Student:	Email:
Bradley Adams	badams10@my.athens.edu

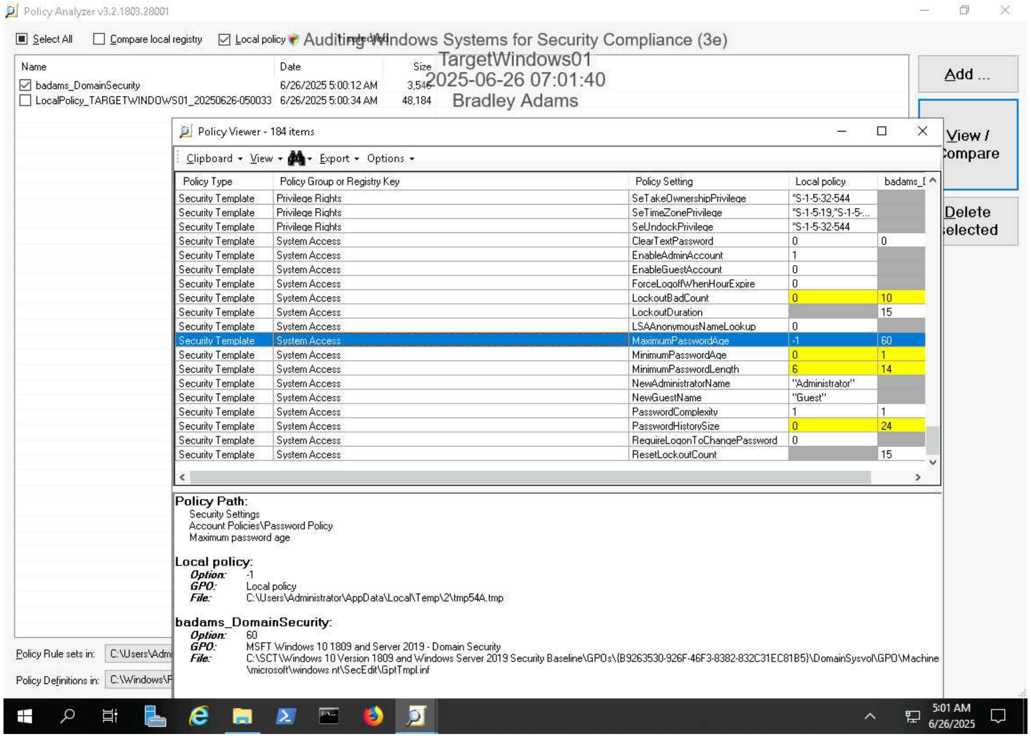
Time on Task:	Progress:
10 hours, 54 minutes	100%

Report Generated: Thursday, June 26, 2025 at 11:51 AM

Section 1: Hands-On Demonstration

Part 1: Audit a Windows System using Policy Analyzer

16. **Make a screen capture** showing the **current MaximumPasswordAge setting in the Policy Viewer**.



Auditing Windows Systems for Security Compliance (3e)
TargetWindows01
2025-06-26 07:01:40
Bradley Adams

Name	Date	Size
☑ badams_DomainSecurity	6/26/2025 5:00:12 AM	3,546
□ LocalPolicy_TARGETWINDOWS01_20250626-050033	6/26/2025 5:00:34 AM	48,184

Policy Type	Policy Group or Registry Key	Policy Setting	Local policy	badams_[
Security Template	Privilege Rights	SeTakeOwnershipPrivilege	*S-1-5-32-544	
Security Template	Privilege Rights	SeTimeZonePrivilege	*S-1-5-19,*S-1-5-...	
Security Template	Privilege Rights	SeUndockPrivilege	*S-1-5-32-544	
Security Template	System Access	ClearTextPassword	0	0
Security Template	System Access	EnableAdminAccount	1	
Security Template	System Access	EnableGuestAccount	0	
Security Template	System Access	ForceLogoffWhenHourExpire	0	
Security Template	System Access	LockoutBadCount	0	10
Security Template	System Access	LockoutDuration		15
Security Template	System Access	LSAAnonymousNameLookup	0	
Security Template	System Access	MaximumPasswordAge	-1	60
Security Template	System Access	MinimumPasswordAge	0	1
Security Template	System Access	MinimumPasswordLength	6	14
Security Template	System Access	NewAdministratorName	"Administrator"	
Security Template	System Access	NewGuestName	"Guest"	
Security Template	System Access	PasswordComplexity	1	1
Security Template	System Access	PasswordHistorySize	0	24
Security Template	System Access	RequireLogonToChangePassword	0	
Security Template	System Access	ResetLockoutCount		15

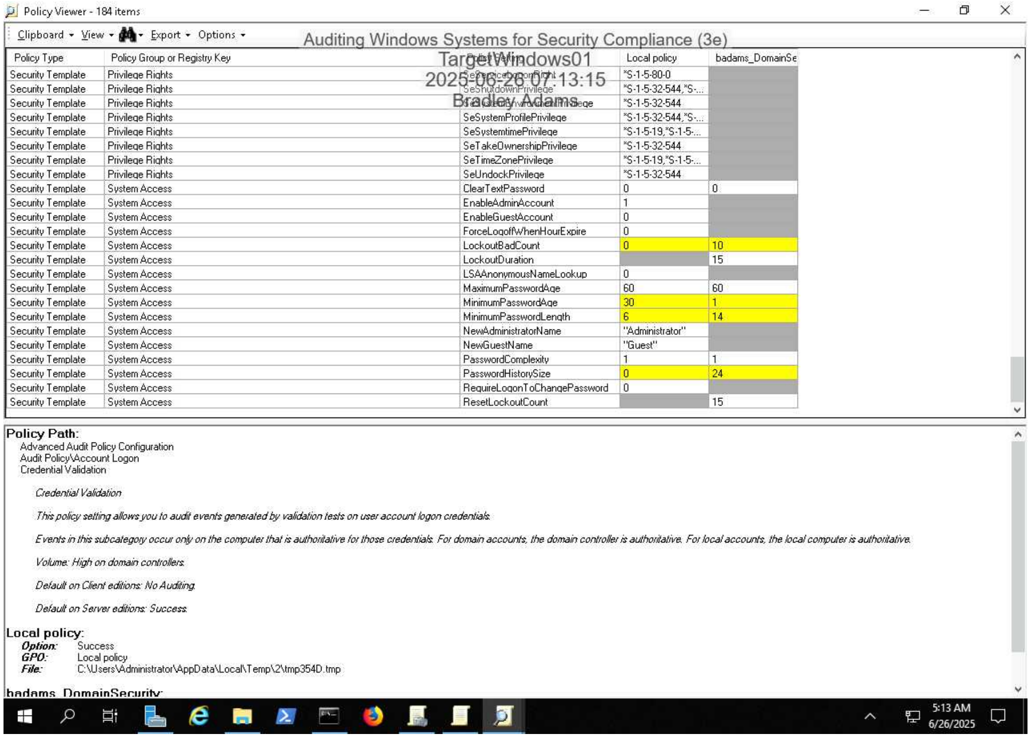
```
Policy Path:
    Security Settings
    Account Policies\Password Policy
    Maximum password age

Local policy:
    Option:   -1
    GPO:      Local policy
    File:     C:\Users\Administrator\AppData\Local\Temp\2\tmp54A.tmp

badams_DomainSecurity:
    Option:   60
    GPO:      MSFT Windows 10 1809 and Server 2019 - Domain Security
    File:     C:\SCT\Windows 10 Version 1809 and Windows Server 2019 Security Baseline\GPOs\{B9263530-926F-46F3-8382-832C31EC81B5}\DomainSysvol\GPO\Machine
              \microsoft\windows nt\SecEdit\GptTmpl.inf
```

Policy Rule sets in: C:\Users\Adm
Policy Definitions in: C:\Windows\F

35. **Make a screen capture** showing the **updated MaximumPasswordAge setting in the Policy Viewer**.



Auditing Windows Systems for Security Compliance (3e)
TargetWindows01
2025-06-26 07:13:15
Bradley Adams

Policy Type	Policy Group or Registry Key	Policy Setting	Local policy	badams_DomainSe
Security Template	Privilege Rights	SeServiceLogonRight	*S-1-5-80-0	
Security Template	Privilege Rights	SeShutdownPrivilege	*S-1-5-32-544,*S-...	
Security Template	Privilege Rights	SeSystemEnvironmentPrivilege	*S-1-5-32-544	
Security Template	Privilege Rights	SeSystemProfilePrivilege	*S-1-5-32-544,*S-...	
Security Template	Privilege Rights	SeSystemtimePrivilege	*S-1-5-19,*S-1-5-...	
Security Template	Privilege Rights	SeTakeOwnershipPrivilege	*S-1-5-32-544	
Security Template	Privilege Rights	SeTimeZonePrivilege	*S-1-5-19,*S-1-5-...	
Security Template	Privilege Rights	SeUndockPrivilege	*S-1-5-32-544	
Security Template	System Access	ClearTextPassword	0	0
Security Template	System Access	EnableAdminAccount	1	
Security Template	System Access	EnableGuestAccount	0	
Security Template	System Access	ForceLogoffWhenHourExpire	0	
Security Template	System Access	LockoutBadCount	0	10
Security Template	System Access	LockoutDuration		15
Security Template	System Access	LSAAnonymousNameLookup	0	
Security Template	System Access	MaximumPasswordAge	60	60
Security Template	System Access	MinimumPasswordAge	30	1
Security Template	System Access	MinimumPasswordLength	6	14
Security Template	System Access	NewAdministratorName	"Administrator"	
Security Template	System Access	NewGuestName	"Guest"	
Security Template	System Access	PasswordComplexity	1	1
Security Template	System Access	PasswordHistorySize	0	24
Security Template	System Access	RequireLogonToChangePassword	0	
Security Template	System Access	ResetLockoutCount		15

Policy Path:
Advanced Audit Policy Configuration
Audit Policy\Account Logon
Credential Validation

Credential Validation

This policy setting allows you to audit events generated by validation tests on user account logon credentials.

Events in this subcategory occur only on the computer that is authoritative for those credentials. For domain accounts, the domain controller is authoritative. For local accounts, the local computer is authoritative.

Volume: High on domain controllers.

Default on Client editions: No Auditing.

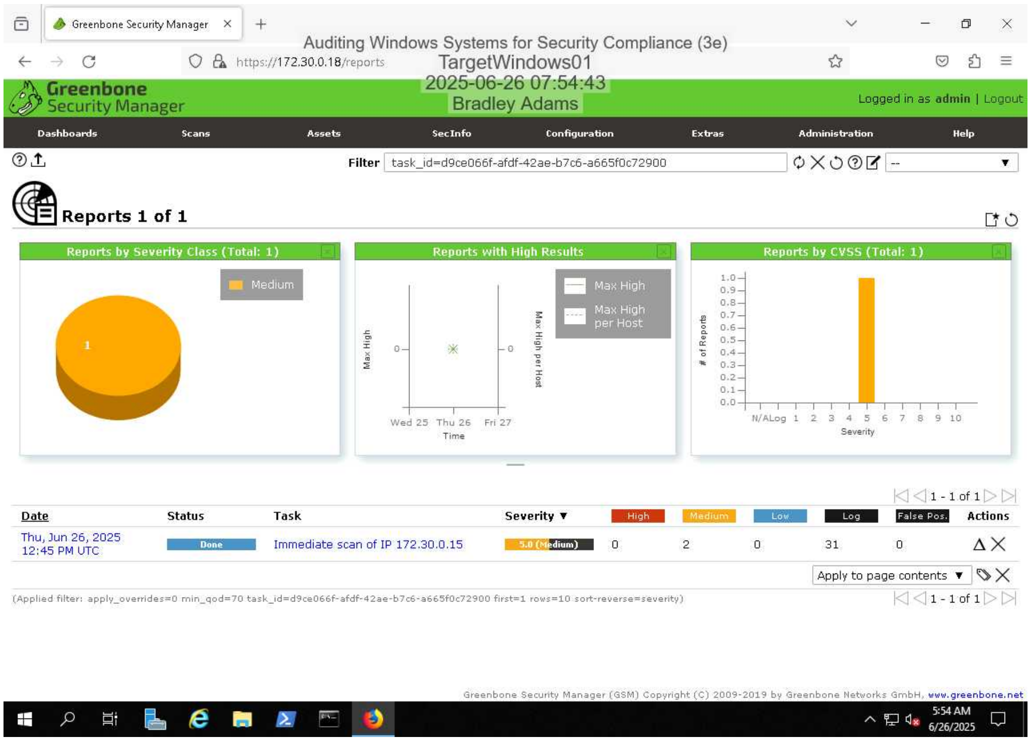
Default on Server editions: Success.

Local policy:
Option: Success
GPO: Local policy
File: C:\Users\Administrator\AppData\Local\Temp\2\tmp354D.tmp

badams_DomainSecurity:

Part 2: Audit a Windows System using OpenVAS

8. **Make a screen capture** showing the **completed scan of TargetWindows01**.



Auditing Windows Systems for Security Compliance (3e)
TargetWindows01
2025-06-26 07:54:43
Bradley Adams

https://172.30.0.18/reports

Logged in as admin | Logout

Filter: task_id=d9ce066f-afdf-42ae-b7c6-a665f0c72900

Reports 1 of 1

1 - 1 of 1

Date	Status	Task	Severity ▼	High	Medium	Low	Log	False Pos.	Actions
Thu, Jun 26, 2025 12:45 PM UTC	Done	Immediate scan of IP 172.30.0.15	5.0 (Medium)	0	2	0	31	0	Δ ✕

Apply to page contents ▼

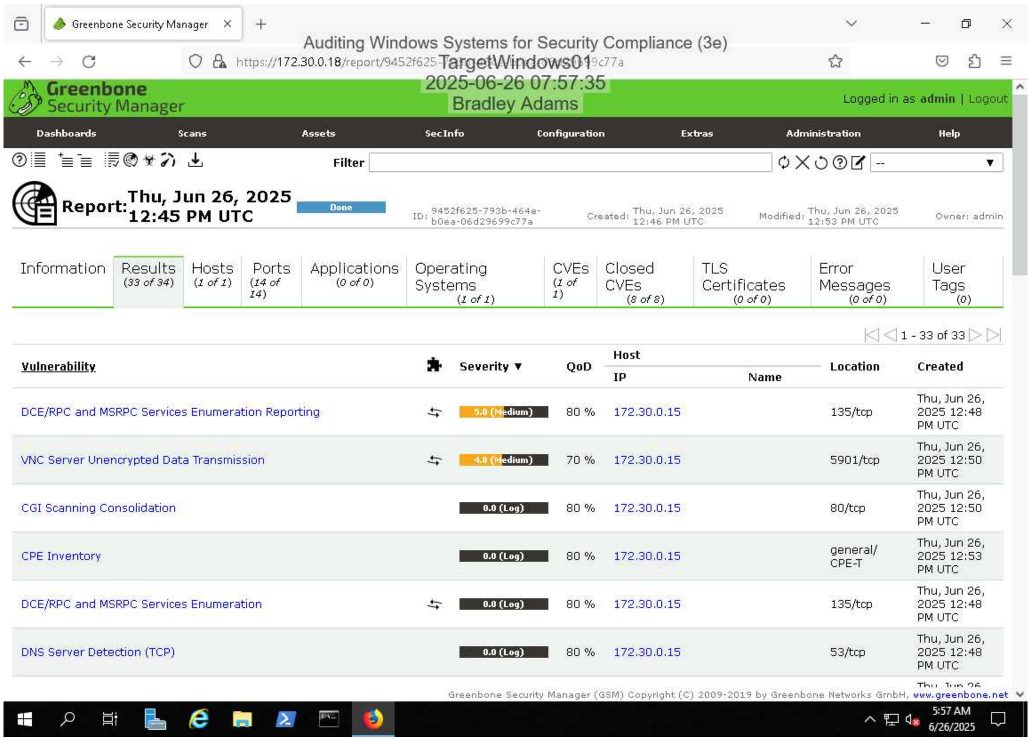
(Applied filter: apply_overrides=0 min_qod=70 task_id=d9ce066f-afdf-42ae-b7c6-a665f0c72900 first=1 rows=10 sort-reverse=severity)

1 - 1 of 1

Greenbone Security Manager (GSM) Copyright (C) 2009-2019 by Greenbone Networks GmbH, www.greenbone.net

5:54 AM
6/26/2025

11. **Make a screen capture** showing the **vulnerabilities from the completed scan of TargetWindows01**.



Auditing Windows Systems for Security Compliance (3e)
TargetWindows01
2025-06-26 07:57:35
Bradley Adams

https://172.30.0.18/report/9452f625-

Logged in as admin | Logout

Filter:

Report: Thu, Jun 26, 2025 12:45 PM UTC — Done

ID: 9452f625-793b-464e-b0ea-06d29699c77a
Created: Thu, Jun 26, 2025 12:46 PM UTC
Modified: Thu, Jun 26, 2025 12:53 PM UTC
Owner: admin

Information | Results (33 of 34) | Hosts (1 of 1) | Ports (14 of 14) | Applications (0 of 0) | Operating Systems (1 of 1) | CVEs (1 of 1) | Closed CVEs (8 of 8) | TLS Certificates (0 of 0) | Error Messages (0 of 0) | User Tags (0)

1 - 33 of 33

Vulnerability		Severity ▼	QoD	Host IP	Host Name	Location	Created
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)	80 %	172.30.0.15		135/tcp	Thu, Jun 26, 2025 12:48 PM UTC
VNC Server Unencrypted Data Transmission	⇆	4.8 (Medium)	70 %	172.30.0.15		5901/tcp	Thu, Jun 26, 2025 12:50 PM UTC
CGI Scanning Consolidation		0.0 (Log)	80 %	172.30.0.15		80/tcp	Thu, Jun 26, 2025 12:50 PM UTC
CPE Inventory		0.0 (Log)	80 %	172.30.0.15		general/CPE-T	Thu, Jun 26, 2025 12:53 PM UTC
DCE/RPC and MSRPC Services Enumeration	⇆	0.0 (Log)	80 %	172.30.0.15		135/tcp	Thu, Jun 26, 2025 12:48 PM UTC
DNS Server Detection (TCP)		0.0 (Log)	80 %	172.30.0.15		53/tcp	Thu, Jun 26, 2025 12:48 PM UTC

Greenbone Security Manager (GSM) Copyright (C) 2009-2019 by Greenbone Networks GmbH, www.greenbone.net

5:57 AM
6/26/2025

13. **Describe** remediation steps for the vulnerability you selected.

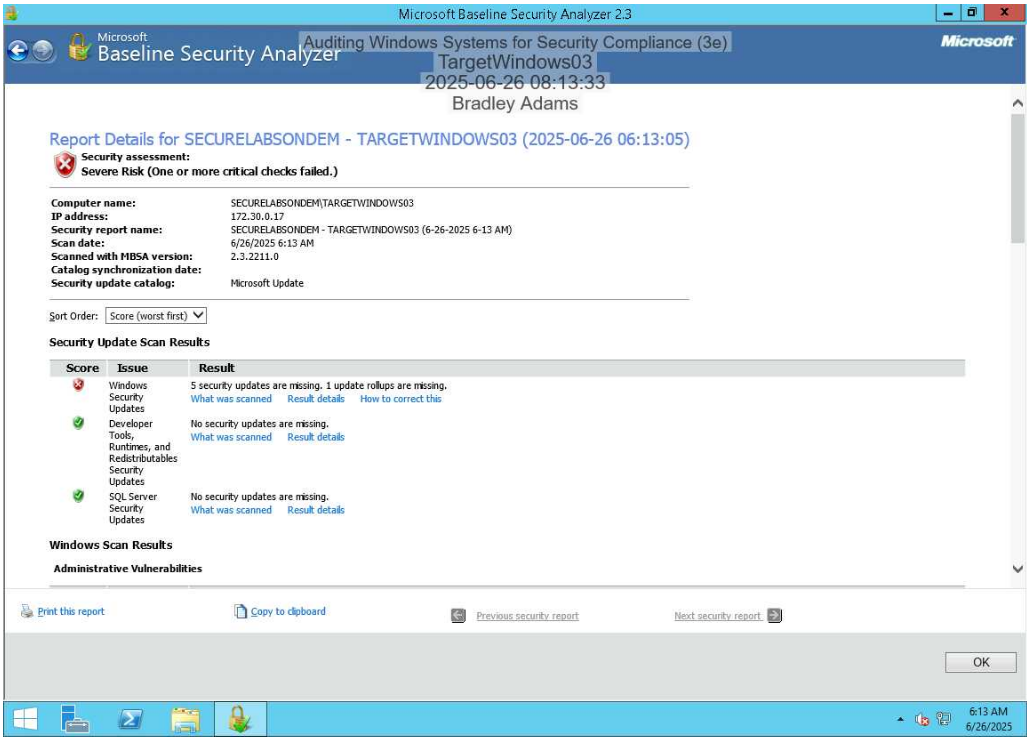
Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Solution
Solution Type: Mitigation
Filter incoming traffic to this ports.

Section 2: Applied Learning

Part 1: Audit a Windows System using MBSA

9. **Make a screen capture** showing the **MBSA scan results**.


Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft

Auditing Windows Systems for Security Compliance (3e)
TargetWindows03
2025-06-26 08:13:33
Bradley Adams

Report Details for SECURELABSONDEM - TARGETWINDOWS03 (2025-06-26 06:13:05)

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name:	SECURELABSONDEM\TARGETWINDOWS03
IP address:	172.30.0.17
Security report name:	SECURELABSONDEM - TARGETWINDOWS03 (6-26-2025 6-13 AM)
Scan date:	6/26/2025 6:13 AM
Scanned with MBSA version:	2.3.2211.0
Catalog synchronization date:	
Security update catalog:	Microsoft Update

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
☒	Windows Security Updates	5 security updates are missing. 1 update rollups are missing. What was scanned Result details How to correct this
✓	Developer Tools, Runtimes, and Redistributables Security Updates	No security updates are missing. What was scanned Result details
✓	SQL Server Security Updates	No security updates are missing. What was scanned Result details

Windows Scan Results

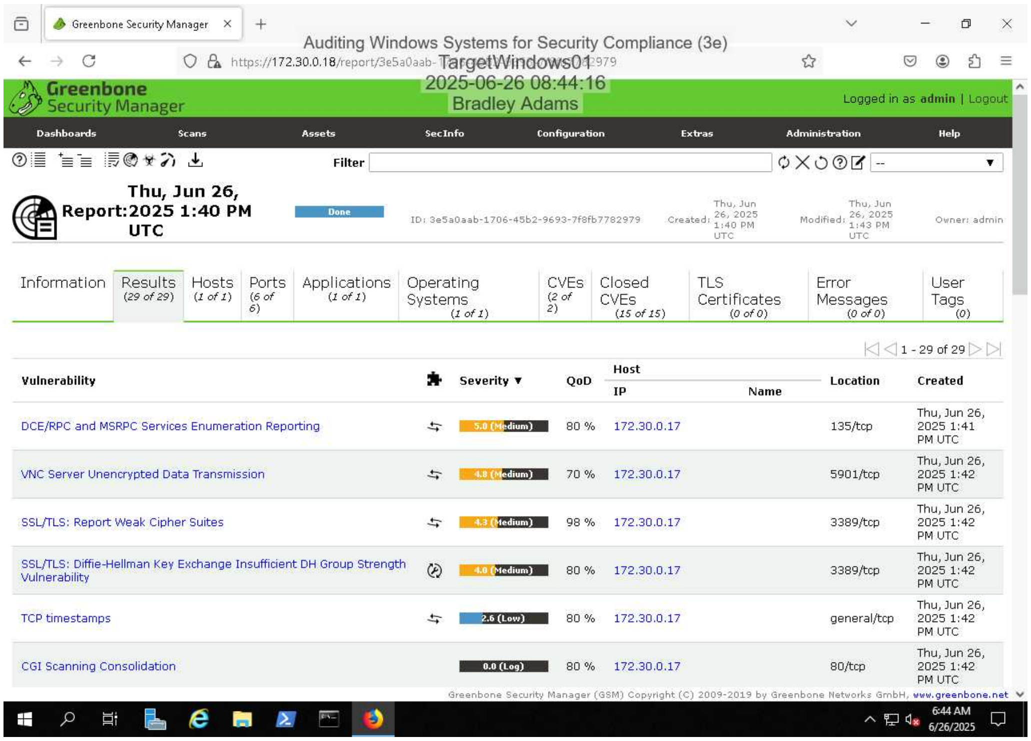
Administrative Vulnerabilities

14. **Describe** the security issue for this missing update.

KB5012170: Security update for Secure Boot DBX
KB5012170 is a security update released by Microsoft to address a critical vulnerability in the Secure Boot process. This update modifies the Secure Boot Forbidden Signature Database to block known vulnerable UEFI bootloaders that could allow an attacker to bypass Secure Boot protections. It prevents the execution of bootloaders that threat actors exploit to install malware before the operating system loads. This update is critical for maintaining Secure Boot integrity across supported Windows platforms.

Part 2: Audit a Windows System using OpenVAS

7. **Make a screen capture** showing the **vulnerabilities from the completed scan of TargetWindows03**.



Auditing Windows Systems for Security Compliance (3e)
TargetWindows01
2025-06-26 08:44:16
Bradley Adams

Greenbone Security Manager
https://172.30.0.18/report/3e5a0aab-
2979
Greenbone Security Manager
Logged in as admin | Logout
Dashboards
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Filter
--

Report: Thu, Jun 26, 2025 1:40 PM UTC — Done — ID: 3e5a0aab-1706-45b2-9693-7f8fb7782979 — Created: Thu, Jun 26, 2025 1:40 PM UTC — Modified: Thu, Jun 26, 2025 1:43 PM UTC — Owner: admin

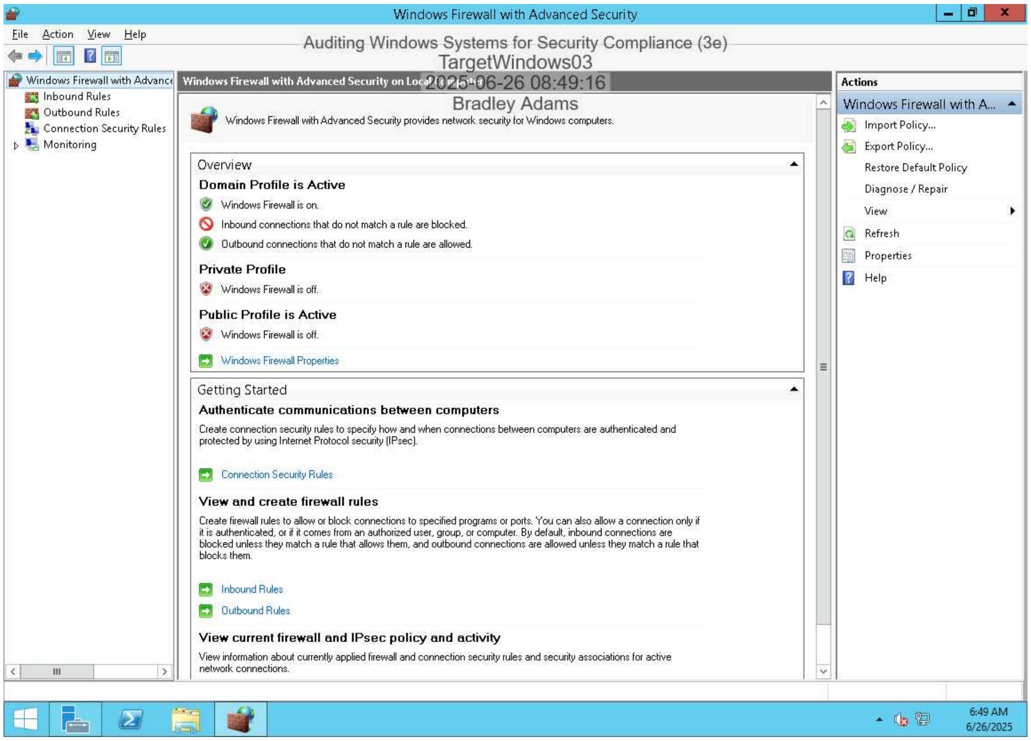
Information | Results (29 of 29) | Hosts (1 of 1) | Ports (6 of 6) | Applications (1 of 1) | Operating Systems (1 of 1) | CVEs (2 of 2) | Closed CVEs (15 of 15) | TLS Certificates (0 of 0) | Error Messages (0 of 0) | User Tags (0)

1 - 29 of 29

Vulnerability		Severity ▼	QoD	Host IP	Host Name	Location	Created
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)	80 %	172.30.0.17		135/tcp	Thu, Jun 26, 2025 1:41 PM UTC
VNC Server Unencrypted Data Transmission	⇆	4.8 (Medium)	70 %	172.30.0.17		5901/tcp	Thu, Jun 26, 2025 1:42 PM UTC
SSL/TLS: Report Weak Cipher Suites	⇆	4.3 (Medium)	98 %	172.30.0.17		3389/tcp	Thu, Jun 26, 2025 1:42 PM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80 %	172.30.0.17		3389/tcp	Thu, Jun 26, 2025 1:42 PM UTC
TCP timestamps	⇆	2.6 (Low)	80 %	172.30.0.17		general/tcp	Thu, Jun 26, 2025 1:42 PM UTC
CGI Scanning Consolidation		0.0 (Log)	80 %	172.30.0.17		80/tcp	Thu, Jun 26, 2025 1:42 PM UTC

Greenbone Security Manager (GSM) Copyright (C) 2009-2019 by Greenbone Networks GmbH, www.greenbone.net

17. **Make a screen capture** showing the **active Windows Firewall**.



Auditing Windows Systems for Security Compliance (3e)
TargetWindows03
2025-06-26 08:49:16
Bradley Adams

Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Actions
Windows Firewall with A...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help
6:49 AM
6/26/2025

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile is Active

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Firewall is off.

Public Profile is Active

- Windows Firewall is off.

Windows Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

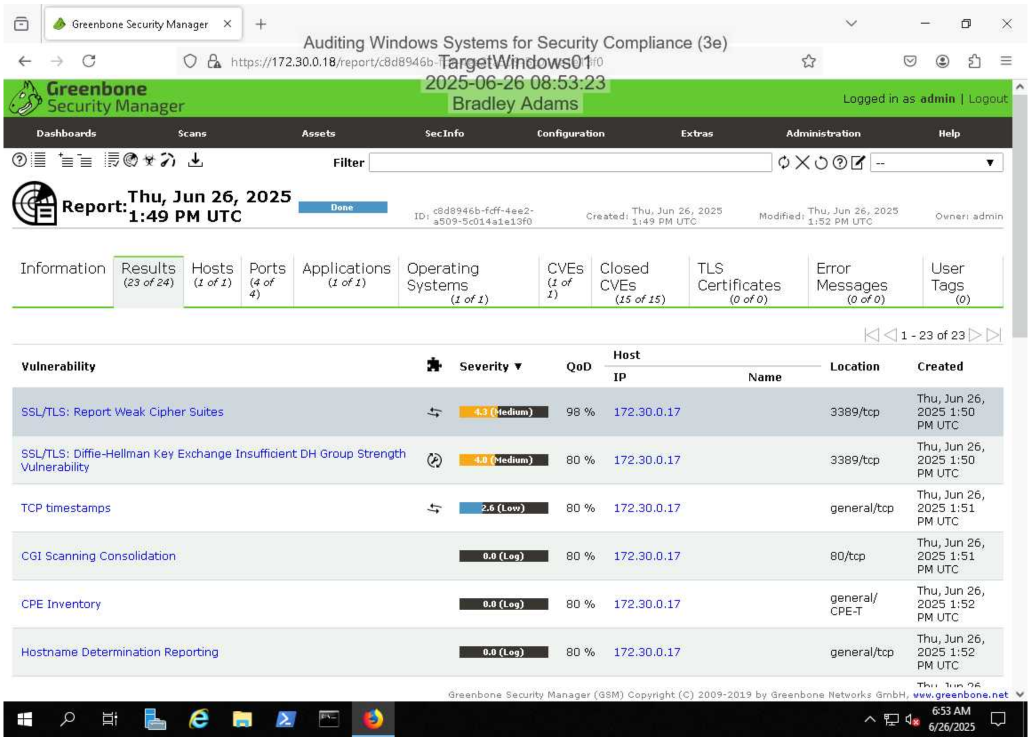
Inbound Rules

Outbound Rules

View current firewall and IPsec policy and activity

View information about currently applied firewall and connection security rules and security associations for active network connections.

21. **Make a screen capture** showing the **vulnerabilities from the latest completed scan of TargetWindows03 (without the DCE/RPC vulnerability listed)**.



https://172.30.0.18/report/c8d8946b-

Auditing Windows Systems for Security Compliance (3e)
TargetWindows01
2025-06-26 08:53:23
Bradley Adams

Report: Thu, Jun 26, 2025 1:49 PM UTC Done

ID: c8d8946b-fcff-4ee2-a509-5c014a1e13f0
Created: Thu, Jun 26, 2025 1:49 PM UTC
Modified: Thu, Jun 26, 2025 1:52 PM UTC
Owner: admin

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
SSL/TLS: Report Weak Cipher Suites	⇆	4.3 (Medium)	98 %	172.30.0.17		3389/tcp	Thu, Jun 26, 2025 1:50 PM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80 %	172.30.0.17		3389/tcp	Thu, Jun 26, 2025 1:50 PM UTC
TCP timestamps	⇆	2.6 (Low)	80 %	172.30.0.17		general/tcp	Thu, Jun 26, 2025 1:51 PM UTC
CGI Scanning Consolidation		0.0 (Log)	80 %	172.30.0.17		80/tcp	Thu, Jun 26, 2025 1:51 PM UTC
CPE Inventory		0.0 (Log)	80 %	172.30.0.17		general/CPE-T	Thu, Jun 26, 2025 1:52 PM UTC
Hostname Determination Reporting		0.0 (Log)	80 %	172.30.0.17		general/tcp	Thu, Jun 26, 2025 1:52 PM UTC

Greenbone Security Manager (GSM) Copyright (C) 2009-2019 by Greenbone Networks GmbH, www.greenbone.net

Section 3: Challenge and Analysis

Part 1: Analysis and Discussion

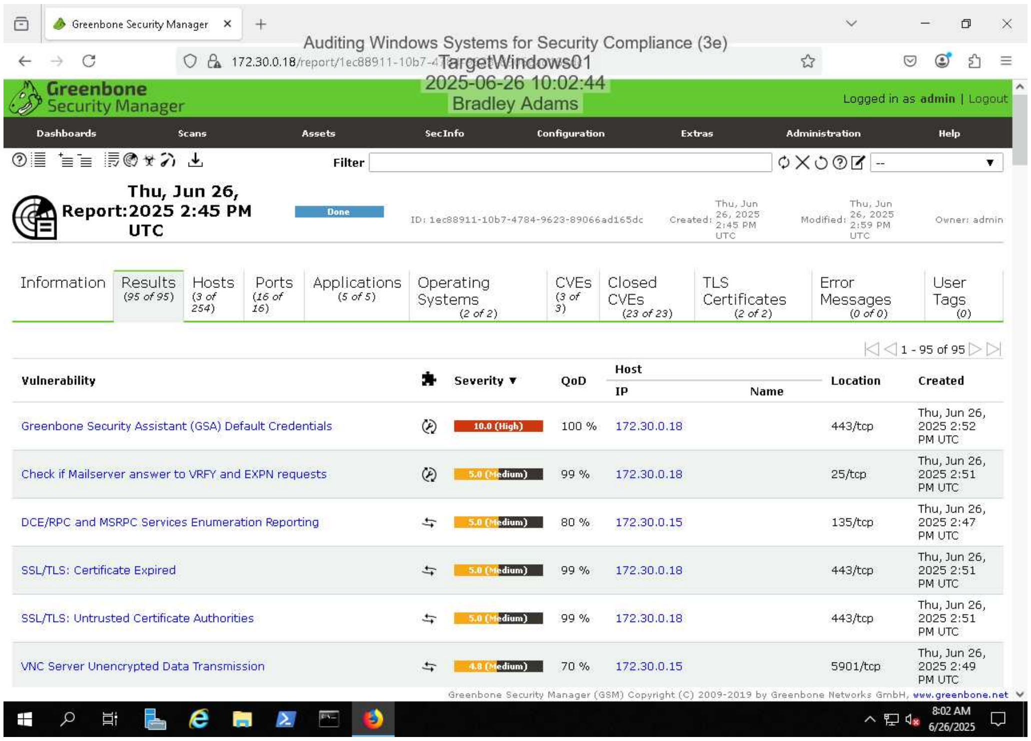
In what context would you consider using the Microsoft Baseline Security Analyzer to conduct a security audit? Is it worth using MBSA at all, or are there similar, more effective tools that could be used in the same context? Use the Internet to research MBSA and alternative tools.

Using MBSA can be justified if your scope is strictly limited to legacy Windows environments and you require a rapid, straightforward audit of Microsoft updates. MBSA is simple and easy to deploy. It offers a basic baseline check for missing Microsoft patches, insecure IIS settings, SQL Server configurations, and Office macro settings. MBSA is increasingly outdated in the context of modern incident detection and vulnerability management. It hasn't been updated for Windows Server 2016 or later. Its checks are hard-coded and limited to Microsoft products. If your goal is to conduct incident detection or vulnerability management across diverse systems, there are far more effective tools. In 2025, it's more effective to use tools that support a broader range of platforms, automate workflows, and integrate into incident response processes. ManageEngine Vulnerability Manager Plus offers cross-platform scanning, patch management, threat intelligence, continuous monitoring, and compliance reporting. OpenVAS is a robust, open-source option for free-form vulnerability assessments that extend beyond Windows, featuring a regularly updated feed and community support. Commercial tools, such as Nessus and Nexpose, provide detailed vulnerability scanning, risk scoring, and integration with tools like Metasploit.

Sources:
https://www.comparitech.com/net-admin/alternatives-to-microsoft-baseline-security-analyzer/
https://www.theknowledgeacademy.com/blog/microsoft-baseline-security-analyzer-alternative/

Part 2: Tools and Commands

Make a screen capture showing the **subnet scan results in the GSM**.



Auditing Windows Systems for Security Compliance (3e)
TargetWindows01
2025-06-26 10:02:44
Bradley Adams

Report: Thu, Jun 26, 2025 2:45 PM UTC

Done

ID: 1ec88911-10b7-4784-9623-89066ad165dc Created: Thu, Jun 26, 2025 2:45 PM UTC Modified: Thu, Jun 26, 2025 2:59 PM UTC Owner: admin

Information | Results (95 of 95) | Hosts (3 of 254) | Ports (16 of 16) | Applications (5 of 5) | Operating Systems (2 of 2) | CVEs (3 of 3) | Closed CVEs (23 of 23) | TLS Certificates (2 of 2) | Error Messages (0 of 0) | User Tags (0)

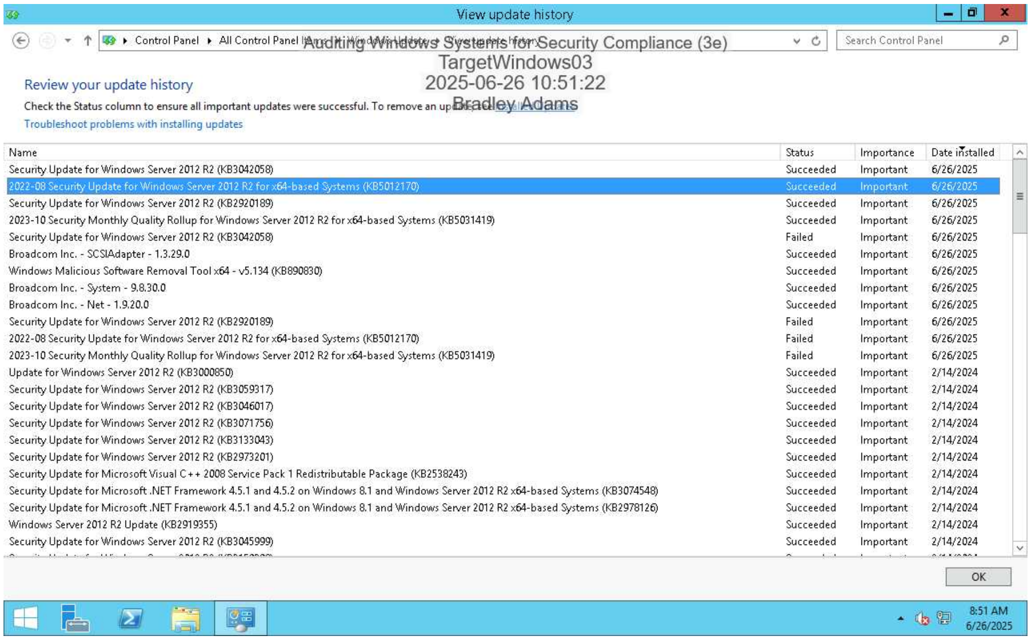
1 - 95 of 95

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Greenbone Security Assistant (GSA) Default Credentials		10.0 (High)	100 %	172.30.0.18		443/tcp	Thu, Jun 26, 2025 2:52 PM UTC
Check if Mailserver answer to VRFY and EXPN requests		5.0 (Medium)	99 %	172.30.0.18		25/tcp	Thu, Jun 26, 2025 2:51 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)	80 %	172.30.0.15		135/tcp	Thu, Jun 26, 2025 2:47 PM UTC
SSL/TLS: Certificate Expired	⇆	5.0 (Medium)	99 %	172.30.0.18		443/tcp	Thu, Jun 26, 2025 2:51 PM UTC
SSL/TLS: Untrusted Certificate Authorities	⇆	5.0 (Medium)	99 %	172.30.0.18		443/tcp	Thu, Jun 26, 2025 2:51 PM UTC
VNC Server Unencrypted Data Transmission	⇆	4.8 (Medium)	70 %	172.30.0.15		5901/tcp	Thu, Jun 26, 2025 2:49 PM UTC

Greenbone Security Manager (GSM) Copyright (C) 2009-2019 by Greenbone Networks GmbH, www.greenbone.net

Part 3: Challenge Exercise

Make a screen capture showing the **update confirmation on TargetWindows03**.



View update history
Control Panel ▸ All Control Panel Items ▸ Windows Update ▸ View update history
Search Control Panel

Auditing Windows Systems for Security Compliance (3e)
TargetWindows03
2025-06-26 10:51:22
Bradley Adams

Review your update history

Check the Status column to ensure all important updates were successful. To remove an update, see Installed Updates.

Troubleshoot problems with installing updates

Name	Status	Importance	Date installed
Security Update for Windows Server 2012 R2 (KB3042058)	Succeeded	Important	6/26/2025
2022-08 Security Update for Windows Server 2012 R2 for x64-based Systems (KB5012170)	Succeeded	Important	6/26/2025
Security Update for Windows Server 2012 R2 (KB2920189)	Succeeded	Important	6/26/2025
2023-10 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5031419)	Succeeded	Important	6/26/2025
Security Update for Windows Server 2012 R2 (KB3042058)	Failed	Important	6/26/2025
Broadcom Inc. - SCSIAdapter - 1.3.29.0	Succeeded	Important	6/26/2025
Windows Malicious Software Removal Tool x64 - v5.134 (KB890830)	Succeeded	Important	6/26/2025
Broadcom Inc. - System - 9.8.30.0	Succeeded	Important	6/26/2025
Broadcom Inc. - Net - 1.9.20.0	Succeeded	Important	6/26/2025
Security Update for Windows Server 2012 R2 (KB2920189)	Failed	Important	6/26/2025
2022-08 Security Update for Windows Server 2012 R2 for x64-based Systems (KB5012170)	Failed	Important	6/26/2025
2023-10 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB5031419)	Failed	Important	6/26/2025
Update for Windows Server 2012 R2 (KB3000850)	Succeeded	Important	2/14/2024
Security Update for Windows Server 2012 R2 (KB3059317)	Succeeded	Important	2/14/2024
Security Update for Windows Server 2012 R2 (KB3046017)	Succeeded	Important	2/14/2024
Security Update for Windows Server 2012 R2 (KB3071756)	Succeeded	Important	2/14/2024
Security Update for Windows Server 2012 R2 (KB3133043)	Succeeded	Important	2/14/2024
Security Update for Windows Server 2012 R2 (KB2973201)	Succeeded	Important	2/14/2024
Security Update for Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package (KB2538243)	Succeeded	Important	2/14/2024
Security Update for Microsoft .NET Framework 4.5.1 and 4.5.2 on Windows 8.1 and Windows Server 2012 R2 x64-based Systems (KB3074548)	Succeeded	Important	2/14/2024
Security Update for Microsoft .NET Framework 4.5.1 and 4.5.2 on Windows 8.1 and Windows Server 2012 R2 x64-based Systems (KB2978126)	Succeeded	Important	2/14/2024
Windows Server 2012 R2 Update (KB2919355)	Succeeded	Important	2/14/2024
Security Update for Windows Server 2012 R2 (KB3045999)	Succeeded	Important	2/14/2024