Intro to Windows Security

Lecture 18 - ECS198F SQ26

Plan of the Day

About Windows

- What's the difference between different versions of Windows?
- What are some overarching themes we see in Windows's design?

Built-In Utilities

- How is security implemented in Windows?
- What are the security utilities that can be used to secure Windows?

Other Useful Tools

- What other utilities are useful for Windows security but do not come installed by default?

1. Windows Versioning and Design

The Stuff You Probably Know

Windows is:

- Designed and maintained by Microsoft
- Releases ~~slop~~ major numbered versions every “few” years
  - XP, Vista, 7, 8, ~~9~~, 10, 11
  - Recently started subversioning out 10 and 11

https://en.wikipedia.org/wiki/List_of_Microsoft_Windows_versions#Personal_computer_versions

Image From:
https://www.youtube.com/watch?v=e843erV5gXg

Stuff You Didn't Care About Before

Each "release" of Windows has 3 versions for different types of users!

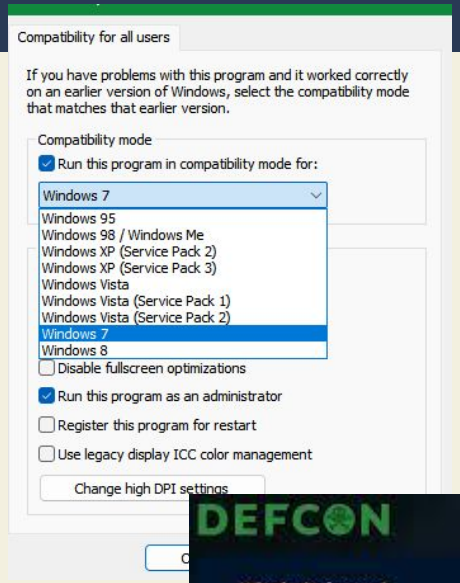
- **Windows Home** - Most basic version sold on consumer computers, contains some features
- **Windows Pro** - "Business"-grade general OS; essentially Home but with extra security features for management
- **Windows Server** - Server OS dedicated to hosting services; has different update schedule and support compared to Home/Pro

Feature	Windows 11 Home	Windows 11 Pro
BitLocker Drive Encryption If your device is lost or stolen, BitLocker puts everything on lockdown, so no one else can access your systems or data. [21]		✓
Device encryption If you turn on device encryption, only authorized individuals will be able to access your device and data. [22]	✓	✓
Find my device Keep track of your devices—even your digital pen!	✓	✓
Firewall and network protection Your Windows device comes with built-in security features to help safeguard against viruses, malware, and ransomware.	✓	✓
Internet protection App & browser control in Windows Security helps protect your device from potentially dangerous apps, files, websites, and downloads. [4] [23]	✓	✓
Parental controls and protection Manage screen time, limit access to mature content, and control online purchases when you connect your family's Microsoft accounts.	✓	✓
Secure boot Helps prevent malicious software applications and unauthorized operating systems from loading during the system start-up process.	✓	✓
Windows Hello Uses facial recognition, fingerprint, or PIN, for a fast, secure, and password-free way to unlock your compatible Windows devices. [23]	✓	✓

Backwards Compatibility

Windows as an operating system first and foremost is:

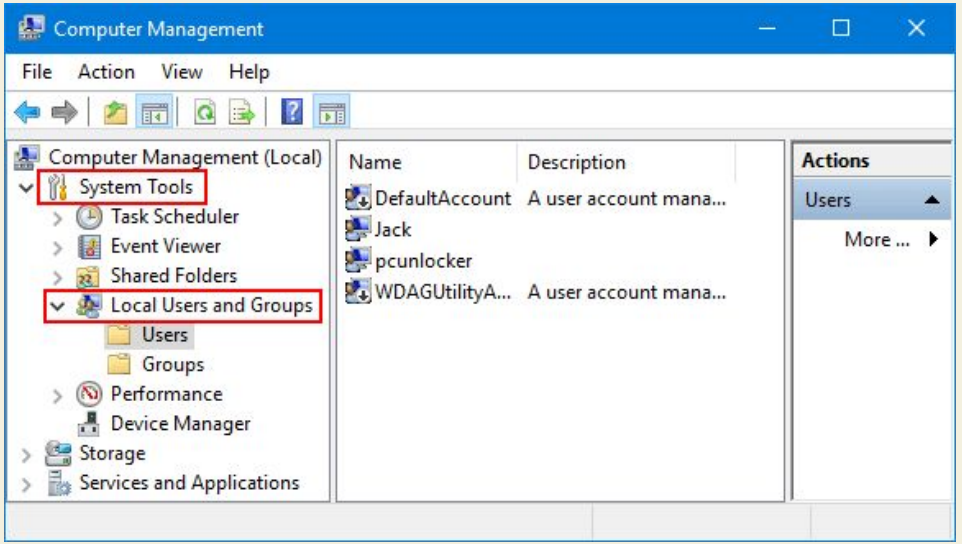
- ~~Secure~~
- **USABLE!**
  - That means making sure old programs can run on newer systems!
  - That means supporting old features *in case* you want to use them!
  - That means allowing you to **downgrade** your security for compatibility purposes!



Administration Style

Welcome back GUI Management!

- Pretty much all management tasks can be done by clicking through menus!
    - User management, firewall policies, setting rules, add or removing programs, etc. etc.
- Command-line options still available...

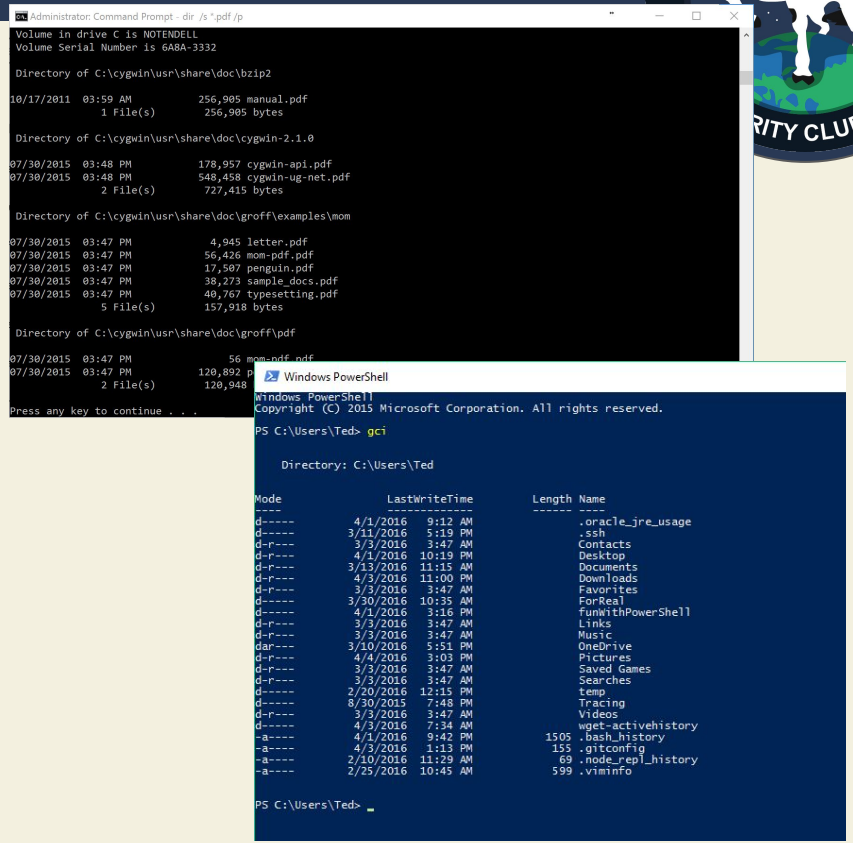


The Windows “Command Line”

You have “2” options for administering Windows through the command line:

- Command Prompt
  - Dates back to the late 80’s
  - Heritage of the original DOS
  - Very different commands!

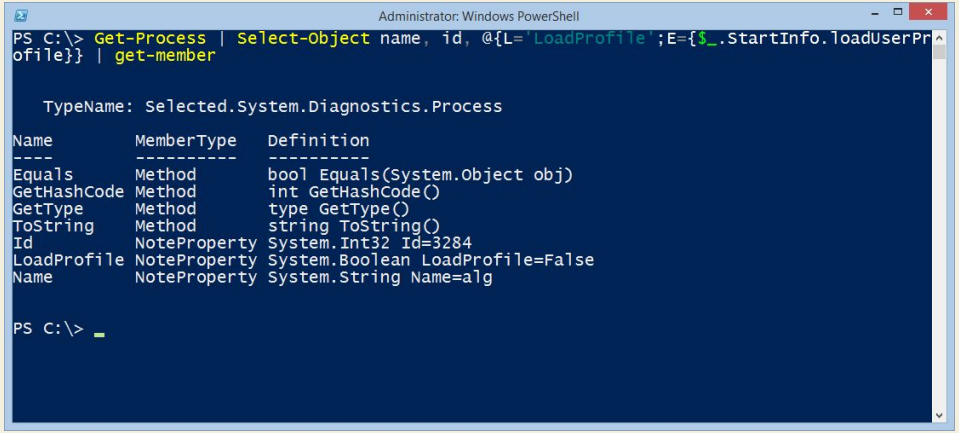
- **PowerShell**
  - Introduced with Windows 7
  - Shell + scripting language!



About PowerShell

- The one that gets bundled into computers is **PowerShell 5.1!** (Newest version is 7)

- Object-based (Kinda like Python)
  - Queries return objects, and you can process those objects
  - Not text-based like bash!



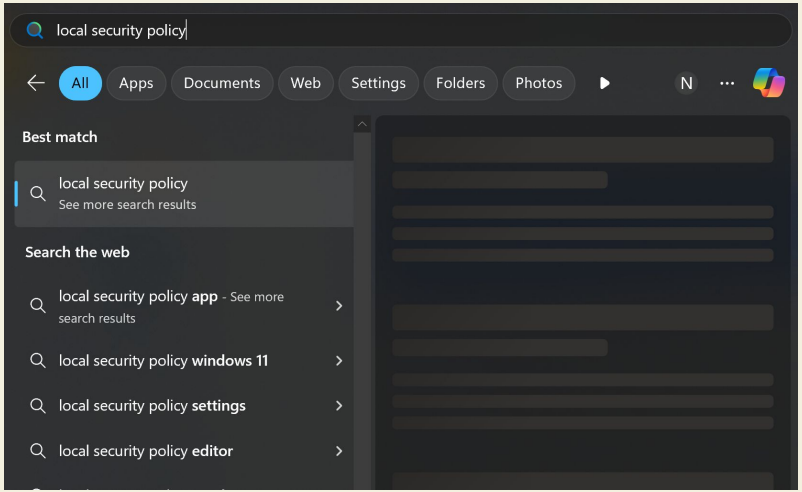
Example: How do you get a list of users in Bash and PowerShell?

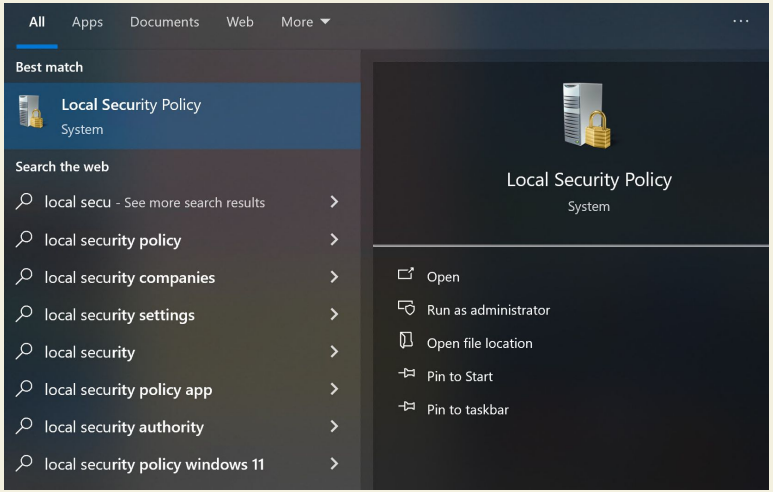
- cut -d: -f1 /etc/passwd (Bash)
- Get-ADUser -Filter * | Select-Object (property)

2. Windows Security Tools

Notes

DISCLAIMER: Some of the tools I'm about to mention do not appear in Windows Home editions, only in Pro / Enterprise / Education

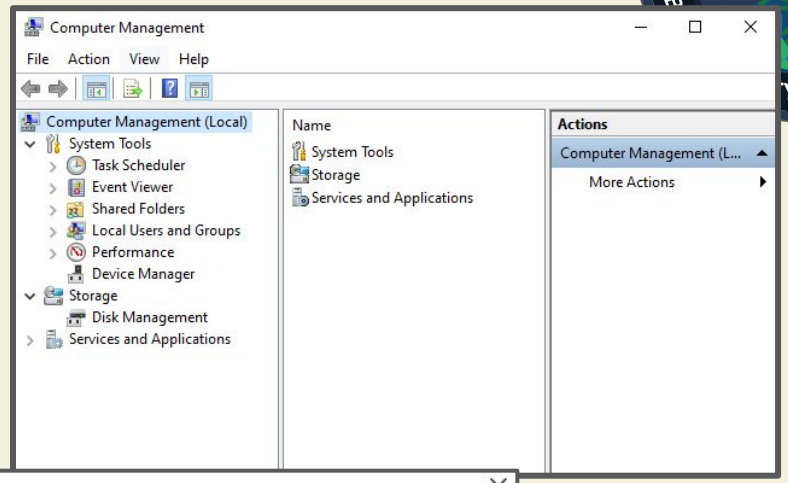


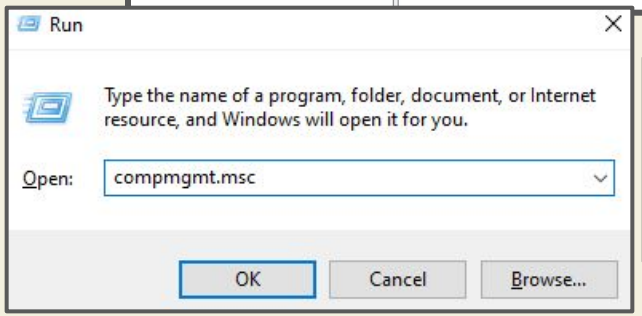


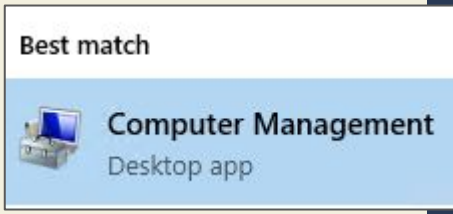
compmgmt.msc

Computer Management

- Interface for performing common administrative tasks
- Control Panel on steroids
- Links to other common administrative tools

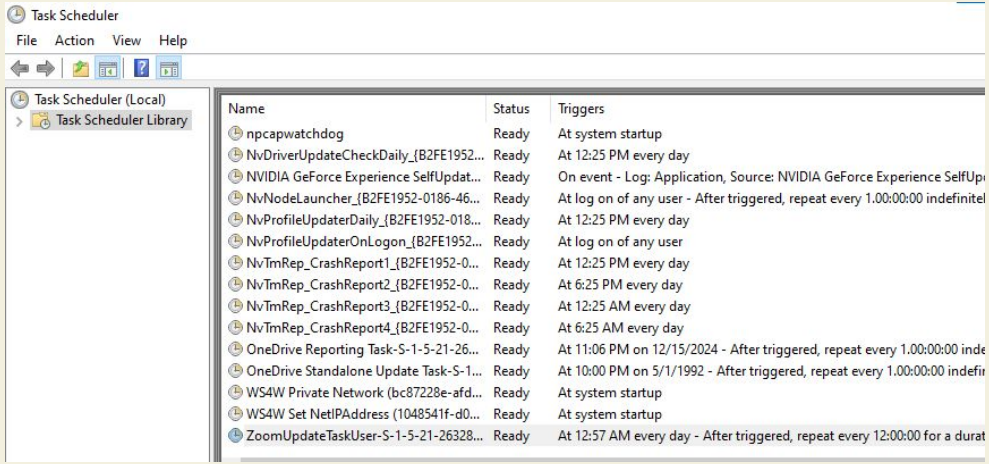






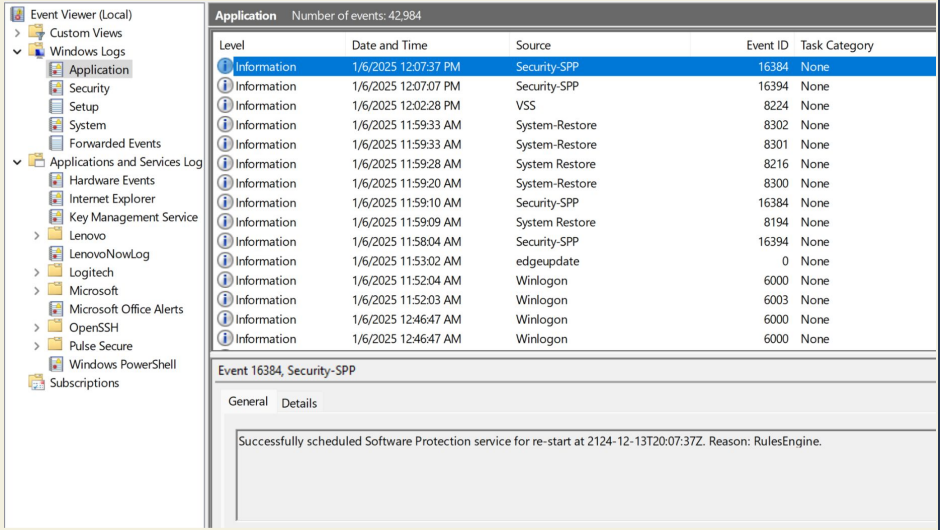
Task Scheduler

- Windows utility for scheduling programs to run at certain times
- Triggers:
  - Times / Dates
  - When certain system events occur (logon, Event IDs, etc.)



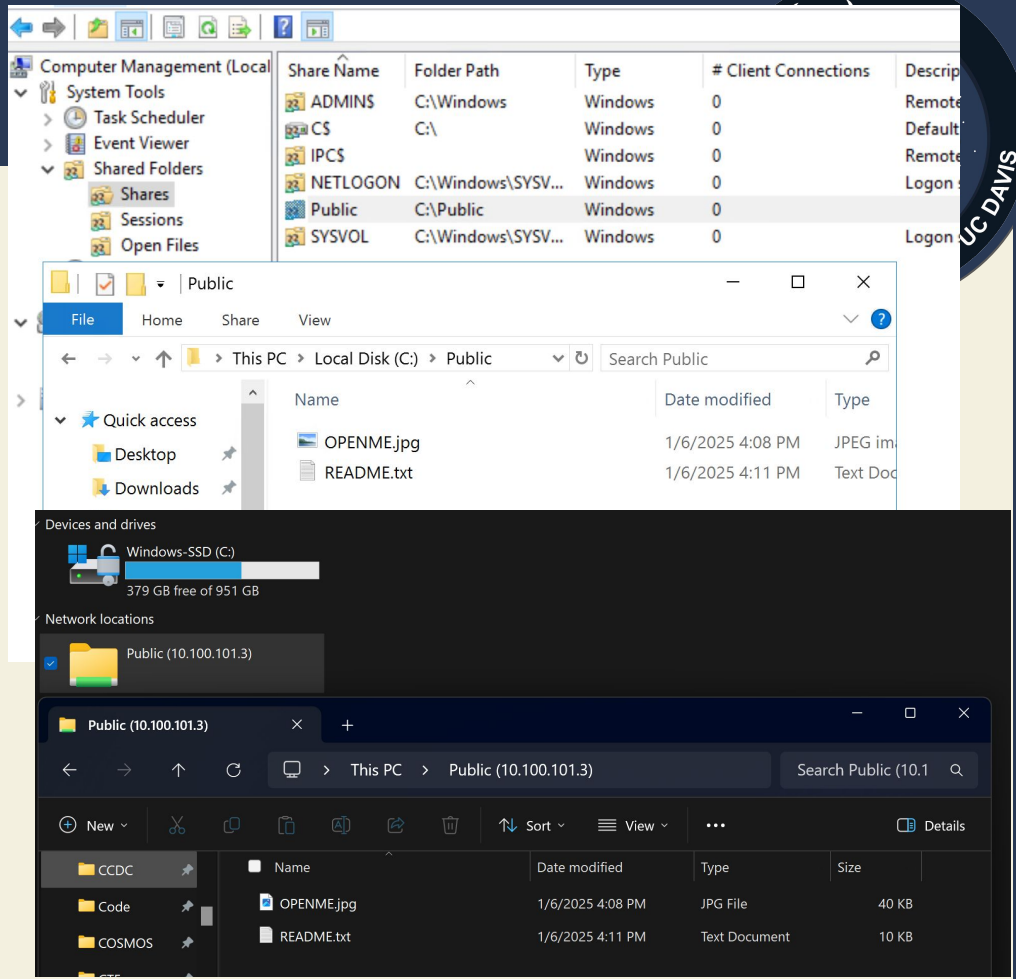
Event Viewer

- “Logging service” of Windows
- Keeps track of events that Windows or other installed software reports to it
- Set what Windows logs in *Local Security Policy*



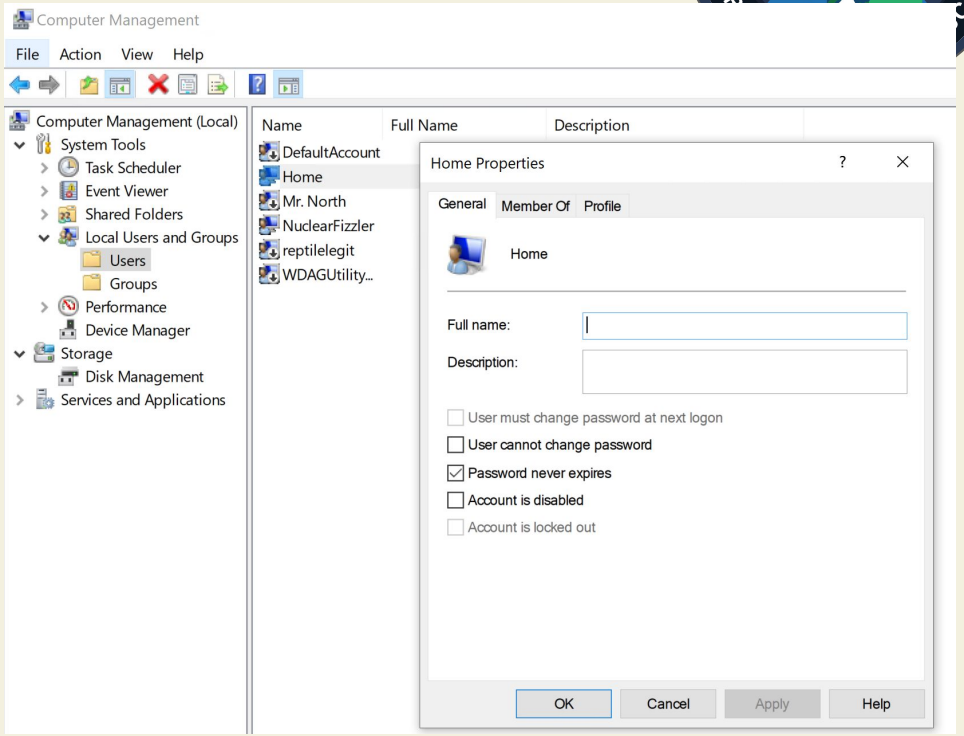
Shared Folders

- Folders on your hard drive can be shared with other computers over the SMB Protocol!
- Shares with ‘$’ at the end are there by default and hidden from normal users
- If you don’t need it, disable it!
    - (And if you do, don’t)



Local Users and Groups

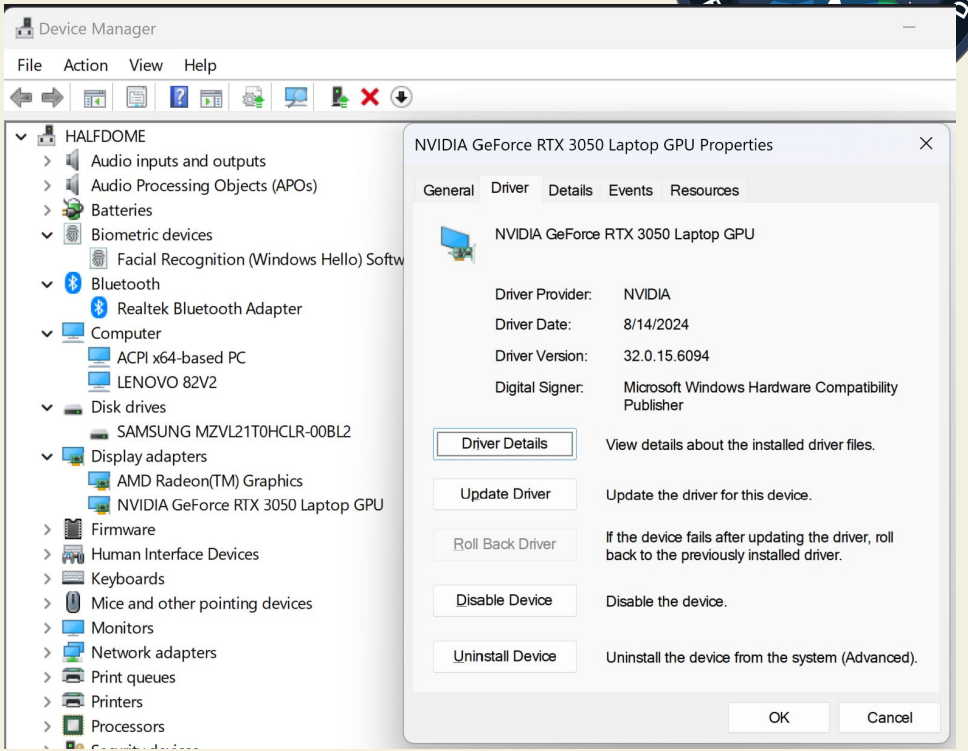
- Fast interface for managing...you guessed it
- Create / delete accounts, manage their properties and what groups they belong to
- Probably exists in Settings/Control Panel as well but this gives you more control



Device Manager

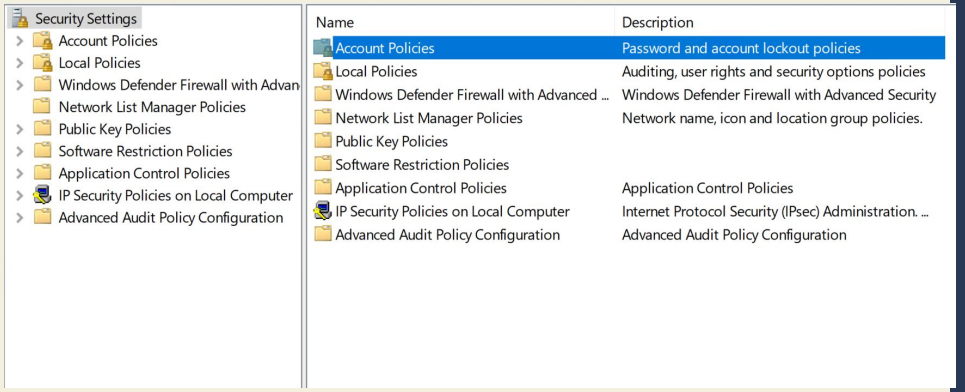
- Settings for devices connected to your computer

See also: msinfo32.exe



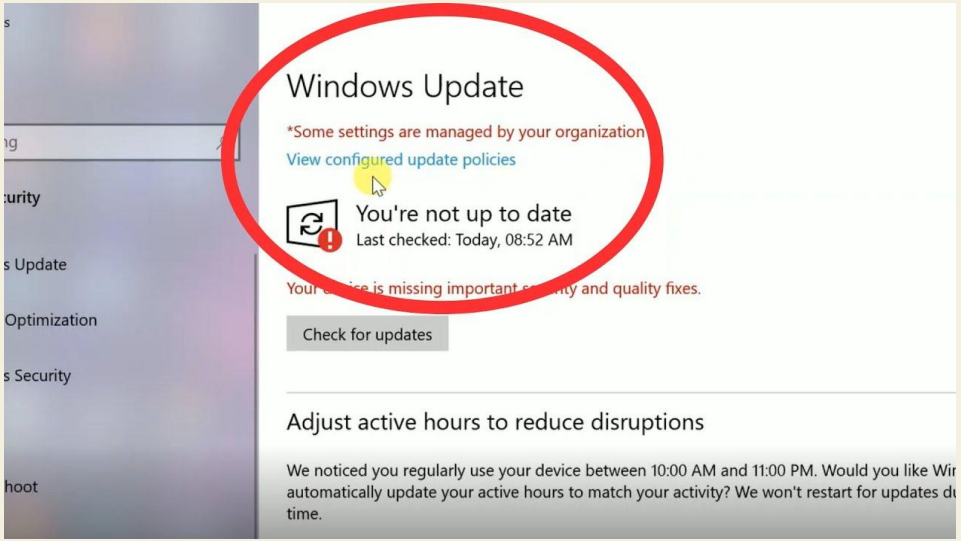
Local Security Policy

- The “main” Windows security settings
- EX: Windows password requirements, Windows logging settings, force CTRL-ALT-DEL, etc.
- A lot! of policies
- See also: Local Group Policy



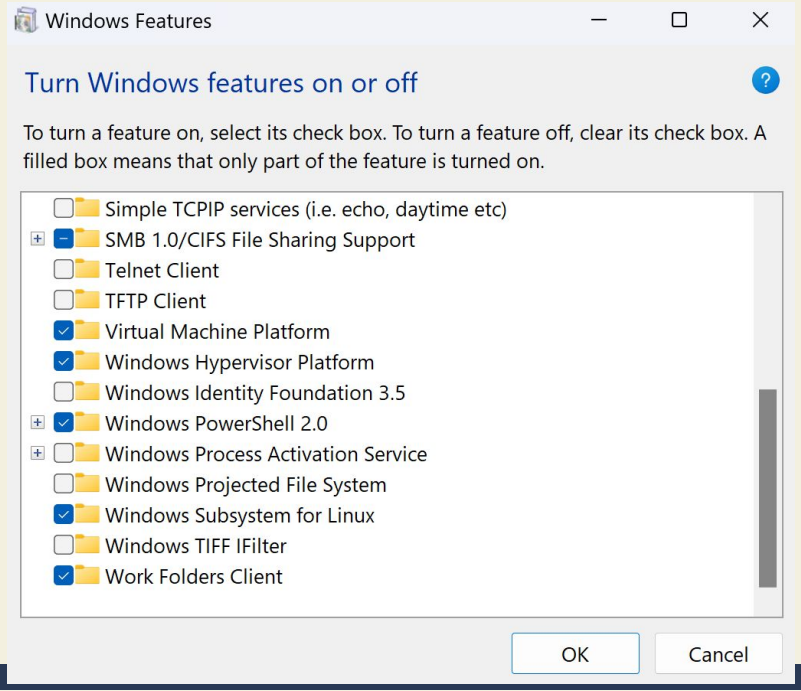
Windows Updates

- You should download them...but you already know how it is
- Certain variants of Windows allow Windows Updates to be controlled via Security Policy



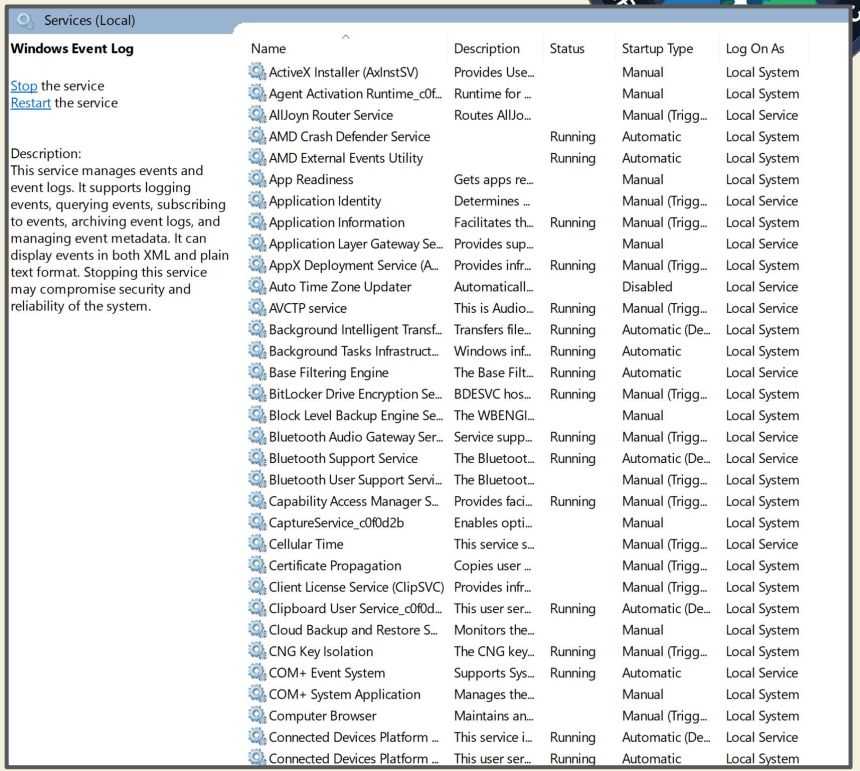
Windows Features

- Additions to Windows that can be installed separately from the operating system
- WSL, HyperV/Virtualization support, IIS (Web servers), etc.
- Again, add/remove at your discretion



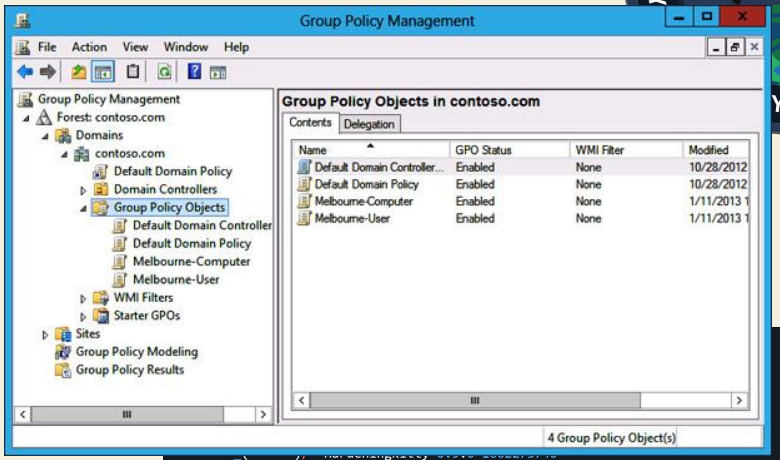
Services

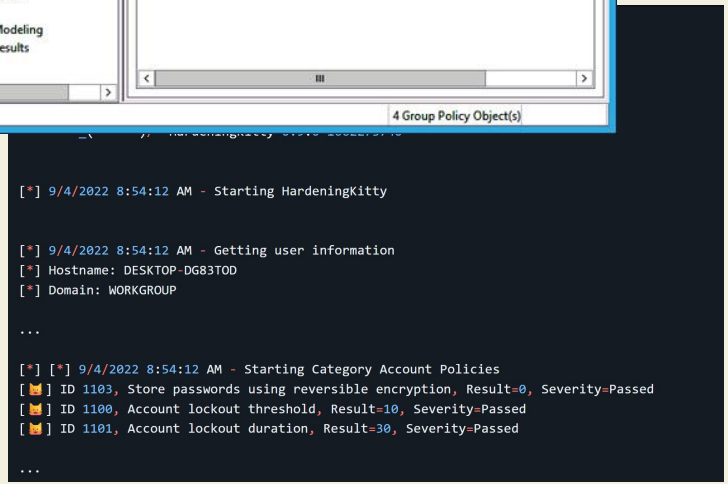
- List of all processes/programs on the computer that may run in the background continuously
- Does not describe if it's running (Task Manager) but its overall status and permissions
- "Things that need to run constantly vs periodically" Services vs Task Scheduler



Command Line Automation

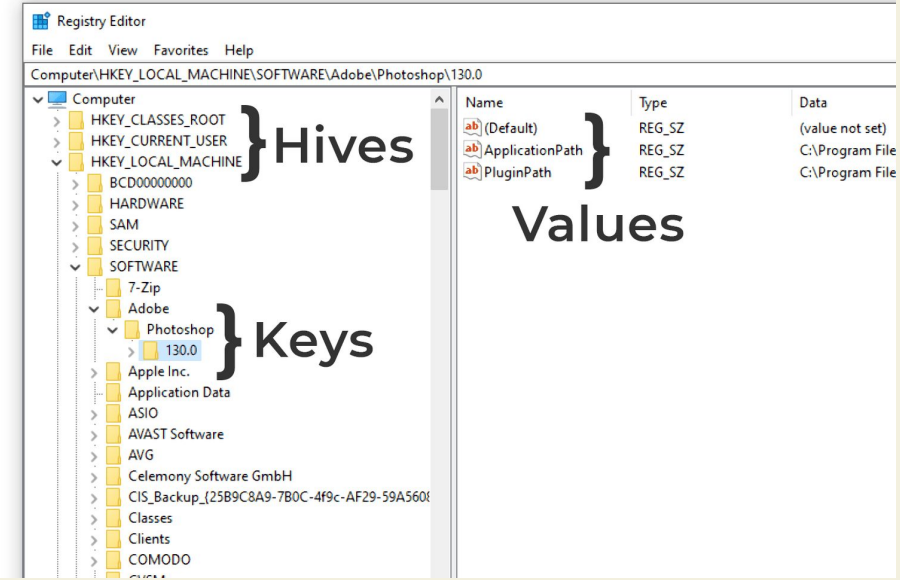
- Everything I just mentioned can be done via PowerShell or Command Prompt!
- Hardening scripts / Policy automation!
  - Deploy Group Policy templates
  - Deploy scripts to set settings and run utilities automatically!





Registry

- All of these menus and GUIs are “front ends” for databases containing security rules!
  - Registry - Stores operating system settings and config data! (Think the `etc` folder!)
  - Authentication / User data databases

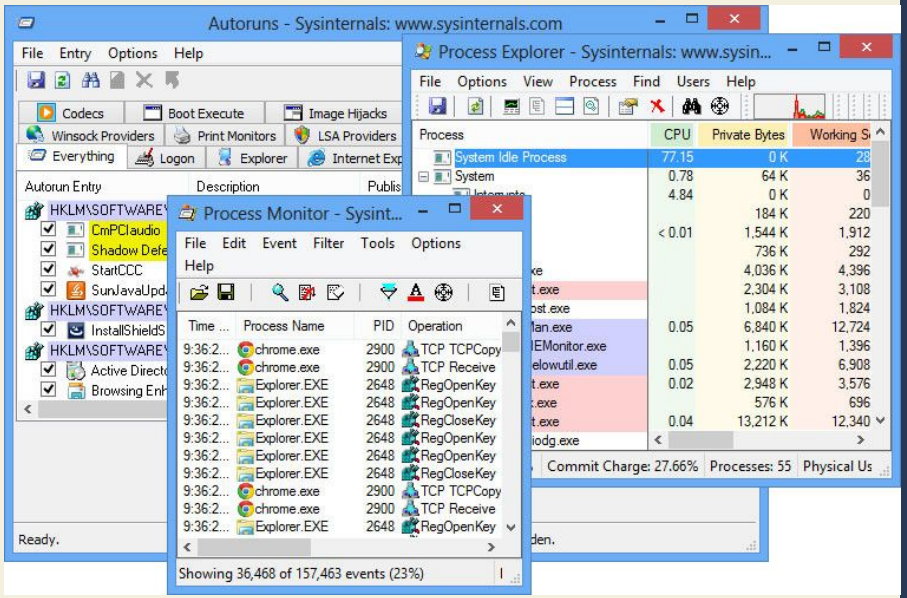


3. Other Security Tools

Sysinternals

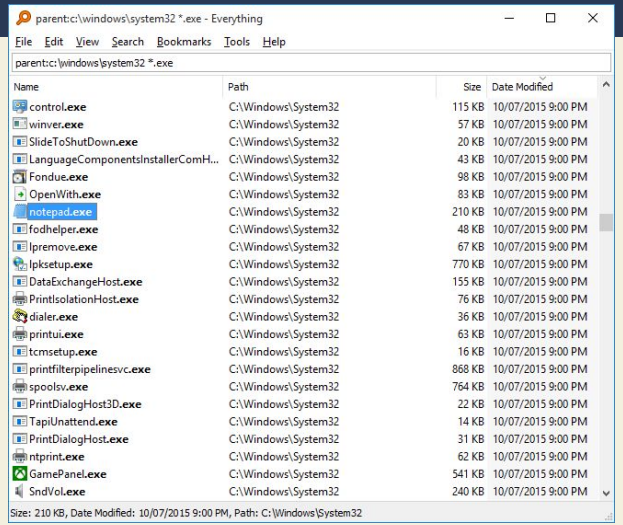
- Suite of tools that are developed by Mark Russinovich (now Microsoft) that are useful for system administration / security
    - Monitor processes, check outgoing connections, scan drivers/loaded libraries, etc.

https://learn.microsoft.com/en-us/sysinternals/



Random Useful Things

- Windows Package Managers
  - Chocolately, Winget
- Everything
  - Fast file searcher
- Ninite
  - Installer bundler for quickly installing software



Let's install Notepad++.

1. Open a command line as an administrator.
2. Type `choco install notepadplusplus` and press Enter.
3. That's it. Pretty simple but powerful little concept!