https://www.youtube.com/watch?v=mTWeU4HtNj0

Gui Panes

- 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
- Windows Security
- 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
    - Make sure to document all the user you deleted because some injects require you to name the users you removed
- Review and remove unneeded shared folders
    - C$ and in some cases ADMIN$
- Check scheduled tasks for anomalies
    - Taske 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
        - you can use this information to see which IP address is spamming the login and then you can block that IP
    - 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
        - W33SVC
- 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 - process that starts when a user log in
- Can create them and kill them (mostly)
- Types
    - App
        - Can be terminated by user
    - Background
        - No user interaction
        - i.e., how fast are fans spinning
    - 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
    - sysinternals.com
    - https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer

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
        - Roles and Features are optional add ons for the OS
            - IIS web server
            - Active Directory Domain Services (ADDS)
            - Microsoft Defender
                - On server editions, Microsoft Defender is considered a feature, therefore hackers may just uninstall it.

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
    - Administrative Templates
        - Everything here is considered a GPO
- What exactly to set?
    - Look up stig for suggested configurations
        - disable auto run when plugging usb

Active Directory

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 UH login work everywhere? (library, canvas, broncodirect)
    - Basically, what happens is that the computer we're logging our UH user into is domain joined, and because it's a part of the domain, you are logging into a domain user. The computer we use goes to the domain controller to see if you're logging into a valid user, if you are, only then your computer lets you log in.
- Forrest
    - A forest 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
- Within Domains you have objects
    - Organizational Units (OUs)
    - Groups
    - Users
        - Can log into every domain joined computer
    - Misc AD data
- Lightweight Directory Access Protocol (LDAP)
    - Query any and all information quickly
    - Can use any LDAP client
        - Dedicated programs
        - Internal Windows tools
        - Powershell

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

`gpupdate /force` = forces a group policy update on the domain joined computer

- 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
        - The reason why windows team can be run by one person
        - Which also means it's what attackers are trying to get into

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

Domain Names

- 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
- User 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 hacking**
- Kerberos
    - Uses the concept of tickets
    - Tickets have a lifetime (10 hours)
    - Derived from the user's password and the krbtgt account password
    - Analogous to the following situation
        - Show QRs 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
- Domain Account
    - Used by the server/ domain controller
- Local Account
    - Used by the local computer/ domain joined computer
    - On the domain joined computer, you can also log in using the domain account

Other Services

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)

- use it to move file
- Connect to filesystems on other computers
    - By default the entire C drive is share to administrators
- Some other fun APIs are exposed during SMB connections
    - Service control
    - Psexec
- Attackers use SMB to upload files
- Most popular method in getting access to a windows machine

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

- Package installer
- Open source
- 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 (Blogs), OpenCart (Ecommerce sites), Drupal (General Management System), MediaWiki (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 file in webroot
2. Setup database in MySQL
3. Configure db cre