non-Compliant

		172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
807	18.6.11.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
808	18.6.11.3 (L1) Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant

809	18.6.11.4 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
810	18.6.14.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled, with 'Require Mutual Authentication', 'Require Integrity', and 'Require Privacy' set for all NETLOGON and SYSVOL shares'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
811	18.6.21.1 (L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 3 = Prevent Wi-Fi when on Ethernet'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146,	Server	Non-Compliant

		172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
812	18.7.2 (L1) Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
813	18.7.3 (L1) Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
814	18.7.4 (L1) Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177,	Server	Non-Compliant

		172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
815	18.7.5 (L1) Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
816	18.7.6 (L1) Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections:' is set to 'Enabled: Negotiate' or higher	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
817	18.7.7 (L1) Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20,	Server	Non-Compliant

		192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
818	18.7.8 (L1) Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
819	18.7.9 (L1) Ensure 'Limits print driver installation to Administrators' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
820	18.7.10 (L1) Ensure 'Manage processing of Queue-specific	172.17.100.31,	Server	Non-Compliant

	files' is set to 'Enabled: Limit Queue-specific files to Color profiles'	172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
821	18.7.11 (L1) Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
822	18.7.12 (L1) Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147,	Server	Non-Compliant

		172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
823	18.9.3.1 (L1) Ensure 'Include command line in process creation events' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
824	18.9.4.1 (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
825	18.9.4.2 (L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53,	Server	Non-Compliant

		172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
826	18.9.7.2 (L1) Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
827	18.9.13.1 (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
828	18.9.19.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20	Server	Non-Compliant

		172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
829	18.9.19.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
830	18.9.19.4 (L1) Ensure 'Configure security policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
831	18.9.19.5 (L1) Ensure 'Configure security policy processing: Process even if the Group Policy objects have	172.17.100.31, 172.17.100.32,	Server	Non-Compliant

	not changed' is set to 'Enabled: TRUE'	172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
832	18.9.19.6 (L1) Ensure 'Continue experiences on this device' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
833	18.9.20.1.1 (L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148,	Server	Non-Compliant

		172.17.100.38, 172.17.100.141, 172.17.100.140,		
834	18.9.20.1.5 (L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
835	18.9.24.1 (L1) Ensure 'Enumeration policy for external devices incompatible with Kernel DMA Protection' is set to 'Enabled: Block All'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
836	18.9.25.1 (L1) Ensure 'Configure password backup directory' is set to 'Enabled: Active Directory' or 'Enabled: Azure Active Directory'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81,	Server	Non-Compliant

		172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
837	18.9.25.2 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
838	18.9.25.3 (L1) Ensure 'Enable password encryption' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
839	18.9.25.4 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56,	Server	Non-Compliant

		172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
840	18.9.25.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
841	18.9.25.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
842	18.9.25.7 (L1) Ensure 'Post-authentication actions: Grace period (hours)' is set to 'Enabled: 8 or fewer hours, but not 0'	172.17.100.31, 172.17.100.32, 172.17.100.33,	Server	Non-Compliant

		172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
843	18.9.25.8 (L1) Ensure 'Post-authentication actions: Actions' is set to 'Enabled: Reset the password and logoff the managed account' or higher	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
844	18.9.28.1 (L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38,	Server	Non-Compliant

		172.17.100.141, 172.17.100.140,		
845	18.9.28.2 (L1) Ensure 'Do not display network selection UI' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
846	18.9.28.3 (L1) Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
847	18.9.28.4 (L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68,	Server	Non-Compliant

		172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
848	18.9.28.5 (L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
849	18.9.28.6 (L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
850	18.9.28.7 (L1) Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59,	Server	Non-Compliant

		172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
851	18.9.33.6.3 (L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
852	18.9.33.6.4 (L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
853	18.9.35.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83,	Server	Non-Compliant

		172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
854	18.9.35.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
855	18.9.36.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141,	Server	Non-Compliant

		172.17.100.140, 172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
856	18.9.51.1.1 (L1) Ensure 'Enable Windows NTP Client' is set to 'Enabled'		Server	Non-Compliant
857	18.9.51.1.2 (L1) Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
858	18.10.6.1 (L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145,	Server	Non-Compliant

		172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
859	18.10.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
860	18.10.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
861	18.10.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66,	Server	Non-Compliant

		172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
862	18.10.9.1.1 (L1) Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
863	18.10.13.1 (L1) Ensure 'Turn off cloud consumer account state content' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
864	18.10.13.2 (L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112,	Server	Non-Compliant

		172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
865	18.10.14.1 (L1) Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
866	18.10.15.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant

867	18.10.15.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
868	18.10.16.1 (L1) Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
869	18.10.16.3 (L1) Ensure 'Disable OneSettings Downloads' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146,	Server	Non-Compliant

		172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
870	18.10.16.4 (L1) Ensure 'Do not show feedback notifications' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
871	18.10.16.5 (L1) Ensure 'Enable OneSettings Auditing' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
872	18.10.16.6 (L1) Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177,	Server	Non-Compliant

		172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
873	18.10.16.7 (L1) Ensure 'Limit Dump Collection' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
874	18.10.18.2 (L1) Ensure 'Enable App Installer Experimental Features' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
875	18.10.18.3 (L1) Ensure 'Enable App Installer Hash Override' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20,	Server	Non-Compliant

		192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
876	18.10.18.4 (L1) Ensure 'Enable App Installer Local Archive Malware Scan Override' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
877	18.10.18.5 (L1) Ensure 'Enable App Installer ms-appinstaller protocol' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
878	18.10.18.6 (L1) Ensure 'Enable App Installer Microsoft	172.17.100.31,	Server	Non-Compliant

	Store Source Certificate Validation Bypass' is set to 'Disabled'	172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
879	18.10.26.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
880	18.10.26.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147,	Server	Non-Compliant

		172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
881	18.10.26.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
882	18.10.26.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
883	18.10.26.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53,	Server	Non-Compliant

		172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
884	18.10.26.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
885	18.10.26.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
886	18.10.26.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20	Server	Non-Compliant

		172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
887	18.10.29.2 (L1) Ensure 'Do not apply the Mark of the Web tag to files copied from insecure sources' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
888	18.10.29.3 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
889	18.10.29.4 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled'	172.17.100.31, 172.17.100.32,	Server	Non-Compliant

		172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
890	18.10.29.5 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
891	18.10.42.1 (L1) Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148,	Server	Non-Compliant

		172.17.100.38, 172.17.100.141, 172.17.100.140,		
892	18.10.43.4.1 (L1) Ensure 'Enable EDR in block mode' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
893	18.10.43.5.1 (L1) Ensure 'Configure local setting override for reporting to Microsoft MAPS' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
894	18.10.43.6.1.1 (L1) Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81,	Server	Non-Compliant

		172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
895	18.10.43.6.1.2 (L1) Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
896	18.10.43.6.3.1 (L1) Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
897	18.10.43.7.1 (L1) Ensure 'Enable file hash computation feature' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56,	Server	Non-Compliant

		172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
898	18.10.43.10.1 (L1) Ensure 'Configure real-time protection and Security Intelligence Updates during OOBE' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
899	18.10.43.10.2 (L1) Ensure 'Scan all downloaded files and attachments' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
900	18.10.43.10.3 (L1) Ensure 'Turn off real-time protection' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33,	Server	Non-Compliant

		172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
901	18.10.43.10.4 (L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
902	18.10.43.10.5 (L1) Ensure 'Turn on script scanning' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38,	Server	Non-Compliant

		172.17.100.141, 172.17.100.140,		
903	18.10.43.11.1.1.2 (L1) Ensure 'Configure Remote Encryption Protection Mode' is set to 'Enabled: Audit' or higher	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
904	18.10.43.13.1 (L1) Ensure 'Scan excluded files and directories during quick scans' is set to 'Enabled: 1'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
905	18.10.43.13.2 (L1) Ensure 'Scan packed executables' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68,	Server	Non-Compliant

		172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
906	18.10.43.13.3 (L1) Ensure 'Scan removable drives' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
907	18.10.43.13.4 (L1) Ensure 'Trigger a quick scan after X days without any scans' is set to 'Enabled: 7'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
908	18.10.43.13.5 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59,	Server	Non-Compliant

		172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
909	18.10.43.16 (L1) Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
910	18.10.43.17 (L1) Ensure 'Control whether exclusions are visible to local users' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
911	18.10.51.1 (L1) Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83,	Server	Non-Compliant

		172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
912	18.10.57.2.2 (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
913	18.10.57.3.3.2 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141,	Server	Non-Compliant

		172.17.100.140, 172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
914	18.10.57.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'		Server	Non-Compliant
915	18.10.57.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
916	18.10.57.3.9.3 (L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145,	Server	Non-Compliant

		172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
917	18.10.57.3.9.4 (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
918	18.10.57.3.9.5 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
919	18.10.57.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66,	Server	Non-Compliant

		172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
920	18.10.57.3.11.2 (L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
921	18.10.58.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
922	18.10.58.2 (L1) Ensure 'Turn on Basic feed authentication over HTTP' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112,	Server	Non-Compliant

		172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
923	18.10.59.3 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
924	18.10.76.2.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant

925	18.10.80.2 (L1) Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
926	18.10.81.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
927	18.10.81.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146,	Server	Non-Compliant

		172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
928	18.10.89.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
929	18.10.89.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
930	18.10.89.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177,	Server	Non-Compliant

		172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
931	18.10.89.2.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
932	18.10.89.2.3 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
933	18.10.89.2.4 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20,	Server	Non-Compliant

		192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
934	18.10.92.2.1 (L1) Ensure 'Prevent users from modifying settings' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
935	18.10.93.1.1 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
936	18.10.93.2.1 (L1) Ensure 'Configure Automatic Updates' is	172.17.100.31,	Server	Non-Compliant

	set to 'Enabled'	172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
937	18.10.93.2.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
938	18.10.93.4.1 (L1) Ensure 'Manage preview builds' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147,	Server	Non-Compliant

		172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
939	18.10.93.4.2 (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
940	18.10.93.4.3 (L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
941	19.5.1.1 (L1) Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53,	Server	Non-Compliant

		172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
942	19.7.5.1 (L1) Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
943	19.7.5.2 (L1) Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
944	19.7.8.1 (L1) Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20	Server	Non-Compliant

		172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
945	19.7.8.2 (L1) Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
946	19.7.8.5 (L1) Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
947	19.7.26.1 (L1) Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled'	172.17.100.31, 172.17.100.32,	Server	Non-Compliant

		172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
948	19.7.44.1 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Non-Compliant
949	1.1.2 (L1) Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant

		172.17.100.38, 172.17.100.141, 172.17.100.140,		
950	1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
951	1.1.6 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
952	1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81,	Server	Compliant

		172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
953	1.2.4 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
954	2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
955	2.2.4 (L1) Ensure 'Act as part of the operating system' is set to 'No One'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56,	Server	Compliant

		172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
956	2.2.10 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
957	2.2.12 (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
958	2.2.13 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE'	172.17.100.31, 172.17.100.32, 172.17.100.33,	Server	Compliant

		172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
959	2.2.14 (L1) Ensure 'Create a pagefile' is set to 'Administrators'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
960	2.2.15 (L1) Ensure 'Create a token object' is set to 'No One'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38,	Server	Compliant

		172.17.100.141, 172.17.100.140,		
961	2.2.16 (L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
962	2.2.17 (L1) Ensure 'Create permanent shared objects' is set to 'No One'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
963	2.2.19 (L1) Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68,	Server	Compliant

		172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
964	2.2.20 (L1) Ensure 'Debug programs' is set to 'Administrators'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
965	2.2.29 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
966	2.2.30 (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59,	Server	Compliant

		172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
967	2.2.33 (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' and (when the Web Server (IIS) Role with Web Services Role Service is installed) 'IIS_IUSRS' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
968	2.2.34 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators, Window Manager\Window Manager Group'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
969	2.2.35 (L1) Ensure 'Load and unload device drivers' is set to 'Administrators'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83,	Server	Compliant

		172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
970	2.2.36 (L1) Ensure 'Lock pages in memory' is set to 'No One'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
971	2.2.39 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141,	Server	Compliant

		172.17.100.140, 172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
972	2.2.40 (L1) Ensure 'Modify an object label' is set to 'No One'		Server	Compliant
973	2.2.41 (L1) Ensure 'Modify firmware environment values' is set to 'Administrators'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
974	2.2.42 (L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145,	Server	Compliant

		172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
975	2.2.43 (L1) Ensure 'Profile single process' is set to 'Administrators'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
976	2.2.44 (L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
977	2.2.49 (L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66,	Server	Compliant

		172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
978	2.3.1.1 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
979	2.3.1.2 (L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
980	2.3.1.3 (L1) Configure 'Accounts: Rename administrator account'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112,	Server	Compliant

		172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
981	2.3.2.2 (L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
982	2.3.4.1 (L1) Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant

983	2.3.6.1 (L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
984	2.3.6.2 (L1) Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
985	2.3.6.3 (L1) Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146,	Server	Compliant

		172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
986	2.3.6.4 (L1) Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
987	2.3.6.5 (L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
988	2.3.6.6 (L1) Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177,	Server	Compliant

		172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
989	2.3.7.1 (L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
990	2.3.7.7 (L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
991	2.3.8.2 (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20,	Server	Compliant

		192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
992	2.3.8.3 (L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
993	2.3.9.1 (L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
994	2.3.9.4 (L1) Ensure 'Microsoft network server: Disconnect	172.17.100.31,	Server	Compliant

	clients when logon hours expire' is set to 'Enabled'	172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
995	2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
996	2.3.10.2 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147,	Server	Compliant

		172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
997	2.3.10.5 (L1) Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
998	2.3.10.7 (L1) Ensure 'Network access: Named Pipes that can be accessed anonymously' is configured (MS only)	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
999	2.3.10.8 (L1) Ensure 'Network access: Remotely accessible registry paths' is configured	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53,	Server	Compliant

		172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
1000	2.3.10.9 (L1) Ensure 'Network access: Remotely accessible registry paths and sub-paths' is configured	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1001	2.3.10.10 (L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1002	2.3.10.12 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20	Server	Compliant

		172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
1003	2.3.10.13 (L1) Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1004	2.3.11.5 (L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1005	2.3.11.8 (L1) Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher	172.17.100.31, 172.17.100.32,	Server	Compliant

		172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
1006	2.3.13.1 (L1) Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1007	2.3.15.1 (L1) Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148,	Server	Compliant

		172.17.100.38, 172.17.100.141, 172.17.100.140,		
1008	2.3.15.2 (L1) Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1009	2.3.17.4 (L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1010	2.3.17.5 (L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81,	Server	Compliant

		172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
1011	2.3.17.6 (L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1012	2.3.17.7 (L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1013	2.3.17.8 (L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56,	Server	Compliant

		172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
1014	17.2.5 (L1) Ensure 'Audit Security Group Management' is set to include 'Success'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1015	17.5.3 (L1) Ensure 'Audit Logoff' is set to include 'Success'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1016	17.5.4 (L1) Ensure 'Audit Logon' is set to 'Success and Failure'	172.17.100.31, 172.17.100.32, 172.17.100.33,	Server	Compliant

		172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
1017	17.5.6 (L1) Ensure 'Audit Special Logon' is set to include 'Success'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1018	17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to include 'Success'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38,	Server	Compliant

		172.17.100.141, 172.17.100.140,		
1019	17.7.2 (L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1020	17.9.2 (L1) Ensure 'Audit Other System Events' is set to 'Success and Failure'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1021	17.9.3 (L1) Ensure 'Audit Security State Change' is set to include 'Success'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68,	Server	Compliant

		172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
1022	17.9.5 (L1) Ensure 'Audit System Integrity' is set to 'Success and Failure'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1023	18.4.5 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1024	18.5.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59,	Server	Compliant

		172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,		
1025	18.9.19.7 (L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1026	18.10.82.1 (L1) Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled'	172.17.100.31, 172.17.100.32, 172.17.100.33, 172.17.100.83, 172.17.100.112, 172.17.100.20, 192.168.10.20 172.17.100.56, 172.17.100.59, 172.17.100.66, 172.17.100.177, 172.17.100.53, 172.17.100.81, 172.17.100.68, 172.17.100.145, 172.17.100.146, 172.17.100.147, 172.17.100.148, 172.17.100.38, 172.17.100.141, 172.17.100.140,	Server	Compliant
1027	1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1028	1.1.3 (L1) Ensure 'Minimum password age' is set to '1 or	172.17.100.60,	Server	Non-Compliant

	more day(s)	172.17.100.73, 172.17.100.120,		
1029	1.1.4 (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1030	1.2.2 (L1) Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1031	1.2.3 (L1) Ensure 'Allow Administrator account lockout' is set to 'Enabled' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1032	2.2.3 (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Authenticated Users' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1033	2.2.6 (L1) Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1034	2.2.8 (L1) Ensure 'Allow log on locally' is set to 'Administrators' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1035	2.2.11 (L1) Ensure 'Back up files and directories' is set to 'Administrators'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1036	2.2.13 (L1) Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1037	2.2.22 (L1) Ensure 'Deny access to this computer from the network' to include 'Guests, Local account and member of Administrators group' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1038	2.2.23 (L1) Ensure 'Deny log on as a batch job' to include 'Guests'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1039	2.2.24 (L1) Ensure 'Deny log on as a service' to include 'Guests'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1040	2.2.25 (L1) Ensure 'Deny log on locally' to include 'Guests'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1041	2.2.27 (L1) Ensure 'Deny log on through Remote Desktop Services' is set to 'Guests, Local account' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1042	2.2.31 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1043	2.2.45 (L1) Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1044	2.2.46 (L1) Ensure 'Restore files and directories' is set to 'Administrators'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1045	2.2.47 (L1) Ensure 'Shut down the system' is set to 'Administrators'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1046	2.3.1.1 (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1047	2.3.1.5 (L1) Configure 'Accounts: Rename guest account'	172.17.100.60,	Server	Non-Compliant

		172.17.100.73, 172.17.100.120,		
1048	2.3.2.1 (L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1049	2.3.7.1 (L1) Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1050	2.3.7.3 (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1051	2.3.7.4 (L1) Configure 'Interactive logon: Message text for users attempting to log on'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1052	2.3.7.5 (L1) Configure 'Interactive logon: Message title for users attempting to log on'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1053	2.3.7.8 (L1) Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1054	2.3.7.9 (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1055	2.3.8.1 (L1) Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1056	2.3.9.2 (L1) Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1057	2.3.9.3 (L1) Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1058	2.3.9.5 (L1) Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1059	2.3.10.3 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1060	2.3.10.11 (L1) Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1061	2.3.11.1 (L1) Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1062	2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1063	2.3.11.3 (L1) Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1064	2.3.11.4 (L1) Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1065	2.3.11.6 (L1) Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant

1066	2.3.11.7 (L1) Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only, Refuse LM & NTLM'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1067	2.3.11.9 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1068	2.3.11.10 (L1) Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1069	2.3.11.11 (L1) Ensure 'Network security: Restrict NTLM: Audit Incoming NTLM Traffic' is set to 'Enable auditing for all accounts'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1070	2.3.11.13 (L1) Ensure 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' is set to 'Audit all' or higher	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1071	2.3.17.1 (L1) Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1072	2.3.17.2 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' or higher	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1073	2.3.17.3 (L1) Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1074	9.1.1 (L1) Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1075	9.1.2 (L1) Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1076	9.1.3 (L1) Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1077	9.1.4 (L1) Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\domainfw.log'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1078	9.1.5 (L1) Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1079	9.1.6 (L1) Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1080	9.1.7 (L1) Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1081	9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1082	9.2.2 (L1) Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1083	9.2.3 (L1) Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant

1084	9.2.4 (L1) Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\privatefw.log'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1085	9.2.5 (L1) Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1086	9.2.6 (L1) Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1087	9.2.7 (L1) Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1088	9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1089	9.3.2 (L1) Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1090	9.3.3 (L1) Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1091	9.3.4 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1092	9.3.5 (L1) Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1093	9.3.6 (L1) Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SystemRoot%\System32\logfiles\firewall\publicfw.log'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1094	9.3.7 (L1) Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1095	9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1096	9.3.9 (L1) Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1097	18.1.1.1 (L1) Ensure 'Prevent enabling lock screen camera' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1098	18.1.1.2 (L1) Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1099	18.1.2.2 (L1) Ensure 'Allow users to enable online speech recognition services' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1100	18.3.1 (L1) Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1101	18.3.2 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1102	18.3.3 (L1) Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant

1103	18.3.4 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1104	18.3.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1105	18.3.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1106	18.4.1 (L1) Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1107	18.4.2 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1108	18.4.3 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1109	18.4.4 (L1) Ensure 'Enable Certificate Padding' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1110	18.4.6 (L1) Ensure 'LSA Protection' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1111	18.4.7 (L1) Ensure 'NetBT NodeType configuration' is set to 'Enabled: P-node (recommended)'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1112	18.4.8 (L1) Ensure 'WDigest Authentication' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1113	18.5.2 (L1) Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1114	18.5.3 (L1) Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level' is set to 'Enabled: Highest protection, source routing is completely disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1115	18.5.4 (L1) Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1116	18.5.6 (L1) Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1117	18.5.8 (L1) Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1118	18.5.9 (L1) Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires' is set to 'Enabled: 5 or fewer seconds'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1119	18.5.12 (L1) Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1120	18.6.4.1 (L1) Ensure 'Configure multicast DNS (mDNS) protocol' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1121	18.6.4.2 (L1) Ensure 'Configure NetBIOS settings' is set to 'Enabled: Disable NetBIOS name resolution on public networks'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant

1122	18.6.4.4 (L1) Ensure 'Turn off multicast name resolution' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1123	18.6.8.1 (L1) Ensure 'Enable insecure guest logons' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1124	18.6.11.2 (L1) Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1125	18.6.11.3 (L1) Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1126	18.6.11.4 (L1) Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1127	18.6.14.1 (L1) Ensure 'Hardened UNC Paths' is set to 'Enabled', with 'Require Mutual Authentication', 'Require Integrity', and 'Require Privacy' set for all NETLOGON and SYSVOL shares'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1128	18.6.21.1 (L1) Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled: 1 = Minimize simultaneous connections'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1129	18.7.1 (L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1130	18.7.2 (L1) Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1131	18.7.3 (L1) Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1132	18.7.4 (L1) Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1133	18.7.5 (L1) Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1134	18.7.6 (L1) Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections' is set to 'Enabled: Negotiate' or higher	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1135	18.7.7 (L1) Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1136	18.7.8 (L1) Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1137	18.7.9 (L1) Ensure 'Limits print driver installation to Administrators' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1138	18.7.10 (L1) Ensure 'Manage processing of Queue-specific files' is set to 'Enabled: Limit Queue-specific files to Color profiles'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1139	18.7.11 (L1) Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1140	18.7.12 (L1) Ensure 'Point and Print Restrictions: When	172.17.100.60,	Server	Non-Compliant

	updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt'	172.17.100.73, 172.17.100.120,		
1141	18.9.3.1 (L1) Ensure 'Include command line in process creation events' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1142	18.9.4.1 (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1143	18.9.4.2 (L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1144	18.9.7.2 (L1) Ensure 'Prevent device metadata retrieval from the Internet' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1145	18.9.13.1 (L1) Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1146	18.9.19.2 (L1) Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1147	18.9.19.3 (L1) Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1148	18.9.19.4 (L1) Ensure 'Configure security policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1149	18.9.19.5 (L1) Ensure 'Configure security policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1150	18.9.19.6 (L1) Ensure 'Continue experiences on this device' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1151	18.9.20.1.1 (L1) Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1152	18.9.20.1.5 (L1) Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1153	18.9.28.1 (L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1154	18.9.28.2 (L1) Ensure 'Do not display network selection UI' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1155	18.9.28.3 (L1) Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1156	18.9.28.4 (L1) Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1157	18.9.28.5 (L1) Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1158	18.9.28.6 (L1) Ensure 'Turn off picture password sign-in' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1159	18.9.28.7 (L1) Ensure 'Turn on convenience PIN sign-in' is	172.17.100.60,	Server	Non-Compliant

	set to 'Disabled'	172.17.100.73, 172.17.100.120,		
1160	18.9.33.6.3 (L1) Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1161	18.9.33.6.4 (L1) Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1162	18.9.35.1 (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1163	18.9.35.2 (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1164	18.9.36.1 (L1) Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1165	18.9.51.1.1 (L1) Ensure 'Enable Windows NTP Client' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1166	18.9.51.1.2 (L1) Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1167	18.10.6.1 (L1) Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1168	18.10.8.1 (L1) Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1169	18.10.8.2 (L1) Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1170	18.10.8.3 (L1) Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1171	18.10.9.1.1 (L1) Ensure 'Configure enhanced anti-spoofing' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1172	18.10.13.1 (L1) Ensure 'Turn off cloud consumer account state content' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1173	18.10.13.2 (L1) Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1174	18.10.14.1 (L1) Ensure 'Require pin for pairing' is set to 'Enabled: First Time' OR 'Enabled: Always'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1175	18.10.15.1 (L1) Ensure 'Do not display the password reveal button' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1176	18.10.15.2 (L1) Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1177	18.10.16.1 (L1) Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1178	18.10.16.3 (L1) Ensure 'Disable OneSettings Downloads' is	172.17.100.60,	Server	Non-Compliant

	set to 'Enabled'	172.17.100.73, 172.17.100.120,		
1179	18.10.16.4 (L1) Ensure 'Do not show feedback notifications' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1180	18.10.16.5 (L1) Ensure 'Enable OneSettings Auditing' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1181	18.10.16.6 (L1) Ensure 'Limit Diagnostic Log Collection' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1182	18.10.16.7 (L1) Ensure 'Limit Dump Collection' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1183	18.10.26.1.1 (L1) Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1184	18.10.26.1.2 (L1) Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1185	18.10.26.2.1 (L1) Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1186	18.10.26.2.2 (L1) Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1187	18.10.26.3.1 (L1) Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1188	18.10.26.3.2 (L1) Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1189	18.10.26.4.1 (L1) Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1190	18.10.26.4.2 (L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1191	18.10.29.2 (L1) Ensure 'Do not apply the Mark of the Web tag to files copied from insecure sources' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1192	18.10.29.3 (L1) Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1193	18.10.29.4 (L1) Ensure 'Turn off heap termination on corruption' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1194	18.10.29.5 (L1) Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1195	18.10.42.1 (L1) Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1196	18.10.43.4.1 (L1) Ensure 'Enable EDR in block mode' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1197	18.10.43.5.1 (L1) Ensure 'Configure local setting override	172.17.100.60,	Server	Non-Compliant

	for reporting to Microsoft MAPS' is set to 'Disabled'	172.17.100.73, 172.17.100.120,		
1198	18.10.43.6.1.1 (L1) Ensure 'Configure Attack Surface Reduction rules' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1199	18.10.43.6.1.2 (L1) Ensure 'Configure Attack Surface Reduction rules: Set the state for each ASR rule' is configured	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1200	18.10.43.6.3.1 (L1) Ensure 'Prevent users and apps from accessing dangerous websites' is set to 'Enabled: Block'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1201	18.10.43.7.1 (L1) Ensure 'Enable file hash computation feature' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1202	18.10.43.10.1 (L1) Ensure 'Configure real-time protection and Security Intelligence Updates during OOBE' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1203	18.10.43.10.2 (L1) Ensure 'Scan all downloaded files and attachments' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1204	18.10.43.10.3 (L1) Ensure 'Turn off real-time protection' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1205	18.10.43.10.4 (L1) Ensure 'Turn on behavior monitoring' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1206	18.10.43.10.5 (L1) Ensure 'Turn on script scanning' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1207	18.10.43.11.1.1.2 (L1) Ensure 'Configure Remote Encryption Protection Mode' is set to 'Enabled: Audit' or higher	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1208	18.10.43.13.1 (L1) Ensure 'Scan excluded files and directories during quick scans' is set to 'Enabled: 1'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1209	18.10.43.13.2 (L1) Ensure 'Scan packed executables' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1210	18.10.43.13.3 (L1) Ensure 'Scan removable drives' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1211	18.10.43.13.4 (L1) Ensure 'Trigger a quick scan after X days without any scans' is set to 'Enabled: 7'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1212	18.10.43.13.5 (L1) Ensure 'Turn on e-mail scanning' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1213	18.10.43.16 (L1) Ensure 'Configure detection for potentially unwanted applications' is set to 'Enabled: Block'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1214	18.10.43.17 (L1) Ensure 'Control whether exclusions are visible to local users' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1215	18.10.51.1 (L1) Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1216	18.10.57.2.2 (L1) Ensure 'Do not allow passwords to be	172.17.100.60,	Server	Non-Compliant

	saved' is set to 'Enabled'	172.17.100.73, 172.17.100.120,		
1217	18.10.57.3.3.2 (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1218	18.10.57.3.9.1 (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1219	18.10.57.3.9.2 (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1220	18.10.57.3.9.3 (L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1221	18.10.57.3.9.4 (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1222	18.10.57.3.9.5 (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1223	18.10.57.3.11.1 (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1224	18.10.57.3.11.2 (L1) Ensure 'Do not use temporary folders per session' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1225	18.10.58.1 (L1) Ensure 'Prevent downloading of enclosures' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1226	18.10.58.2 (L1) Ensure 'Turn on Basic feed authentication over HTTP' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1227	18.10.59.3 (L1) Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1228	18.10.76.2.1 (L1) Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1229	18.10.80.2 (L1) Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Enabled: Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1230	18.10.81.1 (L1) Ensure 'Allow user control over installs' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1231	18.10.81.2 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1232	18.10.89.1.1 (L1) Ensure 'Allow Basic authentication' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1233	18.10.89.1.2 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1234	18.10.89.1.3 (L1) Ensure 'Disallow Digest authentication' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1235	18.10.89.2.1 (L1) Ensure 'Allow Basic authentication' is set	172.17.100.60,	Server	Non-Compliant

	to 'Disabled'	172.17.100.73, 172.17.100.120,		
1236	18.10.89.2.3 (L1) Ensure 'Allow unencrypted traffic' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1237	18.10.89.2.4 (L1) Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1238	18.10.92.2.1 (L1) Ensure 'Prevent users from modifying settings' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1239	18.10.93.1.1 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1240	18.10.93.2.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1241	18.10.93.2.2 (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1242	18.10.93.4.1 (L1) Ensure 'Manage preview builds' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1243	18.10.93.4.2 (L1) Ensure 'Select when Preview Builds and Feature Updates are received' is set to 'Enabled: 180 or more days'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1244	18.10.93.4.3 (L1) Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1245	19.5.1.1 (L1) Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1246	19.7.5.1 (L1) Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1247	19.7.5.2 (L1) Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1248	19.7.8.1 (L1) Ensure 'Configure Windows spotlight on lock screen' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1249	19.7.8.2 (L1) Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1250	19.7.8.5 (L1) Ensure 'Turn off Spotlight collection on Desktop' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1251	19.7.26.1 (L1) Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1252	19.7.44.1 (L1) Ensure 'Always install with elevated privileges' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Non-Compliant
1253	1.1.2 (L1) Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1254	1.1.5 (L1) Ensure 'Password must meet complexity	172.17.100.60,	Server	Compliant

	requirements' is set to 'Enabled'	172.17.100.73, 172.17.100.120,		
1255	1.1.6 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1256	1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1257	1.2.4 (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1258	2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1259	2.2.4 (L1) Ensure 'Act as part of the operating system' is set to 'No One'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1260	2.2.10 (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1261	2.2.12 (L1) Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1262	2.2.14 (L1) Ensure 'Create a pagefile' is set to 'Administrators'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1263	2.2.15 (L1) Ensure 'Create a token object' is set to 'No One'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1264	2.2.16 (L1) Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1265	2.2.17 (L1) Ensure 'Create permanent shared objects' is set to 'No One'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1266	2.2.19 (L1) Ensure 'Create symbolic links' is set to 'Administrators, NT VIRTUAL MACHINE\Virtual Machines' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1267	2.2.20 (L1) Ensure 'Debug programs' is set to 'Administrators'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1268	2.2.29 (L1) Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1269	2.2.30 (L1) Ensure 'Force shutdown from a remote system' is set to 'Administrators'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1270	2.2.33 (L1) Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' and (when the Web Server (IIS) Role with Web Services Role Service is installed) 'IIS_IUSRS' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1271	2.2.34 (L1) Ensure 'Increase scheduling priority' is set to 'Administrators'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1272	2.2.35 (L1) Ensure 'Load and unload device drivers' is set to 'Administrators'	172.17.100.60, 172.17.100.73,	Server	Compliant

		172.17.100.120,		
1273	2.2.36 (L1) Ensure 'Lock pages in memory' is set to 'No One'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1274	2.2.39 (L1) Ensure 'Manage auditing and security log' is set to 'Administrators' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1275	2.2.40 (L1) Ensure 'Modify an object label' is set to 'No One'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1276	2.2.41 (L1) Ensure 'Modify firmware environment values' is set to 'Administrators'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1277	2.2.42 (L1) Ensure 'Perform volume maintenance tasks' is set to 'Administrators'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1278	2.2.43 (L1) Ensure 'Profile single process' is set to 'Administrators'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1279	2.2.44 (L1) Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1280	2.2.49 (L1) Ensure 'Take ownership of files or other objects' is set to 'Administrators'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1281	2.3.1.2 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1282	2.3.1.3 (L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1283	2.3.1.4 (L1) Configure 'Accounts: Rename administrator account'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1284	2.3.2.2 (L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1285	2.3.4.1 (L1) Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1286	2.3.6.1 (L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1287	2.3.6.2 (L1) Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1288	2.3.6.3 (L1) Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1289	2.3.6.4 (L1) Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1290	2.3.6.5 (L1) Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1291	2.3.6.6 (L1) Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled'	172.17.100.60, 172.17.100.73,	Server	Compliant

		172.17.100.120,		
1292	2.3.7.2 (L1) Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1293	2.3.7.7 (L1) Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1294	2.3.8.2 (L1) Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1295	2.3.8.3 (L1) Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1296	2.3.9.1 (L1) Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s)'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1297	2.3.9.4 (L1) Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1298	2.3.10.1 (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1299	2.3.10.2 (L1) Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1300	2.3.10.5 (L1) Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1301	2.3.10.7 (L1) Ensure 'Network access: Named Pipes that can be accessed anonymously' is configured (MS only)	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1302	2.3.10.8 (L1) Ensure 'Network access: Remotely accessible registry paths' is configured	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1303	2.3.10.9 (L1) Ensure 'Network access: Remotely accessible registry paths and sub-paths' is configured	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1304	2.3.10.10 (L1) Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1305	2.3.10.12 (L1) Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1306	2.3.10.13 (L1) Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1307	2.3.11.5 (L1) Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1308	2.3.11.8 (L1) Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1309	2.3.13.1 (L1) Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1310	2.3.15.1 (L1) Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to	172.17.100.60, 172.17.100.73,	Server	Compliant

	'Enabled'	172.17.100.120,		
1311	2.3.15.2 (L1) Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1312	2.3.17.4 (L1) Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1313	2.3.17.5 (L1) Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1314	2.3.17.6 (L1) Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1315	2.3.17.7 (L1) Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1316	2.3.17.8 (L1) Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1317	17.1.1 (L1) Ensure 'Audit Credential Validation' is set to 'Success and Failure'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1318	17.2.1 (L1) Ensure 'Audit Application Group Management' is set to 'Success and Failure'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1319	17.2.5 (L1) Ensure 'Audit Security Group Management' is set to include 'Success'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1320	17.2.6 (L1) Ensure 'Audit User Account Management' is set to 'Success and Failure'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1321	17.3.1 (L1) Ensure 'Audit PNP Activity' is set to include 'Success'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1322	17.3.2 (L1) Ensure 'Audit Process Creation' is set to include 'Success'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1323	17.5.1 (L1) Ensure 'Audit Account Lockout' is set to include 'Failure'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1324	17.5.2 (L1) Ensure 'Audit Group Membership' is set to include 'Success'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1325	17.5.3 (L1) Ensure 'Audit Logoff' is set to include 'Success'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1326	17.5.4 (L1) Ensure 'Audit Logon' is set to 'Success and Failure'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1327	17.5.5 (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1328	17.5.6 (L1) Ensure 'Audit Special Logon' is set to include 'Success'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1329	17.6.1 (L1) Ensure 'Audit Detailed File Share' is set to include 'Failure'	172.17.100.60, 172.17.100.73,	Server	Compliant

		172.17.100.120,		
1330	17.6.2 (L1) Ensure 'Audit File Share' is set to 'Success and Failure'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1331	17.6.3 (L1) Ensure 'Audit Other Object Access Events' is set to 'Success and Failure'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1332	17.6.4 (L1) Ensure 'Audit Removable Storage' is set to 'Success and Failure'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1333	17.7.1 (L1) Ensure 'Audit Audit Policy Change' is set to include 'Success'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1334	17.7.2 (L1) Ensure 'Audit Authentication Policy Change' is set to include 'Success'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1335	17.7.3 (L1) Ensure 'Audit Authorization Policy Change' is set to include 'Success'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1336	17.7.4 (L1) Ensure 'Audit MPSSVC Rule-Level Policy Change' is set to 'Success and Failure'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1337	17.7.5 (L1) Ensure 'Audit Other Policy Change Events' is set to include 'Failure'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1338	17.8.1 (L1) Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1339	17.9.1 (L1) Ensure 'Audit IPsec Driver' is set to 'Success and Failure'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1340	17.9.2 (L1) Ensure 'Audit Other System Events' is set to 'Success and Failure'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1341	17.9.3 (L1) Ensure 'Audit Security State Change' is set to include 'Success'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1342	17.9.4 (L1) Ensure 'Audit Security System Extension' is set to include 'Success'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1343	17.9.5 (L1) Ensure 'Audit System Integrity' is set to 'Success and Failure'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1344	18.4.5 (L1) Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1345	18.5.1 (L1) Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1346	18.9.19.7 (L1) Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1347	18.10.82.1 (L1) Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled'	172.17.100.60, 172.17.100.73, 172.17.100.120,	Server	Compliant
1348	1.1.1.8 Ensure usb-storage kernel module is not available	172.17.100.54	Server	Non-Compliant
1349	1.1.2.1.1 Ensure /tmp is a separate partition	172.17.100.54	Server	Non-Compliant

1350	1.2.2.1 Ensure updates, patches, and additional security software are installed	172.17.100.54	Server	Non-Compliant
1351	1.3.1.3 Ensure SELinux policy is configured	172.17.100.54	Server	Non-Compliant
1352	1.3.1.4 Ensure the SELinux mode is not disabled	172.17.100.54	Server	Non-Compliant
1353	1.4.1 Ensure bootloader password is set	172.17.100.54	Server	Non-Compliant
1354	1.5.1 Ensure address space layout randomization is enabled	172.17.100.54	Server	Non-Compliant
1355	1.5.2 Ensure ptrace scope is restricted	172.17.100.54	Server	Non-Compliant
1356	1.5.3 Ensure core dump backtraces are disabled	172.17.100.54	Server	Non-Compliant
1357	1.5.4 Ensure core dump storage is disabled	172.17.100.54	Server	Non-Compliant
1358	1.6.6 Ensure system wide crypto policy disables chacha20-poly1305 for ssh	172.17.100.54	Server	Non-Compliant
1359	1.7.2 Ensure local login warning banner is configured properly	172.17.100.54	Server	Non-Compliant
1360	1.7.3 Ensure remote login warning banner is configured properly	172.17.100.54	Server	Non-Compliant
1361	1.8.2 Ensure GDM login banner is configured	172.17.100.54	Server	Non-Compliant
1362	1.8.3 Ensure GDM disable-user-list option is enabled	172.17.100.54	Server	Non-Compliant
1363	1.8.4 Ensure GDM screen locks when the user is idle	172.17.100.54	Server	Non-Compliant
1364	1.8.5 Ensure GDM screen locks cannot be overridden	172.17.100.54	Server	Non-Compliant
1365	1.8.6 Ensure GDM automatic mounting of removable media is disabled	172.17.100.54	Server	Non-Compliant
1366	1.8.7 Ensure GDM disabling automatic mounting of removable media is not overridden	172.17.100.54	Server	Non-Compliant
1367	1.8.8 Ensure GDM autorun-never is enabled	172.17.100.54	Server	Non-Compliant
1368	1.8.9 Ensure GDM autorun-never is not overridden	172.17.100.54	Server	Non-Compliant
1369	2.1.2 Ensure avahi daemon services are not in use	172.17.100.54	Server	Non-Compliant
1370	2.1.11 Ensure print server services are not in use	172.17.100.54	Server	Non-Compliant
1371	2.2.4 Ensure telnet client is not installed	172.17.100.54	Server	Non-Compliant
1372	2.3.2 Ensure chrony is configured	172.17.100.54	Server	Non-Compliant
1373	2.4.1.2 Ensure permissions on /etc/crontab are configured	172.17.100.54	Server	Non-Compliant
1374	2.4.1.3 Ensure permissions on /etc/cron.hourly are configured	172.17.100.54	Server	Non-Compliant
1375	2.4.1.4 Ensure permissions on /etc/cron.daily are configured	172.17.100.54	Server	Non-Compliant
1376	2.4.1.5 Ensure permissions on /etc/cron.weekly are configured	172.17.100.54	Server	Non-Compliant
1377	2.4.1.6 Ensure permissions on /etc/cron.monthly are configured	172.17.100.54	Server	Non-Compliant
1378	2.4.1.7 Ensure permissions on /etc/cron.d are configured	172.17.100.54	Server	Non-Compliant
1379	2.4.1.8 Ensure crontab is restricted to authorized users	172.17.100.54	Server	Non-Compliant
1380	2.4.2.1 Ensure at is restricted to authorized users	172.17.100.54	Server	Non-Compliant
1381	3.1.3 Ensure bluetooth services are not in use	172.17.100.54	Server	Non-Compliant
1382	3.3.1 Ensure ip forwarding is disabled	172.17.100.54	Server	Non-Compliant
1383	3.3.3 Ensure bogus icmp responses are ignored	172.17.100.54	Server	Non-Compliant
1384	3.3.4 Ensure broadcast icmp requests are ignored	172.17.100.54	Server	Non-Compliant
1385	3.3.6 Ensure secure icmp redirects are not accepted	172.17.100.54	Server	Non-Compliant
1386	3.3.7 Ensure reverse path filtering is enabled	172.17.100.54	Server	Non-Compliant
1387	3.3.8 Ensure source routed packets are not accepted	172.17.100.54	Server	Non-Compliant
1388	3.3.9 Ensure suspicious packets are logged	172.17.100.54	Server	Non-Compliant
1389	3.3.10 Ensure tcp syn cookies is enabled	172.17.100.54	Server	Non-Compliant
1390	3.3.11 Ensure ipv6 router advertisements are not accepted	172.17.100.54	Server	Non-Compliant
1391	4.1.2 Ensure a single firewall configuration utility is in use	172.17.100.54	Server	Non-Compliant
1392	4.3.4 Ensure nftables loopback traffic is configured	172.17.100.54	Server	Non-Compliant
1393	5.1.1 Ensure permissions on /etc/ssh/ssh_config are	172.17.100.54	Server	Non-Compliant

	configured			
1394	5.1.4 Ensure sshd Ciphers are configured	172.17.100.54	Server	Non-Compliant
1395	5.1.6 Ensure sshd MACs are configured	172.17.100.54	Server	Non-Compliant
1396	5.1.7 Ensure sshd access is configured	172.17.100.54	Server	Non-Compliant
1397	5.1.8 Ensure sshd Banner is configured	172.17.100.54	Server	Non-Compliant
1398	5.1.9 Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured	172.17.100.54	Server	Non-Compliant
1399	5.1.14 Ensure sshd LoginGraceTime is configured	172.17.100.54	Server	Non-Compliant
1400	5.1.16 Ensure sshd MaxAuthTries is configured	172.17.100.54	Server	Non-Compliant
1401	5.1.17 Ensure sshd MaxStartups is configured	172.17.100.54	Server	Non-Compliant
1402	5.1.20 Ensure sshd PermitRootLogin is disabled	172.17.100.54	Server	Non-Compliant
1403	5.2.2 Ensure sudo commands use pty	172.17.100.54	Server	Non-Compliant
1404	5.2.3 Ensure sudo log file exists	172.17.100.54	Server	Non-Compliant
1405	5.2.7 Ensure access to the su command is restricted	172.17.100.54	Server	Non-Compliant
1406	5.3.2.2 Ensure pam faillock module is enabled	172.17.100.54	Server	Non-Compliant
1407	5.3.2.4 Ensure pam pwhistory module is enabled	172.17.100.54	Server	Non-Compliant
1408	5.3.3.1.1 Ensure password failed attempts lockout is configured	172.17.100.54	Server	Non-Compliant
1409	5.3.3.1.2 Ensure password unlock time is configured	172.17.100.54	Server	Non-Compliant
1410	5.3.3.2.1 Ensure password number of changed characters is configured	172.17.100.54	Server	Non-Compliant
1411	5.3.3.2.2 Ensure password length is configured	172.17.100.54	Server	Non-Compliant
1412	5.3.3.2.3 Ensure password complexity is configured	172.17.100.54	Server	Non-Compliant
1413	5.3.3.2.4 Ensure password same consecutive characters is configured	172.17.100.54	Server	Non-Compliant
1414	5.3.3.2.5 Ensure password maximum sequential characters is configured	172.17.100.54	Server	Non-Compliant
1415	5.3.3.2.7 Ensure password quality is enforced for the root user	172.17.100.54	Server	Non-Compliant
1416	5.3.3.3.1 Ensure password history remember is configured	172.17.100.54	Server	Non-Compliant
1417	5.3.3.3.2 Ensure password history is enforced for the root user	172.17.100.54	Server	Non-Compliant
1418	5.3.3.3.3 Ensure pam pwhistory includes use authtok	172.17.100.54	Server	Non-Compliant
1419	5.3.3.4.1 Ensure pam unix does not include nullok	172.17.100.54	Server	Non-Compliant
1420	5.4.1.1 Ensure password expiration is configured	172.17.100.54	Server	Non-Compliant
1421	5.4.1.5 Ensure inactive password lock is configured	172.17.100.54	Server	Non-Compliant
1422	5.4.2.5 Ensure root path integrity	172.17.100.54	Server	Non-Compliant
1423	5.4.3.2 Ensure default user shell timeout is configured	172.17.100.54	Server	Non-Compliant
1424	5.4.3.3 Ensure default user umask is configured	172.17.100.54	Server	Non-Compliant
1425	6.1.1 Ensure AIDE is installed	172.17.100.54	Server	Non-Compliant
1426	6.1.2 Ensure filesystem integrity is regularly checked	172.17.100.54	Server	Non-Compliant
1427	6.1.3 Ensure cryptographic mechanisms are used to protect the integrity of audit tools	172.17.100.54	Server	Non-Compliant
1428	6.2.2.1.1 Ensure systemd-journal-remote is installed	172.17.100.54	Server	Non-Compliant
1429	6.2.2.1.3 Ensure systemd-journal-upload is enabled and active	172.17.100.54	Server	Non-Compliant
1430	6.2.2.2 Ensure journald ForwardToSyslog is disabled	172.17.100.54	Server	Non-Compliant
1431	6.2.2.3 Ensure journald Compress is configured	172.17.100.54	Server	Non-Compliant
1432	6.2.2.4 Ensure journald Storage is configured	172.17.100.54	Server	Non-Compliant
1433	6.2.3.3 Ensure journald is configured to send logs to rsyslog	172.17.100.54	Server	Non-Compliant
1434	6.2.3.4 Ensure rsyslog log file creation mode is configured	172.17.100.54	Server	Non-Compliant
1435	6.2.3.5 Ensure rsyslog logging is configured	172.17.100.54	Server	Non-Compliant
1436	6.2.4.1 Ensure access to all logfiles has been configured	172.17.100.54	Server	Non-Compliant
1437	7.1.11 Ensure world writable files and directories are secured	172.17.100.54	Server	Non-Compliant

1438	7.2.9 Ensure local interactive user dot files access is configured	172.17.100.54	Server	Non-Compliant
1439	1.1.1.1 Ensure cramfs kernel module is not available	172.17.100.54	Server	Compliant
1440	1.1.1.2 Ensure freevxfs kernel module is not available	172.17.100.54	Server	Compliant
1441	1.1.1.3 Ensure hfs kernel module is not available	172.17.100.54	Server	Compliant
1442	1.1.1.4 Ensure hfsplus kernel module is not available	172.17.100.54	Server	Compliant
1443	1.1.1.5 Ensure jffs2 kernel module is not available	172.17.100.54	Server	Compliant
1444	1.1.2.1.2 Ensure nodev option set on /tmp partition	172.17.100.54	Server	Compliant
1445	1.1.2.1.3 Ensure nosuid option set on /tmp partition	172.17.100.54	Server	Compliant
1446	1.1.2.1.4 Ensure noexec option set on /tmp partition	172.17.100.54	Server	Compliant
1447	1.1.2.2.1 Ensure /dev/shm is a separate partition	172.17.100.54	Server	Compliant
1448	1.1.2.2.2 Ensure nodev option set on /dev/shm partition	172.17.100.54	Server	Compliant
1449	1.1.2.2.3 Ensure nosuid option set on /dev/shm partition	172.17.100.54	Server	Compliant
1450	1.1.2.2.4 Ensure noexec option set on /dev/shm partition	172.17.100.54	Server	Compliant
1451	1.1.2.3.2 Ensure nodev option set on /home partition	172.17.100.54	Server	Compliant
1452	1.1.2.3.3 Ensure nosuid option set on /home partition	172.17.100.54	Server	Compliant
1453	1.1.2.4.2 Ensure nodev option set on /var partition	172.17.100.54	Server	Compliant
1454	1.1.2.4.3 Ensure nosuid option set on /var partition	172.17.100.54	Server	Compliant
1455	1.1.2.5.2 Ensure nodev option set on /var/tmp partition	172.17.100.54	Server	Compliant
1456	1.1.2.5.3 Ensure nosuid option set on /var/tmp partition	172.17.100.54	Server	Compliant
1457	1.1.2.5.4 Ensure noexec option set on /var/tmp partition	172.17.100.54	Server	Compliant
1458	1.1.2.6.2 Ensure nodev option set on /var/log partition	172.17.100.54	Server	Compliant
1459	1.1.2.6.3 Ensure nosuid option set on /var/log partition	172.17.100.54	Server	Compliant
1460	1.1.2.6.4 Ensure noexec option set on /var/log partition	172.17.100.54	Server	Compliant
1461	1.1.2.7.2 Ensure nodev option set on /var/log/audit partition	172.17.100.54	Server	Compliant
1462	1.1.2.7.3 Ensure nosuid option set on /var/log/audit partition	172.17.100.54	Server	Compliant
1463	1.1.2.7.4 Ensure noexec option set on /var/log/audit partition	172.17.100.54	Server	Compliant
1464	1.2.1.2 Ensure gpgcheck is globally activated	172.17.100.54	Server	Compliant
1465	1.3.1.1 Ensure SELinux is installed	172.17.100.54	Server	Compliant
1466	1.3.1.2 Ensure SELinux is not disabled in bootloader configuration	172.17.100.54	Server	Compliant
1467	1.3.1.7 Ensure the MCS Translation Service (mcstrans) is not installed	172.17.100.54	Server	Compliant
1468	1.3.1.8 Ensure SETroubleshoot is not installed	172.17.100.54	Server	Compliant
1469	1.4.2 Ensure access to bootloader config is configured	172.17.100.54	Server	Compliant
1470	1.6.1 Ensure system wide crypto policy is not set to legacy	172.17.100.54	Server	Compliant
1471	1.6.2 Ensure system wide crypto policy is not set in sshd configuration	172.17.100.54	Server	Compliant
1472	1.6.3 Ensure system wide crypto policy disables sha1 hash and signature support	172.17.100.54	Server	Compliant
1473	1.6.4 Ensure system wide crypto policy disables macs less than 128 bits	172.17.100.54	Server	Compliant
1474	1.6.5 Ensure system wide crypto policy disables cbc for ssh	172.17.100.54	Server	Compliant
1475	1.6.7 Ensure system wide crypto policy disables EtM for ssh	172.17.100.54	Server	Compliant
1476	1.7.1 Ensure message of the day is configured properly	172.17.100.54	Server	Compliant
1477	1.7.4 Ensure access to /etc/motd is configured	172.17.100.54	Server	Compliant
1478	1.7.5 Ensure access to /etc/issue is configured	172.17.100.54	Server	Compliant
1479	1.7.6 Ensure access to /etc/issue.net is configured	172.17.100.54	Server	Compliant
1480	1.8.10 Ensure XDMCP is not enabled	172.17.100.54	Server	Compliant
1481	2.1.1 Ensure autofs services are not in use	172.17.100.54	Server	Compliant
1482	2.1.3 Ensure dhcp server services are not in use	172.17.100.54	Server	Compliant

1483	2.1.4 Ensure dns server services are not in use	172.17.100.54	Server	Compliant
1484	2.1.5 Ensure dnsmasq services are not in use	172.17.100.54	Server	Compliant
1485	2.1.6 Ensure samba file server services are not in use	172.17.100.54	Server	Compliant
1486	2.1.7 Ensure ftp server services are not in use	172.17.100.54	Server	Compliant
1487	2.1.8 Ensure message access server services are not in use	172.17.100.54	Server	Compliant
1488	2.1.9 Ensure network file system services are not in use	172.17.100.54	Server	Compliant
1489	2.1.10 Ensure nis server services are not in use	172.17.100.54	Server	Compliant
1490	2.1.12 Ensure rpcbind services are not in use	172.17.100.54	Server	Compliant
1491	2.1.13 Ensure rsync services are not in use	172.17.100.54	Server	Compliant
1492	2.1.14 Ensure snmp services are not in use	172.17.100.54	Server	Compliant
1493	2.1.15 Ensure telnet server services are not in use	172.17.100.54	Server	Compliant
1494	2.1.16 Ensure tftp server services are not in use	172.17.100.54	Server	Compliant
1495	2.1.17 Ensure web proxy server services are not in use	172.17.100.54	Server	Compliant
1496	2.1.18 Ensure web server services are not in use	172.17.100.54	Server	Compliant
1497	2.1.19 Ensure xinetd services are not in use	172.17.100.54	Server	Compliant
1498	2.1.21 Ensure mail transfer agents are configured for local-only mode	172.17.100.54	Server	Compliant
1499	2.2.1 Ensure ftp client is not installed	172.17.100.54	Server	Compliant
1500	2.2.3 Ensure nis client is not installed	172.17.100.54	Server	Compliant
1501	2.2.5 Ensure tftp client is not installed	172.17.100.54	Server	Compliant
1502	2.3.1 Ensure time synchronization is in use	172.17.100.54	Server	Compliant
1503	2.3.3 Ensure chrony is not run as the root user	172.17.100.54	Server	Compliant
1504	2.4.1.1 Ensure cron daemon is enabled and active	172.17.100.54	Server	Compliant
1505	3.1.2 Ensure wireless interfaces are disabled	172.17.100.54	Server	Compliant
1506	3.3.2 Ensure packet redirect sending is disabled	172.17.100.54	Server	Compliant
1507	3.3.5 Ensure icmp redirects are not accepted	172.17.100.54	Server	Compliant
1508	4.1.1 Ensure nftables is installed	172.17.100.54	Server	Compliant
1509	4.2.1 Ensure firewalld drops unnecessary services and ports	172.17.100.54	Server	Compliant
1510	4.2.2 Ensure firewalld loopback traffic is configured	172.17.100.54	Server	Compliant
1511	4.3.1 Ensure nftables base chains exist	172.17.100.54	Server	Compliant
1512	4.3.2 Ensure nftables established connections are configured	172.17.100.54	Server	Compliant
1513	4.3.3 Ensure nftables default deny firewall policy	172.17.100.54	Server	Compliant
1514	5.1.2 Ensure permissions on SSH private host key files are configured	172.17.100.54	Server	Compliant
1515	5.1.3 Ensure permissions on SSH public host key files are configured	172.17.100.54	Server	Compliant
1516	5.1.5 Ensure sshd KexAlgorithms is configured	172.17.100.54	Server	Compliant
1517	5.1.12 Ensure sshd HostbasedAuthentication is disabled	172.17.100.54	Server	Compliant
1518	5.1.13 Ensure sshd IgnoreRhosts is enabled	172.17.100.54	Server	Compliant
1519	5.1.15 Ensure sshd LogLevel is configured	172.17.100.54	Server	Compliant
1520	5.1.18 Ensure sshd MaxSessions is configured	172.17.100.54	Server	Compliant
1521	5.1.19 Ensure sshd PermitEmptyPasswords is disabled	172.17.100.54	Server	Compliant
1522	5.1.21 Ensure sshd PermitUserEnvironment is disabled	172.17.100.54	Server	Compliant
1523	5.1.22 Ensure sshd UsePAM is enabled	172.17.100.54	Server	Compliant
1524	5.2.1 Ensure sudo is installed	172.17.100.54	Server	Compliant
1525	5.2.5 Ensure re-authentication for privilege escalation is not disabled globally	172.17.100.54	Server	Compliant
1526	5.2.6 Ensure sudo authentication timeout is configured correctly	172.17.100.54	Server	Compliant
1527	5.3.1.1 Ensure latest version of pam is installed	172.17.100.54	Server	Compliant
1528	5.3.1.2 Ensure latest version of authselect is installed	172.17.100.54	Server	Compliant
1529	5.3.1.3 Ensure latest version of libpwquality is installed	172.17.100.54	Server	Compliant
1530	5.3.2.1 Ensure active authselect profile includes pam modules	172.17.100.54	Server	Compliant

1531	5.3.2.3 Ensure pam_pwquality module is enabled	172.17.100.54	Server	Compliant
1532	5.3.2.5 Ensure pam_unix module is enabled	172.17.100.54	Server	Compliant
1533	5.3.3.2.6 Ensure password dictionary check is enabled	172.17.100.54	Server	Compliant
1534	5.3.3.4.2 Ensure pam_unix does not include remember	172.17.100.54	Server	Compliant
1535	5.3.3.4.3 Ensure pam_unix includes a strong password hashing algorithm	172.17.100.54	Server	Compliant
1536	5.3.3.4.4 Ensure pam_unix includes use_authok	172.17.100.54	Server	Compliant
1537	5.4.1.3 Ensure password expiration warning days is configured	172.17.100.54	Server	Compliant
1538	5.4.1.4 Ensure strong password hashing algorithm is configured	172.17.100.54	Server	Compliant
1539	5.4.1.6 Ensure all users last password change date is in the past	172.17.100.54	Server	Compliant
1540	5.4.2.1 Ensure root is the only UID 0 account	172.17.100.54	Server	Compliant
1541	5.4.2.2 Ensure root is the only GID 0 account	172.17.100.54	Server	Compliant
1542	5.4.2.3 Ensure group root is the only GID 0 group	172.17.100.54	Server	Compliant
1543	5.4.2.4 Ensure root account access is controlled	172.17.100.54	Server	Compliant
1544	5.4.2.6 Ensure root user umask is configured	172.17.100.54	Server	Compliant
1545	5.4.2.7 Ensure system accounts do not have a valid login shell	172.17.100.54	Server	Compliant
1546	5.4.2.8 Ensure accounts without a valid login shell are locked	172.17.100.54	Server	Compliant
1547	6.2.1.1 Ensure journald service is enabled and active	172.17.100.54	Server	Compliant
1548	6.2.1.4 Ensure only one logging system is in use	172.17.100.54	Server	Compliant
1549	6.2.2.1.4 Ensure systemd-journal-remote service is not in use	172.17.100.54	Server	Compliant
1550	6.2.3.1 Ensure rsyslog is installed	172.17.100.54	Server	Compliant
1551	6.2.3.2 Ensure rsyslog service is enabled and active	172.17.100.54	Server	Compliant
1552	6.2.3.6 Ensure rsyslog is configured to send logs to a remote log host	172.17.100.54	Server	Compliant
1553	6.2.3.7 Ensure rsyslog is not configured to receive logs from a remote client	172.17.100.54	Server	Compliant
1554	7.1.1 Ensure permissions on /etc/passwd are configured	172.17.100.54	Server	Compliant
1555	7.1.2 Ensure permissions on /etc/passwd- are configured	172.17.100.54	Server	Compliant
1556	7.1.3 Ensure permissions on /etc/group are configured	172.17.100.54	Server	Compliant
1557	7.1.4 Ensure permissions on /etc/group- are configured	172.17.100.54	Server	Compliant
1558	7.1.5 Ensure permissions on /etc/shadow are configured	172.17.100.54	Server	Compliant
1559	7.1.6 Ensure permissions on /etc/shadow- are configured	172.17.100.54	Server	Compliant
1560	7.1.7 Ensure permissions on /etc/gshadow are configured	172.17.100.54	Server	Compliant
1561	7.1.8 Ensure permissions on /etc/gshadow- are configured	172.17.100.54	Server	Compliant
1562	7.1.9 Ensure permissions on /etc/shells are configured	172.17.100.54	Server	Compliant
1563	7.1.10 Ensure permissions on /etc/security/opasswd are configured	172.17.100.54	Server	Compliant
1564	7.1.12 Ensure no files or directories without an owner and a group exist	172.17.100.54	Server	Compliant
1565	7.2.1 Ensure accounts in /etc/passwd use shadowed passwords	172.17.100.54	Server	Compliant
1566	7.2.2 Ensure /etc/shadow password fields are not empty	172.17.100.54	Server	Compliant
1567	7.2.3 Ensure all groups in /etc/passwd exist in /etc/group	172.17.100.54	Server	Compliant
1568	7.2.4 Ensure no duplicate UIDs exist	172.17.100.54	Server	Compliant
1569	7.2.5 Ensure no duplicate GIDs exist	172.17.100.54	Server	Compliant
1570	7.2.6 Ensure no duplicate user names exist	172.17.100.54	Server	Compliant
1571	7.2.7 Ensure no duplicate group names exist	172.17.100.54	Server	Compliant
1572	7.2.8 Ensure local interactive user home directories are configured	172.17.100.54	Server	Compliant

1573	2.4 (L1) Host image profile acceptance level must be PartnerSupported or higher	172.17.100.232, 172.17.100.233, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237,	VM Ware	Compliant
1574	2.11 (L1) Host must use sufficient entropy for cryptographic operations	172.17.100.232, 172.17.100.233, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237,	VM Ware	Compliant
1575	6.4.1 (L1) Host SNMP services, if enabled, must limit access	172.17.100.232, 172.17.100.233, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237,	VM Ware	Compliant
1576	6.5.1 (L1) Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated ciphers	172.17.100.232, 172.17.100.233, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237,	VM Ware	Compliant
1577	6.5.2 (L1) Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated cryptographic modules	172.17.100.232, 172.17.100.233, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237,	VM Ware	Compliant
1578	6.5.3 (L1) Host SSH daemon, if enabled, must not allow use of gateway ports	172.17.100.232, 172.17.100.233, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237,	VM Ware	Compliant
1579	6.5.4 (L1) Host SSH daemon, if enabled, must not allow host-based authentication	172.17.100.232, 172.17.100.233, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237,	VM Ware	Compliant
1580	6.5.5 (L1) Host SSH daemon, if enabled, must set a timeout count on idle sessions	172.17.100.232, 172.17.100.233, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237,	VM Ware	Compliant
1581	6.5.6 (L1) Host SSH daemon, if enabled, must set a timeout interval on idle sessions	172.17.100.232, 172.17.100.233, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237,	VM Ware	Compliant
1582	6.5.7 (L1) Host SSH daemon, if enabled, must display the system login banner before granting access	172.17.100.232, 172.17.100.233, 172.17.100.234, 172.17.100.235,	VM Ware	Compliant

		172.17.100.236, 172.17.100.237,		
1583	6.5.8 (L1) Host SSH daemon, if enabled, must ignore .rhosts files	172.17.100.232, 172.17.100.233, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237,	VM Ware	Compliant
1584	6.5.9 (L1) Host SSH daemon, if enabled, must disable stream local forwarding	172.17.100.232, 172.17.100.233, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237,	VM Ware	Compliant
1585	6.5.10 (L1) Host SSH daemon, if enabled, must disable TCP forwarding	172.17.100.232, 172.17.100.233, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237,	VM Ware	Compliant
1586	6.5.11 (L1) Host SSH daemon, if enabled, must not permit tunnels	172.17.100.232, 172.17.100.233, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237,	VM Ware	Compliant
1587	6.5.12 (L1) Host SSH daemon, if enabled, must not permit user environment settings	172.17.100.232, 172.17.100.233, 172.17.100.234, 172.17.100.235, 172.17.100.236, 172.17.100.237,	VM Ware	Compliant
1588	Ensure AAA (Authentication, Authorization, Accounting) is enabled	172.17.100.10, 172.17.100.101	Switch	Non-Compliant
1589	Ensure VTY lines use SSH and require local authentication	172.17.100.10, 172.17.100.101	Switch	Non-Compliant
1590	Ensure console exec-timeout is set appropriately	172.17.100.10, 172.17.100.101	Switch	Non-Compliant
1591	Ensure plain-text passwords are not stored in configuration	172.17.100.10, 172.17.100.101	Switch	Non-Compliant
1592	Ensure BGP neighbor authentication (MD5) is configured	172.17.100.10, 172.17.100.101	Switch	Non-Compliant
1593	Ensure VTP version 2 or 3 is used (avoid VTP v1)	172.17.100.10, 172.17.100.101	Switch	Non-Compliant
1594	Ensure unused interfaces are shut down or not left in default VLAN 1	172.17.100.10, 172.17.100.101	Switch	Non-Compliant
1595	Ensure trunk interfaces restrict allowed VLANs explicitly	172.17.100.10, 172.17.100.101	Switch	Non-Compliant
1596	Ensure VLAN 1 is not used for management or user traffic	172.17.100.10, 172.17.100.101	Switch	Non-Compliant
1597	Ensure CDP is disabled on external/untrusted interfaces	172.17.100.10, 172.17.100.101	Switch	Non-Compliant
1598	Ensure HTTP server is disabled (use HTTPS only)	172.17.100.10, 172.17.100.101	Switch	Non-Compliant
1599	Ensure logging to a remote Syslog server is configured	172.17.100.10, 172.17.100.101	Switch	Non-Compliant
1600	Ensure NTP is configured for time synchronization	172.17.100.10,	Switch	Non-Compliant

		172.17.100.101		
1601	Ensure self-signed certificates are replaced with CA-issued certificates	172.17.100.10, 172.17.100.101	Switch	Non-Compliant
1602	Ensure 'enable secret' is configured with strong encryption	172.17.100.10, 172.17.100.101	Switch	Compliant
1603	Ensure username with privilege 15 uses secret (not password)	172.17.100.10, 172.17.100.101	Switch	Compliant
1604	Ensure VTY lines do not allow Telnet (transport input ssh only)	172.17.100.10, 172.17.100.101	Switch	Compliant
1605	Ensure 'login on-success log' is configured	172.17.100.10, 172.17.100.101	Switch	Compliant
1606	Ensure BGP log-neighbor-changes is enabled	172.17.100.10, 172.17.100.101	Switch	Compliant
1607	Ensure Spanning Tree mode is set to Rapid-PVST or MST	172.17.100.10, 172.17.100.101	Switch	Compliant
1608	Ensure 'spanning-tree extend system-id' is enabled	172.17.100.10, 172.17.100.101	Switch	Compliant
1609	Ensure HTTP authentication is set to local or AAA	172.17.100.10, 172.17.100.101	Switch	Compliant
1610	Ensure logging is configured with timestamps	172.17.100.10, 172.17.100.101	Switch	Compliant
1611	Ensure SSH is configured for management access (not Telnet)	172.17.100.10, 172.17.100.101	Switch	Compliant
1612	Ensure PKI certificates use SHA-256 or stronger	172.17.100.10, 172.17.100.101	Switch	Compliant

Annexure A - Engagement Limitations

The security assessment was conducted within the scope and timeline agreed upon during the engagement with the Evaluated organization. Due to time limitations and operational constraints, it may not have been possible to identify every potential vulnerability present within the environment.

Testing activities were limited to the systems, endpoints, and functionalities that were made accessible by the Evaluated organization during the defined assessment period. The findings presented in this report represent the security posture of the evaluated systems at the time of testing and should not be interpreted as a guarantee that no additional vulnerabilities exist.

Annexure B - Retesting Statement

Upon completion of remediation activities by the Evaluated organization, a re-assessment may be conducted to verify whether the identified vulnerabilities have been successfully mitigated. The purpose of the re-assessment is limited to validating the remediation of the specific findings documented in this report.

The Evaluated organization is expected to address the identified vulnerabilities within a period of ninety (90) days from the date of report issuance, in accordance with the agreed remediation service level timelines. Re-assessment requests submitted within this period will be accommodated as part of the engagement to verify the implemented fixes.

Requests for re-assessment submitted after the ninety (90) day remediation window may be subject to a separate engagement or additional scope, as the validity and relevance of the original findings may change over time due to updates in the application environment.

Annexure C - Disclaimer and Precautions for Patch Implementation

Before implementing any remediation, actions based on this report, the following precautions should be observed:

- **Backup & Recovery:** Ensure complete backups of systems, applications, and data are taken prior to changes, along with a defined rollback plan to restore services in case of failure.
- **Controlled Testing:** Validate all fixes in a UAT or staging environment before deploying to production to avoid service disruption.
- **Third-Party References:** External links provided for remediation guidance are for reference only; their accuracy and availability are not guaranteed.
- **Assessment Limitations:** Findings are based on testing performed within the defined scope, timeline, and accessible environment. Certain vulnerabilities, especially those requiring intrusive testing, may not have been identified.
- **Point-in-Time Evaluation:** This report reflects the security posture at the time of assessment. New vulnerabilities may emerge due to system changes or evolving threats.
- **Ongoing Security Responsibility:** Security is a continuous process. The responsibility for implementing fixes and maintaining security controls rests with the Evaluated organization.

Annexure D - CERT-In Reporting and Remediation Compliance

As a CERT-IN empanelled organization, we have received communication stating that all CERT-IN empanelled organizations are required to submit audit-related data (including Cyber Audits, IS Audits, Regulatory audits, and VAPT audits) to CERT-IN starting from the fiscal year 2024. We will be sharing this VAPT Audit Reports or related details with CERT-IN. According to CERT-IN regulations, a period of 90 days is provided for the remediation/patching process from the release date of the audit reports. Therefore, we kindly request you to address all mentioned vulnerabilities within the 90-day timeframe and to inform us for the follow-up audit.