Wildin' with Windows

By JeSSH and Eggvan

IMPORTANT TRYOUTS CHANGE
Sign in: https://da.gd/7hPh

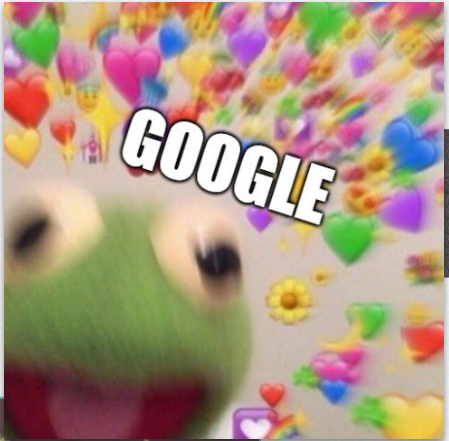
New Time:

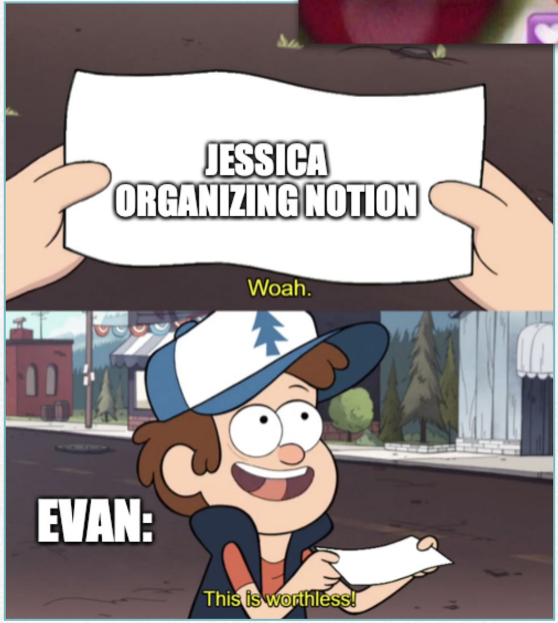
11:00AM – 6:00PM

Important

Here at Team Windows, we love Google.

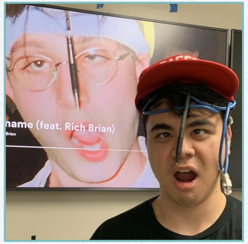
The following slides will be a little vague on purpose.





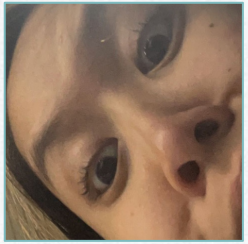
~~WindOS~~ ~~Windwos~~ Windows team

Evan Deters



🍆 Lead

Jessica Leung



OpenSSH Menace

(spirit of) Lawrence Kim

Serial IP Phone Flirt

CIS Student of the Year

Windwos

Windows Basics

Table of Contents

1

Windows basics

Navigating Windows

2

Active Directory

What is a domain?

3

IIS

Webservers, FTP, fun

4

LAB Time

Fun AD Lab :D

01

Windows Basics

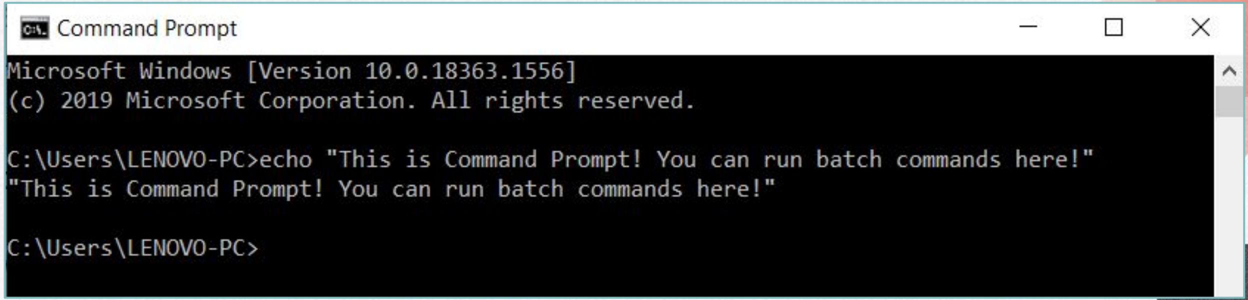
CMD, Powershell, file system, other stuff

CMD vs Powershell?

Command Prompt
C:\Windows\system32\cmd.exe

PowerShell
C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe

CMD

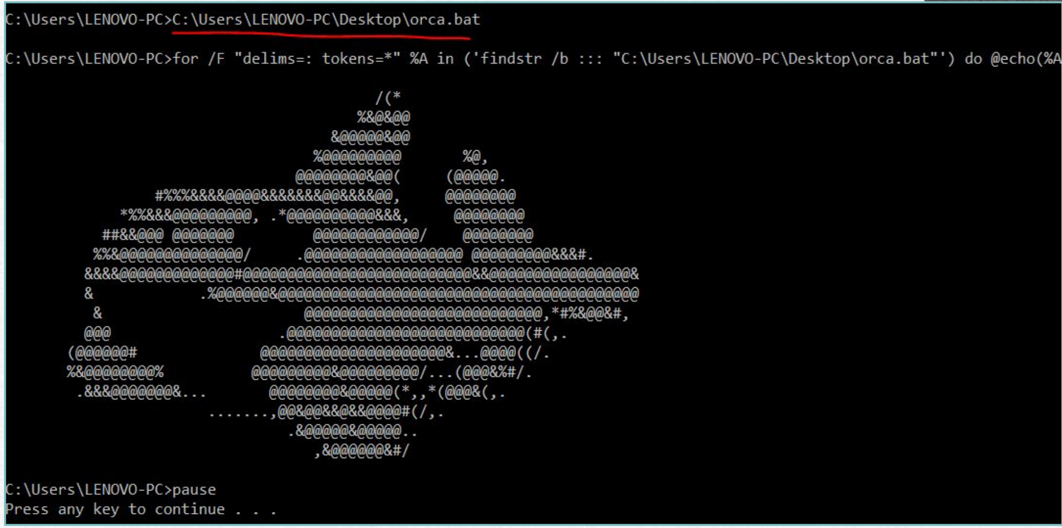


```
Microsoft Windows [Version 10.0.18363.1556]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\LENOVO-PC>echo "This is Command Prompt! You can run batch commands here!"
"This is Command Prompt! You can run batch commands here!"

C:\Users\LENOVO-PC>
```

Runs batch commands

100% compatible with old Windows versions

Stores cmd history for current session only.



```
C:\Users\LENOVO-PC>C:\Users\LENOVO-PC\Desktop\orca.bat

C:\Users\LENOVO-PC>for /F "delims=: tokens=*" %A in ('findstr /b ::: "C:\Users\LENOVO-PC\Desktop\orca.bat"') do @echo(%A

                                          /(*
                                        %&@&@@
                                     &@@@@@&@@
                                   %@@@@@@@@@       %@,
                                 @@@@@@@@&@@(      (@@@@@.
                 #%%%&&&&@@@@&&&&&&&@@&&&&@@,      @@@@@@@@
             *%%&&&@@@@@@@@@, .*@@@@@@@@@@&&&,      @@@@@@@@
           ##&&@@@ @@@@@@@         @@@@@@@@@@@@/     @@@@@@@@
          %%&@@@@@@@@@@@@@@@/     .@@@@@@@@@@@@@@@@@@@ @@@@@@@@@&&&#.
         &&&&@@@@@@@@@@@@@#@@@@@@@@@@@@@@@@@@@@@@@@@&&@@@@@@@@@@@@@@@&
         &            .%@@@@@@&@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
          &                       @@@@@@@@@@@@@@@@@@@@@@@@@@,*#%&@@&#,
         @@@                    .@@@@@@@@@@@@@@@@@@@@@@@@@@(#(,.
       (@@@@@@#                @@@@@@@@@@@@@@@@@@@@@&...@@@@((/.
       %&@@@@@@@@%            @@@@@@@@@&@@@@@@@@@/...(@@@&%#/.
        .&&&@@@@@@@@&...        @@@@@@@@&@@@@@(*,,*(@@@&(,.
                       .......,@@&@@&&@&&@@@@#(/,.
                                .&@@@@@&@@@@@..
                                   ,&@@@@@@&#/

C:\Users\LENOVO-PC>pause
Press any key to continue . . .
```

Useful CMD Commands

`netstat -ano`

- lists open ports and listening connections

`net share`

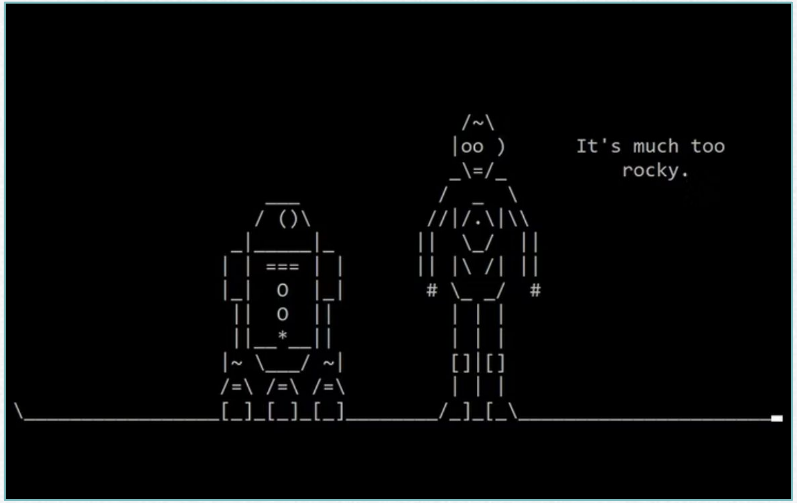
- shows file shares

`net user`

- shows users

`ipconfig`

- shows network config



It's much too rocky.

Powershell

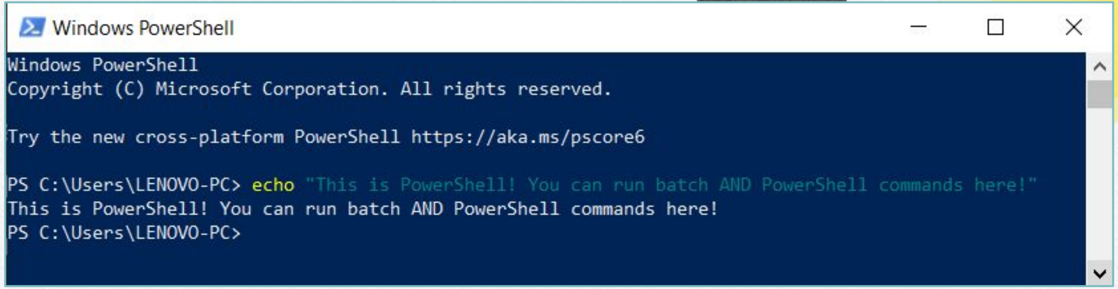
Runs batch and PowerShell commands

Has different versions

Run commands on old version:
powershell.exe -version 2

Can do basically everything

Stores history somewhere. Try to see if you can figure out where its stored!



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

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

PS C:\Users\LENOVO-PC> echo "This is PowerShell! You can run batch AND PowerShell commands here!"
This is PowerShell! You can run batch AND PowerShell commands here!
PS C:\Users\LENOVO-PC>
```

```
Add-Type -AssemblyName System.Speech
$speak = New-Object
System.Speech.Synthesis.SpeechSynthesizer
$words="you like guys?"
$speak.Speak($words)
```

Can be helpful to script common tasks, try it out!

Useful PowerShell Commands

```
Get-Help (man)

Set-ADAccountPassword

Get-ADUser

Add-ADGroupMember

Remove-ADGroupMember
```

Windows Defender

Free kick out the bad :D

May want to find a way to install this one...

File System

Important directories

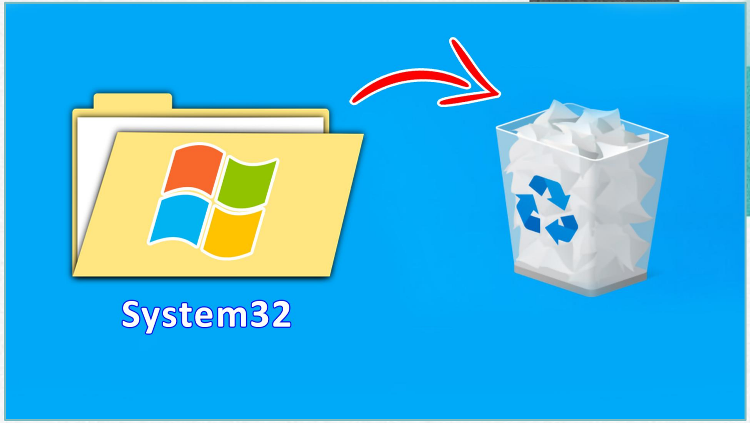
Windows registry (Ugh)

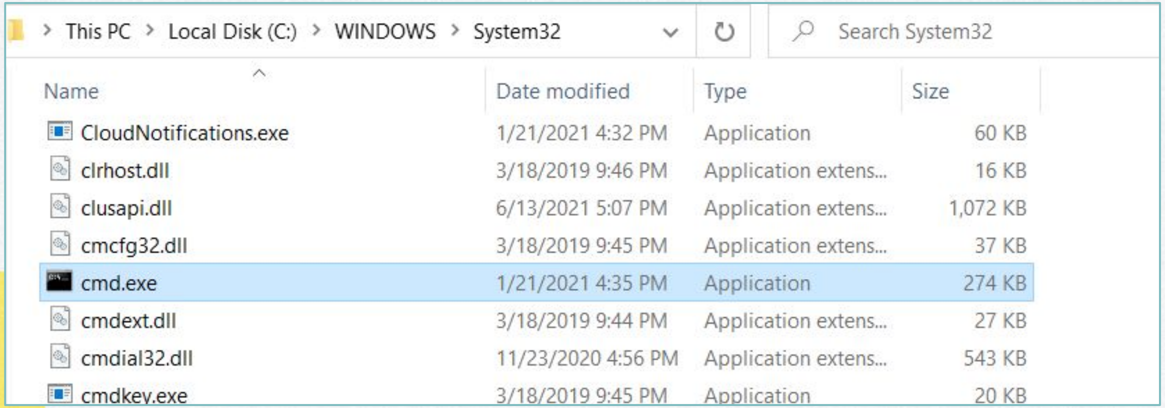
System32

C:\Windows\System32

Contains important system files (binaries and exes)

Easy to hide files here





Name	Date modified	Type	Size
CloudNotifications.exe	1/21/2021 4:32 PM	Application	60 KB
clrhost.dll	3/18/2019 9:46 PM	Application extens...	16 KB
clusapi.dll	6/13/2021 5:07 PM	Application extens...	1,072 KB
cmcfg32.dll	3/18/2019 9:45 PM	Application extens...	37 KB
cmd.exe	1/21/2021 4:35 PM	Application	274 KB
cmdext.dll	3/18/2019 9:44 PM	Application extens...	27 KB
cmdial32.dll	11/23/2020 4:56 PM	Application extens...	543 KB
cmdkey.exe	3/18/2019 9:45 PM	Application	20 KB

No

Windows Registry

regedit

People think it’s scary. It’s just messy.

Lot’s of opportunities for bad things here

- Run/RunOnce
- AlwaysInstallElevated
- Defender Exclusions

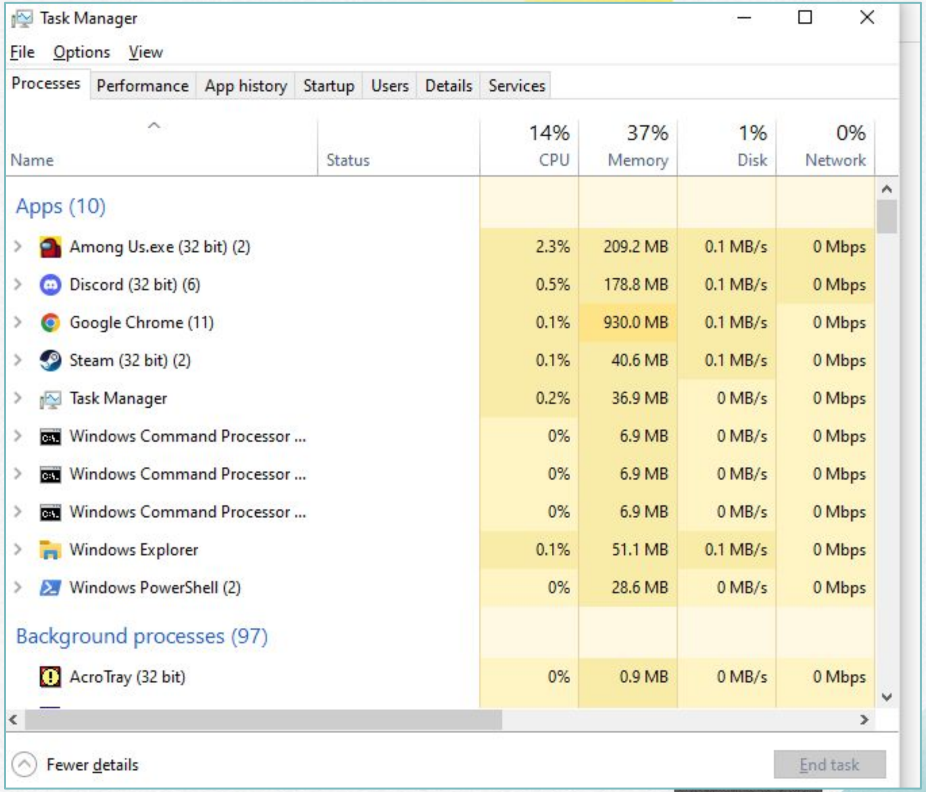
justin's service
jessica deletes registry key
I don't want to play with you anymore

Task Manager

Identify and end processes
See currently logged-on users

Microsoft Sysinternals provides better versions of task manager
- Process Monitor, Process Hacker, Process Explorer

Sysinternals is good, learn them!



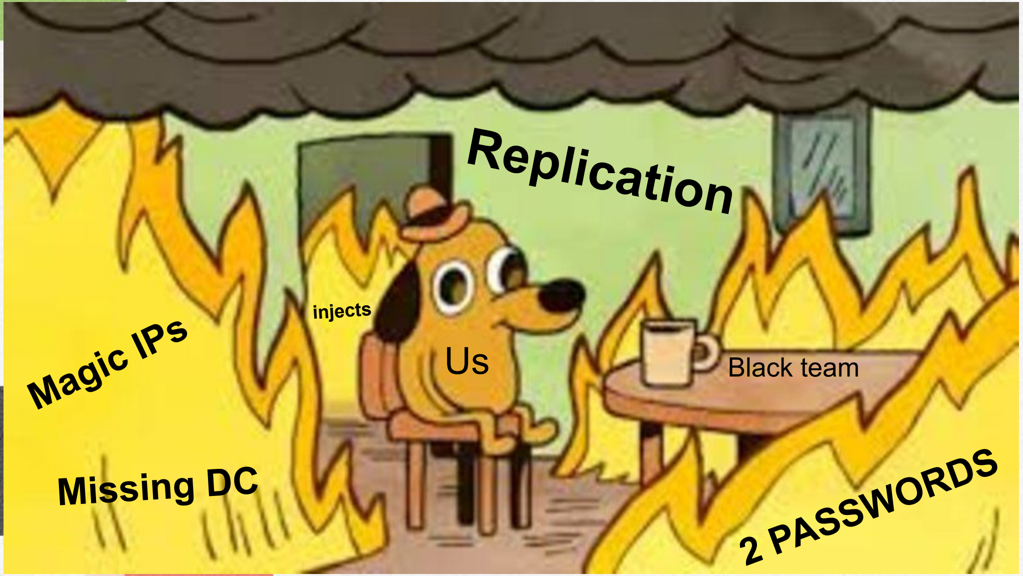
Name	Status	14% CPU	37% Memory	1% Disk	0% Network
Apps (10)					
Among Us.exe (32 bit) (2)		2.3%	209.2 MB	0.1 MB/s	0 Mbps
Discord (32 bit) (6)		0.5%	178.8 MB	0.1 MB/s	0 Mbps
Google Chrome (11)		0.1%	930.0 MB	0.1 MB/s	0 Mbps
Steam (32 bit) (2)		0.1%	40.6 MB	0.1 MB/s	0 Mbps
Task Manager		0.2%	36.9 MB	0 MB/s	0 Mbps
Windows Command Processor ...		0%	6.9 MB	0 MB/s	0 Mbps
Windows Command Processor ...		0%	6.9 MB	0 MB/s	0 Mbps
Windows Command Processor ...		0%	6.9 MB	0 MB/s	0 Mbps
Windows Explorer		0.1%	51.1 MB	0.1 MB/s	0 Mbps
Windows PowerShell (2)		0%	28.6 MB	0 MB/s	0 Mbps
Background processes (97)					
AcroTray (32 bit)		0%	0.9 MB	0 MB/s	0 Mbps

Useful Run Commands

lusrmgr.msc
gpedit.msc
dsa.msc
gpmc.msc
regedit
services.msc
msconfig
appwiz.cpl
mmc

inetmgr
taskschd.msc
wf.msc
optionalfeatures
control
mstsc
cmd
powershell
netplwiz

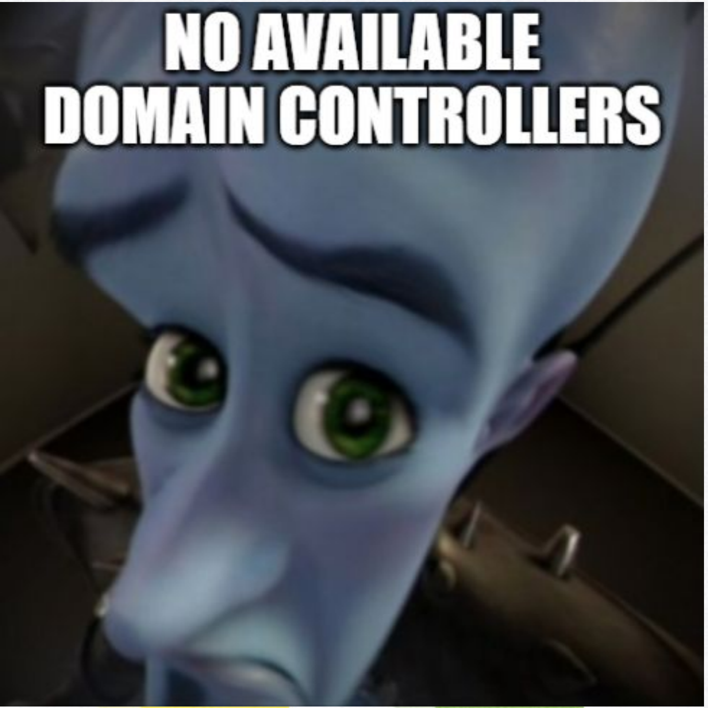
Can you figure out what each command does?



02

Active Directory

Yeah, you could say we have a good time on Windows Team.

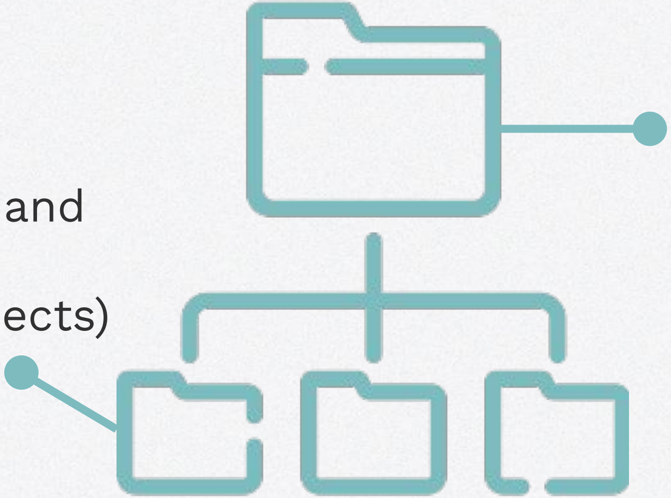


02-01

What is AD?

What is Active Directory

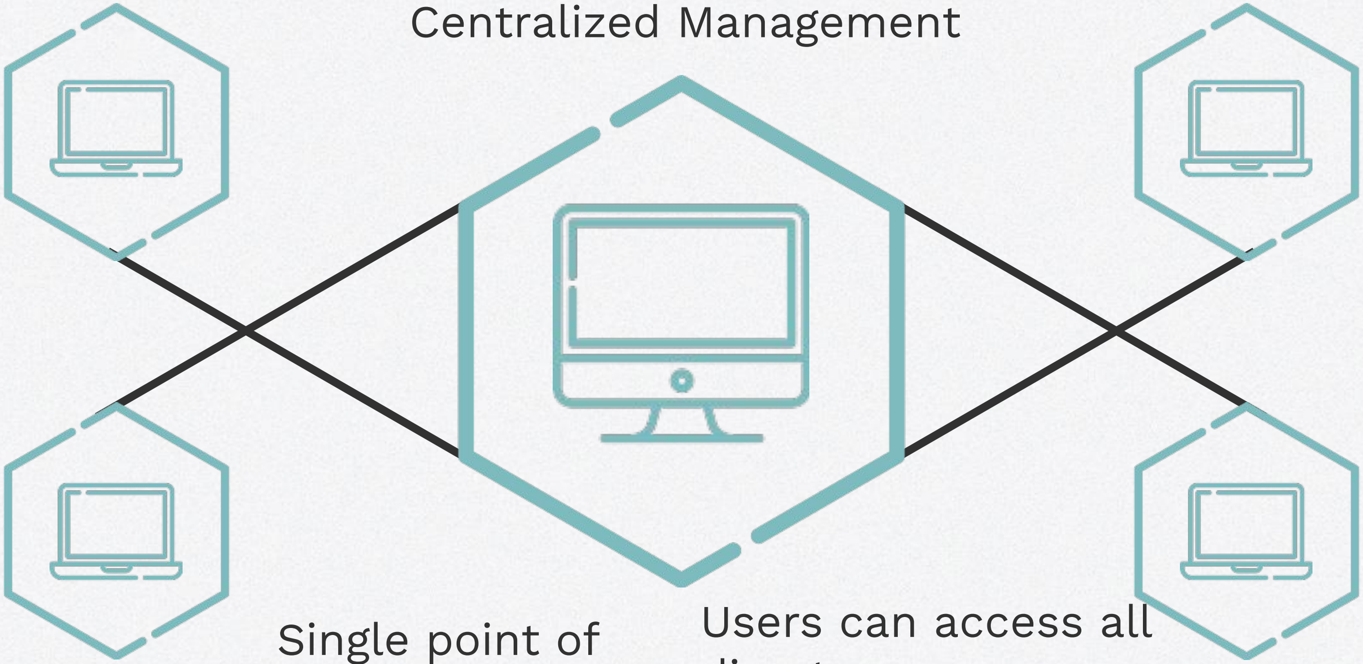
Directory Service (LDAP)



Stores information in a centralized location

Organize, manages and controls network resources (a.k.a objects)

What is Active Directory

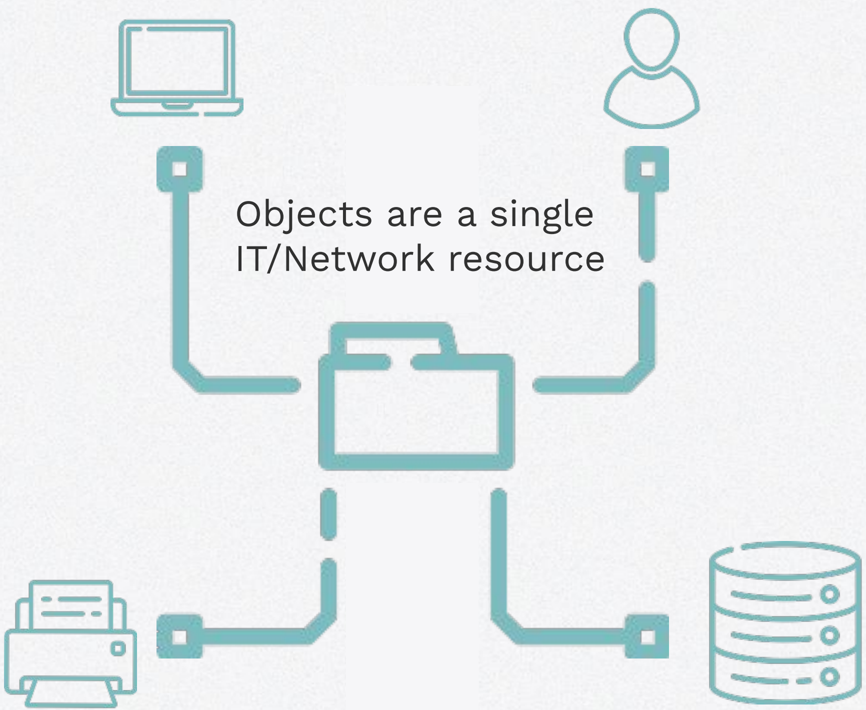


Centralized Management

Single point of administration

Users can access all directory resources with a single logon

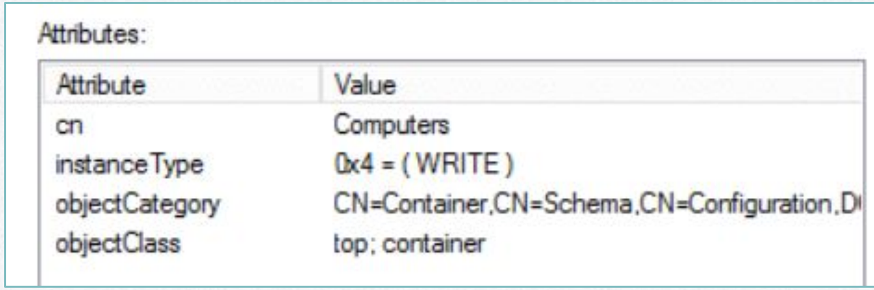
Active Directory Objects



Objects are a single IT/Network resource

Attributes are used to define and describe objects

Possible attributes:
- E-mail
- Phone Number
- Address



Attributes:

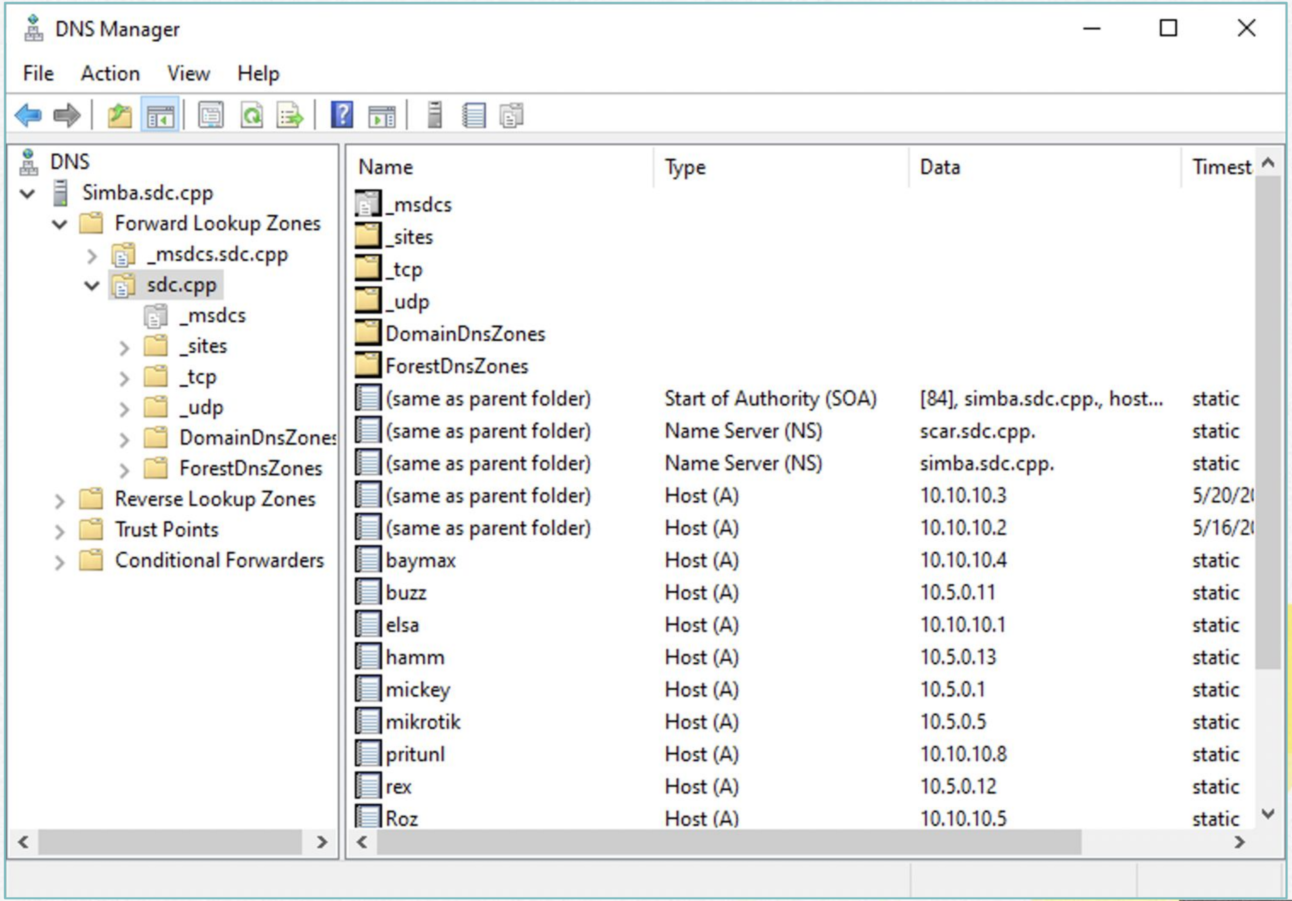
Attribute	Value
cn	Computers
instanceType	0x4 = (WRITE)
objectCategory	CN=Container,CN=Schema,CN=Configuration,D
objectClass	top; container

02-02

DNS

Domain Name Service

It's always DNS



Name	Type	Data	Timest
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[84], simba.sdc.cpp., host...	static
(same as parent folder)	Name Server (NS)	scar.sdc.cpp.	static
(same as parent folder)	Name Server (NS)	simba.sdc.cpp.	static
(same as parent folder)	Host (A)	10.10.10.3	5/20/2
(same as parent folder)	Host (A)	10.10.10.2	5/16/2
baymax	Host (A)	10.10.10.4	static
buzz	Host (A)	10.5.0.11	static
elsa	Host (A)	10.10.10.1	static
hamm	Host (A)	10.5.0.13	static
mickey	Host (A)	10.5.0.1	static
mikrotik	Host (A)	10.5.0.5	static
pritunl	Host (A)	10.10.10.8	static
rex	Host (A)	10.5.0.12	static
Roz	Host (A)	10.10.10.5	static

Important Records, but why?

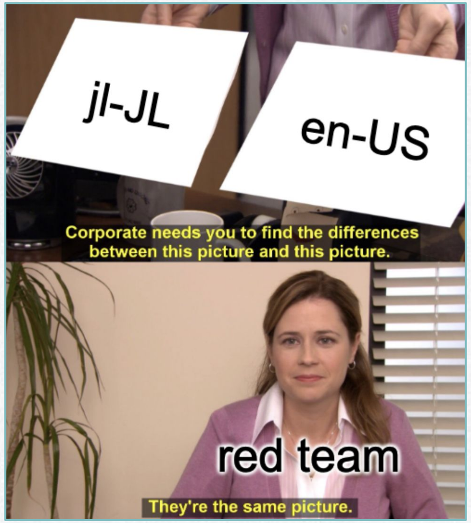
A Records

A records match IPs to hostnames

SRV Records

Point to hostnames for specific domain services

Hmm... Sounds Important


jl-JL
en-US
Corporate needs you to find the differences between this picture and this picture.
red team
They're the same picture.

Maybe I should back up DNS.

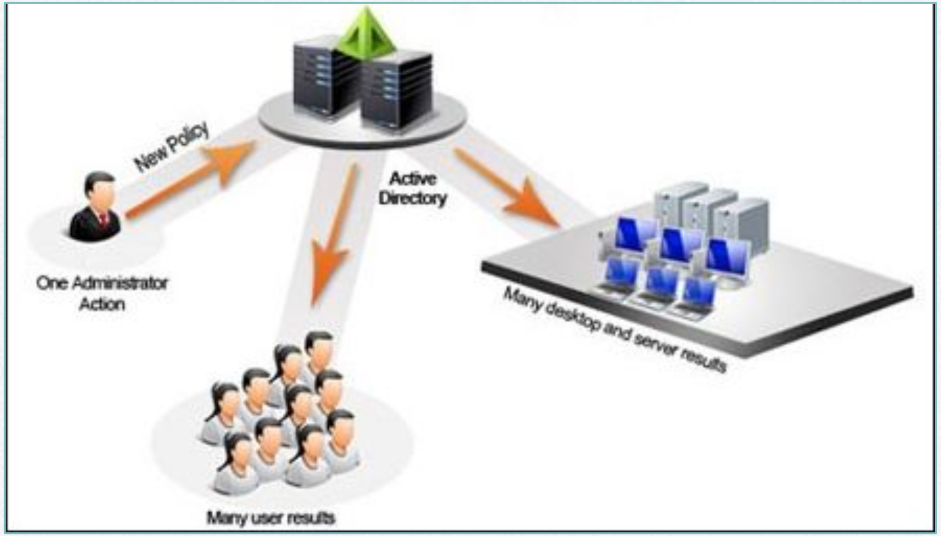
C:\Windows\System32\dns

02-03

What it Do?

It breaks

What can you do with Active Directory?



A Lot!

Very useful for
managing
A network

The Domain Controller(s)

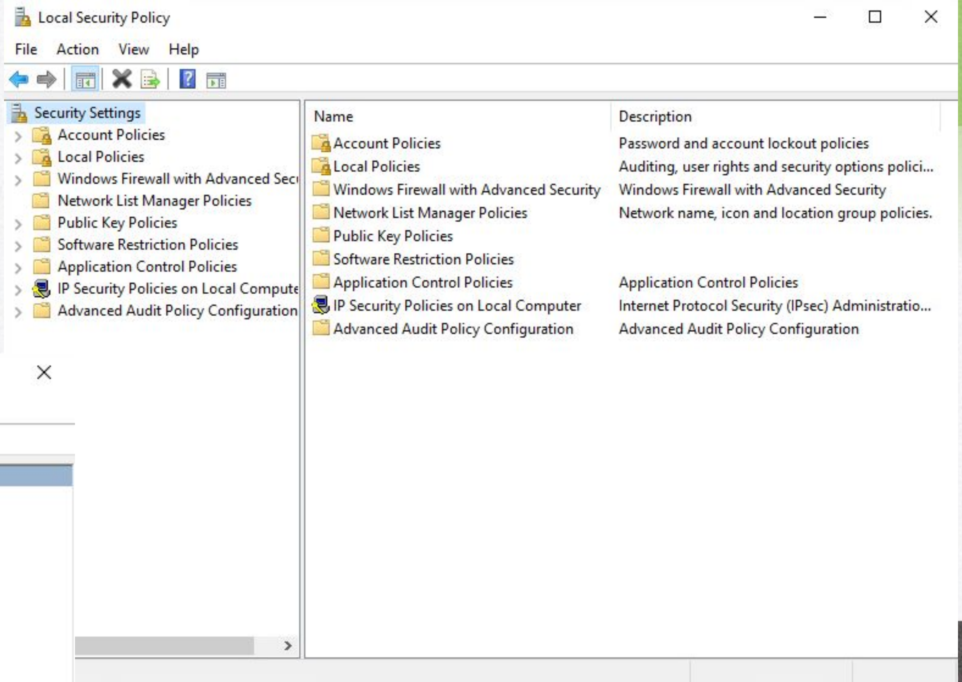
Authenticates and validates domain users on a network

Standardize group policy

Domain-specific PowerShell

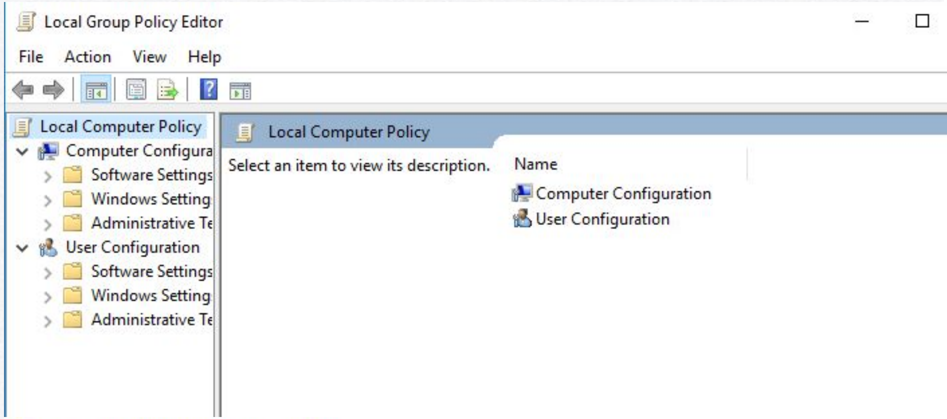
Know the difference between local machines and domain machines!

Remember Deez?



- Security Settings
  - Account Policies
  - Local Policies
  - Windows Firewall with Advanced Secu
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Compute
  - Advanced Audit Policy Configuration

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

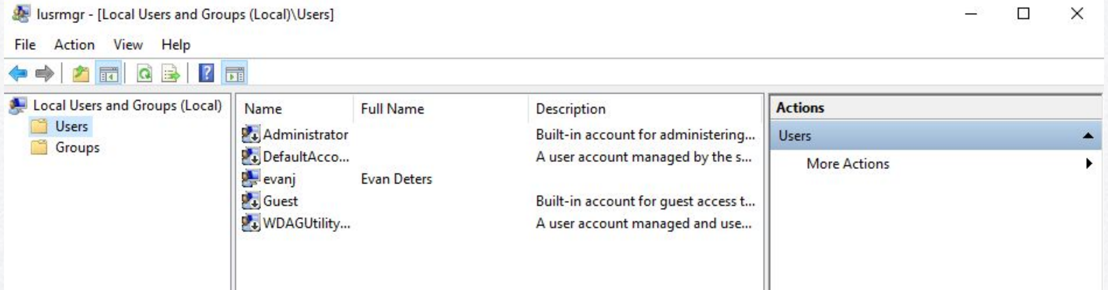


- Local Computer Policy
  - Computer Configura
    - Software Settings
    - Windows Setting
    - Administrative Te
  - User Configuration
    - Software Settings
    - Windows Setting
    - Administrative Te

Local Computer Policy

Select an item to view its description.

Name
Computer Configuration
User Configuration



- Local Users and Groups (Local)
  - Users
  - Groups

Name	Full Name	Description
Administrator		Built-in account for administering...
DefaultAcco...		A user account managed by the s...
evanj	Evan Deters	
Guest		Built-in account for guest access t...
WDAGUtility...		A user account managed and use...

Imagine configuring 100+ Windows machines by hand :(

dsa.msc and gpmc.msc

Active Directory Users and Computers

dsa.msc

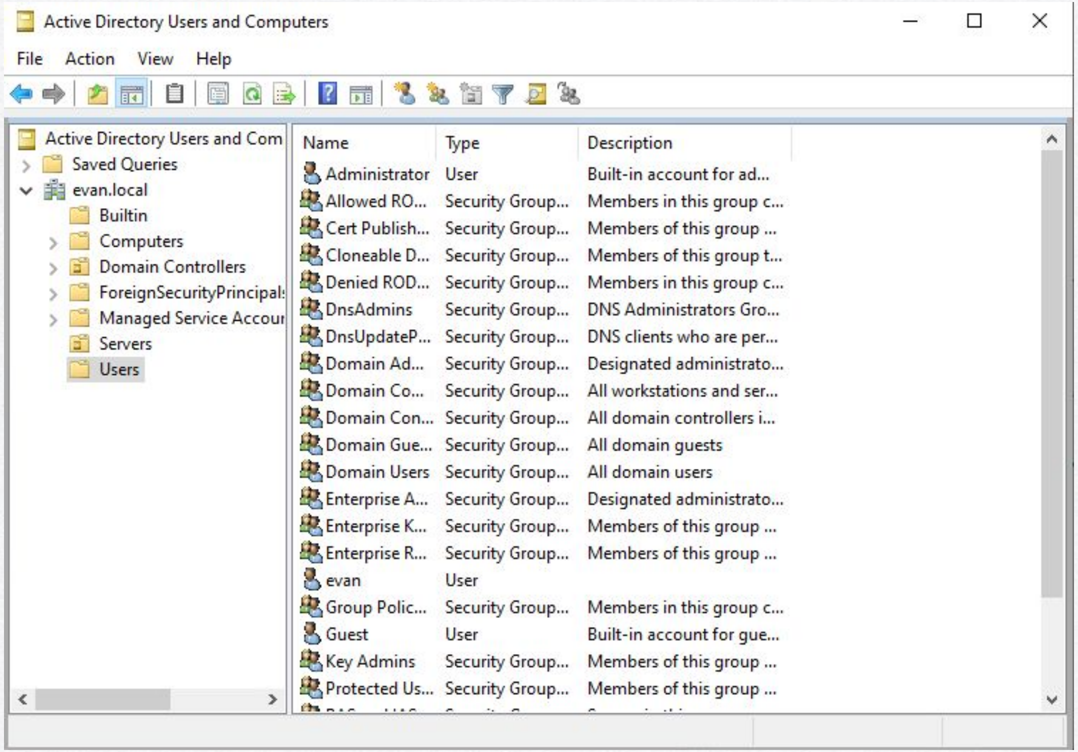
- Manage objects in your domain
- Users, Groups, Computers, etc.

Group Policy Management Console

gpmc.msc

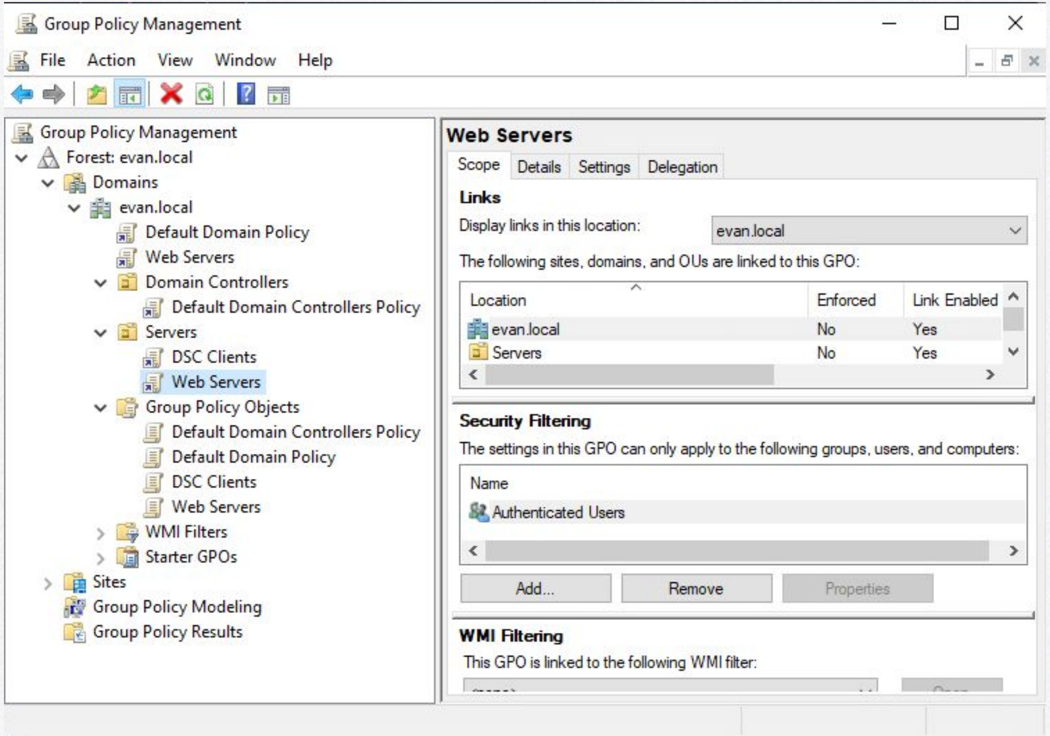
- Manage group policy in your domain
- Push out group policy to domain

User Management (dsa.msc)



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 ...
evan	User	
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 ...

Group Policy Management (gpmc.msc)



Web Servers

Links

Display links in this location: evan.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled
evan.local	No	Yes
Servers	No	Yes

Security Filtering

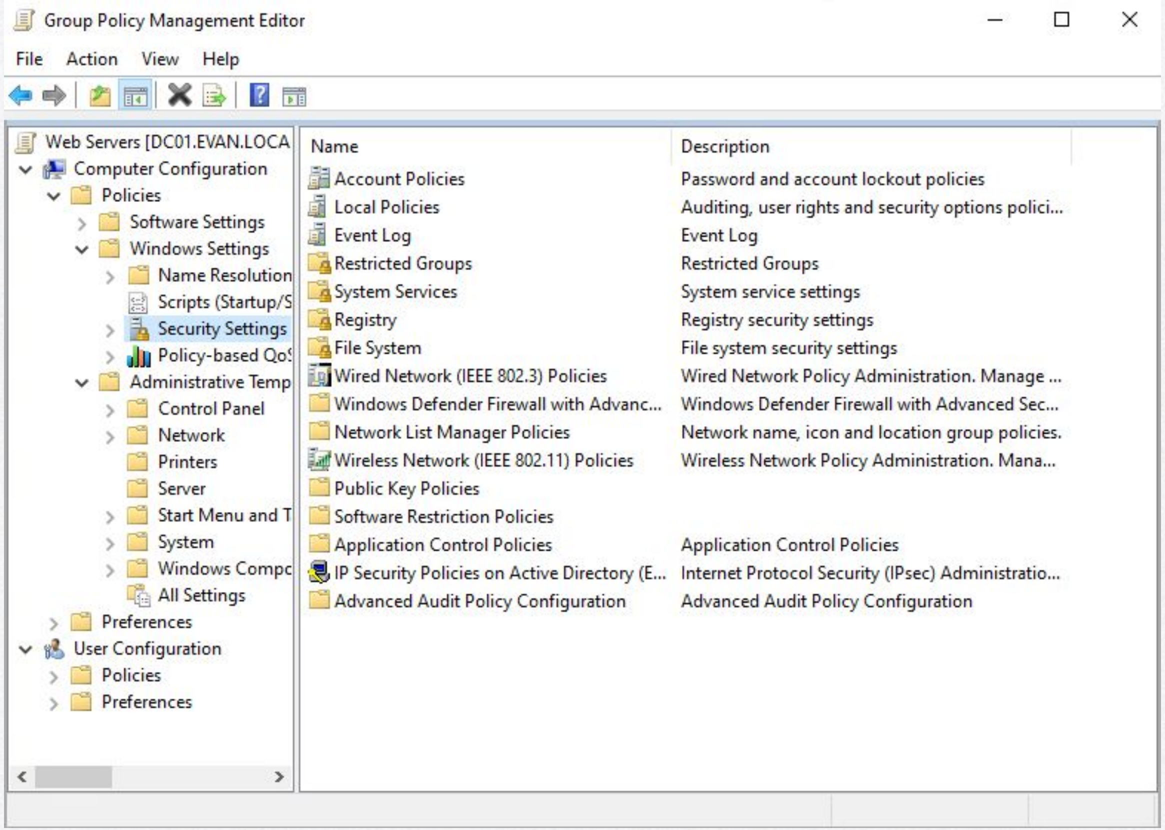
The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:

Group Policy Management Continued

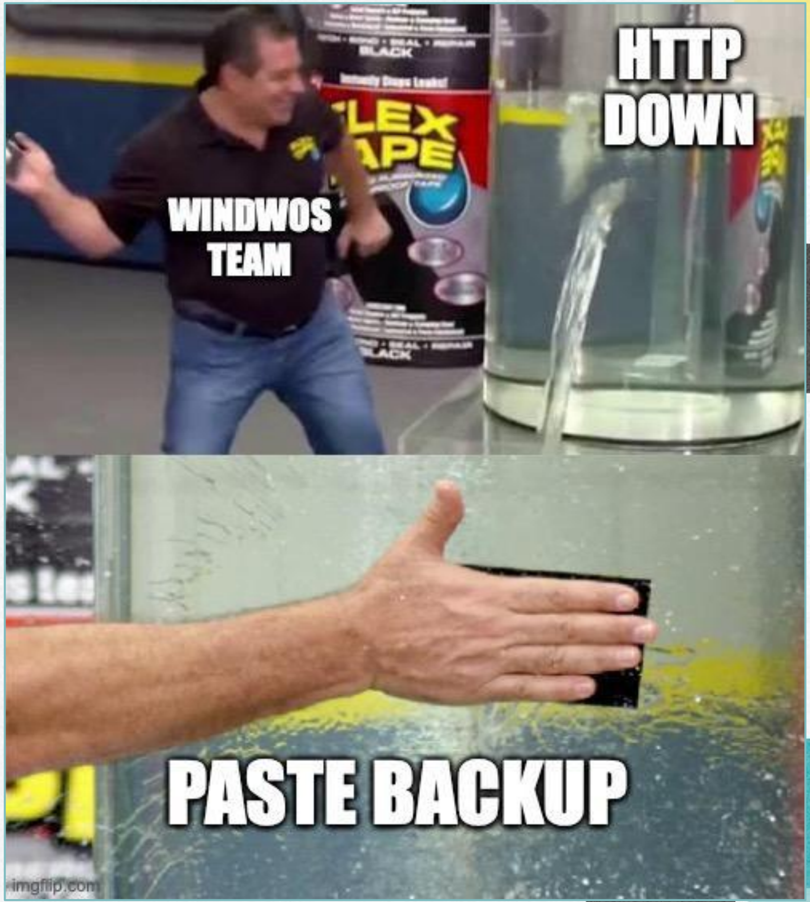


Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Event Log	Event Log
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File system security settings
Wired Network (IEEE 802.3) Policies	Wired Network Policy Administration. Manage ...
Windows Defender Firewall with Advanc...	Windows Defender Firewall with Advanced Sec...
Network List Manager Policies	Network name, icon and location group policies.
Wireless Network (IEEE 802.11) Policies	Wireless Network Policy Administration. Mana...
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Active Directory (E...	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

03

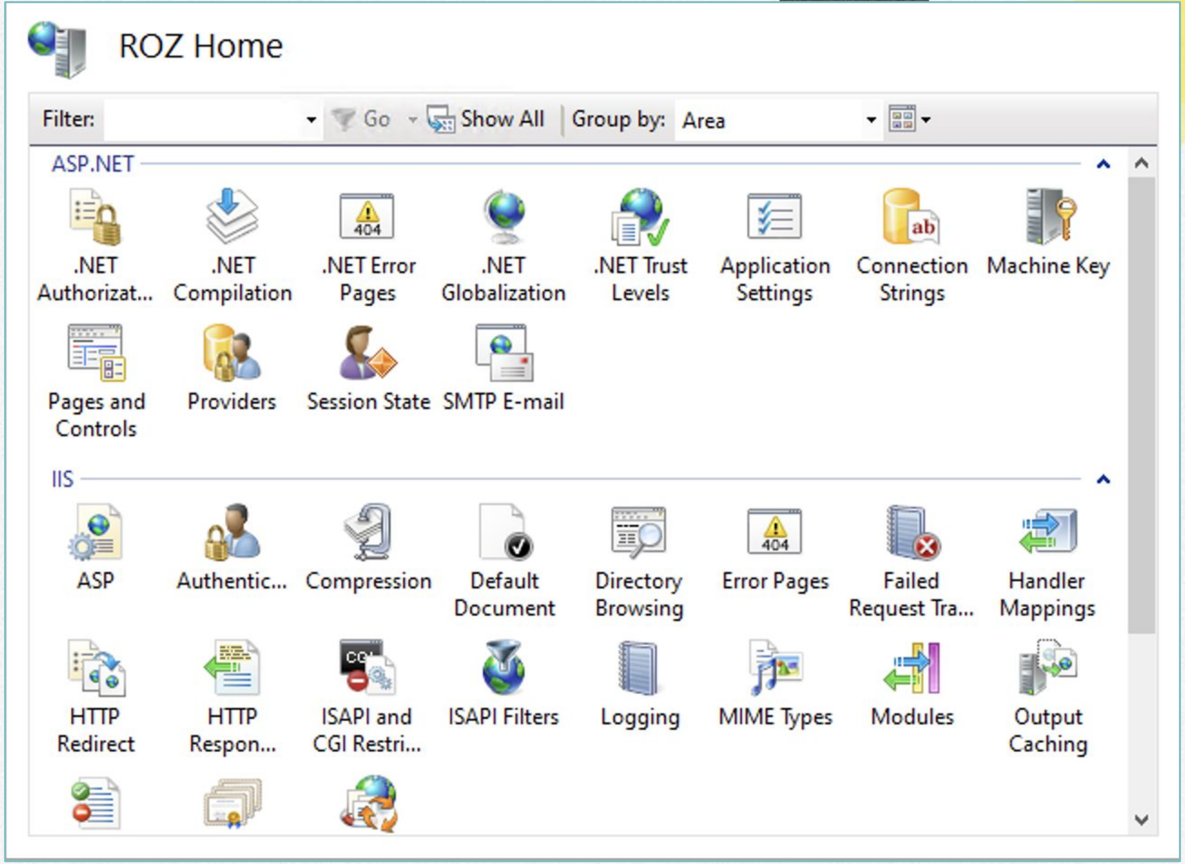
IIS

Web servers, FTP



IIS ugh-ly

Lawrence loves IIS
(unlike u)


ROZ Home

IIS Stuff

HTTP/HTTPS

IIS Configs

Directory browsing, SSL, etc.

Webshells

Who put this file here?

Nice

Never include command execution

FTP

IIS Configs

Directory access control

Websites

Run multiple sites from one server

FTP

Share files

Webshells

- Allows red team to do code execution
- Make sure there are no imposters in ur files
  - Shells could be hiding there 👀
- One of the most common exploits used in RvB

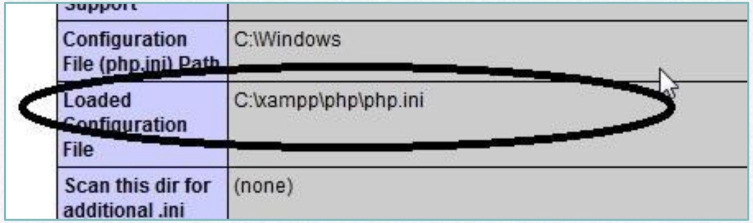
Anti-Webshell Maneuvers

PHP

php.ini disable functions

Having trouble finding php.ini?

```
<?php
phpinfo();
?>
```



Support	
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\xampp\php\php.ini
Scan this dir for additional .ini	(none)

ASP and ASPX

Cry

Search for suspicious strings

```
findstr /s /i /m "shell" *.*
```

downbad

https://github.com/emposha/PHP-Shell-Detector

04

Blooket & LAB

Wordpress on IIS

What do?

Tasks:

- On Eggssica, create a new domain user, make them a Domain Admin
- Create a group policy object to
  - Disable local administrator accounts
  - Configure basic firewall rules and enable firewall
    - Block connections on port 22
- Push the new group policy to only Blobby using GPMC
  - Also find a way using command prompt
- Login to Blobby with your domain user, check group policy
- Create another GPO to Allow Port 80, enable firewall
  - Push this GPO to only Blogic