Final Security Report

Tyra Baxter

Department of Computer Technology, Bowie State University

CTEC 402: Software and OS Security

Dr. Velma Latson

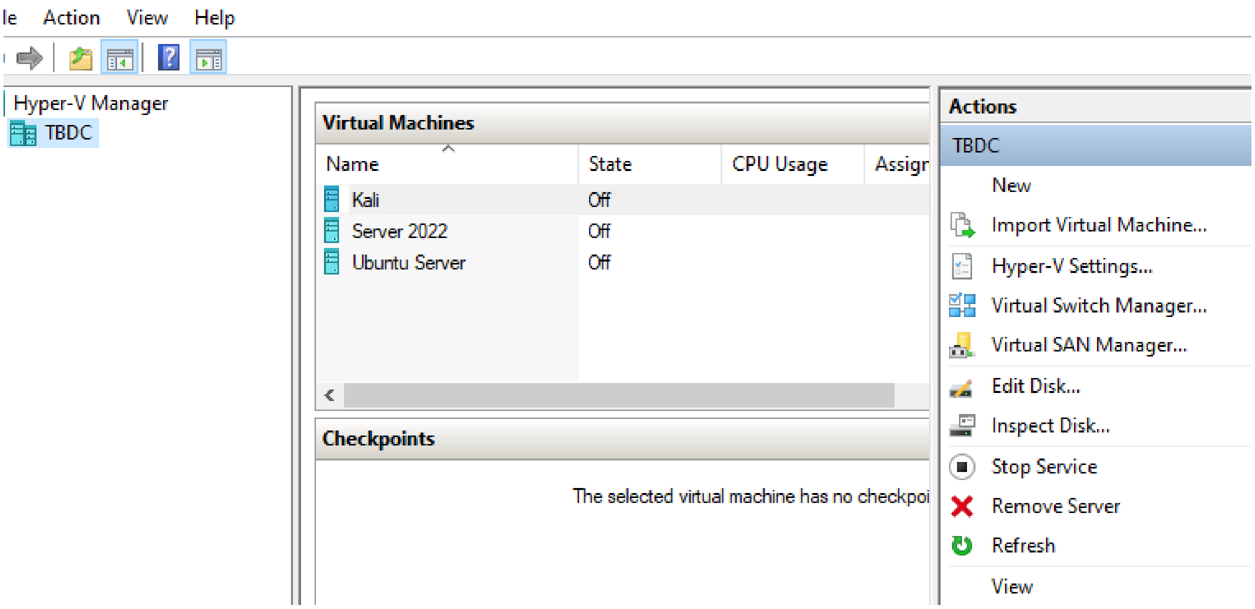
March 13, 2025

Security Harding Report

This report will document the configuration process and installation of the infrastructure of the financial institution, Starlings Savings. It will provide detailed descriptions of hardening techniques and best practices implemented on servers to enhance their security. This document outlines applications for the latest patches, firewall configuration, and installation of services. In addition, a thorough vulnerability assessment was conducted, and findings from this scan will be presented to identify potential weaknesses within the infrastructure. Recommendations for mitigating these vulnerabilities will be discussed. Along with future steps to improve overall security measures of the company.

OS Installation and Configurations

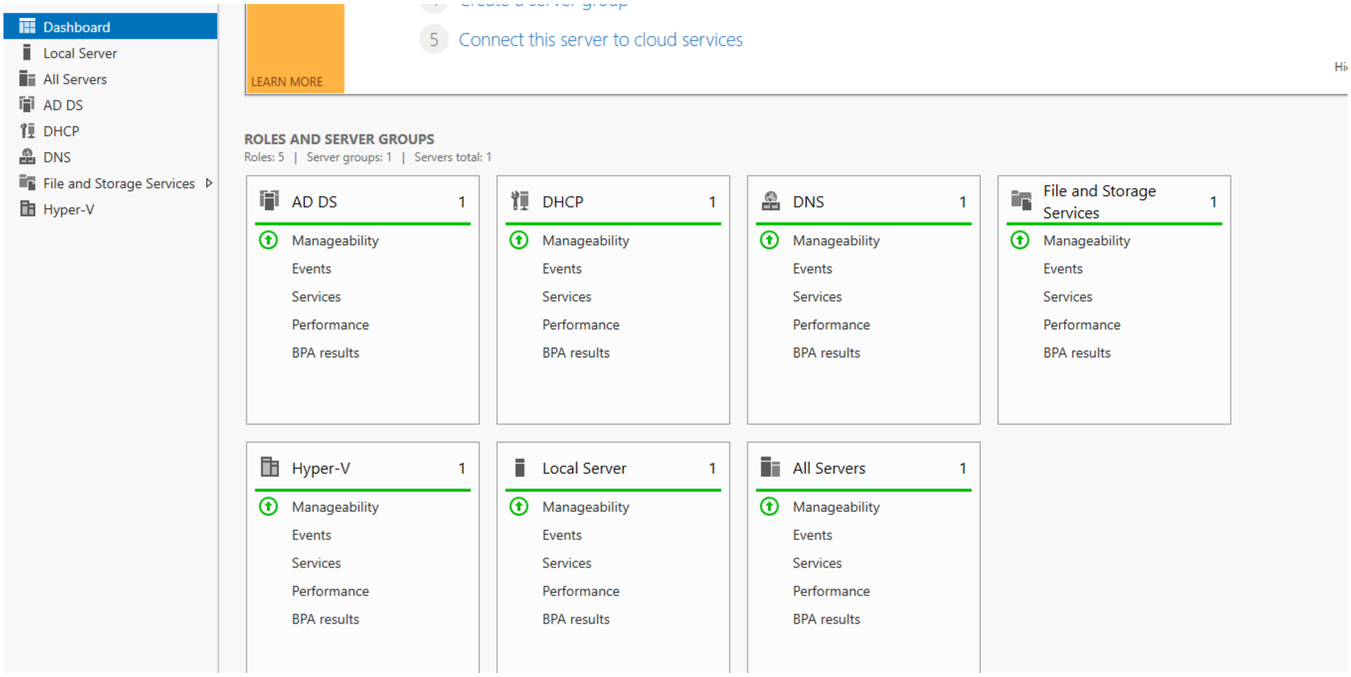
On hard drive installed window server 2022, window sever 2019, and windows 11 pro. On window sever 2022 installed virtual machines of Ubuntu Server, Kali, and window server 2022.



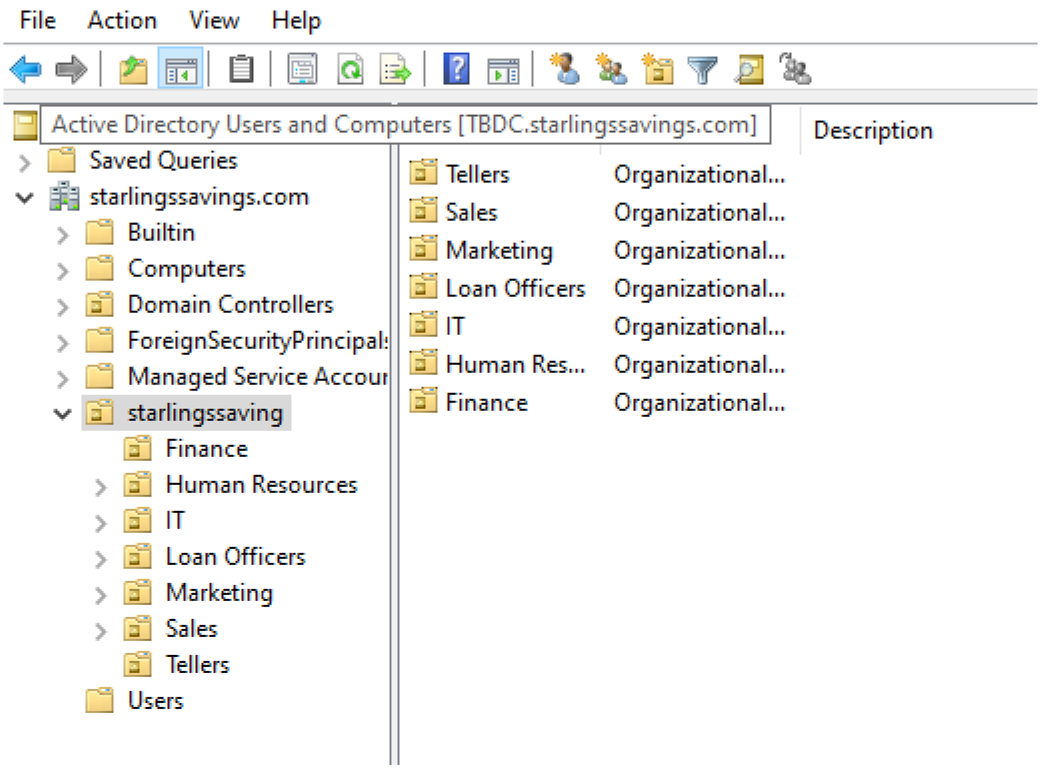
Name	State	CPU Usage	Assigr
Kali	Off		
Server 2022	Off		
Ubuntu Server	Off		

The selected virtual machine has no checkpoi

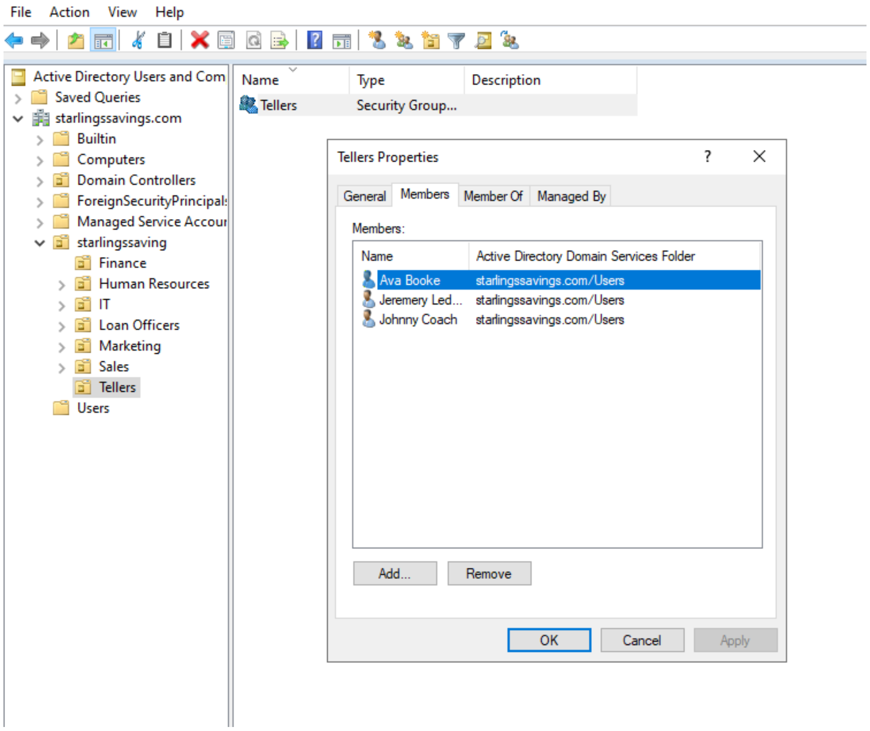
On domain controller installed AD, DNS, and DHCP roles onto server.



Next, created an organization unit for Staling Savings Bank and then created additional organization units for departments under the original. These departments include tellers, sales, marketing, loan officers, information technology, human resources, and finance. After completing this, the process continued by creating security groups with the names of each department. User where than added to each security group, here is an example of the security groups for departments HR and tellers.



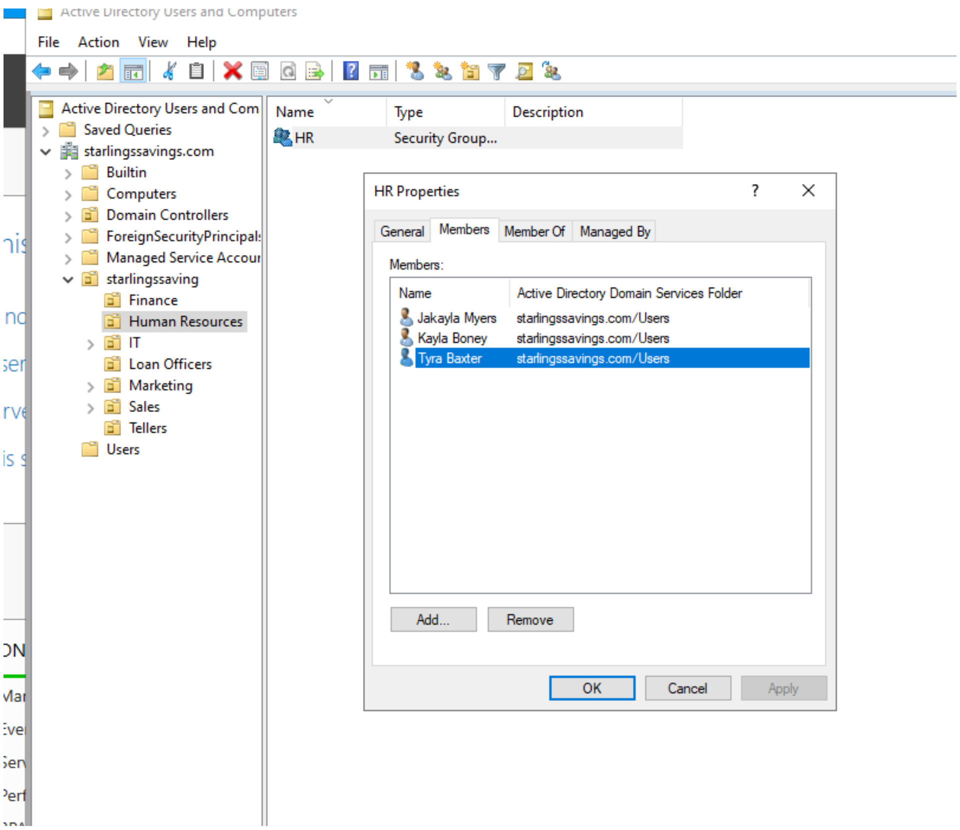
		Description
Tellers	Organizational...	
Sales	Organizational...	
Marketing	Organizational...	
Loan Officers	Organizational...	
IT	Organizational...	
Human Res...	Organizational...	
Finance	Organizational...	



Name	Type	Description
Tellers	Security Group...	

Members:

Name	Active Directory Domain Services Folder
Ava Booke	starlingssavings.com/Users
Jeremery Led...	starlingssavings.com/Users
Johnny Coach	starlingssavings.com/Users

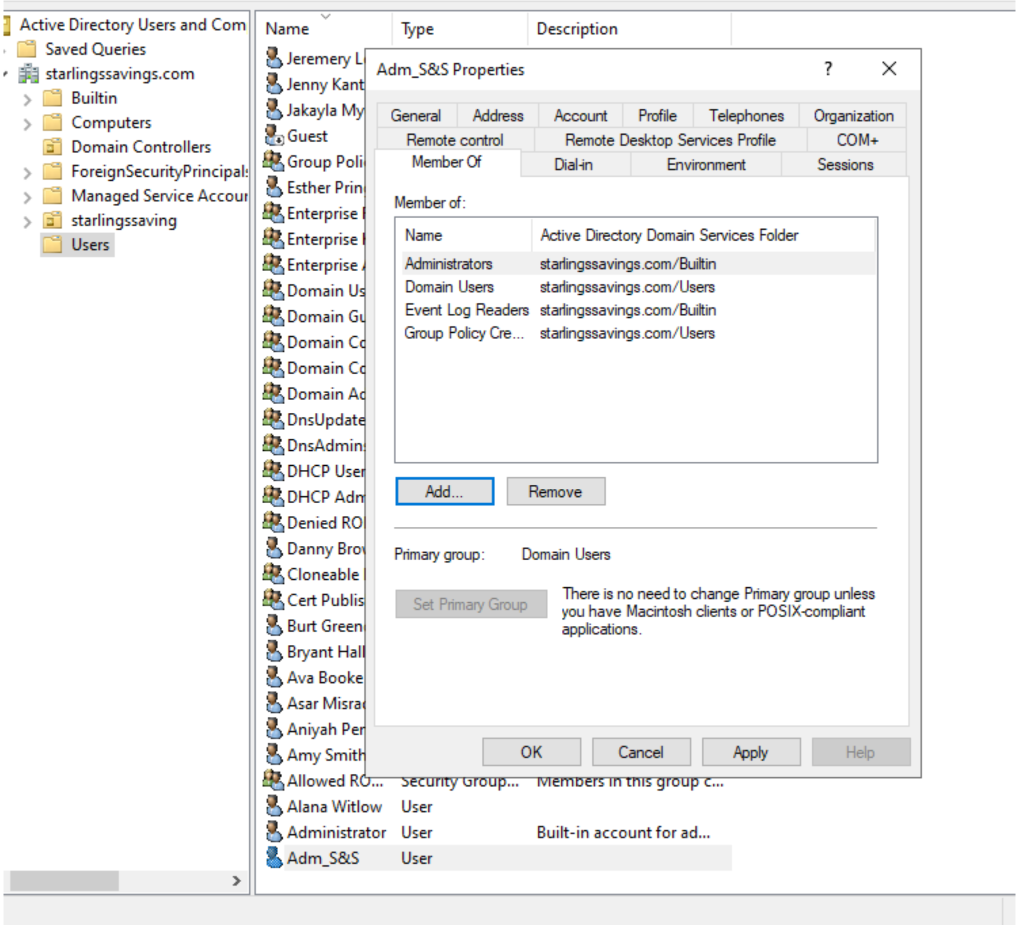


Name	Type	Description
HR	Security Group...	

Name	Active Directory Domain Services Folder
Jakayla Myers	starlingssavings.com/Users
Kayla Boney	starlingssavings.com/Users
Tyra Baxter	starlingssavings.com/Users

Hardening Techniques

A secondary Administrator account was created, but instead of placing it in Domain Admin group the account was set up with minimum permission. This allows administrators to login this account and still complete task but don't have domain admin privileges. They can still add DNS records, create users, and implement group policies etc.



Name	Type	Description
Allowed RO...	Security Group...	Members in this group c...
Alana Witlow	User	
Administrator	User	Built-in account for ad...
Adm_S&S	User	

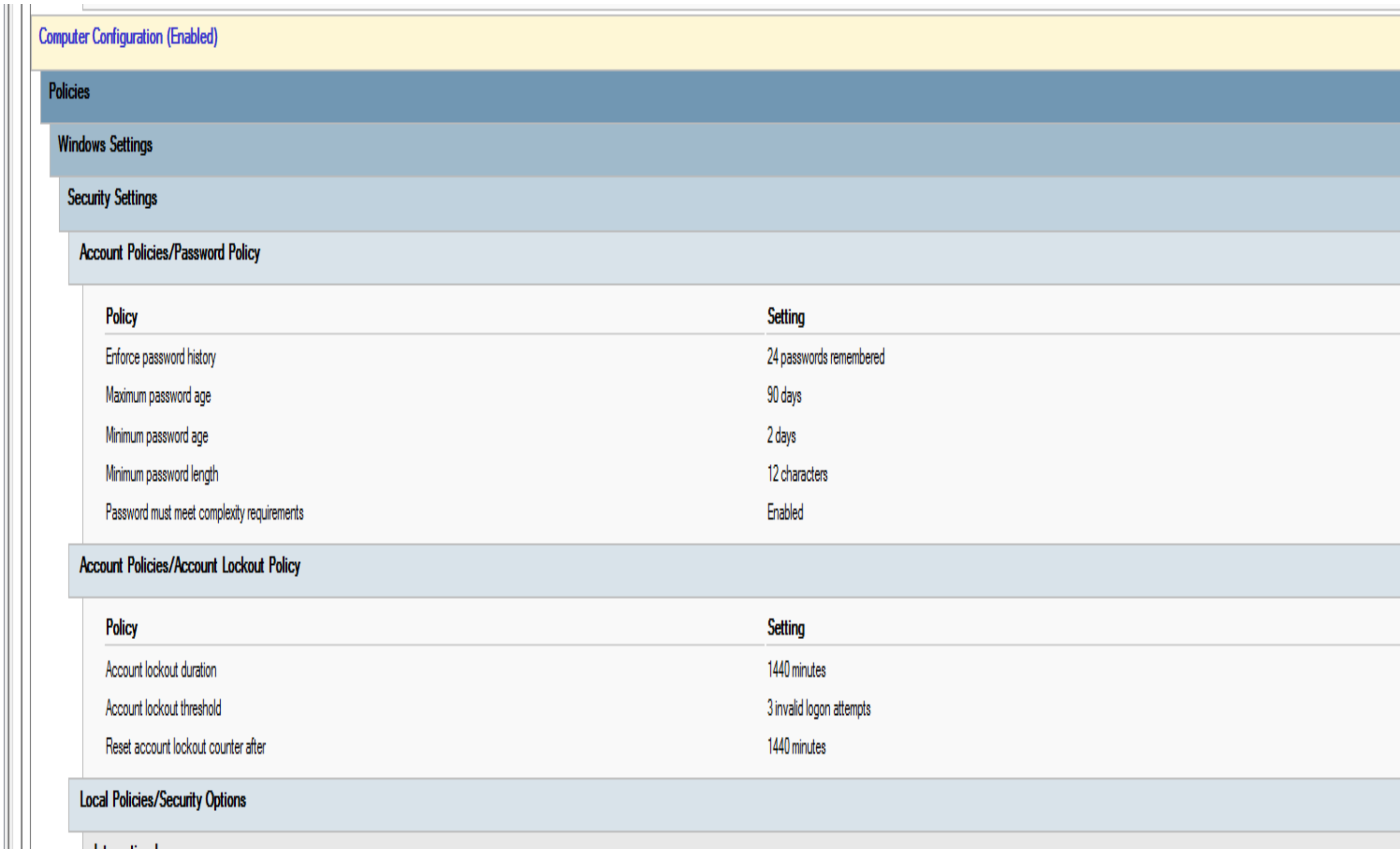
Member of:

Name	Active Directory Domain Services Folder
Administrators	starlingssavings.com/Builtin
Domain Users	starlingssavings.com/Users
Event Log Readers	starlingssavings.com/Builtin
Group Policy Cre...	starlingssavings.com/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Implemented a password policy for users in all departments. There is a 12-character limit minimum and enabled password complexity. Every three months users must rest their password. Also, users are only allowed to make 3 login attempts and when they are not able to login they will be locked out of that account for a day. This makes it difficult for hackers to make multiple login attempts.



Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

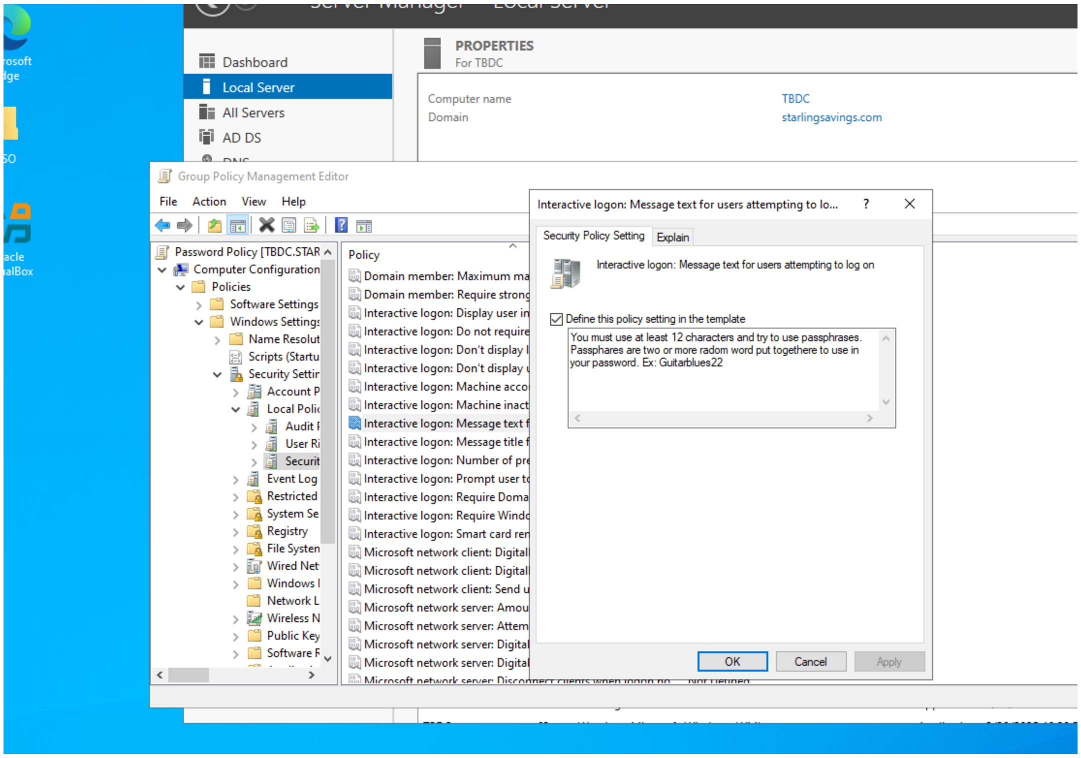
Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	2 days
Minimum password length	12 characters
Password must meet complexity requirements	Enabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	1440 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	1440 minutes

Local Policies/Security Options

Added a password banner that explains to users the password requirements and encourages users to use passphrases. A passphrase is when you put two or more random words together. This technique makes it harder for hackers to use password cracking software.



PROPERTIES
For TBDC

Computer name TBDC
Domain starlingsavings.com

Interactive logon: Message text for users attempting to lo...

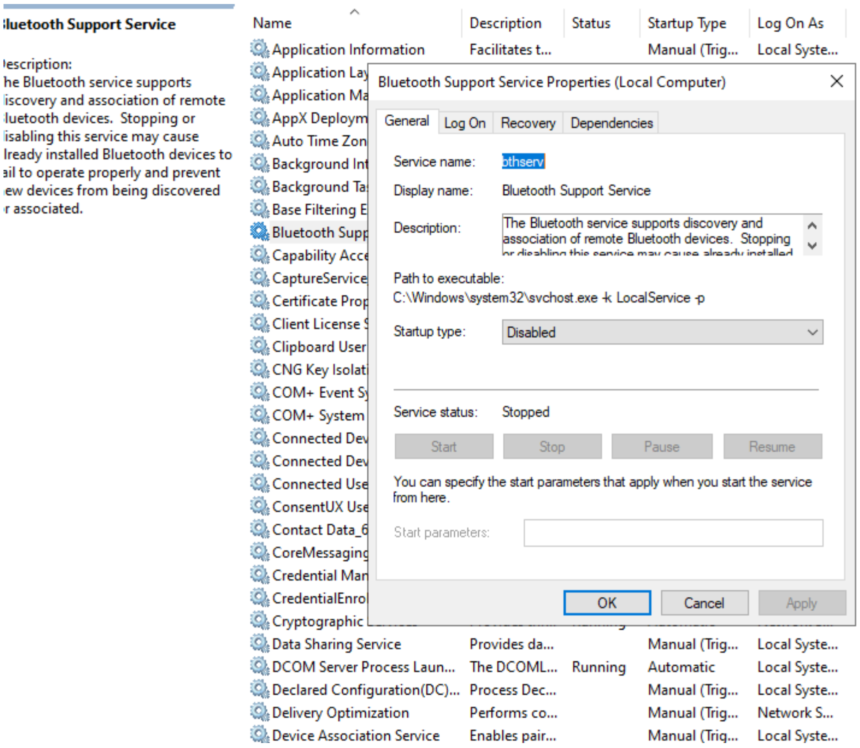
Interactive logon: Message text for users attempting to log on

☑ Define this policy setting in the template

You must use at least 12 characters and try to use passphrases. Passphares are two or more radom word put togethere to use in your password. Ex: Guitarblues22

Server Manager • Local Server
Dashboard
Local Server
All Servers
AD DS
Group Policy Management Editor
File
Action
View
Help
Password Policy [TBDC.STAR
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Security Settir
Account P
Local Polic
Audit I
User Ri
Securit
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows I
Network L
Wireless N
Public Key
Software F
Policy
Domain member: Maximum ma
Domain member: Require strong
Interactive logon: Display user in
Interactive logon: Do not require
Interactive logon: Don't display l
Interactive logon: Don't display u
Interactive logon: Machine acco
Interactive logon: Machine inact
Interactive logon: Message text f
Interactive logon: Message title f
Interactive logon: Number of pre
Interactive logon: Prompt user to
Interactive logon: Require Doma
Interactive logon: Require Windo
Interactive logon: Smart card ren
Microsoft network client: Digitall
Microsoft network client: Digitall
Microsoft network client: Send u
Microsoft network server: Amou
Microsoft network server: Attem
Microsoft network server: Digital
Microsoft network server: Digital
Security Policy Setting
Explain
OK
Cancel
Apply

In Microsoft server services disabled the Bluetooth support service so users are not able to connect unauthorized devices to network. Then disabled telephony service since there isn't no telephone devices on the local computer or through a LAN.



luetooth Support Service

escription:
he Bluetooth service supports iscovery and association of remote luetooth devices. Stopping or isabling this service may cause lready installed Bluetooth devices to ail to operate properly and prevent ew devices from being discovered r associated.

Name	Description	Status	Startup Type	Log On As
Application Information	Facilitates t...		Manual (Trig...	Local Syste...
Application Lay				
Application Ma				
AppX Deploym				
Auto Time Zon				
Background Int				
Background Ta				
Base Filtering E				
Bluetooth Supp				
Capability Acce				
CaptureService				
Certificate Prop				
Client License S				
Clipboard User				
CNG Key Isolati				
COM+ Event Sy				
COM+ System				
Connected Dev				
Connected Dev				
Connected Use				
ConsentUX Use				
Contact Data_6				
CoreMessaging				
Credential Man				
CredentialEnro				
Cryptographic				
Data Sharing Service	Provides da...		Manual (Trig...	Local Syste...
DCOM Server Process Laun...	The DCOML...	Running	Automatic	Local Syste...
Declared Configuration(DC)...	Process Dec...		Manual (Trig...	Local Syste...
Delivery Optimization	Performs co...		Manual (Trig...	Network S...
Device Association Service	Enables pair...		Manual (Trig...	Local Syste...

Bluetooth Support Service Properties (Local Computer)

Service name: bthserv

Display name: Bluetooth Support Service

Description: The Bluetooth service supports discovery and association of remote Bluetooth devices. Stopping or disabling this service may cause already installed

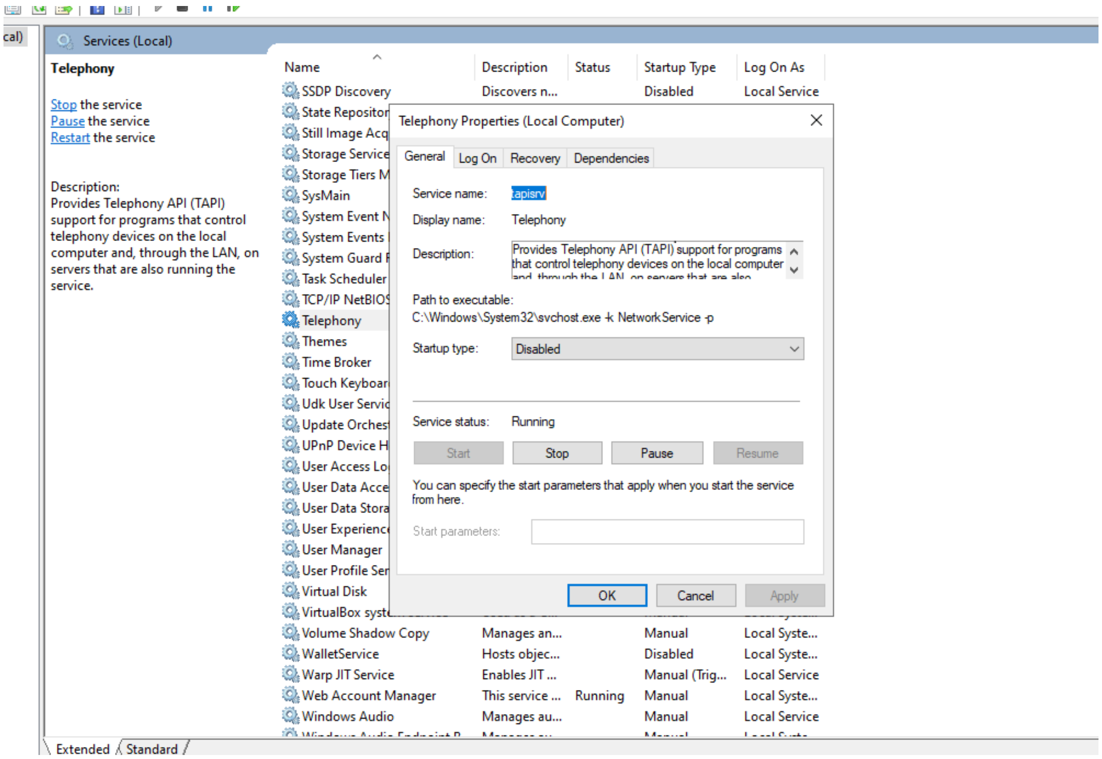
Path to executable:
C:\Windows\system32\svchost.exe -k LocalService -p

Startup type: Disabled

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:



Services (Local)

Telephony

Stop the service
Pause the service
Restart the service

Description:
Provides Telephony API (TAPI) support for programs that control telephony devices on the local computer and, through the LAN, on servers that are also running the service.

Name	Description	Status	Startup Type	Log On As
SSDP Discovery	Discovers n...		Disabled	Local Service
State Repositor				
Still Image Acq				
Storage Service				
Storage Tiers M				
SysMain				
System Event N				
System Events				
System Guard F				
Task Scheduler				
TCP/IP NetBIOS				
Telephony				
Themes				
Time Broker				
Touch Keyboar				
Udk User Servic				
Update Orches				
UPnP Device H				
User Access Lo				
User Data Acce				
User Data Stora				
User Experienc				
User Manager				
User Profile Ser				
Virtual Disk				
VirtualBox syst				
Volume Shadow Copy	Manages an...		Manual	Local Syste...
WalletService	Hosts objec...		Disabled	Local Syste...
Warp JIT Service	Enables JIT ...		Manual (Trig...	Local Service
Web Account Manager	This service ...	Running	Manual	Local Syste...
Windows Audio	Manages au...		Manual	Local Service

Telephony Properties (Local Computer)

Service name: tapisrv

Display name: Telephony

Description: Provides Telephony API (TAPI) support for programs that control telephony devices on the local computer and, through the LAN, on servers that are also

Path to executable:
C:\Windows\System32\svchost.exe -k NetworkService -p

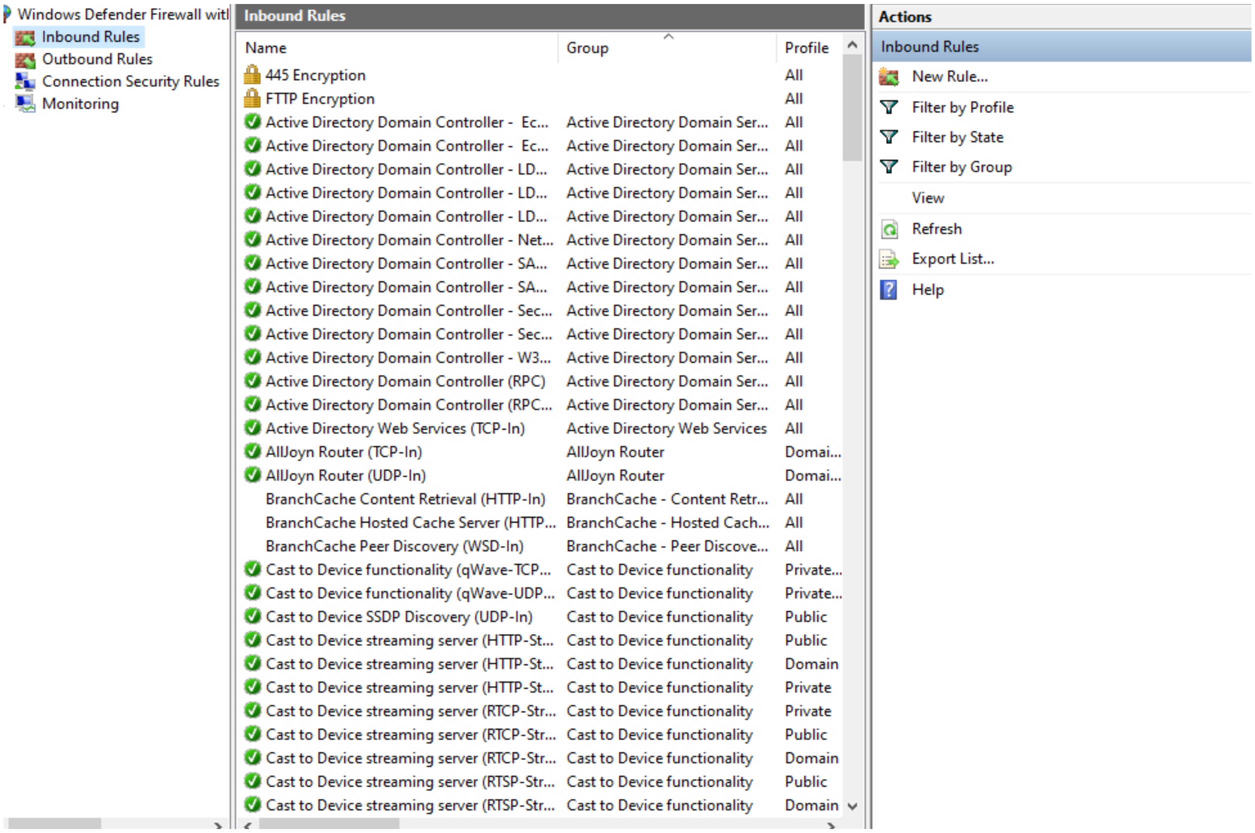
Startup type: Disabled

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Created rule on firewall defender to encrypt and filter port 445, 20, 21. Encrypting traffic on port 445 helps protect sensitive data that is being transmitted over the network, for example files. Encrypting FTP (port 20 and 21) traffic ensures that data transfers between client and server are protected from attacks like eavesdropping and man in the middle attacks. Filtering both of these reports can help prevent threat actors from gaining unauthorized access to sever files and systems.



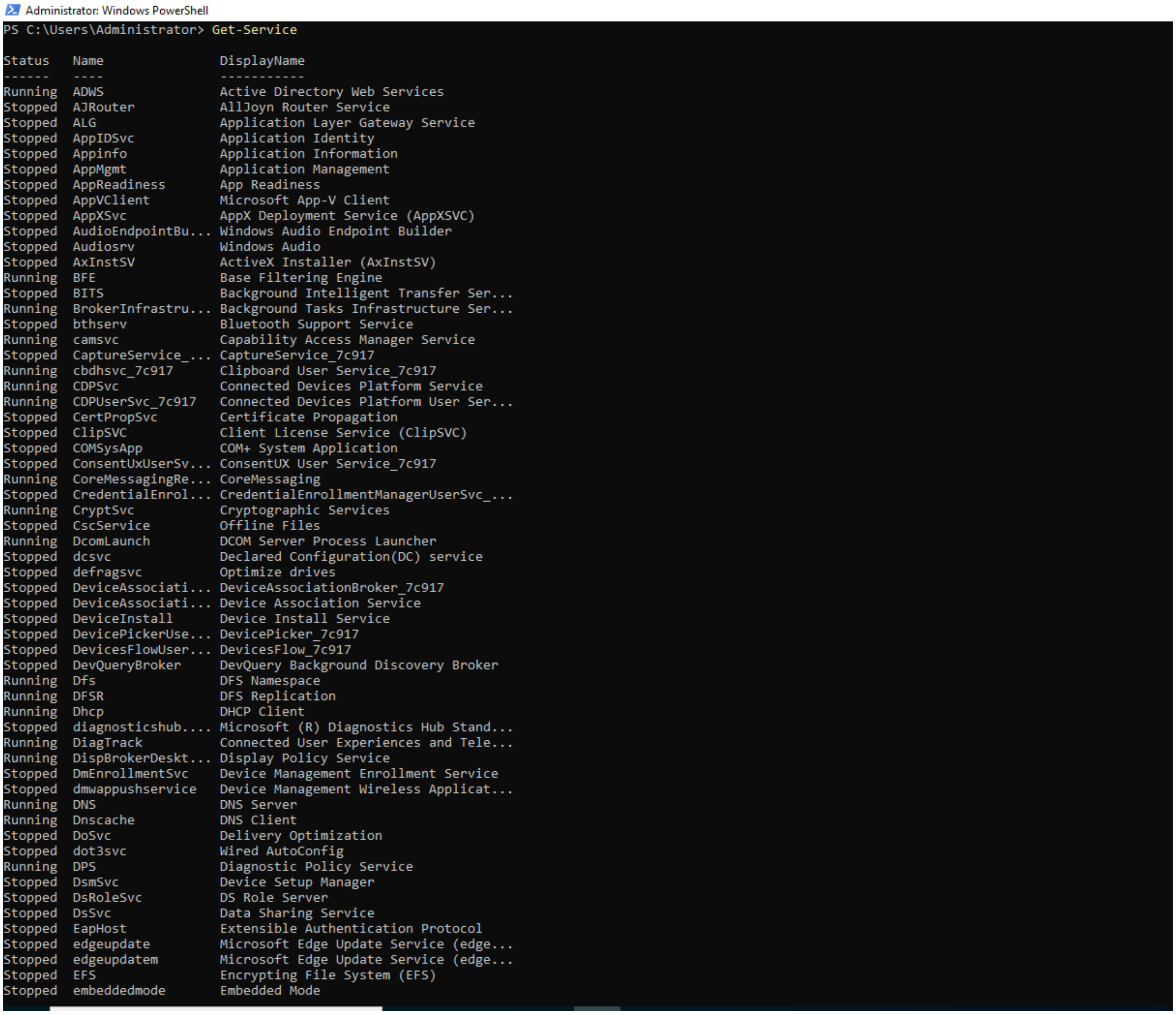
Name	Group	Profile
🔒 445 Encryption		All
🔒 FTTP Encryption		All
✓ Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All
✓ Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All
✓ Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All
✓ Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All
✓ Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All
✓ Active Directory Domain Controller - Net...	Active Directory Domain Ser...	All
✓ Active Directory Domain Controller - SA...	Active Directory Domain Ser...	All
✓ Active Directory Domain Controller - SA...	Active Directory Domain Ser...	All
✓ Active Directory Domain Controller - Sec...	Active Directory Domain Ser...	All
✓ Active Directory Domain Controller - Sec...	Active Directory Domain Ser...	All
✓ Active Directory Domain Controller - W3...	Active Directory Domain Ser...	All
✓ Active Directory Domain Controller (RPC)	Active Directory Domain Ser...	All
✓ Active Directory Domain Controller (RPC...	Active Directory Domain Ser...	All
✓ Active Directory Web Services (TCP-In)	Active Directory Web Services	All
✓ AllJoyn Router (TCP-In)	AllJoyn Router	Domai...
✓ AllJoyn Router (UDP-In)	AllJoyn Router	Domai...
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All
BranchCache Hosted Cache Server (HTTP...	BranchCache - Hosted Cach...	All
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All
✓ Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...
✓ Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...
✓ Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public
✓ Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public
✓ Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain
✓ Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private
✓ Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Private
✓ Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Public
✓ Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Domain
✓ Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Public
✓ Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Domain

Methodology

Conducted vulnerability scan on sever components with tools including Nmap, PowerShell, and Nessus. Nessus is software used to identify security weaknesses in the company’s network and operating systems. Nmap is used to scan ports, Ip addresses, and detect vulnerabilities.

Services Scan

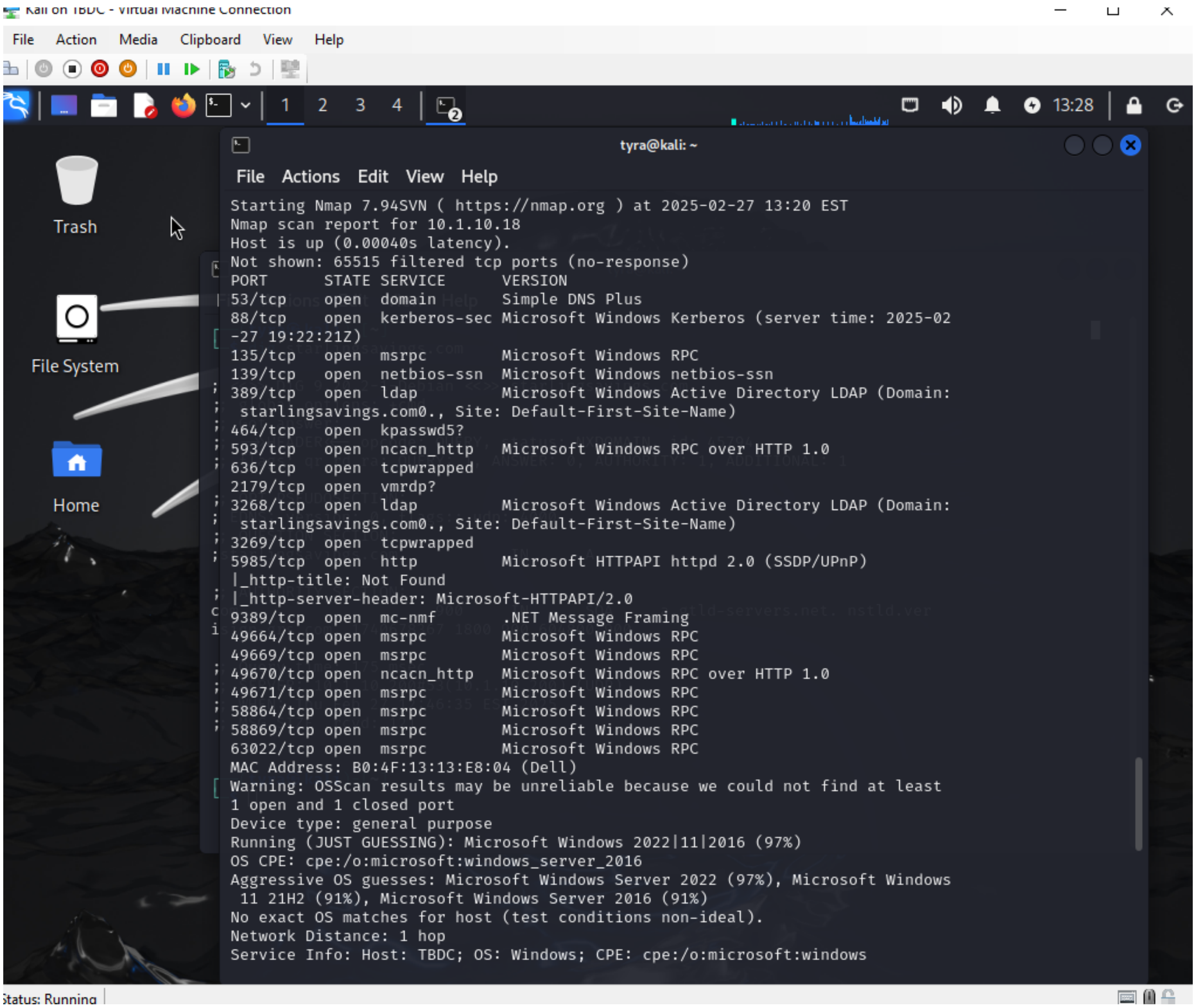
In PowerShell a command can be run to lists all the services currently running on the server. While running this command, it was observed that some services weren't running. For example, BITS, DPS, CryptSv, EFS and W32Time were not running. BITS (Background Intelligence Transfer Service is used to transfer files in the background. Since it is not running, the server could miss critical updates and be exposed to vulnerabilities. CryptSV (Cryptographic Services) manages all cryptographic operations. Without this running, the server might have issues with creating digital signatures, verifying software installation, and managing certificates. All of these operations are crucial for authentication and maintaining a secure environment. DPS (Diagnostic Policy Service) detects and troubleshoots problems within your system. This service also logs diagnostic information about the issue and notifies users. Without running this service, the server won't be able to diagnose any problems within the system which could lead to undetected errors. W32Time (Window Time) is what synchronizes the date and time for all servers and clients connected to them. Without this service, running time stamps of logs for security protocols, authentication, and Kerberos could be affected. EFS (Encryption File System) enables files to be encrypted. As a banking institution we must comply with the Payment Card Industry Security Standards. Which requires the protection of card holder data with encryption. Without this service running Starling Savings is not in compliance with PCI DSS. Sensitive information on servers is at this point exposed. If threat actors gain access to systems, they will have access to our files content. To combat this, enabling EFS service and setting stricter access controls on accounts.



```
PS C:\Users\Administrator> Get-Service

Status   Name               DisplayName
------   ----               -----------
Running  ADWS               Active Directory Web Services
Stopped  AJRouter           AllJoyn Router Service
Stopped  ALG                Application Layer Gateway Service
Stopped  AppIDSvc           Application Identity
Stopped  Appinfo            Application Information
Stopped  AppMgmt            Application Management
Stopped  AppReadiness       App Readiness
Stopped  AppVClient         Microsoft App-V Client
Stopped  AppXSvc            AppX Deployment Service (AppXSVC)
Stopped  AudioEndpointBu... Windows Audio Endpoint Builder
Stopped  Audiosrv           Windows Audio
Stopped  AxInstSV           ActiveX Installer (AxInstSV)
Running  BFE                Base Filtering Engine
Stopped  BITS               Background Intelligent Transfer Ser...
Running  BrokerInfrastru... Background Tasks Infrastructure Ser...
Stopped  bthserv            Bluetooth Support Service
Running  camsvc             Capability Access Manager Service
Stopped  CaptureService_... CaptureService_7c917
Running  cbdhsvc_7c917      Clipboard User Service_7c917
Running  CDPSvc             Connected Devices Platform Service
Running  CDPUserSvc_7c917   Connected Devices Platform User Ser...
Stopped  CertPropSvc        Certificate Propagation
Stopped  ClipSVC            Client License Service (ClipSVC)
Stopped  COMSysApp          COM+ System Application
Stopped  ConsentUxUserSv... ConsentUX User Service_7c917
Running  CoreMessagingRe... CoreMessaging
Stopped  CredentialEnrol... CredentialEnrollmentManagerUserSvc_...
Running  CryptSvc           Cryptographic Services
Stopped  CscService         Offline Files
Running  DcomLaunch         DCOM Server Process Launcher
Stopped  dcsvc              Declared Configuration(DC) service
Stopped  defragsvc          Optimize drives
Stopped  DeviceAssociati... DeviceAssociationBroker_7c917
Stopped  DeviceAssociati... Device Association Service
Stopped  DeviceInstall      Device Install Service
Stopped  DevicePickerUse... DevicePicker_7c917
Stopped  DevicesFlowUser... DevicesFlow_7c917
Stopped  DevQueryBroker     DevQuery Background Discovery Broker
Running  Dfs                DFS Namespace
Running  DFSR               DFS Replication
Running  Dhcp               DHCP Client
Stopped  diagnosticshub.... Microsoft (R) Diagnostics Hub Stand...
Running  DiagTrack          Connected User Experiences and Tele...
Running  DispBrokerDeskt... Display Policy Service
Stopped  DmEnrollmentSvc    Device Management Enrollment Service
Stopped  dmwappushservice   Device Management Wireless Applicat...
Running  DNS                DNS Server
Running  Dnscache           DNS Client
Stopped  DoSvc              Delivery Optimization
Stopped  dot3svc            Wired AutoConfig
Running  DPS                Diagnostic Policy Service
Stopped  DsmSvc             Device Setup Manager
Stopped  DsRoleSvc          DS Role Server
Stopped  DsSvc              Data Sharing Service
Stopped  EapHost            Extensible Authentication Protocol
Stopped  edgeupdate         Microsoft Edge Update Service (edge...
Stopped  edgeupdatem        Microsoft Edge Update Service (edge...
Stopped  EFS                Encrypting File System (EFS)
Stopped  embeddedmode       Embedded Mode
```

Vulnerability Scan

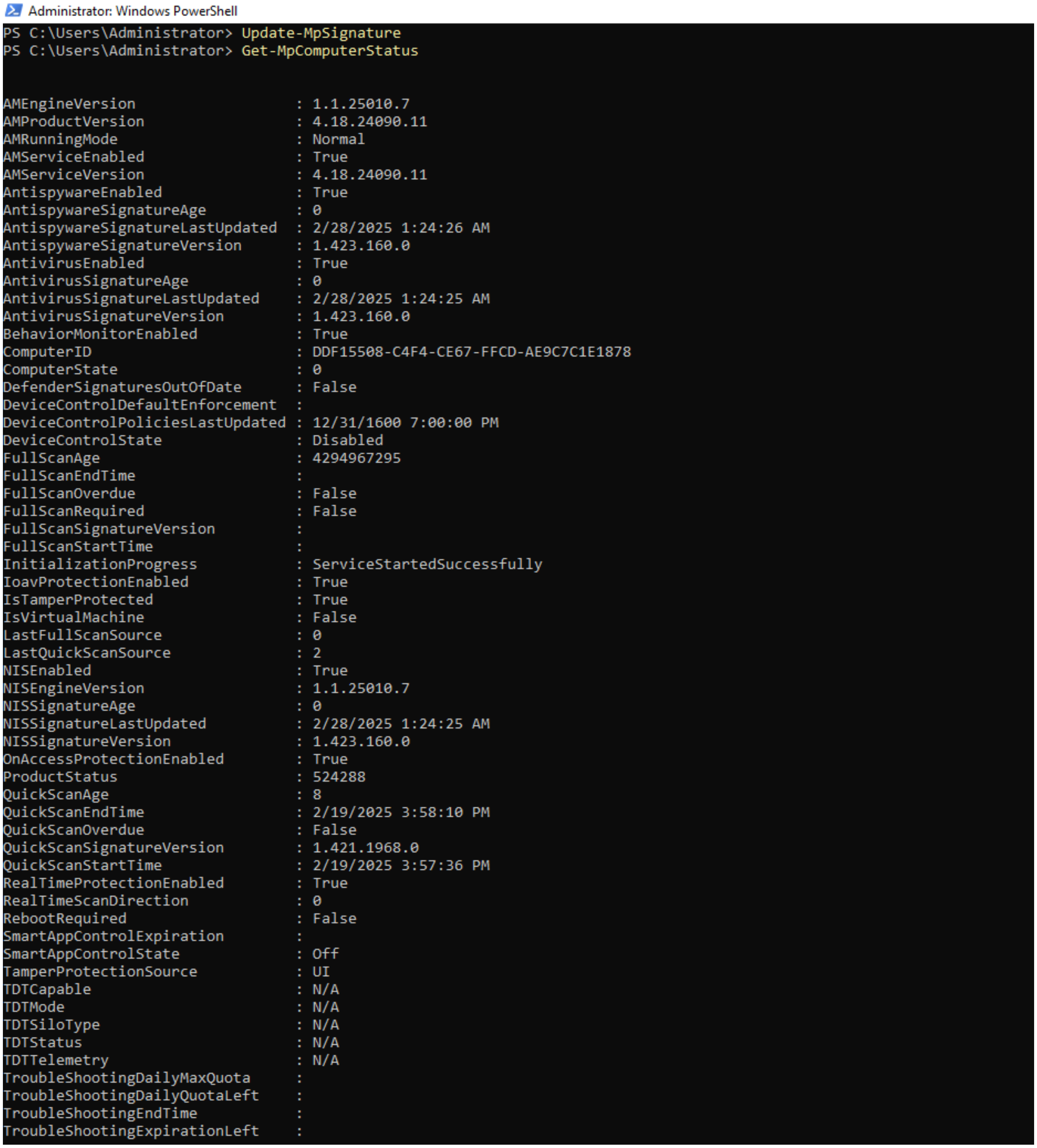
Nmap has the ability to see what ports are opened on a network. The scan showed that ports were open on servers like 3389, 5985, and 3268. Port 3389 is used to regulate remote access to servers and devices. Then port 5985 is used for remote http communication (WinRm), this allows operating systems and hardware to communicate. But this port is susceptible to web-based attacks like cross site scripting. In addition, port 3389 is susceptible to remote code execution and brute force attacks. Since most of the employees will be on premises, it would be best to close port 3389 so it won't be left exposed. Then flitter access controls to port 5985 since only administrators should have remote access to services like PowerShell. Finally, port 3268 is used for the global catalog in Active Directory which allows for faster LDAP queries. These sessions are unencrypted on port 3268 so it would be best to configure the sever to use port 3269 for encrypted communications.



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-27 13:20 EST
Nmap scan report for 10.1.10.18
Host is up (0.00040s latency).
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-02
-27 19:22:21Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain:
 starlingsavings.com0., Site: Default-First-Site-Name)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
2179/tcp  open  vmrdp?
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain:
 starlingsavings.com0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf       .NET Message Framing
49664/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc        Microsoft Windows RPC
58864/tcp open  msrpc        Microsoft Windows RPC
58869/tcp open  msrpc        Microsoft Windows RPC
63022/tcp open  msrpc        Microsoft Windows RPC
MAC Address: B0:4F:13:13:E8:04 (Dell)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022|11|2016 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2022 (97%), Microsoft Windows
 11 21H2 (91%), Microsoft Windows Server 2016 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: TBDC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Microsoft Defender Updates

In PowerShell command was run to list all of Microsoft Defender updates and ensure that the latest updates were installed. The last update ran was on the twenty eighth of February and Microsoft Defender is running normally. It is important to keep this antivirus software up to date since it is a requirement of PCI DSS. Also, according to NIST guidelines for sever security this is a best practice (Scarfone et al., 2008). Which ensure systems are protected against new attacks techniques and malware.

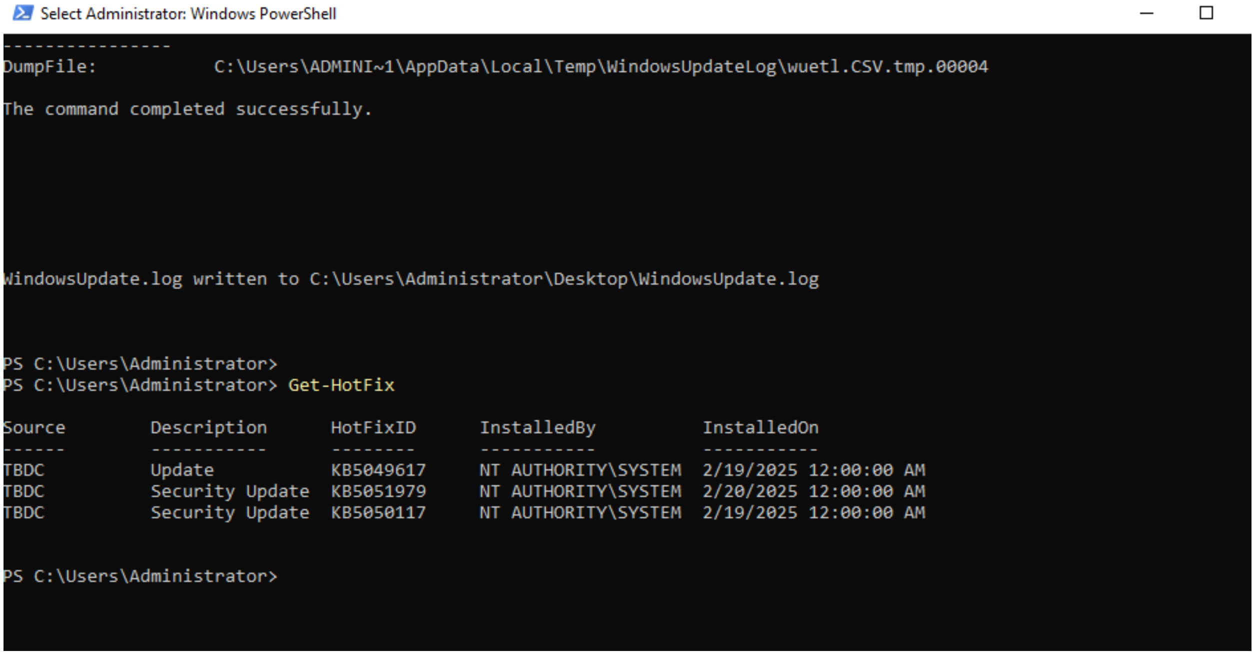


```
PS C:\Users\Administrator> Update-MpSignature
PS C:\Users\Administrator> Get-MpComputerStatus


AMEngineVersion                  : 1.1.25010.7
AMProductVersion                 : 4.18.24090.11
AMRunningMode                    : Normal
AMServiceEnabled                 : True
AMServiceVersion                 : 4.18.24090.11
AntispywareEnabled               : True
AntispywareSignatureAge          : 0
AntispywareSignatureLastUpdated  : 2/28/2025 1:24:26 AM
AntispywareSignatureVersion      : 1.423.160.0
AntivirusEnabled                 : True
AntivirusSignatureAge            : 0
AntivirusSignatureLastUpdated    : 2/28/2025 1:24:25 AM
AntivirusSignatureVersion        : 1.423.160.0
BehaviorMonitorEnabled           : True
ComputerID                       : DDF15508-C4F4-CE67-FFCD-AE9C7C1E1878
ComputerState                    : 0
DefenderSignaturesOutOfDate      : False
DeviceControlDefaultEnforcement  :
DeviceControlPoliciesLastUpdated : 12/31/1600 7:00:00 PM
DeviceControlState               : Disabled
FullScanAge                      : 4294967295
FullScanEndTime                  :
FullScanOverdue                  : False
FullScanRequired                 : False
FullScanSignatureVersion         :
FullScanStartTime                :
InitializationProgress           : ServiceStartedSuccessfully
IoavProtectionEnabled            : True
IsTamperProtected                : True
IsVirtualMachine                 : False
LastFullScanSource               : 0
LastQuickScanSource              : 2
NISEnabled                       : True
NISEngineVersion                 : 1.1.25010.7
NISSignatureAge                  : 0
NISSignatureLastUpdated          : 2/28/2025 1:24:25 AM
NISSignatureVersion              : 1.423.160.0
OnAccessProtectionEnabled        : True
ProductStatus                    : 524288
QuickScanAge                     : 8
QuickScanEndTime                 : 2/19/2025 3:58:10 PM
QuickScanOverdue                 : False
QuickScanSignatureVersion        : 1.421.1968.0
QuickScanStartTime               : 2/19/2025 3:57:36 PM
RealTimeProtectionEnabled        : True
RealTimeScanDirection            : 0
RebootRequired                   : False
SmartAppControlExpiration        :
SmartAppControlState             : Off
TamperProtectionSource           : UI
TDTCapable                       : N/A
TDTMode                          : N/A
TDTSiloType                      : N/A
TDTStatus                        : N/A
TDTTelemetry                     : N/A
TroubleShootingDailyMaxQuota     :
TroubleShootingDailyQuotaLeft    :
TroubleShootingEndTime           :
TroubleShootingExpirationLeft    :
```

The command nslookup was ran to show that DNS server is properly functioning and has the right IP address associated with it. When command was running domain name, starlingssavings.com it showed the domain controller Ip address as 10.1.10.18.

Security Update and Patches

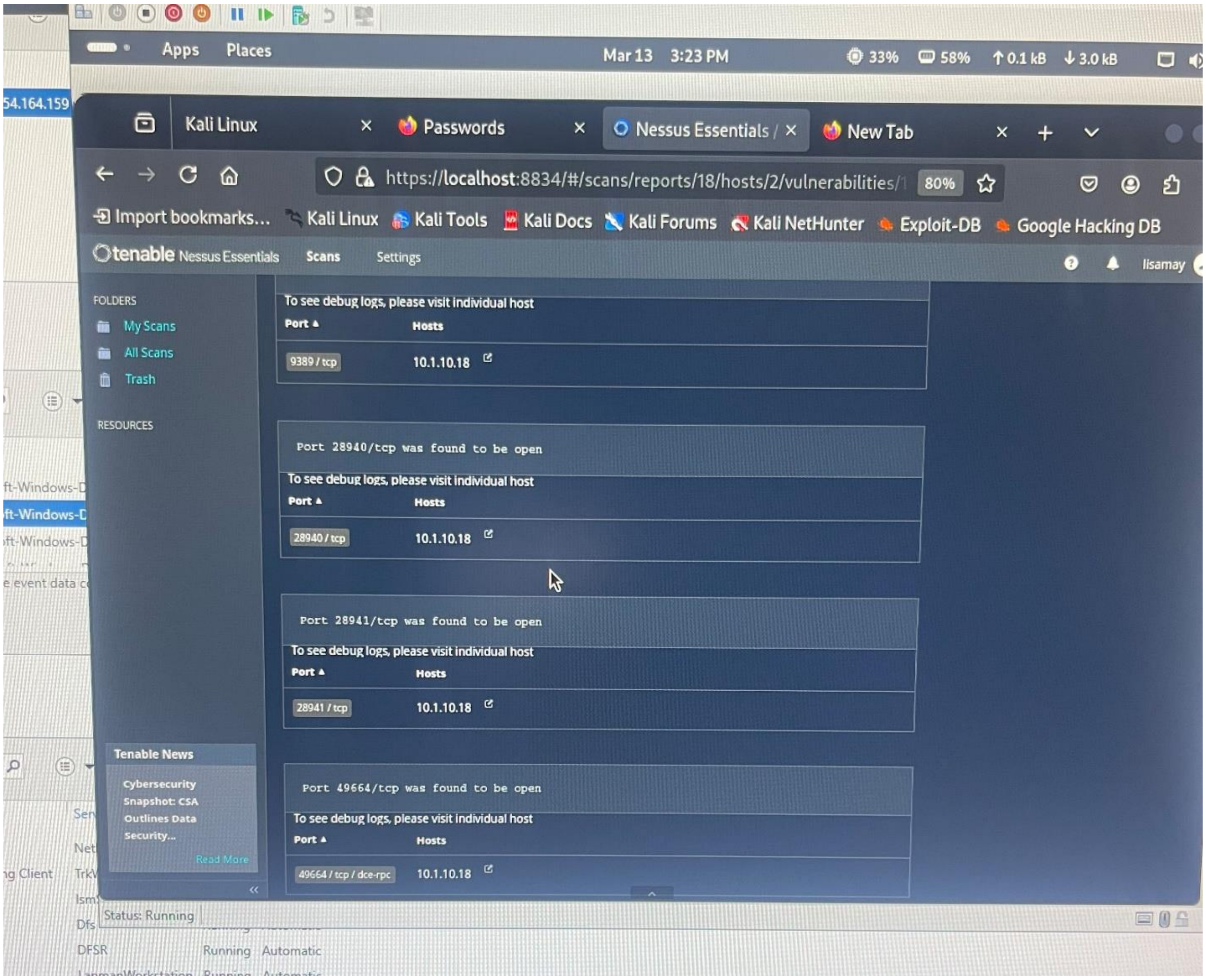
Get-Hotfix command in PowerShell was ran to show security updates and patches that are installed on the server. The last updates that were installed last week on February nineteenth and twentieth.



```
----------------
DumpFile:          C:\Users\ADMINI~1\AppData\Local\Temp\WindowsUpdateLog\wuetl.CSV.tmp.00004

The command completed successfully.




WindowsUpdate.log written to C:\Users\Administrator\Desktop\WindowsUpdate.log


PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-HotFix

Source        Description      HotFixID      InstalledBy          InstalledOn
------        -----------      --------      -----------          -----------
TBDC          Update           KB5049617     NT AUTHORITY\SYSTEM  2/19/2025 12:00:00 AM
TBDC          Security Update  KB5051979     NT AUTHORITY\SYSTEM  2/20/2025 12:00:00 AM
TBDC          Security Update  KB5050117     NT AUTHORITY\SYSTEM  2/19/2025 12:00:00 AM


PS C:\Users\Administrator>
```

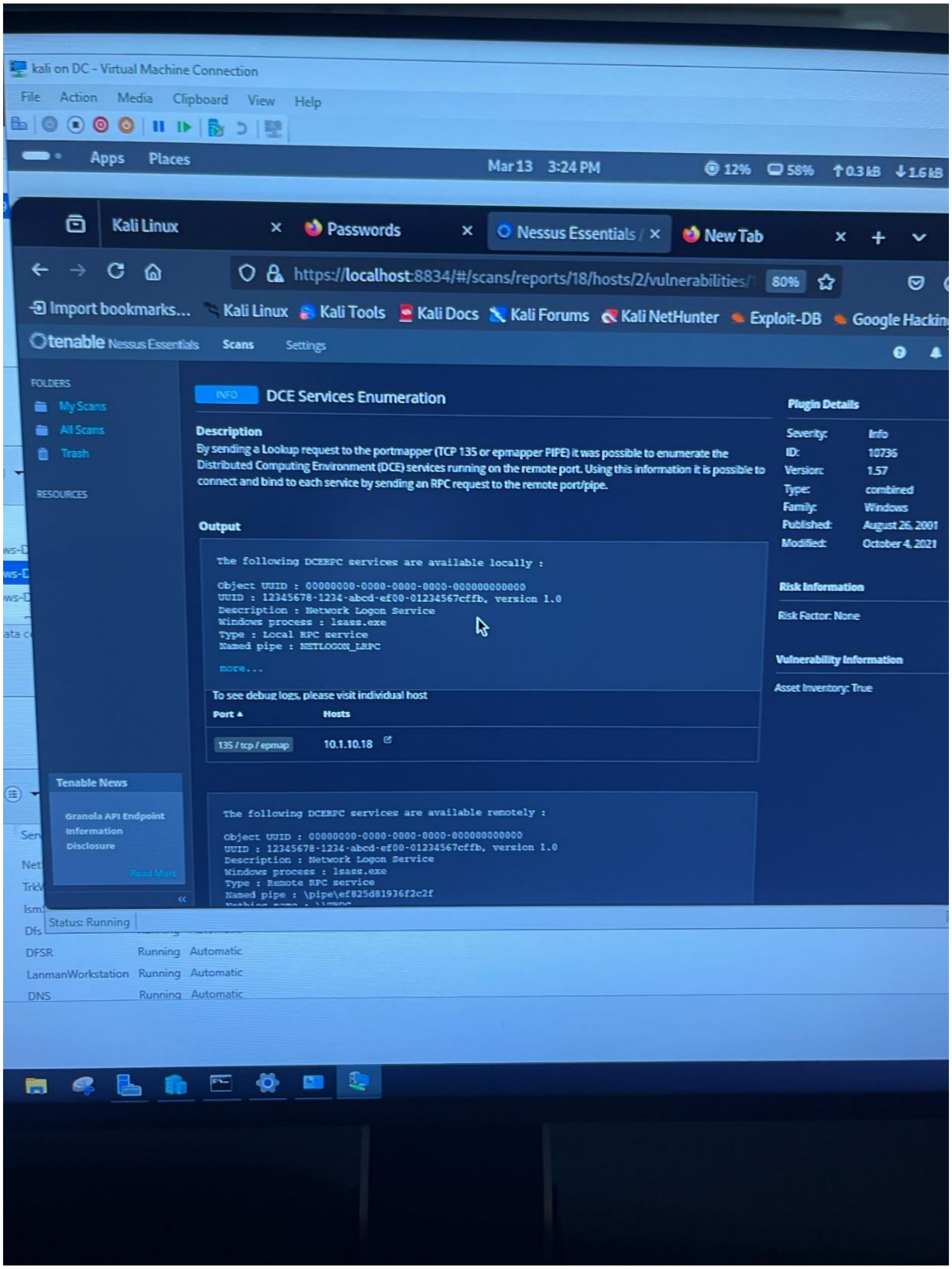
Nessus Scan

Started off by running Active Directory scan, it showed that ports 9389,28940, 28941, 28941, 49664 where opened. Both port 9389 and port 28940 could be exploited by attackers to gain higher privileges on the system and could eventually lead to control over the domain. Port 28941 allows attackers to execute arbitrary code remotely and lead to data breaches.



```
To see debug logs, please visit individual host
Port ▲          Hosts
9389 / tcp      10.1.10.18

Port 28940/tcp was found to be open
To see debug logs, please visit individual host
Port ▲          Hosts
28940 / tcp     10.1.10.18

Port 28941/tcp was found to be open
To see debug logs, please visit individual host
Port ▲          Hosts
28941 / tcp     10.1.10.18

Port 49664/tcp was found to be open
To see debug logs, please visit individual host
Port ▲                      Hosts
49664 / tcp / dce-rpc       10.1.10.18
```

The next scan ran was an advanced network scan, it pointed out that the domain controller had a DCE Services Enumeration vulnerability on port 135. Exposed details about DCE/RPC services, potentially could aid attackers in planning exploits. Attackers might use enumerated services to move across the network, targeting other connected systems.


kali on DC - Virtual Machine Connection
File Action Media Clipboard View Help
Apps Places
Mar 13 3:24 PM
Kali Linux
Passwords
Nessus Essentials
New Tab
https://localhost:8834/#/scans/reports/18/hosts/2/vulnerabilities/
80%
Import bookmarks... Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking
tenable Nessus Essentials Scans Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Tenable News
Granola API Endpoint Information Disclosure
Read More
Status: Running
DFSR Running Automatic
LanmanWorkstation Running Automatic
DNS Running Automatic

INFO DCE Services Enumeration

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Output

```
The following DCERPC services are available locally :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0
Description : Network Logon Service
Windows process : lsass.exe
Type : Local RPC service
Named pipe : NETLOGON_LRPC

more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
135 / tcp / epmap	10.1.10.18

```
The following DCERPC services are available remotely :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0
Description : Network Logon Service
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \pipe\ef825d81936f2c2f
```

Plugin Details

Severity:	Info
ID:	10736
Version:	1.57
Type:	combined
Family:	Windows
Published:	August 26, 2001
Modified:	October 4, 2021

Risk Information

Risk Factor: None

Vulnerability Information

Asset Inventory: True

Conclusion

Overall, ensuring a secure operating system installation was the key component of developing a strong security posture. By removing unnecessary components and services reduced the attacks surface. As well as disabling unnecessary ports, it is also essential to reducing potential attack vectors. Although more ports like 135, 9389, 2698, and 28941 should have had restrictions implemented. It was also important to keep severs up to date with the latest patches to mitigate vulnerabilities.

References

Scarfone, K., Jansen, W., & Tracy, M. (2008, July 25). *Guide to General Server Security*. Csrc.nist.gov. https://csrc.nist.gov/pubs/sp/800/123/final

Wilson, R. (2023). *ComTIA PenTest+ Guide to Penetration Testing* (1st ed.). Cengage Learning. https://ebooks.cenreader.com/#!/reader/1cb8f987-7967-4a0f-b622-0fe53727ef29/page/d72682985c13583798139895a73fbc41