Professor Messer

Professor Messer's

# CompTIA A+

## CORE 2 220-1202

# Course Notes

James "Professor" Messer

# Professor Messer's CompTIA 220-1202 Core 2 A+ Course Notes

*James "Professor" Messer*


http://www.ProfessorMesser.com

**Professor Messer's CompTIA 220-1202 Core 2 A+ Course Notes**
Written by James "Professor" Messer

https://www.ProfessorMesser.com


First Edition: March 2025
This is version 1.3

**Trademark Acknowledgments**


**Warning and Disclaimer**
This book is designed to provide information about the CompTIA 220-1202 A+ certification exam. However, there may be typographical and/or content errors. Therefore, this book should serve only as a general guide and not as the ultimate source of subject information. The author shall have no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have incurred, directly or indirectly, by the information contained in this book.

# Contents

## Introduction

The CompTIA A+ certification requires a broad set of knowledge, and it covers more topics than many industry certifications. It's no surprise that the A+ certification has become one of the most sought-after industry certifications by both aspiring technologists and employers.

I hope this book helps you with your "last mile" of studies before taking your exam. There's a lot to remember, and perhaps some of the information in this book will help jog your memory while you're sitting in the exam room. Best of luck with your studies!

- Professor Messer

## The CompTIA A+ Certification

CompTIA's A+ certification is considered to be the starting point for information technology professionals. Earning the A+ certification requires the completion of two exams and covers a broad range of technology topics. After completing the CompTIA A+ certification, an A+ certified professional will have an understanding of computer hardware, mobile devices, networking, operating systems, security techniques, and much more.

The current series of the A+ certification is based on the successful completion of the 220-1201 and the 220-1202 exams. You must pass both exams to earn your CompTIA A+ certification. This book provides a set of notes for the 220-1202 Core 2 exam.

**The 220-1202 Core 2 exam**

The 220-1202 exam objectives are focused on operating systems, with over half of the exam detailing operating systems and the troubleshooting of software.

Here's the breakdown of the four 220-1202 exam domains:

Domain 1.0 - Operating Systems - 28%
Domain 2.0 - Security - 28%
Domain 3.0 - Software Troubleshooting - 23%
Domain 4.0 - Operational Procedures - 21%

## Study Tips

**Exam Preparation**

- Download the exam objectives, and use them as a master checklist: http://www.ProfessorMesser.com/objectives
- Use as many training materials as possible. Books, videos, and Q&A guides can all provide a different perspective of the same information.
- It's useful to have as much hands-on as possible, especially with network troubleshooting and operating system command prompts.

**Taking the Exam**

- Use your time wisely. You've got 90 minutes to get through everything.
- Choose your exam location carefully. Some sites are better than others.
- Get there early. Don't stress the journey.
- Manage your time wisely. You've got 90 minutes to get through everything.
- Wrong answers aren't counted against you. Don't leave any blanks!
- Mark difficult questions and come back later. You can answer the questions in any order.


Professor
Messer

Professor Messer's
# CompTIA A+
## 220-1102 Course Notes

http://www.ProfessorMesser.com

## 1.1 - Operating Systems Overview

**Why do you need an OS?**
- Control interaction between components
  - Memory, hard drives, keyboard, CPU
- A common platform for applications
  - You're going to do some work, right?
- Humans need a way to interact with the machine
  - The "user interface" - Hardware can't do everything!

**Standard OS features**
- File management
  - Add, delete, rename
- Application support
  - Memory management, swap file management
- Input and Output support
  - Printers, keyboards, storage drives, USB drives
- Operating system configuration and management tools

**Microsoft Windows**
- Major market presence
  - Many different versions
  - Windows 10, Windows 11, Windows Server
- Advantages
  - Large industry support
  - Broad selection of OS options
  - Wide variety of software support
- Disadvantages
  - Large install base provides a big target for security exploitation
  - Large hardware support can create challenging integration exercises

**Linux**
- Free Unix-compatible software system
  - Unix-like, but not Unix
- Many (many) different distributions
  - Ubuntu, Debian, Red Hat / Fedora
- Advantages
  - Cost. Free!
  - Works on wide variety of hardware
  - Passionate and active user community
- Disadvantages
  - Limited driver support, especially with laptops
  - Limited support options

**Apple macOS**
- macOS - Desktop OS running on Apple hardware
- Advantages
  - Easy to use
  - Extremely compatible
  - Relatively fewer security concerns
- Disadvantages
  - Requires Apple hardware
  - Less industry support than the PC platform
  - Higher initial hardware cost

**Chrome OS**
- Google's operating system
  - Based on the Linux kernel
- Centers around Chrome web browser
  - Most apps are web-based
- Many different manufacturers
  - Relatively less expensive
- Relies on the cloud - Connect to the Internet

**Apple iPadOS**
- Operating system for Apple's iPad tablets
  - A variant of Apple's phone iOS
- Tablet features
  - Desktop browser (Safari)
  - Second monitor (Sidecar)
  - Keyboard support
  - Multitasking

**Apple iOS**
- Apple iOS
  - Apple iPhones
  - Based on Unix
  - Closed-source - No access to source code
  - Exclusive to Apple products
- iOS Apps
  - Apps are developed with iOS SDK on macOS
  - Apps must be approved by Apple before release
  - Apps are available to users in the Apple App Store

## 1.1 - Operating Systems Overview (continued)

**Google Android**

- Google Android
  - Open Handset Alliance
  - Open-source OS, based on Linux
  - Supported on many different manufacturer's devices
- Android Apps
  - Apps are developed on Windows, macOS, and Linux with the Android SDK
  - Apps available from Google Play
  - Apps also available from third-party sites (i.e., Amazon Appstore)

**Vendor-specific limitations**

- End-of-life
  - Different companies set their own EOL policies
- Updating
  - iOS, Android, and Windows check and prompt for updates
  - Chrome OS will update automatically
- Compatibility between operating systems
  - Some movies and music can be shared
- Almost no direct application compatibility
  - Fortunately, many apps have been built to run on different OSes
  - Some data files can be moved across systems
  - Web-based apps have potential

## 1.1 - File Systems

**File systems**

- Before data can be written to the partition, it must be formatted
  - Build the foundation
- Operating systems expect data to be written in a particular format
  - FAT32 and NTFS are popular
- Many operating systems can read (and perhaps write) multiple file system types
  - FAT, FAT32, NTFS, exFAT, etc.

**NTFS**

- NTFS – NT File System
  - Extensive improvements over FAT32
  - Quotas, file compression, encryption, symbolic links, large file support, security, recoverability
- Not very compatible across operating systems
  - Many OSes will read NTFS (but not write)
  - Some have limited write functionality to an NTFS file system

**Resilient File System (ReFS)**

- The future of Windows file systems
  - An update to NTFS
  - Server 2012 and later, limited support in Windows 8.1 and later
- Huge storage requirements
  - Support for very large drives and storage arrays
- Constant data availability
  - Self-repairing, ongoing integrity checks - no more chkdsk!
  - The file system also provides RAID-like redundancy
- A measured integration
  - Updates and improvements are ongoing

**FAT**

- FAT - File Allocation Table
  - One of the first PC-based file systems (circa 1980)
- FAT32 - File Allocation Table
  - Larger (2 terabyte) volume sizes
  - Maximum file size of 4 gigabytes
- exFAT - Extended File Allocation Table
  - Microsoft flash drive file system
  - Files can be larger than 4 gigabytes
  - Compatible across many operating systems - Windows, Linux, macOS

**ext4**

- Fourth extended file system
  - An update to ext3
  - Commonly seen in Linux and Android OS

**Extended File System (XFS)**

- High performance file system for Linux
  - Supported in most Linux distributions
- Designed for scalability
  - Large-scale computing and high speed processing
- Features for the enterprise
  - Support for large file system size
  - Built-in journaling
  - Minimal fragmentation

**APFS**

- Apple File System (APFS)
  - Added to macOS High Sierra (10.12.4)
  - Also included with iOS and iPadOS
- Optimized for solid-state storage
  - Encryption, snapshots, increased data integrity

# 1.2 - Installing Operating Systems

**Boot methods**

- USB storage
  - USB must be bootable
  - Computer must support booting from USB
- PXE ("Pixie") - Preboot eXecution Environment
  - Perform a remote network installation
  - Computer must support booting with PXE
- Solid state drives / hard drives
  - Store many OS installation files
- Internet-based
  - Linux distributions, macOS Recovery installation, Windows updates
- External / hot swappable drive
  - Some external drives can mount an ISO image (optical drive image)
  - Boot from USB
- Internal hard drive
  - Install and boot from separate drive
  - Create and boot from new partition
- Multiboot
  - Pick from two or more operating systems from a boot menu
  - Windows, Linux, etc.

**Types of installations**

- Clean install
  - Wipe the slate clean and reinstall
  - Migration tool can help
- In-place upgrade - Maintain existing applications and data
- Image deployment
  - Deploy a clone on every computer
  - Relatively quick
  - Can be completely automated
- Remote network installation
  - Local server or shared drive
  - Install across the Internet
- Recovery partition
  - Hidden partition with installation files
- Repair installation
  - Fix problems with the Windows OS
  - Does not modify user files
- Other considerations
  - Load alternate third party drivers when necessary; disk controller drivers, etc.

**Zero-touch deployment**

- An automatic install
  - Streamlined implementation
- Customize the installation process
  - Automate the entire process
  - Company-specific configurations
- A seamless user experience
  - Turn on the system and go
  - No Domain questions or account issues
- Send a laptop to a user anywhere
  - The installation takes care of itself

**The disk partition**

- Separates the physical drive into logical pieces
  - Useful to keep data separated
  - Multiple partitions are not always necessary
- Useful for maintaining separate operating systems
  - Windows, Linux, etc.
- Formatted partitions are called volumes
  - Microsoft's nomenclature

**GPT partition style**

- GPT (GUID Partition Table)
  - Globally Unique Identifier
  - The latest partition format standard
- Requires a UEFI BIOS
  - Can have up to 128 partitions
  - Maximum partition size is over 9 billion TB
  - Windows max partition is currently 256 TB
- No need for extended partitions or logical drives

**MBR partition style**

- MBR (Master Boot Record)
  - The old standby, with all of the old limitations
  - Maximum partition size of 2 TB
- Primary
  - Bootable partitions
  - Maximum of four primary partitions per hard disk
  - One of the primary partitions can be marked as Active
- Extended
  - Used for extending the maximum number of partitions
  - One extended partition per hard disk (optional)
  - Contains additional logical partitions
  - Logical partitions inside an extended partition are not bootable

## 1.2 - Installing Operating Systems (continued)

### Disk partitioning

- The first step when preparing disks
  - May already be partitioned
  - Existing partitions may not always be compatible with your new operating system
- An MBR-style hard disk can have up to four partitions
- GUID partition tables support up to 128 partitions
  - Requires UEFI BIOS or BIOS-compatibility mode
  - BIOS-compatibility mode disables UEFI SecureBoot
- **BE CAREFUL!**
  - Serious potential for data loss
  - This is not an everyday occurrence

### Quick format vs. full format

- Quick format
  - Creates a new file table
  - Looks like data is erased, but it's not
  - No additional checks
- Quick format the default during installation in Windows 10 and 11
  - Use `diskpart` for a full format
- Full format
  - Writes zeros to the whole disk
  - Your data is unrecoverable
  - Checks the disk for bad sectors (time consuming)

## 1.2 - Upgrading Windows

### Why upgrade?

- Upgrade vs. Install
  - Upgrade - Keep files in place
  - Install - Start over completely fresh
- Maintain consistency
  - Customized configurations
  - Multiple local user accounts
- Upgrades save hours of time
  - Avoid application reinstall
  - Keep user data intact
  - Keep user settings
  - Get up and running quickly

### Upgrade methods

- In-place upgrade
  - Upgrade the existing OS
  - Keeps all applications, documents, and settings
  - Start the setup from inside the existing OS
- Clean install
  - Wipe everything and reload
  - Backup your files
  - Start the setup by booting from the installation media

### Prepare the boot drive

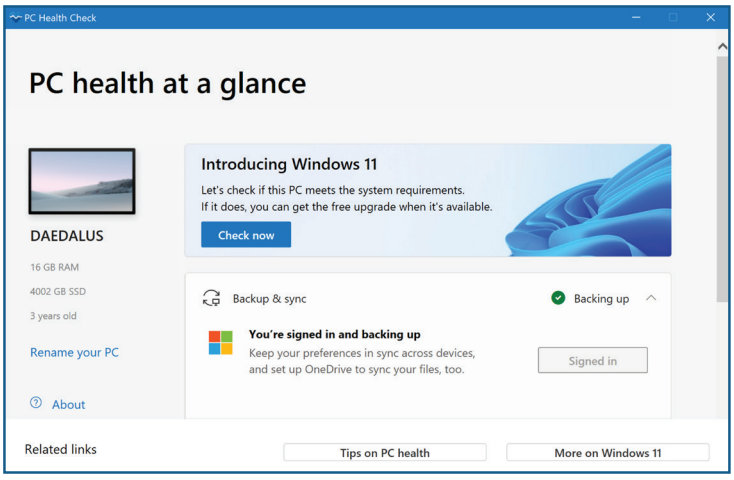
- Know your drive
  - Is data on the drive?
  - Has the drive been formatted?
  - What partitions are on the drive?
- Backup any old data
  - You may need that data again someday
  - Save user preferences
- Most partitioning and formatting can be completed during the installation
  - Clear the drive and start fresh

### Before the installation

- Check minimum OS requirements
  - Memory, disk space, etc.
  - And the recommended requirements
- Run a hardware compatibility check
  - Runs when you perform an upgrade
  - Run manually from the Windows setup screen
  - PC Health Check for Windows 11
- Plan for installation questions
  - Drive/partition configuration, license keys, etc.
- Application and driver compatibility
  - Check with the app developer and hardware manufacturer

### Windows product life cycle

- Quality updates
  - Monthly security updates and bug fixes
- Feature updates
  - Annual update with new features
  - Used to occur every three to five years
- Support is provided after the release
  - 18 to 36 months
  - Dependent on the Windows version and edition
- Also called the Modern Lifecycle Policy
  - For continuously supported products



## 1.2 - Upgrading Windows (continued)

**Windows 11 hardware requirements**

- Some additional requirements
  - More than usual
  - May require some planning
- TPM - Trusted Platform Module
  - Security hardware on the motherboard
  - Must be TPM 2.0 compatible
  - Used for BitLocker, Windows Hello
- Check your hardware
  - Run tpm.msc
- UEFI BIOS
  - The hardware must be Secure Boot capable
- Enable Secure Boot for additional security
  - Check in System Information / System Summary
- May not be available on legacy systems
  - Check with the PC manufacturer

## 1.3 - An Overview of Windows

**Windows on the Core 2 exam**

- Two Windows versions available
- Windows 10 and Windows 11

- CompTIA considers all in-support Windows versions to be in scope for the exam
  - Mainstream support is 5 years after release
- Windows versions are listed in the objectives
  - Windows 10 and 11
- Fortunately, these are remarkably similar
  - Once you know one, you effectively know the other!

**Windows 10**

- Released on July 29, 2015 - We skipped Windows 9
- A single platform
  - Desktops, laptops, tablets, phones, all-in-one devices
- Ongoing updates
  - More than 14 different released versions
  - November 2021 (Version 21H2)

**Windows 10 Home and Pro support ending**

- October 14, 2025
- This doesn't mean Windows 10 will suddenly disappear

**Windows 10 Home**

- Home user - Retail sales
- Integration with Microsoft account
  - Microsoft OneDrive backup
- Windows Defender
  - Anti-virus and anti-malware
- Cortana - Talk to your operating system

**Windows 10 Pro**

- The business version of Windows
  - Additional management features
- Remote Desktop host
  - Remote control each computer
- BitLocker - Full disk encryption (FDE)
- Join a Windows domain
  - Group Policy management

**Windows 10 Pro for Workstations**

- An edition for high-end desktops
  - Enhanced performance and storage options
- More physical CPUs - Up to four
- High maximum RAM - Supports up to 6 TB
- Support for ReFS - Resilient File System
  - Same as Windows Server

**Windows 10 Enterprise**

- Built for large implementations
  - Volume licensing
- AppLocker - Control what applications can run
- BranchCache - Remote site file caching
- Granular User Experience (UX) control
  - Define the user environment
  - Useful for kiosk and workstation

| Windows 10 Edition | Domain Access | BitLocker | Remote Desktop | Group Policy Management | Max x86 RAM | Max x64 RAM |
|---|---|---|---|---|---|---|
| Home | ✖ | ✖ | Client only | ✖ | 4 GB | 128 GB |
| Pro | ✓ | ✓ | Client and Host | ✓ | 4 GB | 2 TB |
| Pro for Workstations | ✓ | ✓ | Client and Host | ✓ | 4 GB | 6 TB |
| Enterprise | ✓ | ✓ | Client and Host | ✓ | 4 GB | 6 TB |

| Windows 11 Edition | Domain Access | BitLocker | Remote Desktop | Group Policy Management | Max x86 RAM | Max x64 RAM |
|---|---|---|---|---|---|---|
| Home | ✖ | ✖ | Client only | ✖ | N/A | 128 GB |
| Pro | ✓ | ✓ | Client and Host | ✓ | N/A | 2 TB |
| Enterprise | ✓ | ✓ | Client and Host | ✓ | N/A | 6 TB |

## 1.3 - An Overview of Windows (continued)

**Windows 11**
- An upgrade to Windows 10
  - No support for 32-bit CPUs
- Updated user interface
  - New Start menu and new taskbar widgets
- Usability updates
  - Snap layouts
  - Integrated Microsoft Teams
  - Better touch-based integration
  - Windows Copilot AI-powered assistant

**Windows 11 Home**
- The consumer version
  - Designed for home use
- Integrated with Microsoft accounts
  - Can be installed with a local account
- Limited management functionality
  - No support for Active Directory
- Includes Device Encryption
  - A consumer version of full disk encryption
  - Stores the recovery information in the user's Microsoft account

**Windows 11 Pro**
- Designed for business
  - Large-scale system management
- Integrates with Active Directory
  - Microsoft's directory services
- BitLocker available
  - Full disk encryption
- Integrated virtualization
  - Microsoft Hyper-V
- Remote access
  - Remote Desktop service support

**Windows 11 Enterprise**
- Built for large company deployments
  - Volume licensing
  - Server features
- Device management
  - Includes Mobile Device Management (MDM) and Mobile Application Management (MAM)
- Support for ReFS
  - Resilient File System

**Windows N editions**
- Windows editions for Europe
  - The result of antitrust investigations by the European Commission
  - N = Not with Media Player
- No Windows Media Player
  - Or any other multimedia utilities
- Can be added to Windows later
  - Media Feature Pack for N edition
  - Settings > Apps > Optional features > Add an optional feature > Media Feature Pack

## 1.3 - Windows Features

**Windows at work**
- Large-scale support
  - Thousands of devices
- Security concerns
  - Mobile devices with important data
  - Local file shares
- Working on a spreadsheet
  - Watching a movie
- Geographical sprawl - Cache data between sites

**Domain Services**
- Active Directory Domain Services
  - Large database of your network
- Everything documented in one place
  - User accounts, servers, volumes, printers
- Distributed architecture
  - Many servers - Not suitable for home use
- Many different uses
  - Authentication
  - Centralized management

**Organizing network devices**
- Windows Workgroups
  - Logical groups of network devices
  - Each device is a standalone system, everyone is a peer
- Windows Domain
  - Business network
  - Centralized authentication and device access
  - Supports thousands of devices across many networks

**Desktop styles**
- Your computer has many different uses
  - Those change depending on where you are
- Work
  - Standard desktop
  - Common user interface
  - Customization very limited
  - You can work at any computer
- Home
  - Complete flexibility
  - Background photos, colors, UI sizing

## 1.3 - Windows Features (continued)

### Availability of RDP

- Remote Desktop Protocol
  - View and control the desktop of a remote device
- RDP client
  - Connects to a Remote Desktop Service
  - Clients available for almost any operating system
- Remote Desktop Service
  - Provides access for the RDP client
  - Available in Windows 10 and 11 Pro and Enterprise
  - Not available in Windows 10 and 11 Home

### RAM support limitations

- RAM support varies between editions
  - More advanced editions allow additional RAM

| Windows 10 and 11 | Max x86 RAM (Win 10 only) | Max x64 RAM |
|---|---|---|
| Home | 4 GB | 128 GB |
| Pro | 4 GB | 2 TB |
| Enterprise | 4 GB | 6 TB |

### BitLocker and EFS

- Data confidentiality
  - Encrypt important information
- Encrypting File System (EFS)
  - Protect individual files and folders
  - Built-in to the NTFS file system
- BitLocker
  - Full Disk Encryption (FDE)
  - Everything on the drive is encrypted
  - Even the operating system
- Home and business use
  - Especially on mobile devices

### Group Policy editor

- Centrally manage users and systems
  - Policies can be part of Active Directory or a local system
- Local Group Policy
  - Manages the local device - `gpedit.msc`
- Group Policy Management Console
  - Integrated with Active Directory
  - Powerful system management - `gpmc.msc`

## 1.4 - Task Manager

### Task Manager

- Real-time system statistics
  - CPU, memory, disk access, etc.
- Starting the Task Manager
  - *Ctrl-Alt-Del*, select Task Manager
  - Right mouse click the taskbar and select Task Manager
  - *Ctrl-Shift-Esc*

### Services

- Non-interactive applications
  - Hundreds of background processes
- Manage from one screen - Start, stop, restart

### Startup

- Manage which programs start with a Windows login
  - Easily toggle on and off
- Multiple reboots
  - Enable and disable - You'll find it

### Processes

- View all running processes
  - Interactive and system tray apps
  - View processes from other accounts
- Manage the view
  - Move columns, add metrics
- Combine all apps, processes, and services into a single tab
  - Easy to view and sort

### Performance

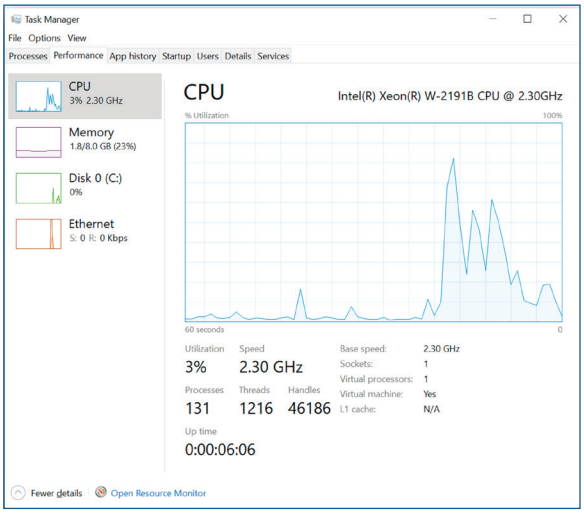
- What's happening? - CPU, memory, etc.
- Statistical views - Historical, real-time
- Current versions include CPU, memory, disk, Bluetooth, and network in the Performance tab

### Networking

- Network performance
  - Integrated into the Performance tab
- View utilization, link speeds, and interface connection state

### Users

- Who is connected? What are they doing?
- Other options - Disconnect a user, manage user accounts



# 1.4 - The Microsoft Management Console

**Build your own console**
- **mmc.exe**
- A handy starting point
  - Event Viewer
  - Local Users and Groups
  - Disk management
  - Task Scheduler
  - And more!

**Event Viewer**
- Central event consolidation
  - What happened?
- Application, Security, Setup, System
- Information, Warning, Error, Critical, Successful Audit, Failure Audit
- **eventvwr.msc**

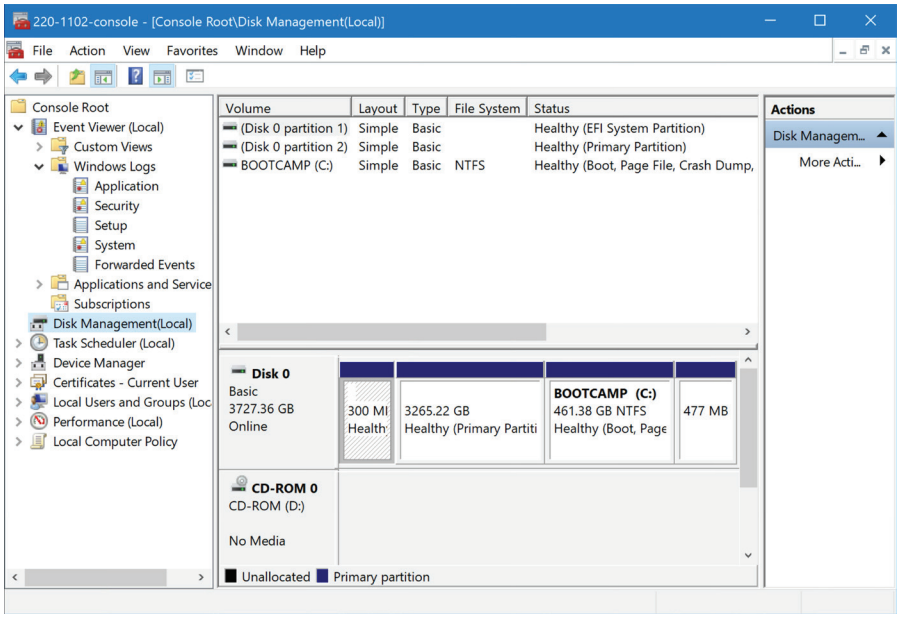
**Disk Management**
- Manage disk operations
  - Individual computers and file servers
- **diskmgmt.msc**
- **WARNING**
  - **YOU CAN ERASE DATA**
  - **ALWAYS HAVE A BACKUP**

**Task Scheduler**
- Schedule an application or script
  - Plan your future
- Includes predefined schedules
  - Click and go
- Organize
  - Manage with folders
- **taskschd.msc**

**Device Manager**
- The OS doesn't know how to talk directly to most hardware
- Device drivers are hardware specific and operating system specific
  - Older device drivers may not necessarily work in Windows 10 or 11
- **devmgmt.msc**

**Certificate Manager**
- View user and trusted certs
  - Add and remove
- **certmgr.msc**

**Local users and groups**
- Users
  - Administrator - the Windows super-user
  - Guest -Limited access
  - "Regular" Users
- Groups
  - Administrators, Users, Backup Operators, Power Users, etc.
- **lusrmgr.msc**




**Performance Monitor**
- Gather long-term statistics
  - **perfmon.msc**
- OS metrics
  - Disk, memory, CPU, etc.
- Set alerts and automated actions
  - Monitor and act
- Store statistics
  - Analyze long-term trends
- Built-in reports
  - View the data

**Group Policy Editor**
- Centrally manage users and systems
  - Policies can be part of Active Directory or a local system
- Local Group Policy Editor
  - Manages the local device
  - **gpedit.msc**
- Group Policy Management Console
  - Integrated with Active Directory
  - Powerful system management
  - **gpmc.msc**

## 1.4 - Additional Windows Tools

**System Information**
- System overview
  - **msinfo32.exe**
- Hardware Resources
  - Memory, DMA, IRQs, conflicts
- Components
  - Multimedia, display, input, network
- Software Environment
  - Drivers, print jobs, running tasks

**Resource Monitor**
- Detailed real-time view of performance
  - Separated by category
- Categories
  - Overview, CPU, Memory,
  - Disk, and Network
- **resmon.exe**

**System Configuration**
- Manage boot processes, startup, services, etc.
  - One-stop shop
- **msconfig.exe**

**Disk Cleanup**
- Find unused or unneeded files
  - A quick way to free up space
- Select the categories
  - Click the button
- **cleanmgr.exe**

**defrag**
- Disk defragmentation
  - Moves file fragments so they are contiguous
  - Improves read and write time
- Not necessary for solid state drives
  - Windows won't defrag an SSD
- Graphical version in the drive properties
- Requires elevated permissions
  - Command line:
  - **defrag <volume>**
  - **defrag C:**

**regedit.exe**
- The Windows Registry Editor
  - The big huge master database
  - Hierarchical structure
- Used by almost everything
  - Kernel, Device drivers
  - Services
  - Security Account Manager (SAM)
  - User Interface, Applications
- Backup your registry!
  - Built into regedit

## 1.5 - Windows Command Line Tools

**Privileges**
- Not all users can run all commands
  - Some tasks are for the administrator only
- Standard privileges
  - Run applications as normal user
  - This works fine for many commands
- Administrative/elevated privileges
  - You must be a member of the Administrators group
  - Right-click Command Prompt, choose *Run as Administrator*
  - **cmd**, *Ctrl+Shift+Enter*

**Command line troubleshooting**
- Use "**help**" if you're not sure

```
> help dir
> help chkdsk
```

- Also use:

```
[command] /?
```

  - Close the prompt with **exit**

**Navigation**
- **dir**
  - List files and directories
- **cd** or **chdir**
  - Change working directory
  - Use backslash **** to specify volume or folder name
- **..**
  - Two dots/periods
  - The folder above the current folder
- **md / mkdir**
  - Make a directory
- **rd / rmdir**
  - Remove directory

**Drive letters**
- Each partitions is assigned a letter
  - Primary storage drive is usually C
- Reference the drive with the letter and a colon
  - C:
- Combine with the folder
  - Folder names are separated with backslashes
  - C:\Users\professor

## 1.5 - Windows Command Line Tools (continued)

**Check Disk**

- **chkdsk /f**
  - Fixes logical file system errors on the disk
- **chkdsk /r**
  - Locates bad sectors and recovers readable information
  - Implies **/f**
- If volume is locked, run during startup

**format**

- Formats a disk for use with Windows
- BE CAREFUL - YOU CAN LOSE DATA
  - **format c:**

**DiskPart**

- Manage disk configurations
- BE CAREFUL - YOU CAN LOSE DATA
  - **diskpart** - start the DiskPart command interpreter

**copy (/v, /y)**

- Copy files from one location to another
  - **/v** - Verifies that new files are written correctly
  - **/y** - Suppresses prompting to confirm you want to overwrite an existing destination file

**xcopy**

- Copies files and directory trees
  - **xcopy /s Documents m:\backups**

**Robust Copy**

- **robocopy**
  - A better Xcopy
  - Included with Windows 10 and 11

**hostname**

- View the name of the device
  - This is very useful when there are 10 different terminal screen tabs in use
- This is the Windows Device name
  - Name can be changed in the System settings

**winver**

- View the About Windows dialog
  - A quick check
- Useful when troubleshooting
  - Are you running the latest version?

**whoami**

- User and group information
  - And other details
  - Security identifier (SID), privileges, etc.
- Can be useful when many windows are open
  - Different systems with different permissions
- Get everything with one command
  - **whoami /all**

**Managing Group Policy**

- Group Policy
  - Manage computers in an Active Directory Domain
  - Group Policy is usually updated at login
- **gpupdate**
  - Force a Group Policy update
  - **gpupdate /target:{computer|user} /force**
  - **gpupdate /target:user /force**
- **gpresult**
  - Verify policy settings for a computer or user
  - **gpresult /r**
  - **gpresult** /user sgc/professor /v

**sfc**

- System File Checker
  - Scan integrity of all protected system files
- **sfc /scannow**

## 1.5 - The Windows Network Command Line

**ipconfig**

- Most of your troubleshooting starts with your IP address
  - Ping your local router/gateway
- Determine TCP/IP and network adapter information
  - And some additional IP details
- View additional configuration details
  - DNS servers, DHCP server, etc.

**ping**

- Test reachability
  - Determine round-trip time
  - Uses Internet Control Message Protocol (ICMP)
- One of your primary troubleshooting tools
  - Can you ping the host?

**netstat**

- Network statistics
  - Many different operating systems
- **netstat -a**
  - Show all active connections
- **netstat -b**
  - Show binaries (Windows)
- **netstat -n**
  - Do not resolve names

**nslookup**

- Lookup information from DNS servers
  - Canonical names, IP addresses, cache timers, etc.
- Lookup names and IP addresses
  - Many different options

## 1.5 - The Windows Network Command Line (continued)

### net
- Windows network commands
- View network resources
  - `net view \\<servername>`
  - `net view /workgroup:<workgroupname>`
- Map a network share to a drive letter
  - `net use h: \\<servername>\<sharename>`
- View user account information and reset passwords
  - `net user <username>`
  - `net user <username> * /domain`

### tracert
- Determine the route a packet takes to a destination
  - Map the entire path
- Takes advantage of ICMP Time to Live Exceeded message
  - The time in TTL refers to hops, not seconds or minutes
  - TTL=1 is the first router, TTL=2 is the second router, etc.
- Not all devices will reply with ICMP Time Exceeded
  - Some firewalls filter ICMP
  - ICMP is low-priority for many devices

**Flavors of traceroute**
- Not all traceroutes are the same
  - Minor differences in the transmitted payload
- Windows commonly sends ICMP echo requests
  - Receives ICMP time exceeded messages
  - And an ICMP echo reply from the final/destination device
  - Unfortunately, outgoing ICMP is commonly filtered
- Some operating systems allow you to specify the protocol Linux, Unix, macOS, etc.
- IOS devices send UDP datagrams over port 33434
  - The port number can be changed with extended options
  - The mechanics of traceroute

### pathping
- Combine ping and traceroute
  - Included with Windows NT and later
- First phase runs a traceroute
  - Build a map
- Second phase
  - Measure round trip time and packet loss at each hop

## 1.6 - The Windows Control Panel

**Internet Options**
- General - Basic display
- Security - Different access based on site location
- Privacy - Cookies, pop-up blocker, InPrivate browsing
- Content - Certificates and auto-complete
- Connections - VPN and proxy settings
- Programs - Default browser, plugins, etc.
- Advanced - Detailed configuration options (and reset!)

**Devices and Printers**
- Everything on the network
  - Desktops, laptops, printers, multimedia devices, storage
- Quick and easy access
  - Much less complex than Device Manager
  - Properties, device configurations

**Programs and Features**
- Installed applications - Uninstall, size, version
- Windows features - Enable and disable

**Network and Sharing Center**
- All network adapters - Wired, wireless, etc.
- All network configs
  - Adapter settings, network addressing

**System**
- Computer information
  - Including version and edition
- Performance
  - Virtual memory
- Remote settings
- System protection

**Windows Defender Firewall**
- Protect from attacks
  - Scans, malicious software
- Integrated into the operating system
- Control Panel > Windows Firewall

**Mail**
- Icon does not appear unless a mail client, e.g., Outlook, is installed
  - Otherwise not an option
- Access to local mail configuration
  - Account information, data files

**Sound**
- Output options
  - Multiple sound devices may be available
- Set levels for output and input
  - Speakers and microphone

## 1.6 - The Windows Control Panel (continued)

**User Accounts**
- Local user accounts
  - Domains accounts are stored elsewhere
- Account name and type
- Change password
- Change picture
- Certificate information

**Device Manager**
- The OS doesn't know how to talk directly to most hardware
  - You need drivers
- Manage devices
  - Add, remove, disable
- First place to go when hardware isn't working
  - Instant feedback

**Indexing Options**
- Speed up the search process
  - Constantly updates an index
- Searches browser history and user folders
  - Good default options
- Add other locations
  - Modify to include other folders

**Administrative Tools**
- Not commonly used utilities
  - Used for system administration
- Useful system tools
  - Often used options for system administrators and technicians

**File Explorer Options**
- Manage File Explorer - Many options
- General - Windows, expand folders
- View - View hidden files, hide extensions
- Search
  - Disable index searches, search non-indexed areas

**Power Options**
- Hibernate
  - Open docs and apps are saved to disk
  - Common on laptops - Used by Fast Startup
- Sleep (standby)
  - Open apps are stored in memory
  - Save power, startup quickly
  - Switches to hibernate if power is low
- Power plans - Customize power usage
- Choose what closing the lid does
  - Useful for docking stations
- USB selective suspend
  - Disable individual USB devices
  - Save power
  - Fingerprint readers, biometrics
- Fast startup
  - Enable or disable - Useful for troubleshooting

**Ease of Access Center**
- Usability enhancements - Useful for everyone
- Change display, keyboard, mouse, and other input/output options
  - Use Windows without a display
  - Change the mouse pointers

## 1.6 - Windows Settings

**Settings**
- An updated interface
  - A migration from the Control Panel
- One place for most configuration settings
  - A common UI
- Search for "Settings", Or scroll down to "S"

**Time and Language**
- Windows can automatically set the time
  - Active Domain is very sensitive to synchronized clocks
  - Five minutes of tolerance by default
- Windows can speak many different languages
  - Change or add a language

**Update and Security**
- Keep your OS up to date - Security patches, bug fixes
- Automatic installation - Updates are always installed
- Active hours - You control the update time

**Personalization**
- Change the way Windows looks and feels
  - Colors, wallpaper, lock screen
- Extensive customization - Make Windows your own

**Apps**
- Manage installed applications
  - Uninstall or modify an existing app
- Add Windows features
  - Fonts for other languages
  - OpenSSH Server
  - SNMP support

**Privacy**
- Share app activity - Customized advertising
- Share your language - Website content
- Speech recognition - Sends audio to an online service

## 1.6 - Windows Settings (continued)

**System**
- Change display settings
  - Night light, scaling, resolution
- Audio settings
  - Input and output
- Notifications
  - Enable/disable
  - Show on lock screen

**Devices**
- Manage devices
  - Bluetooth, printers, etc.
- Mouse settings
  - Button and wheel options
- Typing and writing
  - Keyboard and pen

**Network and Internet**
- Network settings
  - Internet connectivity
- View Internet status
  - Up or down?
- Change IP settings
  - Modify address information

**Gaming**
- Xbox Game Bar - Xbox gaming network
- Chat, join games - Look for friends

**Accounts**
- Manage login account information
  - Microsoft account or local account
- Email configuration - Specify an email app
- Sign-in options - PIN, password, security key, etc.

## 1.7 - Windows Network Technologies

**Shared resources**
- Make a folder or printer available on the network
  - "Share" with others, view in File Explorer
- Assign (map) a drive letter to a share
  - Access a file server
  - Reconnect automatically
- Shares ending with a dollar sign ($) are "hidden"
  - Not a security feature
- Administrative Tools > Computer Management

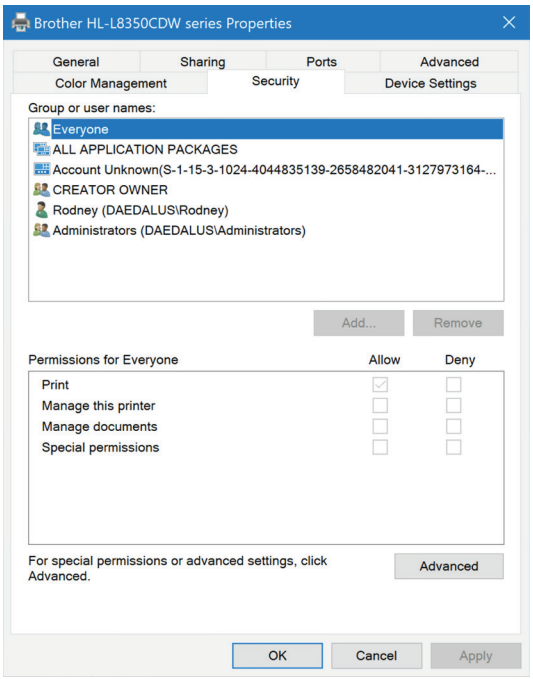
**Organizing network devices**
- Windows Workgroups
  - Logical groups of network devices
  - Each device is a standalone system, everyone is a peer
- Windows Domain
  - Business network
  - Centralized authentication and device access
  - Supports thousands of devices across many networks

**Workgroups**
- Small departments
  - Each computer maintains its own user information
  - Non-centralized
- Manage in Control Panel / System

**Join a domain**
- Cannot be a Windows Home edition
  - Needs to be Pro or better
- Control Panel / System
- Need proper rights to add a computer

**Sharing printers**
- Similar to sharing a folder
  - But it's a printer instead
- Printer Properties
  - Access through File Explorer, the Settings app, or any other Printer Properties
  - Share an existing printer

**Using a shared printer**
- Similar to sharing a folder
  - But it's a printer instead
- Add a printer
  - File Explorer
  - Settings app



## 1.7 - Configuring Windows Firewall

**Windows Defender Firewall**
- Your firewall should always be enabled
  - Sometimes you need to troubleshoot
- Temporarily disable from the main screen
  - Turn Windows Firewall on or off
  - Requires elevated permissions
- Different settings for each network type
  - Public / Private

**Windows Firewall configuration**
- Block all incoming connections
  - Ignores your exception list
  - Useful when you need the most security
- Modify notification
  - App blocking

**Creating a firewall exception**
- Allow an app or feature through Windows Firewall
  - The more secure exception
- Port number
  - Block or allow
- Predefined exceptions
  - List of common exceptions
- Custom rule
  - Every firewall option

## 1.7 - Windows IP Address Configuration

**How Windows gets an IP address**
- DHCP (Dynamic Host Configuration Protocol)
  - Automatic IP addressing - this is the default
- APIPA (Automatic Private IP Addressing)
  - There's no static address or DHCP server
  - Communicate locally (link-local address)
  - Assigns 169.254.1.0 to 169.254.254.255
  - No Internet connectivity
- Static address
  - Assign all IP address parameters manually
  - You need to know very specific details

**TCP/IP host addresses**
- IP Address – Unique identifier
  Subnet mask – Identifies the subnet
  Gateway – The route off the subnet to the rest of the world
- DNS – Domain Name Services
  - Converts domain names to IP addresses
- DHCP – Dynamic Host Configuration Protocol
  - Automates the IP address configuration process
- Loopback address - 127.0.0.1 - It's always there!

**A backup for the DHCP server**
- Multiple DHCP servers should be installed for redundancy
  - There will always be one available
- If a DHCP server isn't available, Windows uses the Alternate Configuration
  - The default is APIPA addressing
- You can also configure a static IP address
  - Keep working normally

## 1.7 - Windows Network Connections

**Network setup**
- Control Panel
  - Network and Sharing Center
  - Set up a new connection or network
- Step-by-step wizard
  - Confirmation during the process
- Many different connections
  - Direct, VPN, dial-up, etc.

**VPN connections**
- Built-in VPN client
  - Included with Windows
  - Connect to a workplace
- Integrate a smart card
  - Multi-factor authentication
    - Something you know, something you have, something you are
- Connect from the network status icon
  - Click and provide credentials

**Wireless connections**
- Network name - SSID (Service Set Identification)
- Security type - Encryption method
- Encryption type - TKIP, AES
- Security key
  - WPA2/3-Personal - Pre-shared key
  - WPA2/3-Enterprise - 802.1X authentication

**Wired connections**
- Ethernet cable - Direct connection
- Fastest connection is the default - Ethernet, Wireless, WWAN
- Alternate configurations - When DHCP isn't available

**WWAN connections**
- Wireless Wide Area Network
  - Built-in mobile technology
- Hardware adapter - Antenna connections
- USB connected or 802.11 wireless - Tether or hotspot
- Requires third-party software - Each provider is different

## 1.7 - Windows Network Connections (continued)

**Proxy settings**
- Change the traffic flow
  - An Internet go-between
- Settings > Network and Internet
  - Or use Control Panel > Internet Options > Connections > LAN settings
- Define address and exceptions
  - Proxies don't work for everything

**Network locations**
- Private
  - Share and connect to devices
  - Home or work network
- Public
  - No sharing or connectivity
  - Public Wi-Fi
- Customize security settings
  - Profile is determined automatically
  - Change the settings at any time

**Network paths**
- View network paths in File Explorer
  - Server and share name
- Map network drive
  - Add a drive letter
- Disconnect
  - Toolbar - Right-click the drive

**Mapping drives**
- Access a share
  - This PC / Map network drive
- Local drive letter and share name
  - May require additional authentication
- Or use the command line:

```
net use h: "\\Daedalus\Gate Room"
```

**Metered Connections**
- Reduce data usage
  - Slow network links
  - Limited bandwidth
  - Usage-based billing
- Can modify application communication
  - Windows Updates, OneDrive sync

## 1.8 - macOS Overview

**File types**
- .dmg
  - Apple Disk Image
  - Mountable as a drive in Finder
- .pkg
  - Installer Package
  - Used to distribute software
  - Runs through an installer script
- .app
  - Application bundle
  - Contains the necessary files to use the application
  - "View Package Contents" from the Finder

**App store**
- Centralized updates and patches
  - For both OS and apps
- App Store application
  - The "Updates" option
- Automatic updates - Or manual install
- Patch management
  - Install and view previous updates

**Uninstallation process**
- Move the .app file to the Trash
- The .app package contains all of the application files
- Quick and easy
- Some applications include a separate uninstall program
  - Usually included in the Application folder

**macOS system folders**
- /Applications
  - Manage all applications in the same folder
- /Users
  - User documents are saved in their own folder
  - Folder name matches the User Name
- /Library
  - Support files, scripts, fonts, etc.
  - Used by everyone on the system
- ~/Library
  - Similar preference information, but for a specific user
  - The tilde (~) refers to the home directory (i.e., /Users/Professor)
  - Users shouldn't be directly accessing this data
- /System
  - The operating system files
  - This is similar in function to the \Windows directory

**Apple ID and corporate restrictions**
- Personal Apple products use a personal Apple ID
  - Associated with personal data and digital purchases
- Companies use Managed Apple IDs using Apple Business Manager
  - Integrate with Active Directory
  - Connect with an existing
  - MDM (Mobile Device Manager)
  - Assign and move apps and digital content to selected users

## 1.8 - macOS Overview (continued)

**Backups**
- Time Machine - Included with macOS
- Hourly backups - The past 24 hours
- Daily backups - The past month
- Weekly backups - All previous months
- Starts deleting oldest information when disk is full

**Anti-virus**
- macOS does not include anti-virus
  – Or anti-malware
- Many 3rd-party options
  – From the usual companies
- An emerging threat
  – Still doesn't approach Windows
  – It's all about the number of desktops
- Automate your signature updates
  – New updates every hour / day

**macOS updates and patches**
- System Settings > General > Software Updates
  – Not part of the Apple App Store
- Automatic Updates - Let macOS install new patches
- Beta Updates
  – Get updates before they are public
  – Not a great best practice
  – Very useful for planning in the lab

**Rapid Security Response (RSR)**
- Some patches are more important than others
  – And they need to be installed quickly
  – Zero-day updates, widespread security issues
- Part of Automatic Updates
  – Enable or disable in System Settings
- Also available in iOS and iPadOS
  – Security issues can happen anywhere
- After installation, the macOS version number includes a letter
  – macOS 13.3.1 (a)

## 1.8 - macos System Preferences

**System Preferences**
- The macOS version of the Windows Control Panel
  – A close comparison
- Access to most customization and personalization options
  – Includes important configuration utilities
- A good place to start
  – It's probably in here

**Displays**
- Configure the location of multiple displays
  – Side by side, top to bottom
- Menu can be moved to any display
  – Doesn't have to be the primary
- Modify individual display settings
  – Resolution, brightness, colors

**Network**
- Configure network interfaces - Wired, wireless
- IPv4 and IPv6 - Manual and automatic (DHCP)
- Detailed network settings - IP, DNS, 802.1X, etc.

**Printers & Scanners**
- Add and remove printers and scanners
  – Configure individual settings
- Share printers and scanners
  – Configure rights and permissions
- View status - Ink and toner levels, scanning status

**Privacy**
- Limit application access to private data
  – Location services, photos, calendars
- Control access to cameras and microphones
  – Enable on a per-app basis
- Unauthorized apps can't view your private data
  – Malware, other apps

**Accessibility**
- Allow apps to use system input
  – Keyboard, mouse, audio, video
- Scripting and automation
  – Requires access for input
- Limits third-party applications
  – Can't take over the keyboard

**Time Machine**
- Automated backups
  – Included with macOS
- Hourly backups
  – The past 24 hours
- Daily backups
  – The past month
- Weekly backups
  – All previous months
- Starts deleting oldest information when disk is full

# 1.8 - macos Features

**Mission Control and Spaces**
- Quickly view everything that's running
  - Spread out the desktop into a viewable area
  - Swipe upwards with three fingers or
  - Control-Up arrow
- Spaces
  - Multiple desktops
  - Add Spaces inside of
  - Mission Control

**Keychain**
- Password management
  - Passwords, notes, certificates, etc.
- Integrated into the OS - Keychain Access
- Passwords and Secure Notes are encrypted
  - Login password is the key

**Spotlight**
- Find files, apps, images, etc.
  - Similar to Windows search
- Magnifying glass in upper right
- Or press Command-Space
- Type anything in - See what you find
- Define search categories in System Preferences / Spotlight
  - Enable/disable categories

**iCloud**
- Integrates Apple technologies
  - macOS, iOS, iPadOS
- Share across systems
  - Calendars, photos, documents, contacts, etc.
- Backup iOS devices
  - Never lose data again
- Store files in an iCloud drive
  - Similar to Google Drive, Dropbox
  - Integrated into the operating systems
- iMessage/Messages
  - iMessage is the service,
  - Messages is the app
- FaceTime
  - Audio/video conferencing
- Drive
  - Cloud-based file storage
  - Integrated into the Apple apps
- Configure sync options in the Apple Account section

**Gestures**
- You can do more than just point and click
  - Extend the capabilities of your trackpad
- Use one, two, three fingers
  - Swipe, pinch, click
- Customization
  - Enable/disable
  - System Preferences / Trackpad

**Finder**
- The central OS file manager - Compare with File Explorer
- File management - Launch, delete, rename, etc.
- Integrated access to other devices
  - File servers, remote storage, screen sharing

**Remote Disc**
- Use an optical drive from another computer
  - Has become more important over time
  - Designed for copying files
  - Will not work with audio CDs or video DVDs
- Set up sharing in System Preferences
  - Sharing options - Appears in the Finder

**Dock**
- Fast access to apps - Quickly launch programs
- View running applications - Dot underneath the icon
- Keep folders in the dock - Easy access to files
- Move to different sides of the screen
  - Auto-hide or always display

**Continuity**
- Work easily between devices
  - iPhone to iPad to macOS to others
- Share resources across operating systems
  - Use an iPhone as a Mac webcam
  - Mirror iPhone screen
  - Forward text messages
  - Airdrop files
  - And lots more
- Synchronized through iCloud

**Disk Utility**
- Manage disks and images - Resolve issues
- File system utilities
  - Verify and repair file systems, modify partition details, erase disks
- Create, convert, and restore images
  - Manage disk images

**FileVault**
- Full Disk Encryption (FDE) for macOS
  - Decryption uses a local key or iCloud authentication
- Proper authentication is required before macOS can start
  - Data is unavailable to others
- Available in System Preferences
  - Security & Privacy > FileVault

## 1.8 - macos Features (continued)

**Terminal**
- Command line access to the operating system
  - Manage the OS without a graphical interface
- OS access
  - Run scripts, manage files
  - Configure OS and application settings

**Force Quit**
- Stop an application from executing
  - Some applications are badly written
- Command-Option-Escape - List application to quit
- Hold the option key when right-clicking the app icon in the dock
  - Choose Force Quit

## 1.9 - Linux

**Linux**
- Free Unix-compatible software system
- Unix-like, but not Unix
- Many (many) different distributions
  - Ubuntu, Debian, Red Hat
- Advantages
  - Cost. Free!
  - Works on wide variety of hardware
  - Passionate and active user community
- Disadvantages
  - Limited driver support, especially with newer hardware
  - Limited support options

**Bootloader**
- How does your computer know the location of the operating system?
  - It could be on any storage device
- The BIOS knows which device is used for booting
  - You can change it in the BIOS configuration
- The BIOS runs the bootloader
  - Located in the boot sector of the specified boot drive
  - The bootloader then starts the operating system

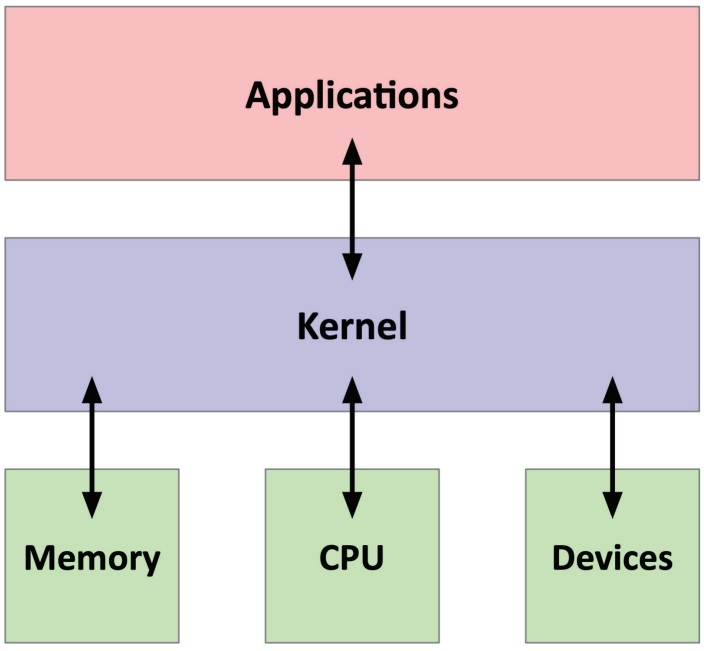
**The kernel**
- The core of the operating system
  - It sees and controls the system
- Manages application execution
  - Start system processes
  - Interact with devices
- Kernel space is a protected area
  - Applications run in user space
- Kernel upgrades
  - Bug fixes, security patches, additional device support

**systemd**
- A system and service manager
  - Starts, stops, and manages important daemons
  - Logging, networking, user sessions, login
  - Not just one utility - a suite of software
- Started by the kernel
  - All other processes are launched by systemd
  - Or child processes of systemd
- Manage all of the system daemons with a common set of tools
  - Easy to follow, understand, and troubleshoot

**Root account**
- A system and service manager
  - Similar in function to the Windows “Administrator”
- The root user has full control
  - User ID of 0
  - Run any command
  - Modify any file in the system
  - Change rights and permissions
- Required to perform many admin functions
  - Installing software
  - Updating the operating system
  - Changing file ownership

**Configuration files**
- Linux can be managed at the command line
  - Does not require a graphical user interface
  - Most servers don’t even install a graphical desktop
- Most application and service parameters are configured in a text file
  - It’s relatively easy to make changes
  - All you need is a text editor

**The kernel**



## 1.9 - Linux (continued)

### /etc/passwd
- A list of registered users
  - And other information, parsed with a colon
- The file format
  - Username
  - Password
  - User ID (UID)
  - Group ID (GID)
  - User ID Info
  - Home directory
  - Command or shell

### /etc/shadow
- All of your account passwords
  - A text file
- The format
  - Username
  - Password hash
  - Date of last password change
  - Minimum days
  - Maximum days
  - Warning days
  - Inactive days
  - Expiration date

### /etc/hosts
- Resolve an IP address from a FQDN
  - Fully Qualified Domain Name
  - www.professormesser.com = 10.1.10.222
- This was the first method of name resolution
  - Put all of your names and
  - IP addresses in a file
- Why not just use DNS?
  - You might want to override the DNS settings

### /etc/resolv.conf
- DNS is important
  - We can't remember every IP address
- Almost every service uses DNS
  - A misconfiguration can cause many issues
- Confirm all DNS details
  - Check **/etc/resolv.conf**

### /etc/fstab
- Linux File Systems Table
  - Lists all of the system disks and partitions
- The **mount** command reads the **/etc/fstab** configuration file
  - Provides access through the file system
- Runs automatically on startup
  - If a drive or directory is missing, check **/etc/fstab**

## 1.9 - Linux Commands Part 1

**Linux commands**
- The command line - Terminal, XTerm, or similar
- Commands are similar in both Linux and macOS
  - Mac OS derived from BSD (Berkeley Software Distribution) Unix
  - This section is specific to Linux
- Download a Live CD or install a virtual machine
  - Many pre-made Linux distributions are available
- Use the **man** command for help - An online manual

```
> man grep
```

### ls
- List directory contents
  - Similar to the dir command in Windows
- Lists files, directories
  - May support color coding;
  - Blue is a directory, red is an archive file, etc.
- For long output, pipe through more:

```
> ls -l | more
```

(use **q** or **Ctrl-c** to exit)

### pwd
- Print Working Directory
  - Displays the current working directory path
  - Useful when changing directories often

### mv
- Move a file or rename a file
- **mv SOURCE DEST**

```
> mv first.txt second.txt
```

### cp
- Copy a file - Duplicate files or directories
- **cp SOURCE DEST**

```
> cp first.txt second.txt
```

### rm
- Remove files or directories - Deletes the files
- Does not remove directories by default
  - Directories must be empty to be removed or must be removed with **-r**

### chown
- Change file owner and group - Modify file settings
- **sudo chown [OWNER:GROUP] file**

```
> sudo chown professor script.sh
```

### grep
- Find text in a file
  - Search through many files at a time

```
grep PATTERN [FILE]
> grep failed auth.log
```

# 1.9 - Linux Commands Part 1 (continued)

## chmod

- Change mode of a file system object
  - r=read, w=write, x=execute
  - Can also use octal notation
  - Set for the file owner (u), the group(g), others(o), or all(a)
- **chmod mode FILE**
  **> chmod 744 script.sh**
- **chmod 744 first.txt**
  - User; read, write, execute
  - Group; read only
  - Other; read only
- **chmod a-w first.txt**
  - All users, no writing to first.txt

| # | Permission | r w x |
|---|---|---|
| 7 | Read, Write, and Execute | r w x |
| 6 | Read and Write | r w - |
| 5 | Read and Execute | r - x |
| 4 | Read only | r - - |
| 3 | Write and Execute | - w x |
| 2 | Write only | - w - |
| 1 | Execute only | - - x |
| 0 | none | - - - |

- **chmod u+x script.sh**
  - The owner of script.sh can execute the file

## find

- Find a file by name or extension
  - Search through any or all directories
- Find files with a specific extension
  **> find . -name "*.txt"**

## fsck

- File System Check
  - Check the file system for logical errors
  - File size inconsistencies, orphaned files
  - Similar in function to Windows **chkdsk** utility
- Repairs issues
  - Runs during startup
  - Non-mounted or read-only volume

## mount

- Associates a storage device with the file system
  - Assigns it to a directory name
  - Similar in functionality to the Windows **net use** command
- View all mount points
  - There might be a big list
- Manually mount a storage device, i.e., USB
  - If your distribution doesn't mount automatically

## su / sudo

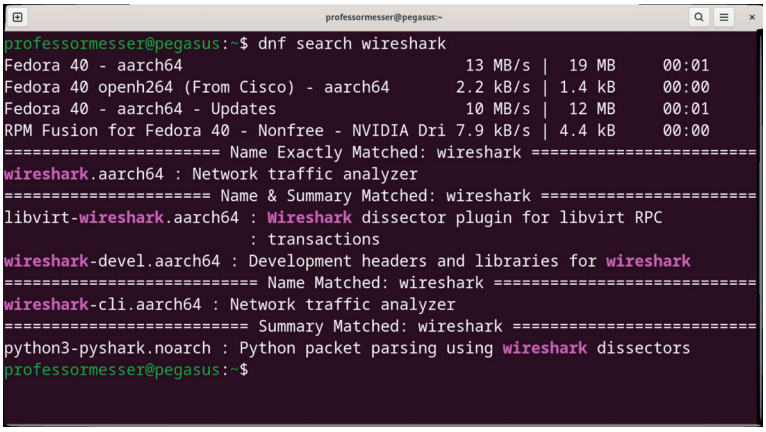
- Some commands require elevated rights
- **sudo**
  - Execute a command as the super user or user ID
  - Only that command executes as the super user
- **su**
  - Become super user or change to a different user
  - You continue to be that user until you exit

## apt

- Advanced Packaging Tool
  - Handles the management of application packages
  - Applications and utilities
- Install, update, remove
- **> sudo apt install wireshark**

## dnf

- Dandified YUM
  - Another package manager for Linux
  - Install, delete, update
- Replaces Yellowdog Updater, Modified (yum)
  - Almost identical in use and syntax
- Manages RPM packages
  - Red Hat Package Manager
  - RPM Package Manager
  - A Linux distribution will commonly use either **dnf** or **apt**



# 1.9 - Linux Commands Part 2

## ip
- Manage the network interfaces
  - Enable, disable, configure addresses, manage routes, ARP cache, etc.
- **ip address**
  - View interface addresses
- **ip route**
  - View the IP routing table
- **sudo ip address add 192.168.121.241/24 dev eth0**
  - Configure the IP address of an interface

## ping
- Test reachability
  - Determine round-trip time
  - Uses Internet Control Message Protocol (ICMP)
- One of your primary troubleshooting tools
  - Can you ping the host?
- **ping <ip address>** - Test reachability to a TCP/IP address
- **ping -t <ip address>** - Ping until stopped with Ctrl-c
- **ping -n <count> <ip address>**
  Send # of echo requests

## curl
- Client URL
  - Retrieve data using a URL
  - Uniform Resource Locator
  - Web pages, FTP, emails, databases, etc.
- Grab the raw data
  - Search
  - Parse
  - Automate

## dig
- Lookup information from DNS servers
  - Canonical names, IP addresses, cache timers, etc.
- **dig** (Domain Information Groper)
  - Detailed domain information

## traceroute
- Determine the route a packet takes to a destination
  - Map the entire path
  - **tracert** (Windows) or **traceroute** (Unix/Linux/macOS)
- Takes advantage of ICMP Time to Live Exceeded error message
  - The time in TTL refers to hops, not seconds or minutes
  - TTL=1 is the first router, TTL=2 is the second router, etc.
- Not all devices will reply with ICMP Time Exceeded messages
  - Some firewalls filter ICMP
  - ICMP is low-priority for many devices
- **traceroute <ip address>**

## man
- Display a system reference manual
  - Command documentation
- man page
  - Displays the manual for the provided command
  - Displays in a full-page viewer
  - Press “q” to quit

## cat
- Concatenate - Link together in a series
- Copy a file/files to the screen
  ```
  cat file1.txt file2.txt
  ```
- Copy a file/files to another file
  ```
  cat file1.txt file2.txt > both.txt
  ```

## top
- View CPU, RAM, and resource utilizations
  - The “Task Manager” for Linux
- Process information
  - Easy to find the highly utilized applications
- Summary of overall load
  - One, five, and fifteen minutes
- Many different options
  - Check the man page for startup options and keys

## ps
- View the current processes
  - And the process ID (PID)
  - Similar to the Windows Task Manager
- View user processes
  ```
  ps
  ```
- View all processes
  ```
  ps -e | more
  ```

## df
- Disk Free - View file systems and free space
- **df**
  - View number of blocks
- **df -h**
  - View human-readable sizes

## du
- Disk usage
  - Show the storage space used by file or directory
- Find which files are using the most space
  - A common challenge
- **du -h**
  - Human-readable output
  - Displays in bytes / KB / MB
  - View number of blocks

## nano
- Full-screen text editor - Easy to edit
- Included with many Linux distributions - Easy to install
- Select, mark, copy/cut, and paste text
  - Similar features to graphical-based editors

# 1.10 - Installing Applications

**Installing applications**
- Extend the functionality of your operating system
  - Specialized applications
- Available everywhere
  - Find the application you need
  - Install on your operating system
- Not every computer can run every application
  - Some simple checks can help manage your desktop

**Operating system platform**
- 32-bit vs. 64-bit
  - Processor specific
- 32-bit processors can store $2^{32}$ = 4,294,967,296 values
- 64-bit processors can store $2^{64}$ = 18,446,744,073,709,551,616 values
  - 4 GB vs. 17 billion GB
  - The OS has a maximum supported value
- Hardware drivers are specific to the OS version
  - 32-bit (x86), 64-bit (x64)
- 32-bit OS cannot run 64-bit apps
  - But 64-bit OS can run 32-bit apps
- Apps in a 64-bit Windows OS
  - 32-bit apps: \Program Files (x86)
  - 64-bit apps: \Program Files

**Graphics requirements**
- Integrated graphics
  - CPU and GPU are the same chip
  - Uses system memory for graphics
  - Common in laptops
- Dedicated graphics card
  - Also called a discrete graphics card
  - Uses its own VRAM (Video RAM)
  - High-end graphics requirements
- Check the application
  - Integrated or dedicated
  - VRAM requirements

**RAM requirements**
- Random Access Memory
  - Memory modules
- A critical specification
  - Application may perform poorly
  - Or not at all
- This would be above and beyond the OS requirements
  - Dependent on the application
  - Consider all of the other running applications

**CPU requirements**
- Central Processing Unit
  - Processing speed
  - Usually measured in gigahertz (GHz)
- A broad measurement
  - Higher numbers are faster CPUs
- Application requirements vary
  - Word processing vs. video editing

**External hardware tokens**
- Manage application usage
  - Limit access to authorized users
- Application will only operate with the hardware token connected
  - Commonly a USB device
  - Can be a challenge to manage
- Often used with high-end software
  - High per-seat licensing costs

**Storage requirements**
- Drive space concerns
  - Initial installation space requirement
  - Application use requirement
- Some applications use a LOT of storage space after installation
  - The initial install requirements may not be the most important specification

**Distribution methods**
- Downloadable
  - Direct from the manufacturer
  - Centralized app store
  - Avoid 3rd-party downloads
- Physical media
  - Optical media, USB drive, etc.
  - Increasingly rare

**ISO files**
- Optical disk image
  - A single ISO file / ISO image
  - Files and folders
- Sector by sector copy of the data on an optical disc
  - ISO 9660 file system
  - International Organization for Standardization
- Mount in the OS
  - Appears as a separate drive

## 1.10 - Installing Applications (continued)

**Image deployment**

- Install everything at one time
  - Including the operating system
  - The application is included with the image
- Often designed for a specific platform
  - Device drivers to match the hardware
- A perfect option for virtual machines
  - All of the hardware is "virtually" identical
- Very fast deployment
  - No questions to answer
  - The image is a perfect and complete system build

**Installation considerations**

- There's a reason we are careful when installing applications
  - Applications have the same rights and permissions as the user
  - An unknown application can cause significant issues
- Impact to device
  - Application upgrade stops working
  - Slowdowns
  - Deleted files
- Impact to network
  - Access to internal services
  - Rights and permissions to file shares
- Impact to operation
  - Many jobs are time-sensitive
  - An updated application may require a change to the workflow
  - Or may not work at all
- Impact to the business
  - Critical processes are sensitive to downtime and outages
  - A change to an application can create issues
  - Other parts of the business rely on your results

## 1.11 - Cloud Productivity Tools

**Cloud productivity tools**

- The cloud has changed everything
  - We no longer run our own data centers
- We can run almost any service in the cloud
  - The technology can exist anywhere
- Instant access to resources
  - One click server farms
- "Infinite" scalability
  - Need more CPU/storage/network?
  - Pay for what you use

**Email systems**

- A mission critical service
  - Continues to be our primary communication method
- The email server is in the cloud
  - Better connectivity
  - Faster communication
  - Integrated redundancy and backups
  - Centralized security services
- Many different services
  - Outlook in the Microsoft Cloud
  - Google Workspace email

**Storage**

- The cloud brings enormous capacity
  - Seemingly unlimited storage
- Synchronization
  - Save a file locally
  - It's automatically uploaded to the cloud
  - And downloaded to all other registered devices
- Folder settings
  - Select which folders are stored
  - Choose local or streaming access

**Collaboration tools**

- Work with others in real-time
  - Or near real-time
- A more creative way to work with others
  - Spreadsheets, video conferencing, presentation tools, word processing tools, instant messaging
- The cloud brings it together
  - Access from anywhere

**Identity synchronization**

- We used to have one directory
  - Maintained at our local site
- Cloud applications are everywhere
  - And can use many different identity providers
  - Microsoft Entra ID, Okta, Google Identity, etc.
- Directory synchronized identity
  - Changes in one directory are sync'd to others
- New user?
  - Appears in remote directories automatically
  - Make the change in one place

**Licensing assignment**

- Users are no longer associated with a single device
  - And applications are no longer on a local device
  - Physical license keys aren't very useful or manageable
- License in the cloud
  - No paper license keys to lose
- Centralized management
  - See every license you own
  - Move licenses between users
  - No wasted licenses!

# 2.1 - Physical Security

**Barricades / bollards**
- Prevent access
  - There are limits to the prevention
- Channel people through a specific access point
  - And keep out other things
  - Allow people, prevent cars and trucks
- Identify safety concerns
  - And prevent injuries
- Can be used to an extreme
  - Concrete barriers / bollards
  - Moats

**Access control vestibule**
- All doors normally unlocked
  - Opening one door causes others to lock
- All doors normally locked
  - Unlocking one door prevents others from being unlocked
- One door open / other locked
  - When one is open, the other cannot be unlocked
- One at a time, controlled groups
  - Managed control through an area

**Badge reader**
- Magnetic swipe, RFID, or NFC
  - Many different identification methods
- Different applications
  - Time clocks
  - Security guard patrols
  - Door access

**Video surveillance**
- CCTV (Closed circuit television)
  - Can replace physical guards
- Camera features are important
  - Object detection can identify a license plate or person's face
- Often many different cameras
  - Networked together and recorded over time
- Motion detection
  - Radio reflection or passive infrared
  - Useful in areas not often in use

**Alarm systems**
- Circuit-based
  - Circuit is opened or closed
  - Door, window, fence
  - Useful on the perimeter
- Motion detection
  - Identify motion without a camera
- Duress
  - Triggered by a person
  - The big red button

**Door locks**
- Conventional - Lock and key
- Deadbolt - Physical bolt
- Electronic - Keyless, PIN
- Token-based - RFID badge, magnetic swipe card, or key fob
- Biometric - Hand, fingers or retina
- Multi-factor - Smart card and PIN

**Equipment locks**
- Data center hardware is usually managed by different groups
  - Responsibility lies with the owner
- Racks can be installed together
  - Side-to-side
- Enclosed cabinets with locks
  - Ventilation on front, back, top, and bottom

**Guards and access lists**
- Security guard
  - Physical protection at the reception area of a facility
  - Validates identification of existing employees
  - Provides guest access
- ID badge
  - Picture, name, other details
  - Must be worn at all times
- Access list
  - Physical list of names
  - Enforced by security guard
- Maintains a visitor log

**Fences**
- Build a perimeter
  - Usually very obvious
  - May not be what you're looking for
- Transparent or opaque
  - See through the fence (or not)
- Robust
  - Difficult to cut the fence
- Prevent climbing
  - Razor wire
  - Build it high

# 2.1 - Physical Access Security

**Key fobs**
- Small RFID key
  - Add to physical keychain
- Replaces a physical key
  - Commonly used for door locks
  - Proximity operation and contactless

**Smart cards**
- Certificate-based authentication
  - Something you have
  - Usually requires additional factors
- Integrated card reader
  - Built into the laptop
- External reader
  - USB connected

**Mobile digital key**
- Replace physical keys
  - With your phone
- Many different apps
  - Automobile unlocking and starting
  - Hotel or office door locks
  - Doors at home
- Better authentication than a physical key
  - Must have access to the phone
  - Unlock for verification

**Keys**
- Some doors may not have an electronic lock
  - Rarely used
  - Standalone locks
  - Safe, storage bin, cabinet
- Use a key cabinet
  - Formal check in/check out
  - Well-defined storage location
  - Allows for auditing and timestamps

**Biometrics**
- Biometric authentication
  - Usually stores a mathematical representation of your biometric
  - Your actual fingerprint isn't usually saved
- Difficult to change
  - You can change your password
  - You can't change your fingerprint
- Used in very specific situations
  - Not foolproof

**Biometric factors**
- Retina scanner
  - Unique capillary structure in the back of the eye
- Fingerprint scanner - Phones, laptops, door access
- Palmprint scanner - Shape of the hand and fingers

**Facial recognition technology (FRT)**
- Authenticate using a common biometric feature
  - Authenticate using a common biometric feature
  - Your face
- Create a digital "key" from your facial features
  - Laser dot projector
  - Infrared camera
  - 3D facial map
- Use for any secure authentication
  - Mobile devices, doors, financial, etc.
- Relatively secure
  - 1 in 1,000,000 false acceptance rate

**Voice recognition technology**
- Use an individual's voice as a key
  - Voice authentication
- The system is "trained" by speaking phrases
  - The results are evaluated and stored
- Verify yourself with a different phrase
  - Voice recognition software can listen for the original speaker
- Questionable security
  - May be best combined with other factors
  - You may not always be able to speak

**Lighting**
- More light means more security
  - Attackers avoid the light
  - Easier to see when lit
  - Non IR cameras can see better
- Specialized design
  - Consider overall light levels
  - Lighting angles may be important
  - Facial recognition
  - Avoid shadows and glare

**Magnetometers**
- Passive scanning - Detect metal objects
- Not useful for non-metal objectives
  - Won't identify ceramic or plastic

# 2.1 - Logical Security

**Least privilege**
- Rights and permissions should be set to the bare minimum
  - You only get exactly what's needed to complete your objective
- All user accounts must be limited
  - Applications should run with minimal privileges
- Don't allow users to run with administrative privileges
  - Limits the scope of malicious behavior

**Zero trust**
- Many networks are relatively open on the inside
  - Once you're through the firewall, there are few security controls
- Zero trust is a holistic approach to network security
  - Covers every device, every process, every person
  - Everything must be verified
- Nothing is inherently trusted
  - Multi-factor authentication, encryption, system permissions, additional firewalls, monitoring and analytics, etc.

**Access Control Lists (ACLs)**
- Used to allow or deny traffic
  - Also used for NAT, QoS, etc.
  - Commonly used on the ingress or egress of a router interface
- ACLs evaluate on certain criteria
  - Source IP, Destination IP,
  - TCP port numbers, UDP port numbers, ICMP
- Deny or permit
  - What happens when an ACL matches the traffic?
- Also used in operating systems
  - Allow or deny access to the filesystem

**Multi-factor authentication**
- Prove who you are
  - Use different methods
  - A memorized password, a mobile app, and your location
- Factors
  - Something you know, something you have, something you are, somewhere you are
- There are other factors as well

**Email authentication**
- Associate a person with an email address
  - Validate a person at that email
- Useful during registration
  - Verify a user's email address
- Use instead of a password
  - Username is your email
- Can be helpful at a later date
  - Password resets
  - Validation code delivery

**Authentication apps**
- Pseudo-random token generators
  - A useful authentication factor
- Carry around a physical hardware token generator
  - Where are my keys again?
- Use software-based token generator on your phone
  - Powerful and convenient

**Short message service (SMS)**
- Text messaging
  - Includes more than text these days
- Login factor can be sent via SMS to a predefined phone number
  - Provide username and password
  - Phone receives an SMS
  - Input the SMS code into the login form
- Security issues exist
  - Phone number can be reassigned to a different phone
  - SMS messages can be intercepted
  - SMS spoofing

**Voice call**
- A phone call provides the token
  - The computer is talking to you
  - "Your code is 1-6-2-5-1-7."
- Similar disadvantages to SMS
  - Phone call can be intercepted or forwarded
  - Phone number can be added to another phone

**TOTP**
- Time-based One-Time Password algorithm
  - Use a secret key and the time of day
  - No incremental counter
- Secret key is configured ahead of time
  - Timestamps are synchronized via NTP
- Timestamp usually increments every 30 seconds
  - Put in your username, password, and TOTP code
- One of the more common OTP methods
  - Used by Google, Facebook, Microsoft, etc.

**OTP**
- One-Time passwords
  - Use them once, and never again
  - Once a session, once each authentication attempt
- One-Time Password algorithm
  - The keys are based on a secret key and a counter
- Token-based authentication
  - The hash is different every time
- Hardware and software tokens available
  - You'll need additional technology to make this work

# 2.1 - Authentication and Access

**Security Assertion Markup Language (SAML)**
- Open standard for authentication and authorization
  - You can authenticate through a third-party to gain access
  - One standard does it all, sort of
- Not originally designed for mobile apps
  - This has been SAML's largest roadblock

**Single sign-on (SSO)**
- Provide credentials one time
  - Get access to all available or assigned resources
  - No additional authentication required
- Usually limited by time
  - A single authentication can work for 24 hours
  - Authenticate again after the timer expires
- The underlying authentication infrastructure must support SSO
  - Not always an option

**Just-in-time access**
- In many organizations, the IT team is assigned administrator/root elevated account rights
  - This would be a great account to attack
- Grant admin access for a limited time
  - No permanent administrator rights
  - The principle of least privilege
- A breached user account never has elevated rights
  - Narrow the scope of a breach
- Request access from a central clearinghouse
  - Grants or denies based on predefined security policies
- Password vaulting
  - Primary credentials are stored in a password vault
  - The vault controls who gets access to credentials
- Accounts are temporary
  - Just-in-time process creates a time-limited account
  - Administrator receives ephemeral credentials
  - Primary passwords are never released
  - Credentials are used for one session then deleted

**Privileged access management (PAM)**
- A broader approach to manage superuser access
  - Administrator and Root
  - Just-in-time access is part of PAM
- Store privileged accounts in a digital vault
  - Access is only granted from the vault by request
  - These privileges are temporary
- PAM advantages
  - Centralized password management
  - Enables automation
  - Manage access for each user
  - Extensive tracking and auditing

**Mobile Device Management (MDM)**
- Manage company-owned and user-owned devices
  - BYOD - Bring Your Own Device
- Centralized management of the mobile devices
  - Specialized functionality
- Set policies on apps, data, camera, etc.
  - Control the remote device
  - The entire device or a "partition"
- Manage access control
  - Force screen locks and PINs on these devices

**Data Loss Prevention (DLP)**
- Where's your data?
  - Social Security numbers, credit card numbers, medical records
- Stop the data before the attacker gets it - Data "leakage"
- So many sources, so many destinations
  - Often requires multiple solutions
  - Endpoint clients, Cloud-based systems, Email, cloud storage, collaboration tools

**Identity and Access Management (IAM)**
- Applications are available anywhere
  - Desktop, browser, mobile device, etc.
- Data can be located anywhere
  - Cloud storage, private data centers, etc.
- Many different application users
  - Employees, vendors, contractors, customers
- Give the right permissions to the right people at the right time
  - Prevent unauthorized access
- Identify lifecycle management
  - Every entity (human and non-human) gets a digital identity
- Access control
  - An entity only gets access to what they need
- Authentication and authorization
  - Entities must prove they are who they claim to be
- Identity governance
  - Track an entity's resource access
  - May be a regulatory requirement

**Directory services**
- A database of everything on the network
  - Computers, user accounts, file shares, printers, groups, and more
  - Primarily Windows-based (Active Directory)
- Manage authentication
  - Users login using their AD credentials
- Centralized access control
  - Determine which users can access resources
- Commonly used by the help desk
  - Reset passwords, add and remove accounts

## 2.2 - Defender Antivirus

**Microsoft Defender Antivirus**
- Built-in antivirus for Windows
  - No additional third-party products required
- Included in the Windows Security app
  - Virus & threat protection
- May not specifically display "Defender Antivirus"
  - The name has changed over time
  - Windows Defender
  - Microsoft Defender Antivirus

**Activate or deactivate**
- Don't disable your security protection
  - This is for temporary troubleshooting
  - This will increase risk
  - Make sure you know what you're doing
- Defender Antivirus operates in real-time
  - Enable or disable this feature
- Windows Security app
  - Virus & threat protection settings >
  - Manage settings > Real-time protection

**Updated definitions**
- Antivirus is only as good as the latest signatures
  - It's important to stay up to date
- Virus & threat protection updates
  - Check for updates
- Click the "Check for updates" button
  - Automatic updates are normally configured

## 2.2 - Windows Firewall

**Enabling and disabling Windows Firewall**
- Your firewall should always be enabled
  - Sometimes you need to troubleshoot
- Temporarily disable from the Control Panel or from Windows Security
  - Turn Windows Firewall on or off
  - Requires elevated permissions
- Different settings for each network type
  - Public / Private

**Windows Firewall configuration**
- Block all incoming connections
  - Ignores your exception list
  - Useful when you need security
- Modify notification - App blocking

**Creating a firewall exception**
- Allow an app or feature through Windows Firewall
  - The more secure exception
- Port number
  - Block or allow
- Predefined exceptions
  - List of common exceptions
  - Custom rule
  - Every firewall option

## 2.2 - Windows Security Settings

**Windows authentication**
- Login to the Windows desktop
  - And access network resources
- Local accounts
  - Only associated with a specific Windows device
- Microsoft accounts
  - Sync settings between devices, integrate applications (Skype, Office) with OneDrive, and more
- Windows Domain accounts
  - Centrally managed from Active Directory

**Users and groups**
- Users
  - Administrator - The Windows super-user
  - Guest (Limited access)
  - Standard Users
- Groups
  - Power Users
  - Not much more control than a regular user
  - Permissions removed in Windows Vista and later

**Login options**
- Username / password
  - Common authentication credentials
- Personal Identification Number (PIN)
  - A local access code
- Biometrics - Fingerprint, facial recognition
- Single sign-on (SSO)
  - Windows Domain credentials
  - Sign in one time

**Passwordless authentication**
- Many breaches are due to poor password control
  - Weak passwords, insecure implementation
- Authenticate without a password
  - This solves many password management issues
- You may already be passwordless
  - Facial recognition, security key, Windows Hello
- Passwordless may not be the primary authentication method
  - Used with a password or additional factors

## 2.2 - Windows Security Settings (continued)

**NTFS vs. Share permissions**
- NTFS permissions apply from local and network connections
- Share permissions only apply to connections over the network
  - A "network share"
- The most restrictive setting wins
  - Deny beats allow
- NTFS permissions are inherited from the parent object
  - Unless you move to a different folder on the same volume

**Explicit and inherited permissions**
- Explicit permissions
  - Set default permissions for a share
- Inherited permissions
  - Propagated from the parent object to the child object
  - Set a permission once, it applies to everything underneath
- Explicit permissions take precedence over inherited permissions
  - Even inherited deny permissions

**Run as administrator**
- Administrators have special rights and permissions
  - Editing system files, installing services
- Use rights and permissions of the administrator
  - You don't get these by default, even if you're in the Administrators group
- Right-click the application
  - Run as administrator
  - Or search and click "Run as administrator"

**UAC (User Account Control)**
- Limit software access - Protect your computer
- Standard users
  - Use the network or change your password
- Administrators
  - Install applications or configure Remote Desktop
- Secure Desktop - Limits automated access

**BitLocker**
- Encrypt an entire volume
  - Protects all of your data, including the OS
  - Support for all Windows editions except Home
- Lose your laptop? - Doesn't matter without the password
- Data is always protected
  - Even if the physical drive is moved to another computer
- BitLocker To Go - Encrypt removable USB flash drives

**EFS**
- Encrypting File System
  - Encrypt at the file system level
  - Requires the NTFS file system
- OS support
  - Support for all Windows editions except Home
- Uses password and username to encrypt the key
  - Administrative resets will cause EFS files to be inaccessible

## 2.2 - Active Directory

**Active Directory**
- A database of everything on the network
  - Computers, user accounts, file shares, printers, groups, and more
- Manage authentication
  - Users login using their AD credentials
- Centralized access control
  - Determine which users can access resources
- Commonly used by the help desk
  - Reset passwords
  - Add and remove accounts

**Domain**
- The name associated with this related group of users, computers, and resources
  - Each domain has a name
- Domain controllers store this central domain database
  - Active Directory is the service that manages this directory
- Often referenced when troubleshooting
  - Is this computer on the domain?
  - Can you reset the domain password?

**Joining the domain**
- Manage devices and users
  - Must be part of the Active Directory domain
- Add devices from the System Properties
  - Computer Name
  - Add your domain information
  - Welcome to the domain!
- This can also be automated
  - PowerShell scripting

## 2.2 - Active Directory (continued)

**Assigning a log-in script**
- Automate a series of tasks during login
  - Assign a script to a specific user, group, or OU
- Associate the script with a Group Policy
  - User Configuration > Policies >
  - Windows Settings > Scripts
- Create different login scripts for different OUs
  - Customize based on your needs

**Organizational Units (OU)**
- Keep the (very large) database organized
  - Users, Computers
- Create your own hierarchy
  - Countries, states, buildings, departments, etc.
- Apply policies to an OU
  - Can be very large: Domain Users
  - Can be for a specific group: Marketing, North America, Pegasus galaxy

**Moving objects within organizational units**
- Use the Active Directory Users and Computers (ADUC) tool
  - May need to be installed separately
- Select an object
  - Right-click > Move
  - Move to the target OU
  - Click OK

**Assigning home folders**
- Assign a user Home folder to a network folder
  - Manage and backup files from the network
  - Avoid storing files on the local computer
- When added to the user profile, the directories are automatically created
  - And proper permissions are assigned
- Requires some training
  - Encourage users to store files on the network Home folder

**Applying Group Policy**
- Manage the computers or users with Group Policies
  - Local and Domain policies
  - Group Policy Management Editor
- A central console
  - Login scripts
  - Network configurations (QoS)
  - Security parameters

  Update a client with the **gpupdate** utility:

```
> gpupdate /force
```

**Selecting security groups**
- Create a group
  - Assign permissions to the group
- Set the rights and permissions to the group
  - Add users to the group
- Some built-in groups
  - Users, guests
  - Remote management users
  - Event Log Readers
- Save time
  - Avoid confusion and mistakes

**Configuring folder redirection**
- Some users and applications use the Windows Library folders
  - Desktop, Downloads,
  - Music, Documents, etc.
- Redirect the folders to a network share
  - Group Policy > User Configuration >
  - Windows settings > Folder Redirection
- This is often paired with the Offline Files feature
  - You're not always connected

## 2.3 - Wireless Encryption

**Securing a wireless network**
- An organization's wireless network can contain confidential information
  - Not everyone is allowed access
- Authenticate the users before granting access
  - Who gets access to the wireless network?
  - Username, password, multi-factor authentication
- Ensure that all communication is confidential
  - Encrypt the wireless data
- Verify the integrity of all communication
  - The received data should be identical to the original sent data
  - A message integrity check (MIC)

**Wireless encryption**
- All wireless computers are radio transmitters and receivers
  - Anyone can listen in
- Solution: Encrypt the data
  - Everyone has an encryption key
- Only people with the right key can transmit and listen
  - WPA2 and WPA3

## 2.3 - Wireless Encryption (continued)

**WPA (Wi-Fi Protected Access)**
- 2002: WPA was the replacement for serious cryptographic weaknesses in WEP (Wired Equivalent Privacy)
  - Don't use WEP
- Needed a short-term bridge between WEP and whatever would be the successor
  - TKIP is used in WPA for encryption
  - Ran on existing hardware

**WPA2**
- Wi-Fi Protected Access II (WPA2)
  - WPA2 certification began in 2004
- A replacement for WPA
  - WPA was the bridge between WEP and WPA2
- Used AES for encryption
  - Advanced Encryption Standard
  - A stronger encryption than TKIP in WPA
- Often required a physical access point upgrade
  - AES requires more CPU than TKIP

**WPA3**
- Wi-Fi Protected Access 3 (WPA3)
  - Introduced in 2018
- An upgrade to WPA2
  - Increase to AES cryptographic strength options
  - Increased security for initial key exchange
- Provides encryption even on open networks
  - Protection in your favorite coffee shop

**Wireless security modes**
- Configure the authentication on your wireless access point / wireless router
- Open System
  - No authentication password is required
- WPA/2/3-Personal / WPA/2/3-PSK
  - WPA2 or WPA3 with a pre-shared key
  - Everyone uses the same 256-bit key
- WPA/2/3-Enterprise / WPA/2/3-802.1X
  - Authenticates users individually with an authentication server (i.e., RADIUS)

## 2.3 - Authentication Methods

**RADIUS (Remote Authentication Dial-in User Service)**
- One of the more common AAA protocols
  - Supported on a wide variety of platforms and devices
  - Not just for dial-in
- Centralize authentication for users
  - Routers, switches, firewalls
  - Server authentication
  - Remote VPN access
  - 802.1X network access
- RADIUS services available on almost any server OS

**TACACS**
- Terminal Access Controller Access-Control System
  - Remote authentication protocol
  - Created to control access to dial-up lines to ARPANET
- TACACS+
  - The latest version of TACACS
  - More authentication requests and response codes
  - Released as an open standard in 1993

**Kerberos**
- Network authentication protocol
  - Authenticate once, trusted by the system
  - No need to re-authenticate to everything
  - Mutual authentication - the client and the server
  - Protect against on-path or replay attacks
- Standard since the 1980s
  - Developed by the Massachusetts Institute of Technology (MIT)
- Microsoft starting using Kerberos in Windows 2000
  - Based on Kerberos 5.0 open standard
  - Compatible with other operating systems and devices

**SSO with Kerberos**
- Authenticate one time
  - Lots of backend ticketing
  - Cryptographic tickets
- No constant username and password input!
  - Save time
- Only works with Kerberos
  - Not everything is Kerberos-friendly
- There are many other SSO methods
  - Smart-cards, SAML, etc.

**Which method to use?**
- Many different ways to communicate to an authentication server
  - More than a simple login process
- Often determined by what is at hand
  - VPN concentrator can talk to a RADIUS server
  - We have a RADIUS server
- TACACS+
  - Probably a Cisco device
- Kerberos - Probably a Microsoft network

## 2.3 - Authentication Methods

**Which method to use?**

- Many different ways to communicate to an authentication server
  - More than a simple login process
- Often determined by what is at hand
  - VPN concentrator can talk to a RADIUS server
  - We have a RADIUS server
- TACACS+
  - Probably a Cisco device
- Kerberos
  - Probably a Microsoft network

**Multi-factor authentication**

- More than one factor
  - Something you are
  - Something you have
  - Something you know
  - Somewhere you are
  - Something you do
- Can be expensive
  - Separate hardware tokens
  - Specialized scanning equipment
- Can be inexpensive - Free smartphone applications

## 2.4 - Malware

**Malware**

- Malicious software - These can be very bad
- Gather information - Keystrokes
- Participate in a group - Controlled over the 'net
- Show you advertising - Big money
- Viruses and worms
  - Encrypt your data and ruin your day

**How you get malware**

- These all work together
  - Malicious software takes advantage of a vulnerability
  - Installs malware that includes a remote access backdoor
  - Bot may be installed later
- Your computer must run a program
  - Email link - Don't click links
  - Web page pop-up
  - Drive-by download
  - Worm
- Your computer is vulnerable
  - Operating system - Keep your OS updated!
  - Applications - Check with the publisher

**Trojan horse**

- Used by the Greeks to capture Troy from the Trojans
  - A digital wooden horse
- Software that pretends to be something else
  - So it can conquer your computer
  - Doesn't really care much about replicating
- Circumvents your existing security
  - Anti-virus may catch it when it runs
  - The better Trojans are built to avoid and disable AV
- Once it's inside it has free reign
  - And it may open the gates for other programs

**Rootkits**

- Originally a Unix technique
  - The "root" in rootkit
- Modifies core system files
  - Part of the kernel
- Can be invisible to the operating system
  - Won't see it in Task Manager
- Also invisible to traditional anti-virus utilities
  - If you can't see it, you can't stop it
- The UEFI BIOS Secure Boot feature has helped
  - Won't boot if the OS has been modified

**Finding and removing rootkits**

- Look for the unusual
  - Anti-malware scans
  - Rootkit scanning built into many anti-malware tools
- Use a remover specific to the rootkit
  - Usually built after the rootkit is discovered
- Secure boot with UEFI
  - Security in the BIOS

**Virus**

- Malware that can reproduce itself
  - It needs you to execute a program
- Reproduces through file systems or the network
  - Just running a program can spread a virus
- May or may not cause problems
  - Some viruses are invisible, some are annoying
- Anti-virus is very common
  - Thousands of new viruses every week
  - Is your signature file updated?

**Spyware**
- Malware that spies on you
  - Advertising, identity theft, affiliate fraud
- Can trick you into installing
  - Peer to peer, fake security software
- Browser monitoring - Capture surfing habits
- Keyloggers
  - Capture every keystroke
  - Send it back to the mother ship

**Ransomware**
- A particularly nasty malware
  - Your data is unavailable until you provide cash
- Malware encrypts your data files
  - Pictures, documents, music, movies, etc.
  - Your OS remains available
  - They want you running, but not working
- You must pay the bad guys to obtain the decryption key
  - Untraceable payment system
  - An unfortunate use of public-key cryptography

**Keyloggers**
- Your keystrokes contain valuable information
  - Web site login URLs, passwords, email messages
- Save all of your input - Send it to the bad guys
- Circumvents encryption protections
  - Your keystrokes are in the clear
- Other data logging
  - Clipboard logging, screen logging, instant messaging, search engine queries

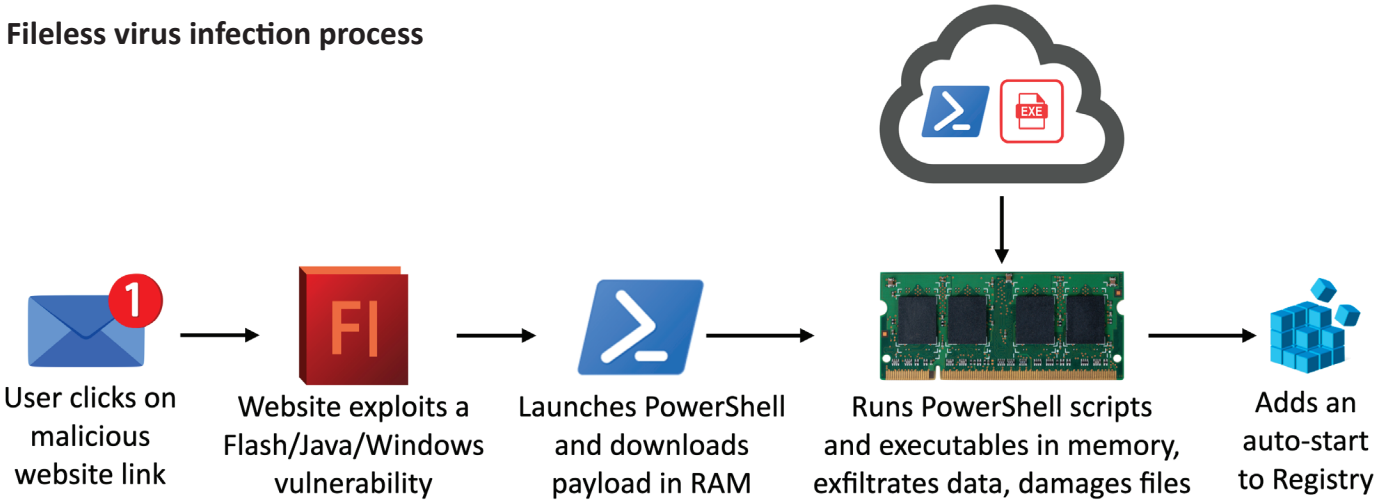
**Cryptominers**
- Some cryptocurrency mining requires "proof of work"
  - Usually consists of a difficult math problem
  - Answer the problem and earn some currency
- This requires extensive CPU processing
  - One CPU isn't enough
  - Attackers want to use your CPU
- May appear in different ways
  - Visit a website and CPU utilization spikes
  - Malware is installed and mining is always occurring

**Boot sector virus**
- Most viruses run after the OS is loaded
  - Like most applications
- Some boot loaders can be modified to run malware
  - Runs every time you start your computer
- Modern UEFI BIOS includes Secure Boot
  - Prevent unsigned software from running during the boot process

**Cryptominers**
- Some cryptocurrency mining requires "proof of work"
  - Usually consists of a difficult math problem
  - Answer the problem and earn some currency
- This requires extensive CPU processing
  - One CPU isn't enough
  - Attackers want to use your CPU
- May appear in different ways
  - Visit a website and CPU utilization spikes
  - Malware is installed and mining is always occurring

**Fileless virus**
- A stealth attack
  - Does a good job of avoiding anti-virus detection
- Operates in memory
  - But never installed in a file or application

**Fileless virus infection process**



## 2.4 - Malware (continued)

**Stalkerware**
- Software designed to surveil
  - Intentionally tracking another person's activities
- Many commercial products available
  - This is not usually an accident or malware
- Broad access to a system
  - Screenshots, location details, microphone, camera, etc.
- Can also be used for government spying
  - Stalkerware on a phone can be used by an enemy
- Keep your anti-malware signatures updated
  - Don't click links in an emails or text messages

**Potentially Unwanted Program (PUP)**
- Identified by anti-virus/anti-malware
  - Potentially undesirable software
  - Often installed along with other software
- Usually associated with adware
  - Shows advertising but not otherwise malicious
- Overly aggressive browser toolbar
- A backup utility that displays ads
- Browser search engine hijacker

## 2.4 - Anti-Malware Tools

**Windows Recovery Environment**
- Very powerful
- Very dangerous
  - Last resort
- Complete control
  - Fix your problems before the system starts
  - Remove malicious software
- Requires additional information
  - Use, copy, rename, or replace operating system files and folders
  - Enable or disable service or device startup
  - Repair the file system boot sector or the master boot record (MBR)

**Starting the console**
- All Windows versions
  - Hold Shift key while clicking Restart
  - Or boot from installation media
- Windows 10
  - Settings > Update and Security > Recovery > Advanced startup
- Windows 11
  - System > Recovery > Advanced startup > Restart now
- After rebooting
  - Troubleshoot > Advanced Options > Command Prompt

**Endpoint detection and response (EDR)**
- A different method of threat protection
  - Scale to meet the increasing number of threats
- Detect a threat
  - Signatures aren't the only detection tool
  - Behavioral analysis, machine learning, process monitoring
  - Lightweight agent on the endpoint
- Investigate the threat
  - Root cause analysis
- Respond to the threat
  - Isolate the system, quarantine the threat, rollback to a previous config
  - API driven, no user or technician intervention required

**Managed detection and response (MDR)**
- Third-party EDR services
  - Provided by a managed security service provider (MSSP)
- Manages the entire process
  - Monitors all EDR endpoints
  - Detects any threats
- Responds to all issues
  - Contains the malware, investigates the incident
  - Provides guidance to help prevent further issues
- Expertise from trained professionals
  - Can supplement an organization's security team

**Extended Detection and Response (XDR)**
- An evolution of EDR
  - Improve missed detections, false positives, and long investigation times
  - Attacks involve more than just the endpoint
- Add network-based detection
  - Investigate and respond to network anomalies
- Correlate endpoint, network, and cloud data
  - Improve detection rates
  - Simplify security event investigations

**Anti-virus and anti-malware**
- You need both
  - Often included together
- Real-time options
  - Not just an on-demand scan
- Modern anti-malware recognizes malicious activity
  - Doesn't require a specific set of signatures

## 2.4 - Anti-Malware Tools (continued)

**Email security gateway**
- The gatekeeper
  - Evaluates the source of inbound email messages
  - Blocks it at the gateway before it reaches the user
  - On-site or cloud-based

**Software firewalls**
- Monitor the local computer
  - Alert on unknown or unauthorized network communication
- Prevent malware communication
  - Downloads after infection
  - Botnet communication
- Use Microsoft Defender Firewall - At a minimum
- Runs by default
  - Constantly monitoring - Any network connection

**Anti-phishing training**
- No single technology can stop social engineering
  - Don't give away private information
  - The user is the best anti-phishing
- Extensive training - Avoid becoming a victim
- Test the users
  - Send a phishing email
  - Find out who clicks and gives up information
- Train again

**End user education**
- One on one
  - Personal training
- Posters and signs
  - High visibility
- Message board posting
  - The real kind
- Login message
  - These become invisible
- Intranet page
  - Always available

**OS reinstallation**
- Only one way to guarantee malware removal
  - Delete everything
  - Install from scratch
- Restore from backup (fast)
  - As long as the backup is not also infected
- Manual installation (slowest)
  - Backup data files
  - Install Windows from installation media
- Image the system (fastest)
  - User's data files are on a network share
  - Recover from a prebuilt image

## 2.5 - Social Engineering

**Effective social engineering**
- Constantly changing - You never know what they'll use next
- May involve multiple people
  - And multiple organizations
  - There are ties connecting many organizations
- May be in person or electronic
  - Phone calls from aggressive "customers"
  - Emailed funeral notifications of a friend or associate

**Phishing**
- Social engineering with a touch of spoofing
  - Often delivered by email, text, etc.
- Don't be fooled - Check the URL
- Usually there's something not quite right
  - Spelling, fonts, graphics

**Phishing with a different bait**
- Vishing (Voice phishing) is done over the phone or voicemail
  - Caller ID spoofing is common
  - Fake security checks or bank updates
- Smishing (SMS phishing) is done by text message
  - Spoofing is a problem here as well
  - Forwards links or asks for personal information
- QR code phishing
  - Swap a QR code for a different image
  - Directs to a malware site instead

**Spear phishing**
- Targeted phishing with inside information
  - Makes the attack more believable
- Spear phishing the CEO is "whaling"
  - Targeted phishing with the possibility of a large catch
  - The CFO (Chief Financial Officer) is commonly speared
- These executives have direct access to the corporate bank account
  - The attackers would love to have those credentials

**Shoulder surfing**
- You have access to important information
  - Many people want to see
  - Curiosity, industrial espionage, competitive advantage
- This is surprisingly easy
  - Airports / Flights, hallway-facing monitors, or coffee shops
- Surf from afar
  - Binoculars / Telescopes (easy in the big city)
  - Webcam monitoring

## 2.5 - Social Engineering (continued)

**Preventing shoulder surfing**

- Control your input
  - Be aware of your surroundings
- Use privacy filters
  - It's amazing how well they work
- Keep your monitor out of sight
  - Away from windows and hallways
- Don't sit in front of me on your flight
  - I can't help myself

**Tailgating and piggybacking**

- Tailgating uses an authorized person to gain unauthorized access to a building
  - The attacker does not have consent
  - Sneaks through when nobody is looking
- Piggybacking follows the same process, but the authorized person is giving consent
  - Hold the door, my hands are full of donut boxes
  - Sometimes you shouldn't be polite
- Once inside, there's little to stop you
  - Most security stops at the border

**Impersonation**

- Pretend to be someone you aren't
  - Halloween for the fraudsters
- Use some of those details you got from the dumpster
  - You can trust me, I'm with your help desk
- Attack the victim as someone higher in rank
  - Office of the Vice President for Scamming
- Throw tons of technical details around
  - Catastrophic feedback due to the depolarization of the differential magnetometer
- Be a buddy - How about those Cubs?

**Dumpster diving**

- Mobile garbage bin
  - United States brand name "Dumpster"
  - Similar to a rubbish skip
- Important information thrown out with the trash
  - Thanks for bagging your garbage for me!
- Gather details that can be used for a different attack
  - Impersonate names, use phone numbers
- Timing is important
  - Just after end of month, end of quarter
  - Based on pickup schedule

## 2.5 - Denial of Service

**Denial of service**

- Force a service to fail
  - Overload the service
- Take advantage of a design failure or vulnerability
  - Keep your systems patched!
- Cause a system to be unavailable
  - Competitive advantage
- Create a smokescreen for some other exploit
  - Precursor to a DNS spoofing attack
- Doesn't have to be complicated
  - Turn off the power

**A "friendly" DoS**

- Unintentional DoSing
  - It's not always a ne'er-do-well
- Network DoS
  - Layer 2 loop without STP
- Bandwidth DoS
  - Downloading multi-gigabyte Linux distributions over a DSL line
- The water line breaks
  - Get a good shop vacuum

**Distributed Denial of Service (DDoS)**

- Launch an army of computers to bring down a service
  - Use all the bandwidth or resources - traffic spike
- This is why the bad guys have botnets
  - Thousands or millions of computers at your command
  - At its peak, Zeus botnet infected over 3.6 million PCs
  - Coordinated attack
- The attackers are zombies
  - Many people have no idea they are participating in a botnet

**Mitigating DDoS attacks**

- May be able to filter out traffic patterns
  - Stop the traffic at your firewall
- Internet service provider may have anti-DDoS systems
  - These can help "turn down" the DDoS volume
- Third-party technologies
  - CloudFlare, etc.

# 2.5 - Spoofing and On-Path Attacks

**On-path network attack**

- How can an attacker watch without you knowing?
  - Formerly known as man-in-the-middle
- Redirects your traffic
  - Then passes it on to the destination
  - You never know your traffic was redirected
- ARP poisoning
  - On-path attack on the local IP subnet
  - ARP has no security
  - ARP poisoning (spoofing)

**On-path browser attack**

- What if the middleman was on the same computer as the victim?
  - Malware/Trojan does all of the proxy work
  - Formerly known as man-in-the-browser
- Huge advantages for the attackers
  - Relatively easy to proxy encrypted traffic
  - Everything looks normal to the victim
- The malware in your browser waits for you to login to your bank
  - And cleans you out

**Wireless evil twins**

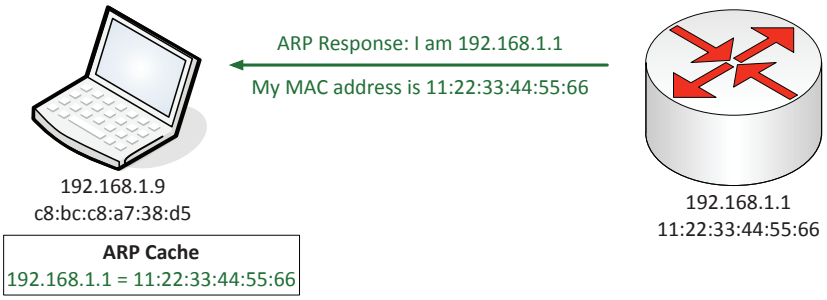
- Looks legitimate, but actually malicious
  - The wireless version of phishing
- Configure an access point to look like an existing network
  - Same (or similar) SSID and security settings/ captive portal
- Overpower the existing access points
  - May not require the same physical location
- WiFi hotspots (and users) are easy to fool
  - And they're wide open
- You encrypt your communication, right?
  - Use HTTPS and a VPN

**ARP poisoning (spoofing)**

1

A legitimate response to an ARP request is received from the default gateway.

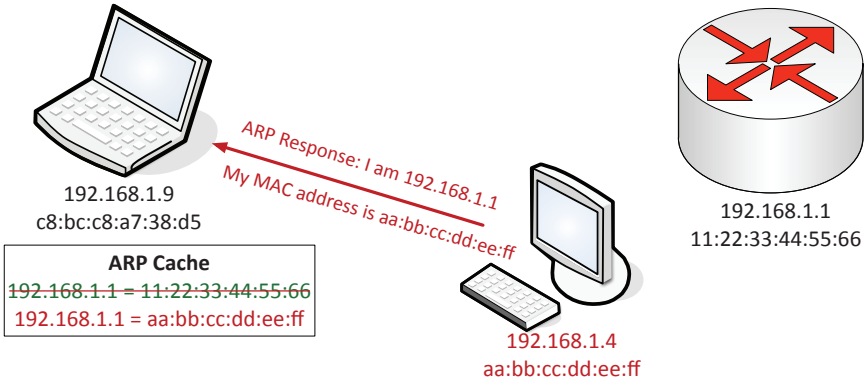
The ARP response is cached on the local device.




2

An attacker sends an ARP response that spoofs the IP address of the router and includes the attacker's MAC address.

The malicious ARP information replaces the cached record, completing the ARP poisoning.



## 2.5 - Zero-Day Attacks

**Zero-day attacks**

- Many applications have vulnerabilities
  - We've just not found them yet
- Someone is working hard to find the next big vulnerability
  - The good guys share these with developers
- Attackers keep these yet-to-be-discovered holes to themselves
  - They want to use these vulnerabilities for personal gain
- Zero-day
  - The vulnerability has not been detected or published
  - Zero-day exploits are increasingly common
- Common Vulnerabilities and Exposures (CVE)
  - https://cve.mitre.org/

**Zero-day vulnerabilities**

- December 9, 2021 - Log4j remote code execution
  - Java-based logging utility provided as an Apache service
  - Installed on millions of servers
  - Vulnerability introduced on September 14th, 2013
- December 14th - Fix is released
  - Extensive patching
- December 17th -
  - Two new issues fixed
  - Everyone is looking for bugs

## 2.5 - Password Attacks

**Plaintext / unencrypted passwords**

- Some applications store passwords "in the clear"
  - No encryption. You can read the stored password.
  - This is rare, thankfully
- Do not store passwords as plaintext
  - Anyone with access to the password file or database has every credential
- What to do if your application saves passwords as plaintext:
  - Get a better application

**Hashing a password**

- Hashes represent data as a fixed-length string of text
  - A message digest, or "fingerprint"
- Will not have a collision (hopefully)
  - Different inputs will not have the same hash
- One-way trip
  - Impossible to recover the original message from the digest
  - A common way to store passwords

**The password file**

- Different across operating systems and applications
  - Different hash algorithms

**Brute force**

- Try every possible password combination until the hash is matched
- This might take some time
  - A strong hashing algorithm slows things down
- Brute force attacks - Online
  - Keep trying the login process
  - Very slow
  - Most accounts will lockout after a number of failed attempts
- Brute force the hash - Offline
  - Obtain the list of users and hashes
  - Calculate a password hash, compare it to a stored hash
  - Large computational resource requirement

**Dictionary attacks**

- Use a dictionary to find common words
  - Passwords are created by humans
- Many common wordlists available on the 'net
  - Some are customized by language or line of work
- The password crackers can substitute letters
  - p&ssw0rd
- This takes time
  - Distributed cracking and GPU cracking is common

## 2.5 - Insider Threats

**Insider threats**

- More than just passwords on sticky notes
  - Some insiders are out for no good
- Sophistication may not be advanced, but the insider has institutional knowledge
  - Attacks can be directed at vulnerable systems
  - The insider knows what to hit
- Extensive resources
  - Eating away from the inside

**Recruiting insiders**

- We're getting better with protecting the network perimeter
  - It's an ongoing race
- Ransomware actors are targeting insiders
  - Offering Bitcoin in exchange for access
  - One ransomware infection can earn millions for an attacker
- Keep aware
  - Maintain good security fundamentals
  - Always have backups

## 2.5 - SQL Injection

**Code injection**

- Code injection
  - Adding your own information into a data stream
- Enabled because of bad programming
  - The application should properly handle input and output
- So many different data types
  - HTML, SQL, XML, LDAP, etc.

**SQL injection**

- SQL - Structured Query Language
  - The most common relational database management system language
- SQL Injection
  - Modify SQL requests (Your application shouldn't allow this)
- If you can manipulate the database, then you control the application
  - A significant vulnerability

- An example of website code:
  - `"SELECT * FROM users WHERE name = '" + userName + "'";`
- How this looks to the SQL database:
  - `"SELECT * FROM users WHERE name = 'Professor'";`
- Add more information to the query:
  - `"SELECT * FROM users WHERE name = 'Professor' OR '1' = '1'";`
- This could be very bad
  - View all database information, delete database information, add users, denial of service, etc.

## 2.5 - Cross-site Scripting

**Cross-site scripting**

- XSS
  - Cascading Style Sheets (CSS) are something else entirely
- Originally called cross-site because of browser security flaws
  - Information from one site could be shared with another
- One of the most common web application development errors
  - Takes advantage of the trust a user has for a site
  - Complex and varied
- Malware that uses JavaScript
  - Do you allow scripts? Me too.

**Non-persistent (reflected) XSS attack**

- Web site allows scripts to run in user input
  - Search box is a common source
- Attacker emails a link that takes advantage of this vulnerability
  - Runs a script that sends credentials / session IDs / cookies to the attacker
- Script embedded in URL executes in the victim's browser
  - As if it came from the server
- Attacker uses credentials/session IDs/ cookies to steal victim's information without their knowledge
  - Very sneaky

**Persistent (stored) XSS attack**

- Attacker posts a message to a social network
  - Includes the malicious payload
- It's now "persistent"- Everyone gets the payload
- No specific target - All viewers to the page
- For social networking, this can spread quickly
  - Everyone who views the message can have it posted to their page
  - Where someone else can view it and propagate it further...

**Hacking a Subaru**

- June 2017, Aaron Guzman - Security researcher
- When authenticating with Subaru, users get a token
  - This token never expires (bad!)
- A valid token allowed any service request
  - Even adding your email address to someone else's account
  - Now you have full access to someone else's car
- Web front-end included an XSS vulnerability
  - A user clicks a malicious link, and you have their token

**Protecting against XSS**

- Be careful when clicking untrusted links
  - Never blindly click in your email inbox. Never.
- Consider disabling JavaScript
  - Or control with an extension
  - This offers limited protection
- Keep your browser and applications updated
  - Avoid the nasty browser vulnerabilities
- Validate input
  - Don't allow users to add their own scripts to an input field

## 2.5 - Business Email Compromise

**Business email compromise (BEC)**

- Email continues to be a significant attack vector
  - A popular form of business communication
- An opportunity for the attackers
  - Takes advantage of a trusted messaging system
- Remarkably common
  - Everyone has an email address
  - Not everyone is trained in IT security
- A large social engineering component
  - Difficult to identify and prevent
  - This is not always a business email issue

**Examples of business email compromise**

- A title company email provides wire transfer account information
  - A title company email provides wire transfer account information
  - But it's not your actual title company
- A message from the CEO asks you to buy a stack of gift cards for "employee awards"
  - And you email the card number and secret code to the "CEO"
- An email to the payroll department requests an update to an employee's banking information
  - It's not the employee or their bank account

**How BEC works**

- Step 1: Attackers identify a target
  - Social media, company records, third-party documentation
- Step 2: Attackers use emails to get the victim comfortable
  - Small talk, simple requests, and other conversation
- Step 3: The attacker provides fake wiring instructions
  - No reason to doubt this perfectly reasonable request
- Step 4: After the wire transfer is complete, the attacker may be back for more
  - It worked once, so it might work again

**Preventing business email compromise**

- Watch for email spoofing
  - My email is NOT james@profesormesser.com
- Spearphishing is a common theme
  - Directed towards a specific person or department
- Often part of a larger breach
  - Hacks one company and uses invoice information against others
- Verify all requests directly
  - Especially if there's a push to act quickly
  - Voice/video calls can save the day
  - Train your user community!

## 2.5 - Supply Chain Attacks

**Supply chain risk**

- The chain contains many moving parts
  - Raw materials, suppliers, manufacturers, distributors, customers, consumers
- Attackers can infect any step along the way
  - Infect different parts of the chain without suspicion
  - People trust their suppliers
- One exploit can infect the entire chain
  - There's a lot at stake

**Service providers**

- You can control your own security posture
  - You can't always control a service provider
- Service providers often have access to internal services
  - An opportunity for the attacker
- Many different types of providers
  - Network, utility, office cleaning, payroll/accounting, cloud services, system administration, etc.
- Consider ongoing security audits of all providers
  - Should be included with the contract

**Target service provider attack**

- Target Corp. breach - November 2013
  - 40 million credit cards stolen
- Heating and AC firm in Pennsylvania was infected
  - Malware delivered in an email
  - VPN credentials for HVAC techs was stolen
- HVAC vendor was the supplier
  - Attackers used a wide-open Target network to infect every cash register at 1,800 stores
- Do these technicians look like an IT security issue?

**Hardware providers**

- Can you trust your new server/router/switch/firewall/software?
  - Supply chain cyber security
- Use a small supplier base
  - Tighter control of vendors
- Strict controls over policies and procedures
  - Ensure proper security is in place
- Security should be part of the overall design
  - There's a limit to trust1

## 2.5 - Supply Chain Attacks (continued)

**Cisco or not Cisco?**
- All network traffic flows through switches and routers
  - A perfect visibility and pivot point
- July 2022 - DHS arrests reseller CEO
  - Sold more than $1 billion of counterfeit Cisco products
  - Created over 30 different companies
  - Had been selling these since 2013
- Knock-offs made in China
  - Sold as authentic Cisco products
  - Until they started breaking and catching on fire

**Software providers**
- Trust is a foundation of security
  - Every software installation questions our trust
- Initial installation
  - Digital signature should be confirmed during installation
- Updates and patches
  - Some software updates are automatic
  - How secure are the updates?
- Open source is not immune
  - Compromising the source code itself

**SolarWinds supply chain attack**
- SolarWinds Orion
  - Used by 18,000 customers
  - Including Fortune 500 and US Federal Government
- Software updates compromised in March and June 2020
  - Upgrades to existing installations
  - Not detected until December 2020
- Additional breaches took advantage of the exploit
  - Microsoft, Cisco, Intel, Deloitte
  - Pentagon, Homeland Security, State Department, Department of Energy, National Nuclear Security Administration, Treasury

## 2.5 - Security Vulnerabilities

**Non-compliant systems**
- A constant challenge
  - There are always changes and updates
- Standard operating environments (SOE)
  - A set of tested and approved hardware/software systems
  - Often a standard operating system image
- Operating system and application updates
  - Must have patches to be in compliance
  - OS updates, anti-virus signatures
  - Can be checked and verified before access is given

**Protecting against non-compliant systems**
- Operating system control
  - Apply policies that will prevent non-compliant software
- Monitor the network for application traffic
  - Next-generation firewalls with application visibility
- Perform periodic scans
  - Login systems can scan for non-compliance
  - Require correction before the system is given access

**Unpatched systems**
- Microsoft Patch Tuesday
  - Second Tuesday of each month (10:00 AM PST)
- Suddenly, systems are vulnerable to security flaws
  - Patch the operating system and applications
- An organization might have thousands of systems
  - Some of those are major services
- One forgotten system may be the weakest link
  - This happens quite a bit
- Patch management is a critical practice
  - Test, prioritize, and deploy

**Unprotected systems**
- Security issues are often roadblocks
  - Applications may not work properly without additional configurations
- Some troubleshooting tasks can be insecure
  - Disable antivirus and try again
  - Disable the firewall and try again
- Permanently disabling security isn't the answer
  - You don't fix a bad door lock by removing the door
  - Become an expert in application troubleshooting

**Product support lifetime**
- End of life (EOL) operating systems
  - Manufacturer stops selling an OS
  - May continue supporting the OS
  - Important for security patches and updates
- End of service life (EOSL)
  - Manufacturer stops selling an OS
  - Support is no longer available
  - No ongoing security patches or updates
  - May have a premium-cost support option
- Technology EOSL is a significant concern
  - Security patches are part of normal operation

**BYOD**
- Bring Your Own Device / Bring Your Own Technology
- Employee owns the device
  - Need to meet the company's requirements
- Difficult to secure
  - It's both a home device and a work device
  - How is data protected?
  - What happens to the data when a device is sold or traded in?
  - An infected device could disclose proprietary information

# 2.6 - Removing Malware

**Malware removal**
- This is almost never the best practice
  - It's impossible to know if all of the malware has been removed
- Ideally, you should delete everything and start over
  - Restore from a known-good backup
  - Install from the original media
- There are reasons to remediate
  - Important user documents may need to be recovered
  - Get the system running well enough to backup certain files

**1. Investigate and verify malware symptoms**
- Odd error messages
  - Application failures, security alerts
- System performance issues
  - Slow boot, slow applications
- Research the malware
  - Know what you're dealing with

**2. Quarantine infected systems**
- Disconnect from the network
  - Keep it contained
- Isolate all removable media
  - Everything should be contained
- Prevent the spread
  - Don't transfer files, don't try to backup
  - That ship sailed

**3. Disable System Restore**
- Restore points make it easy to rewind
  - Malware infects restore points
- This may be already be disabled in a corporate environment
  - Disable in Windows Home
- Disable System Protection
  - No reason to save an infected config
- Delete all restore points
  - Remove all infection locations

**4. Remediate infected systems**
- Provide a remedy
  - Resolve the malware issue
- Remove any malicious files
  - This could be an easy fix
- Quarantine the files
  - Remove them from direct access
  - Cannot execute in the protected folder
- Malware may not want to be removed
  - This is often a difficult and involved process

**5. Update anti-virus software**
- Signature and engine updates
  - The active anti-virus engine
  - Signature updates
  - A very, very tiny shelf life
- Automatic vs. manual
  - Manual updates are almost pointless
- Your malware may prevent the update process
  - Copy from another computer

**6. Scan and removal techniques**
- Safe mode
  - Load the bare minimum operating system
  - Just enough to get the OS running
  - Can also prevent the bad stuff from running
- Pre-installation environment (WinPE)
  - Recovery Console, bootable CD/DVDs/USBs
  - Build your own from the Windows
  - Assessment and Deployment Kit (ADK)
- May require the repair of boot records and sectors

**7. Reimage / reinstall**
- Delete everything and reinstall
  - The best way to ensure complete removal
  - This can be time consuming
- Reimage with a known-good image
  - Relatively quick recovery
  - Includes all necessary software
- This is why we save documents on a network server
  - Delete everything on the local machine
  - Nothing of value is lost

**8. Schedule scans and run updates**
- Built into the antivirus software
  - Automated signature updates and scans
- Task scheduler - Run any task
- Operating system updates
  - Make sure its enabled and working

**9. Enable System Protection**
- Now you're clean
  - Put things as they were
- Create a restore point - Start populating again

**10. Educate the end user**
- One on one
  - Personal training
- Posters and signs
  - High visibility
- Message board posting
  - The real kind
- Login message
  - These become invisible
- Intranet page
  - Always available

# 2.7 - Security Best Practices

**Data encryption**
- Full-disk encryption
  - Encrypt data-at-rest
- File system encryption
  - Individual files and folders
- Removable media
  - Protect those USB flash drives
- Key backups are critical
  - You always need to have a copy
  - This may be integrated into Active Directory
  - You'll want to keep the key handy

**Password complexity and length**
- Make your password strong
  - Resist guessing or brute-force attack
- Increase password entropy
  - Different character types
  - No single words, no obvious passwords
  - Mix upper and lower case and use special characters
- Stronger passwords are at least 8 characters
  - Consider a phrase or set of words

**Password age and expiration**
- Password age
  - How long since a password was modified
- Password expiration
  - Password works for a certain amount of time
  - 30 days, 60 days, 90 days, etc.
  - After the expiration date, the password does not work
  - System remembers password history, requires unique passwords
- Critical systems might change more frequently
  - Every 15 days or every week

**Password best practices**
- Change default usernames/passwords
  - All devices have defaults
  - There are many web sites that document these
- BIOS/UEFI passwords
  - Supervisor/Administrator password: Prevent BIOS changes
  - User password: Prevent booting
- Requiring passwords
  - Always require passwords
  - No blank passwords
  - No automated logins

**End-user best practices**
- Require a screensaver password
  - Integrate with login credentials
  - Can be administratively enforced
- Does not require user intervention
  - Automatically locks after non-use or timeout
- Secure critical hardware
  - Laptops can easily walk away
  - Lock them down

**Securing PII and passwords**
- Personally identifiable information
  - Name, address, social security number, etc.
- Control your input
  - Be aware of your surroundings
- Use privacy filters
  - It's amazing how well they work
- Keep your monitor out of sight
  - Away from windows and hallways

**Password managers**
- Important to use different passwords for each account
  - Remembering all of them would be impractical
- Store all of your passwords in a single database
  - Encrypted, protected
  - Can include multifactor tokens
- Built-in to many operating systems
  - And some browsers
- Enterprise password managers
  - Centralized management and recovery options

**Account management**
- User permissions
  - Everyone isn't an Administrator
  - Assign proper rights and permissions
  - This may be an involved audit
- Assign rights based on groups
  - More difficult to manage per-user rights
  - Becomes more useful as you grow
- Login time restrictions
  - Only login during working hours
  - Restrict after-hours activities

**Disable unnecessary accounts**
- All operating systems include other accounts
  - Guest, root, mail, etc.
- Not all accounts are necessary
  - Disable/remove the unnecessary
  - Disable the guest account
- Disable interactive logins
  - Not all accounts need to login
- Change the default admin usernames
  - User:admin Password:admin
  - Helps with brute-force attacks

## 2.7 - Security Best Practices (continued)

**Lock the desktop**
- Failed password attempts
  - Should lock the account and/or reboot after a certain threshold
  - Prevents online brute force attacks
- Automatically lock the system
  - After a certain amount of inactivity
  - Or when you walk away
- Use expiration dates
  - Some accounts should automatically disable themselves
  - Contractors, temporary workers

**AutoRun and AutoPlay**
- Disable AutoRun on older Oses
  - autorun.inf in Vista
  - No Autorun in Windows 7, 8/8.1, 10, or 11
  - Disabled through the registry
- Disable AutoPlay
  - Configure in Settings >
  - Bluetooth & devices > AutoPlay

**Disable unnecessary services**
- Unused or unknown services
  - Installed with the OS or from other applications
- Each service is a potential breach
  - Access from the outside
- Disabling a service removes the potential threat
  - Nothing for the attacker to use against you

## 2.8 - Mobile Device Security

**Full device encryption**
- Encrypt all device data
  - Phone keeps the key
- iOS 8 and later
  - Personal data is encrypted with your passcode
- Android
  - Version 5.0 and later is probably already encrypted

**Screen locks**
- Restrict access to the device
  - You're going to leave it somewhere
- Facial recognition
  - Unlock with your face
- PIN
  - Choose a personal identification number
- Fingerprint
  - Built-in fingerprint reader
- Swipe
  - Choose a pattern
- Failed attempts
  - iOS: Erase everything after 10 failed attempts
  - Android: Lock the device and require a Google login or wipe the device

**Configuration profiles**
- Mobile Device Management (MDM)
  - Centrally manage mobile devices
- Corporate configuration profiles speed up the process
  - A pre-defined set of system configurations
- Basic setup
  - Corporate email configurations
- Security settings
  - Lock screens and data encryption
- Push to devices through the MDM
  - Makes the process easy to manage

**Creating a configuration profile**
- Microsoft Intune, Apple Configurator
  - Easy-to-use front-end for building profiles
- Select all of the features and restrictions
  - Enable or disable
  - Add email server details
- Include any security restrictions
  - Lock screens, passcode requirements

**Patching/OS updates**
- All devices need updates - Even mobile devices
- Device patches - Security updates
- Operating system updates
  - New features, bug fixes
- Application updates
  - Always a new version
- Don't get behind!
  - Avoid security problems

**Anti-virus and anti-malware**
- Apple iOS
  - Closed environment, tightly regulated
  - Malware has to find a vulnerability
- Android
  - More open, apps can be installed from anywhere
  - Easier for malware to find its way in
- Third-party virus and malware protection
  - Available from the usual providers
- Content filtering
  - Restrict access to certain websites and applications

## 2.8 - Mobile Device Security (continued)

**Locator applications and remote wipe**
- Built-in GPS
  - And location "helpers"
- Find your phone
  - On a map.
- Control from afar
  - Make a sound
  - Display a message
- Wipe everything - At least your data is safe

**Remote backup**
- Difficult to backup something that's always moving
  - Backup to the cloud
- Constant backup
  - No manual process
- Backup without wires
  - Use the existing network
- Restore with one click
  - Restores everything - Authenticate and wait

**Firewalls**
- Mobile phones don't include a firewall
  - Most activity initiates outbound, not inbound
- Some mobile firewall apps are available
  - Most for Android - None seem to be widely used
- Enterprise environments can control mobile apps
  - Firewalls can allow or disallow access

**Policies and procedures**
- Manage company-owned and user-owned mobile devices
  - BYOD - Bring Your Own Device
- Centralized management of the mobile devices
  - Specialized functionality / Mobile Device Manager (MDM)
- Set policies on apps, data, camera, etc.
  - Control the remote device
  - The entire device or a "partition"
- Manage access control
  - Force screen locks and PINs on these single user devices

## 2.9 - Data Destruction

**Physical destruction**
- Drill / Hammer
  - Quick and easy - Platters, all the way through
- Shredder - Heavy machinery - complete destruction
- Electromagnetic (degaussing)
  - Remove the magnetic field
  - Destroys hard drive data and renders the hard drive unusable
  - Degaussing doesn't work for SSD and flash memory technologies
- Incineration - Fire hot.

**Erasing data**
- Recycle or repurpose a storage device
  - Delete all previously stored data
- File level overwriting
  - Sdelete – Windows Sysinternals
  - Remaining files are still available
- Whole drive wipe secure data removal
  - DBAN - Darik's Boot and Nuke
  - Removes all data on the drive
  - Use the drive again

**Disk formatting**
- Low-level formatting
  - Provided at the factory
  - Not recommended for the user
- Standard formatting / Quick format
  - Sets up the file system, installs a boot sector
  - Clears the master file table but not the data
  - Can be recovered with the right software
- Standard formatting / Regular format
  - Overwrites every sector with zeros
  - Default for Windows Vista and later
  - Can't recover the data

**Physical drive destruction**
- A single drive, or industrial remove and destroy
  - Drive is no longer usable afterwards
- May be required
  - Healthcare, financial services, research organizations
  - Any organization with privacy or confidentiality concerns
- Check with your local regulations and policies
  - May have a legal mandate to destroy storage drives

**Certificate of destruction**
- Destruction is often done by a 3rd party
  - How many drills and degaussers do you have?
- Need confirmation that your data is destroyed
  - Service should include a certificate
- A paper trail of broken data
  - You know exactly what happened

**Hard drive security**
- 2019 study from Blancco and Ontrack
  - 159 storage drives from eBay
  - 42% of the used drives contain sensitive data
- Different data types
  - 66 drives had data, 25 drives with PII
- Varied data sources
  - Travel company email archive
  - Freight company shipping details
  - University student papers
  - Audio, video, and other personal files

# 2.10 - Securing a SOHO Network

### Change default passwords
- All access points have default usernames and passwords
  - Change yours!
- The right credentials provide full control
  - Administrator access
- Very easy to find the defaults for your access point or router
  - https://www.routerpasswords.com

### IP address filtering
- Content filtering, IP address ranges
  - Or a combination
- Allow list
  - Nothing pass through the firewall unless it's approved
  - Very restrictive
- Deny list
  - Nothing on the "bad list" is allowed
  - Specific URLs
  - Domains
  - IP addresses

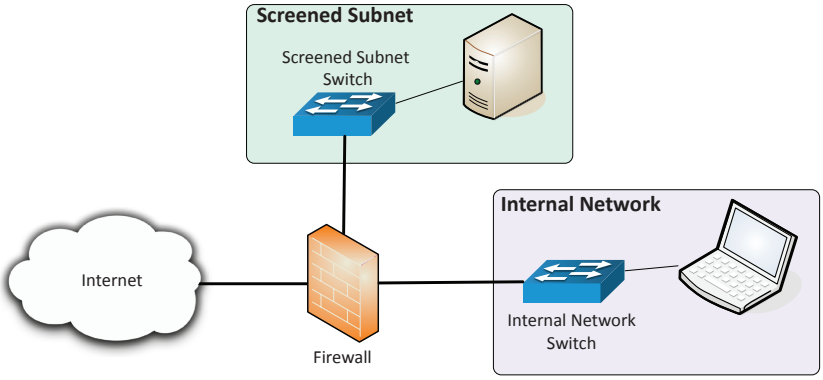
### Firmware updates
- Small office / home office appliances
  - Appliance are usually a closed architecture
  - Updates are provided by the manufacturer
- Updates may address different requirements
  - Bug fixes
  - New features
  - Security patches
- Install the latest software
  - Update and upgrade the firmware
  - Firewalls, routers, switches, etc.

### Content filtering
- Control traffic based on data within the content
  - URL filtering, website category filtering
- Corporate control of outbound and inbound data
  - Sensitive materials
- Control of inappropriate content
  - Not safe for work
  - Parental controls
- Protection against evil
  - Anti-virus, anti-malware

### Physical placement
- Often a single device
  - Router, switch, access point, firewall, etc.
- Location may be restricted to a secure room
  - Prevent access to servers and network devices
- For wireless, location becomes more important
  - Above ceiling tiles or another high point
  - This may cause problems for power cycling
- Plan before the installation
  - May require additional setup time

### UPnP (Universal Plug and Play)
- Allows network devices to automatically configure and find other network devices
  - Zero-configuration
- Applications on the internal network can open inbound ports using UPnP
  - No approval needed
  - Used for many peer-to-peer (P2P) applications
- Best practice would be to disable UPnP
  - Only enable if the application requires it
  - And maybe not even then

### Screened subnet
- Previously known as the demilitarized zone (DMZ)
  - An additional layer of security between the Internet and you
  - Public access to public resources




### Secure management access
- Management access to a SOHO router should be tightly controlled
  - An administrator login provides complete control
- Use strong authentication credentials
  - A relatively complex password
  - Additional authentication factor, if available
  - Some devices provide cloud login options
- Limit management access by IP
  - Local logins only
  - Disable remote access

### SSID management
- Service Set Identifier
  - Name of the wireless network
  - LINKSYS, DEFAULT, NETGEAR
- Change the SSID to something not-so obvious
- Disable SSID broadcasting?
  - SSID is easily determined through wireless network analysis
  - Security through obscurity

## 2.10 - Securing a SOHO Network (continued)

**Wireless channels and encryption**

- Open System
  - No authentication password is required
- WPA/2/3-Personal / WPA/2/3-PSK
  - WPA2 or WPA3 with a pre-shared key
  - Everyone uses the same 256-bit key
- WPA/2/3-Enterprise / WPA/2/3-802.1X
  - Authenticates users individually with an authentication server (i.e., RADIUS, LDAP, etc.)
- Use an open frequency
  - Some access points will automatically find good frequencies

**Disable guest networks**

- Limit access to outsiders
  - Guest networks are often enabled by default
- Some guest networks can be used for other connections
  - Internet of Things
  - Lab networks
- Don't enable without security
  - WPA2 or WPA3

**Disabling ports**

- Enabled physical ports
  - Conference rooms
  - Break rooms
- Administratively disable unused ports
  - More to maintain, but more secure
- Network Access Control (NAC)
  - 802.1X controls
  - You can't communicate unless you are authenticated

**Port forwarding**

- 24x7 access to a service hosted internally
  - Web server, gaming server, security system, etc.
- External IP/port number maps to an internal IP/port
  - Does not have to be the same port number
- Also called Destination NAT or Static NAT
  - Destination address is translated from a public IP to a private IP
  - Does not expire or timeout

## 2.11 - Browser Security

**Browser download and installation**

- Always use trusted sources
  - Attackers want you to install the malware for them
  - No fancy exploit required
- Avoid untrusted third-party sites
  - Don't click links in emails
  - Don't follow links from other websites
  - Always visit a browser site directly
- Use hashes to verify the download
  - Confirm the downloaded file matches the version on the server

**Hash verification**

- Install a hash checking application
  - Available for command line and GUI
  - Options available in the Microsoft Store
- Hash values may be available on the download site
  - Usually includes a digital signature for verification
- Verify the downloaded file
  - Compare the downloaded file hash with the posted hash value

**Browser patching**

- Important to stay up to date
  - Security patches, especially
- Often integrated into the OS update manager
  - That's how important it is
- May also be upgraded from the browser itself
  - Check the browser

**Extensions and plug-ins**

- Trusted sources
  - Official browser extension library
  - Chrome Web Store
  - Microsoft Store
  - Known-good websites
- Untrusted sources
  - Random or unfamiliar websites
  - Installed by malware
- This is a significant attack vector
  - Almost everything we do is in our browser

**Malicious browser extensions**

- March 2021
  - More than 24 malicious
  - Google Chrome extensions identified
  - Includes 40 malicious domains
  - Not identified by security technologies
- Malicious activity identified
  - Credential theft
  - Screenshots and keylogging
  - Data exfiltration
- Don't trust any software - Always have backups

# 2.11 - Browser Security (continued)

**Password managers**
- Password vaults
  - All passwords in one location
  - A database of credentials
- Secure storage
  - All credentials are encrypted
  - Cloud-based synchronization options
- Create unique passwords
  - Passwords are not the same across sites
- Personal and enterprise options
  - Corporate access

**Secure connections**
- Security alerts and invalid certificates
  - Something isn't quite right
  - Should raise your interest
- Look at the certificate details
  - May be expired or the wrong domain name
  - The certificate may not be properly signed (untrusted certificate authority)
  - Correct time and date is important

**Enable pop-up blockers**
- Pop-up blocker
  - Prevent unwanted notification windows
- Enable or disable
  - Should usually be enabled
  - Disable temporarily when troubleshooting
- Block and allow
  - Control pop-up blocking on certain websites

**Clearing private data**
- Clear browsing data
  - History
  - Saved passwords
  - List of downloaded files
- Clear cache
  - Parts of a website are stored locally
  - Remove all local data

**Private browsing mode**
- Don't store information from a browsing session
  - Good for privacy
  - Useful when testing or troubleshooting
- Removes the information when the browser is closed
  - No history tracking
  - No download file list
  - Cached information is deleted

**Browser data synchronization**
- Share browsing data across multiple systems
  - Sign in to the browser
- Use with other computers, tablets, and mobile devices
  - Browsing history, favorites, installed extensions, other settings

**Ad blockers**
- Some browsers can block advertising
  - This isn't always an option
- Many sites will track visits
  - And recognize a return visit
- Difficult to always recognize an advertisement
  - You can control the security level

**Proxy**
- Sits between the users and the external network
- Receives the user requests and sends the request on their behalf (the proxy)
- Useful for caching information, access control, URL filtering, content scanning
- Applications may need to know how to use the proxy (explicit)
- Some proxies are invisible (transparent)

**Proxy configuration**
- Choose the proxy settings in the browser
  - These are usually linked back to the OS settings
  - The proxy is used for all communication
- Only required for an explicit proxy
  - You configure the proxy IP address and port number
- A transparent proxy is invisible to the user
  - The proxy works without any specific configuration settings
- May be a required configuration
  - Without a proxy, you can't browse the Internet

**Secure DNS**
- DNS normally sends traffic in the clear
  - We can see every FQDN you're visiting
- Time to encrypt the DNS settings
  - DNS over HTTPS (DoH)
  - The same HTTPS we use for web servers
- The DNS server needs to support DoH
  - Many large DNS providers already support DoH
  - The list is growing

**Browser feature management**
- Enable / disable
  - Plugins
  - Extensions
  - Features
- Manual installation
  - Manage from the user interface
- Some extensions may be a security risk
  - Only use trusted plugins

# 3.1 - Troubleshooting Windows

**Bluescreens and frequent shutdowns**

- Startup and shutdown BSOD
  - Bad hardware, bad drivers, bad application
- Use Last Known Good, System Restore, or Rollback Driver
  - Try Safe mode
- Reseat or remove the hardware
  - If possible
- Run hardware diagnostics
  - Provided by the manufacturer
  - BIOS may have hardware diagnostics

**Degraded performance**

- Task Manager
  - Check for high CPU utilization and I/O
- Windows Update - Latest patches and drivers
- Disk space - Check for available space and defrag
- Laptops may be using power-saving mode
  - Throttles the CPU
- Anti-virus and anti-malware - Scan for attackers

**Boot errors**

- Can't find operating system
  - "Operating system not found", "Missing operating system"
- Boot loader replaced or changed
  - Multiple operating systems installed
- Check boot drives - Remove any media
- Startup Repair
- Modify the Windows Boot Configuration Database (BCD)
  - Formerly boot.ini
  - Recovery Console: `bootrec /rebuildbcd`

**Startup Repair**

- Missing NTLDR
  - The main Windows boot loader is missing
  - Run Startup Repair or replace manually and reboot
  - Disconnect removable media
- Missing operating system
  - Boot Configuration Data may be incorrect
  - Run Startup Repair or manually configure BCD store
- Boots to Safe Mode
  - Windows is not starting normally
  - Run Startup Repair

**Starting the system**

- Device not starting
  - Check Device Manager and Event Viewer
  - Often a bad driver
  - Remove or replace driver
- "One or more services failed to start"
  - Bad/incorrect driver, bad hardware
  - Try starting manually
  - Check account permissions
  - Confirm service dependencies
  - Windows service; check system files
  - Application service; reinstall application

**Applications crashing**

- Application stops working
  - May provide an error message
  - May just disappear
- Check the Event Log
  - Often includes useful reconnaissance
- Check the Reliability Monitor
  - A history of application problems
  - Checks for resolutions
- Reinstall the application
  - Contact application support

**Low memory warnings**

- Your computer is low on memory
  - Applications need RAM to run
  - More applications need more RAM
- Close large-memory processes
  - Check Task Manager
- Increase virtual memory
  - More room for swapping applications
  - System > About > Advanced system settings > Performance > Settings > Virtual memory

**USB controller resource warnings**

- USB devices contain buffers called "endpoints"
  - Different USB controllers support a different number of endpoints (96 endpoints, 254 endpoints, etc.)
- Different devices require a different number of endpoints
  - Exceed the number of endpoints and you run out of resources
  - It's difficult to determine the number of endpoints used by a device
- The controller does not have enough resources for this device.
  - The endpoints are these resources
- Move the device to a different USB interface
  - USB 2.0 interfaces might support a larger number of endpoints
- Match the USB interface to the device capabilities
  - USB 2.X devices or USB 3.X devices
  - More endpoints for all devices

## 3.1 - Troubleshooting Windows (continued)

### System instability

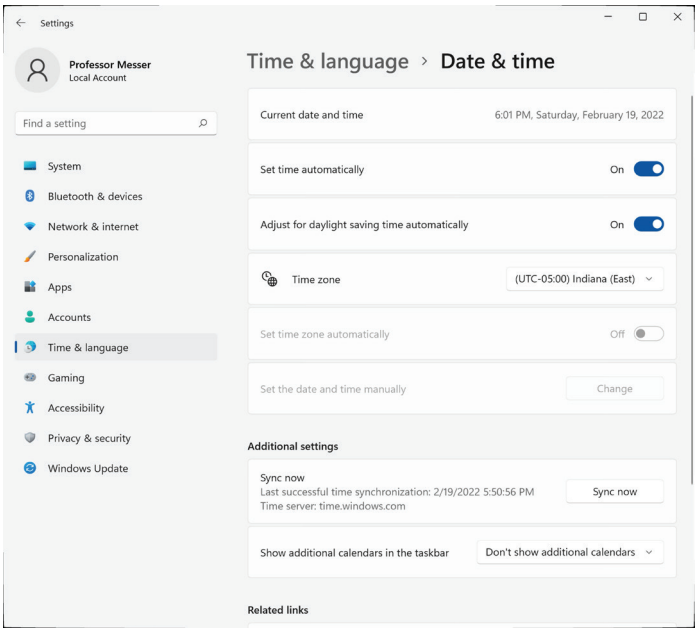
- General system failures
  - Software errors, system hangs, application failures
- Time for a full diagnostic - This could be anything
- Hardware diagnostic
  - Most systems include manufacturer diagnostics
  - Also run storage and memory checks
- Check the operating system
  - Run SFC (System File Checker)
  - Perform an anti-malware scan

### Slow profile load

- Roaming user profile
  - Your desktop follows you to any computer
  - Changes are synchronized
- Network latency to the domain controller
  - Slows login script transfers
  - Slow to apply computer and user policies
  - May require many hundreds (or thousands) of LDAP queries
- Client workstation picks a remote domain controller instead of local DC
  - Problems with local infrastructure

### Time drift

- A computer's internal clock will drift over time
  - Computers aren't great timekeepers
- The solution is to fix the symptom
  - Fixing the problem would require changing the design of every computer
- Enable automatic time setting
  - Settings > Time & language > Date & time
  - Time zone may need to be configured manually if privacy settings are enabled




## 3.2 - Troubleshooting Mobile Devices

### App issues

- Problematic apps
  - Apps not loading
  - Slow app performance
- Restart the phone
  - Hold power button, power off
- Stop the app and restart
  - iPhone: Double-tap home|slide up, slide app up
  - Android: Settings/Apps, select app, Force stop
- Update the app - Get the latest version

### App fails to close or crashes

- App hangs
  - But other apps are still working
- App crashes
  - May provide an error message, or just disappear
- Restart the device
  - Clear the slate, try the app again
- Update the app
  - A bug fix might resolve the issue
- Delete and reinstall the app
  - Be careful not to remove important app data

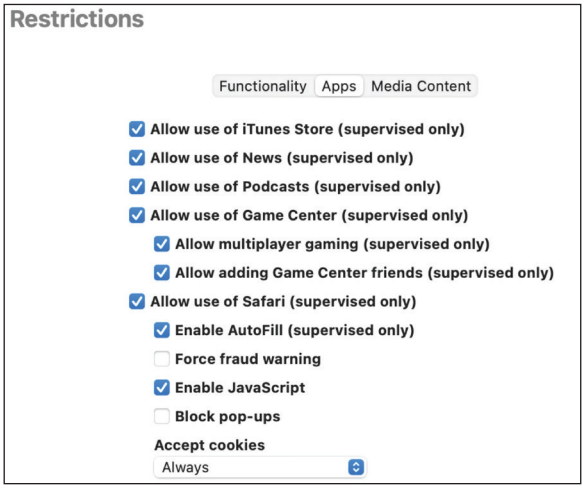
### App fails to update

- App does not update to a new version
  - But other apps are still working
- Check the Store to manually upgrade
  - Force the upgrade process
  - Some stores require a valid method of payment on file
- Restart the device
  - Try the update process again

### App fails to install

- Degraded Internet connection
  - Everything is downloaded from the cloud
- Limited storage space
  - Check for available space and clear enough room for the install

- Payment method not working
  - A valid payment method may also be required for free apps
  - Check the App Store or
  - Google Play account details
- MDM policies
  - An organization's mobile device manager (MDM) won't allow the installation
  - Compare against the existing policy list
- App store issues
  - Check the store status page and try again later




**OS fails to update**

- Device operating system will not update
  - New features, bug fixes, security updates
- Check available storage
  - Remove unused documents and apps
- Check download bandwidth
  - Connect to Wi-Fi
- Try a different network connection
  - Update server may not be accessible
- Reboot - Always a good idea

**Battery life issues**

- Bad reception
  - Always searching for signal
  - Airplane mode on the ground
- Aging battery
  - There's only so many recharges
- Disable unnecessary features
  - 802.11 wireless, Bluetooth, GPS
- Check application battery usage
  - iOS/iPadOS: Settings/Battery
  - Android: Settings/Battery

**Random reboots**

- A device reboots during normal operation
  - May occur randomly
- Check the OS and app versions
  - Keep everything up to date
- Perform a hardware check
  - Check the battery health
  - Not many diagnostics options
- Contact Tech Support for options
  - Crash logs should be on the device

**Connectivity issues**

- Intermittent connectivity
  - Move closer to access point
  - Try a different access point
- No WiFi connectivity
  - Check/Enable WiFi
  - Check security key configuration
  - Hard reset can restart wireless subsystem
- No Bluetooth connectivity
  - Check/Enable Bluetooth
  - Check/Pair Bluetooth component
  - Hard reset to restart Bluetooth subsystem
- NFC not working
  - Limited troubleshooting options
  - Device may allow disable/enable of NFC
  - Reset the device
  - If payment related, remove and add the card again
- AirDrop not working
  - Distance between devices < 30 feet
  - Turn on Wi-Fi and Bluetooth
  - Check AirDrop discovery options
  - "Allow me to be discovered by"

**Screen does not autorotate**

- Turning the device doesn't rotate the view
  - It should know which way is up
- Disable rotation lock
  - Prevents autorotation when enabled
- Restart the app
  - The device might be working properly
- Restart the device
  - Perhaps the device isn't working properly
- Contact device support
  - If nothing rotates, you could have a sensor issue

# 3.3 - Troubleshooting Mobile Device Security

**Unofficial application stores**
- Once malware is on a phone, it has a huge amount of access
  - Don't install APK (Android Package Kit) files from an untrusted source
- iOS - All apps are curated by Apple
- Android
  - Apps can be downloaded from Google Play or a trusted app store
  - Sideloading is where problems can occur

**Developer mode**
- Enables developer-specific settings
  - USB debugging, memory statistics, demo mode settings
- iOS and iPadOS
  - Enable using Xcode - Must use macOS
- Android
  - Enabled from Settings > About Phone
  - Tap the build number seven times

**Root access/jailbreaking**
- Mobile devices are purpose-built systems
  - You don't need direct access to the operating system
- Gaining access
  - Android - Rooting / Apple iOS - Jailbreaking
- Install custom firmware
  - Replaces the existing operating system
- Uncontrolled access
  - Circumvent security features, sideload apps without using an app store
  - The MDM becomes relatively useless

**Application spoofing**
- Install what appears to be a legitimate app
  - Actually a bootleg or malicious application
- Google removed 150 apps from the store in 2021
  - Photo editing, camera filters, games, QR code scanners
  - UltimaSMS app tried to subscribe users to $40/month SMS service
- Infect the application used to build the apps
  - A malicious version of Xcode: XcodeGhost malware
- Always check the source of a download
  - And the legitimacy of the app
  - You are giving this app permissions and control

**High network traffic**
- Higher than normal network use
  - May indicate installed malware
  - Command & control
  - Proxy network use
- Check built-in data use reports
  - Some of these are quite detailed
- Use a third-party reporting app
  - Use a trusted source
- Run a malware scan - Always a good precaution

**Degraded response time**
- Running slowly
  - Screen lags, poor input response time
- Restart
  - Clear the slate
- Check for OS and app updates
  - Fix the buggy code
- Close apps that are not in use
  - Less resources to manage
- Factory reset
  - A last chance to resolve the problem

**Data-usage limit notification**
- Built-in Android feature
  - Not native in iOS
  - iOS can limit a downloadable file size
- Set a warning and limit
  - Get notification when traffic is excessive
- Can indicate a malware infection
  - Drill-down on individual app usage
- Run a malware scan - Find the problem app

**Limited or no Internet connectivity**
- Malware doesn't want to be removed
  - It will prevent access to network resources
- Disable and enable Wi-Fi
  - Or enable/disable airplane mode
- Restart the device
  - Clear memory and reload drivers
- Perform a malware scan - Find and remove

**High number of ads**
- Malware wants to show you advertising
  - Revenue for each view and click
- May be difficult to find
  - 2019: Ads Blocker for Android promised to remove ads
  - Actually did the opposite
  - Once installed, wasn't listed in available apps
  - FakeAdsBlock malware strain
- Run anti-malware utility - Remove the adware

**Fake security warnings**
- The easiest way to get on a phone
  - Have the user install their own malware
- The warnings seem legitimate
  - They are not actual security issues
  - Do not install any software
- Malware can directly access user data
  - Steals credit card details, stored passwords, browsing history, text messages
- Don't click
  - If you click, run a malware removal tool

## 3.3 - Troubleshooting Mobile Device Security (continued)

**Unexpected application behavior**
- Apps unexpectedly close
  - Or have excessive delays
- App doesn't seem to have all of the normal features
  - Or included features are not working
- High battery utilization
  - Only when this application is running
- Update the app
  - Get the latest version

**Leaked personal files**
- Unauthorized account access
  - Unauthorized root access
  - Leaked personal files and data
- Determine cause of data breach
  - Perform an app scan, run anti-malware scan
- Factory reset and clean install
  - This is obviously a huge issue
- Check online data sources
  - Apple iCloud/Apple Configurator, Google Workspace, Microsoft OneDrive
  - Change passwords

## 3.4 - Troubleshooting Security Issues

**Unable to access the network**
- Slow performance, lock-up
  - Malware isn't the best written code
- Internet connectivity issues
  - Malware likes to control everything
  - You go where it wants you to go
  - You can't protect yourself if you can't download
- OS updates failures
  - Malware keeps you vulnerable
  - Some malware uses multiple communication paths
- Reload or clean
  - Malware cleaner or recover from known good backup

**Desktop alerts**
- Browser push notification messages
  - Pretends to be a malware infection
  - Actual notifications come from your antivirus utility
- Disable browser notifications
  - Create an allow list of legit sites
- Scan for malware
  - Consider a cleaning
  - Rebuild from scratch or known good backup to guarantee removal

**False antivirus alerts**
- False antivirus message
- May include recognizable logos and language
  - May require money to "unlock" your PC
  - Or to "subscribe" to their service
- Often requires a specific anti-malware removal utility or technique
  - The attackers are very, very good

**Altered system or personal files**
- Renamed system files
  - Won't need that anymore
- Files disappearing
  - Or encrypted
- File permission changes
  - Protections are modified
- Access denied
  - Malware locks itself away
  - It doesn't leave easily
- Use a malware cleaner or restore from known good backup
  - Some malware is exceptionally difficult to remove

**Unwanted OS notifications**
- Notifications can be useful
  - And can also be annoying
- Control notifications from the OS Settings
  - Available in almost any operating system
- Globally enable or disable notifications
  - Affects all applications and system services
- Manage on a per-application basis
  - Enable for mail, disable for Chrome

**OS update failures**
- The OS automatically updates
  - Unless there's an issue
- Updates from the cloud
  - Network connectivity
  - Firewalls or filtering
  - Bandwidth restrictions
- Windows includes their own troubleshooter
  - Windows Update troubleshooter
  - Settings / System / Troubleshoot /
  - Other troubleshooters

## 3.4 - Troubleshooting Security Issues (continued)

**Random pop-ups**

- Pop-ups in your browser
  - May look like a legitimate application
  - May be a malware infection
- Update your browser
  - Use the latest version
  - Check pop-up block feature
- Scan for malware
  - Consider a cleaning
  - Rebuild from scratch or known good backup to guarantee removal

**Certificate warnings**

- Security alerts and invalid certificates
  - Something isn't quite right
  - Should raise your interest
- Look at the certificate details
  - Click the lock icon
  - May be expired or the wrong domain name
  - The certificate may not be properly signed (untrusted certificate authority)
  - Correct time and date is important

**Browser redirection**

- Instead of your Google result, your browser goes somewhere else
  - This shouldn't ever happen
- Malware is the most common cause
  - Makes money for the bad guys
- Use an anti-malware/anti-virus cleaner
  - This is not the best option
- Restore from a good known backup
  - The only way to guarantee removal

**Degraded browser performance**

- A very complex application - So many potential issues
- Check for the latest version
  - Always keep the browser updated
- How many tabs are open? - I bet it's a lot
- Clear the cache and cookies
  - Cache problems are easy to fix; delete and try again
  - Cookies can hold session and authentication information
- Check the local device performance
  - Task Manager - CPU, RAM, network
- Malware might cause issues
  - Crypto-mining in the browser, anyone?
- Try a different browser
  - If the problem follows, it's not the browser

# 4.0 - Operational Procedures

## 4.1 - Ticketing Systems

**Ticketing systems**

- The best way to manage support requests
  - Document, assign, resolve, report
- Usually a responsibility of the help desk
  - Take the calls and triage
- Determine the best next step
  - Assign the ticket and monitor
- There are many different ticketing systems
  - They're all very similar in function

**Managing a support ticket**

- Information gathering
  - User and device information
  - Problem description
- Applying context
  - Categorization of the problem
  - Assign severity
  - Determine if escalation is required
- Clear and concise communication
  - Problem description, progress notes, resolution details

**User information**

- You can't address a person's problem unless you know who has the issue
  - Add the name of the person reporting the problem
- Usually integrated into a name service
  - Active Directory or similar
- May be added automatically
  - Many issues arrive from a portal or email gateway
- Always confirm the contact information
  - The database may not be up to date

**Device and description**

- Device information
  - Laptop, printer, conference room projector, etc.
- Description
  - One of the most important fields in the ticket
  - Make the description clear and concise
- The description determines the next step
  - Call back for more information
  - Associate with another event
  - Assign to another person

## 4.1 - Ticketing Systems (continued)

**Categorization and escalation**

- Categories
  - Broad description
  - Change request, hardware request, problem investigation, hardware failure, onboarding/offboarding, etc.
- Severity
  - Often an established set of standards
  - Low, medium, high, critical
- Escalation levels
  - Difficult problems can be handled by a specialist
  - Escalate to a new tier or to a specific group

**Resolving the issue**

- Progress notes
  - Many people may read and/or work on a single ticket
  - Keep the progress information concise
  - Document any changes or additional information
- Problem resolution
  - Document the solution
  - May be referenced later by others with the same problem
  - A "live" knowledgebase of issues and resolutions

## 4.1 - Asset Management

**Asset management**

- A record of every asset
  - Laptops, desktops, servers, routers, switches, cables, fiber modules, tablets, etc.
- Associate a support ticket with a device make and model
  - Can be more detailed than a user's description
- Financial records, audits, depreciation
  - Make/model, configuration, purchase date, location, etc.
- Add an asset tag
  - Barcode, RFID, visible tracking number, organization name

**Configuration management database (CMDB)**

- A central asset tracking system
  - Used by different parts of the organization
- Assigned users
  - Associate a person with an asset
  - Useful for tracking a system
- Warranty
  - A different process if out of warranty
- Licensing
  - Software costs
  - Ongoing renewal deadlines

**Procurement life cycle**

- The purchasing process
  - Multi-step process for requesting and obtaining goods and services
- Start with a request from the user
  - Usually includes budgeting information and formal approvals
- Negotiate with suppliers
  - Terms and conditions
- Purchase, invoice, and payment
  - The money part

## 4.1 - Document Types

**Incident reports**

- Security policy - An ongoing challenge
- Documentation must be available - No questions
- Incidents are ongoing
  - Organizations have formal incident plans
- Reports and documentation
  - Details of any security incident
  - Create a reference for future incidents

**Standard operating procedures**

- Organizations have different business objectives
  - Processes and procedures
- Operational procedures
  - Downtime notifications, facilities issues
- Software installation and upgrades
  - Custom installation of a software package
  - Testing, change control
- Documentation is the key
  - Everyone can review and understand the policies

**On-boarding**

- Bring a new person into the organization
  - New user setup checklist
- IT agreements need to be signed
  - May be part of the employee handbook or a separate AUP
- Create accounts
  - Associate the user with groups and departments
- Provide required IT hardware
  - Laptops, tablets, etc.
  - Preconfigured and ready to go

## 4.1 - Document Types (continued)

**Off-boarding**
- All good things… / End-user termination checklist
- This process should be predefined
  - You don't want to decide how to do things at this point
- What happens to the hardware?
- What happens to the data?
- Account information is usually deactivated
  - But not always deleted

**Service level agreement (SLA)**
- Minimum terms for services provided
  - Uptime, response time agreement, etc.
  - Commonly used between customers and service providers
  - May also be used for internal "customers"
- Contract with an Internet provider
  - SLA is no more than four hours of unscheduled downtime
  - Technician will be dispatched
  - May require customer to keep spare equipment on-site

**Knowledge base and articles**
- External sources
  - Manufacturer knowledge base
  - Internet communities
- Internal documentation
  - Institutional knowledge
  - Usually part of help desk software
- Find the solution quickly
  - Searchable archive
  - Automatic searches with helpdesk ticket keywords

## 4.2 - Change Management

**Change management**
- How to make a change
  - Upgrade software, patch an application, change firewall configuration, modify switch ports
- One of the most common risks in the enterprise
  - Occurs very frequently
- Often overlooked or ignored - Did you feel that bite?
- Have clear policies
  - Frequency, duration, installation process, rollback procedures
- Sometimes extremely difficult to implement
  - It's hard to change corporate culture

**Change management process**
- A formal process for managing change
  - Avoid downtime, confusion, and mistakes
- Nothing changes without the process
  - Complete the request forms
  - Determine the purpose of the change
  - Identify the scope of the change
  - Schedule a date and time of the change
  - Determine affected systems and the impact
  - Analyze the risk associated with the change
  - Get approval from the change control board
  - Get end-user acceptance after the change is complete

**Rollback plan**
- The change will work perfectly and nothing will ever go bad
  - Of course it will
- You should always have a way to revert your changes
  - Prepare for the worst, hope for the best
- This isn't as easy as it sounds
  - Some changes are difficult to revert
- Always have backups

**Backup plan**
- Complete the mission
  - This might require a number of different tactics
- Install a software update on a firewall
  - Connect to the web-based management front-end
  - Click Update
  - Wait for the download to complete
  - Press the reset button to restart the firewall
  - Test the firewall settings with the new software
- What if something goes wrong?
  - You need a backup plan
- It doesn't work.
  - Internet is down. Browser isn't properly interpreting the page. The download is failing halfway through. The update file isn't validating.
  - You thought this might happen, right?
- You need a plan B, C, and D
  - Download the file prior to the change
  - Have the file ready on a flash drive
  - Upload it via TFTP on the management interface
  - Perform the upgrade through the command line console
- These can be difficult to do in the moment
  - You should already have anticipated these issues

**Sandbox testing**
- Isolated testing environment
  - No connection to the real world or production system
  - A technological safe space
- Use before making a change to production
  - Try the upgrade, apply the patch
  - Test and confirm before deployment
- Confirm the rollback plan
  - Move everything back to the original
  - A sandbox can't consider every possibility

**Responsible staff members**
- A team effort
  - Many different parts of the organization
- IT team - Implements the change
- Business customer
  - The user of the technology or software
- Organization sponsor
  - Someone's budget is responsible for the process
  - Or responsible for the profit

**Change request forms**
- A formal process always seems to include a bit of paperwork
  - This is usually an online system
- Nothing gets missed
  - Easy to manage
  - Create detailed reports and statistics
- Usually a transparent process
  - Many different groups and people are usually involved

**Purpose of the change**
- Why are we doing this?
  - There needs to be a compelling reason
- Application upgrades
  - New features, bug fixes, performance enhancements
- Security fixes
  - Monthly patches and vulnerability fixes
- There needs to be a good reason
  - Changes are costly

**Scope of the change**
- Determine the effect of the change
  - May be limited to a single server
  - Or an entire site
- A single change can be far reaching
  - Multiple applications, Internet connectivity, remote site access, external customer access
- How long will this take?
  - Specific date and time for the change
  - May have no impact, could have hours of downtime

**Change types**
- Standard - low risk
  - A pre-approved change
  - This change happens all the time and is well-documented
  - Replacing the monitor on a user's desk
- Normal - medium risk
  - Not urgent. Follows the full change management process
  - Upgrading the database engine software
  - Replacing a core switch
- Emergency - high risk
  - Must be implemented quickly
  - A patch for a public-facing zero-day vulnerability

**Date and time of the change**
- Maintenance windows
  - Picking the right date and time is always a challenge
- On-demand / scheduled change windows
  - The date and time is determined as needed
- Regularly scheduled downtime
  - Always Sunday at 2 AM
- Change freeze
  - No changes for any reason
  - Usually during a specific block of time
  - For example, November 15 through January 5

**Affected systems and impact**
- A change is more than a single service
  - Rebooting a firewall brings down all Internet traffic
- This might be very limited
  - Or it might impact every user in the company
- Upgrade the software on a database server
  - What applications store data on this server?
  - What business systems are no longer working?
- Determine the total number of services
  - And understand the impact before getting approval

**Risk analysis**
- Determine a risk value - i.e., high, medium, low
- The risks can be minor or far-reaching
  - The "fix" doesn't actually fix anything
  - The fix breaks something else
  - Operating system failures
  - Data corruption
- What's the risk with NOT making the change?
  - Security or application vulnerability
  - Unexpected downtime to other services

## 4.2 - Change Management (continued)

**Change board and approvals**
- Go or no go
  - Lots of discussion
- All important parts of the organization are represented
  - Potential changes can affect the entire company
- Some changes have priority
  - The change board makes the schedule
  - Some changes happen quickly, some take time
- This is the last step
  - The actual work comes next

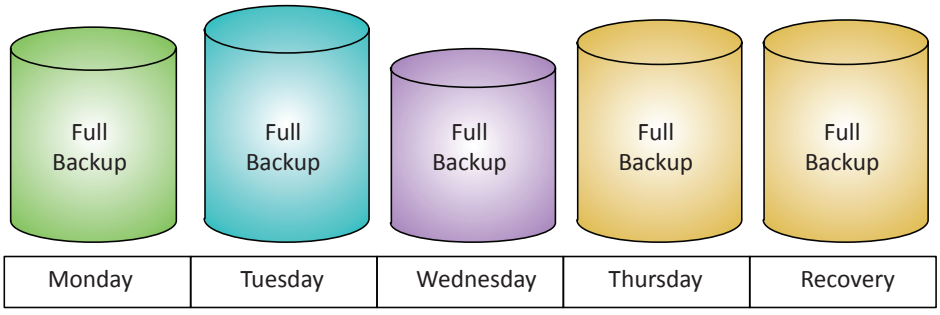
**Implementation and peer review**
- You've built a plan for the firewall update
  - Is it a good plan?
  - It's worth getting a second opinion
- Others will evaluate the plan
  - They might think of other issues
  - You might not have the complete picture
- This is a valuable part of change control
  - Institutional knowledge and smart people
  - Save time, avoid problems

**End-user acceptance**
- Nothing happens without a sign-off
  - The end users of the application / network
- One of your jobs is to make them successful
  - They ultimately decide if a change is worth it to them
- Ideally, this is a formality
  - Of course, they have been involved throughout this entire process
  - There's constant communication before and after

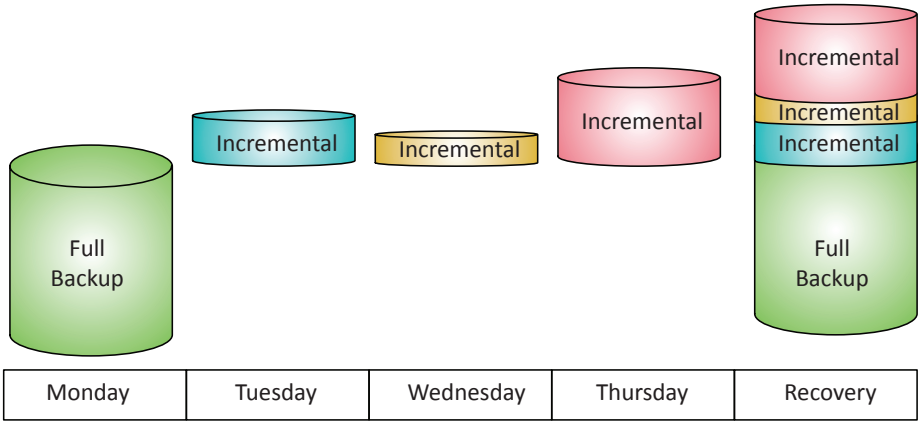
## 4.3 - Managing Backups

**Backups**
- Incredibly important
  - Recover important and valuable data
  - Plan for disaster
- Many different implementations
  - Total amount of data
  - Type of backup
  - Backup media
  - Storage location
  - Backup and recovery software
  - Day of the week

**Full Backup**
- Backup everything
  - All operating system and user files
- This is usually the longest backup process
  - It's everything in one backup
- Might be impractical every day
  - Long backup times
  - Lots of storage space



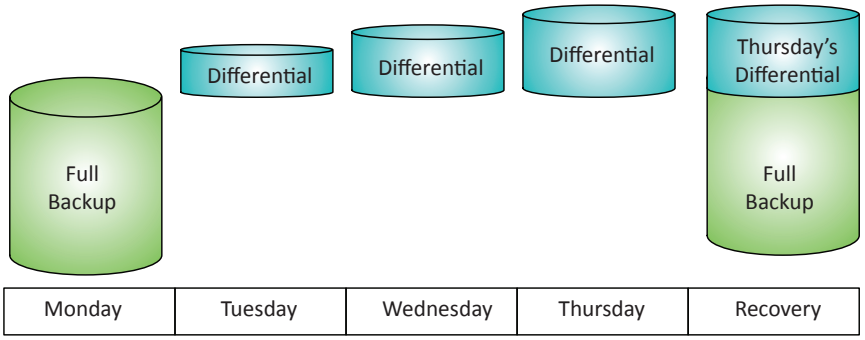

**Incremental Backup**
- A full backup is taken first
- Subsequent backups contain data changed since the last full backup and last incremental backup
  - These are usually smaller than the full backup
- A restoration requires the full backup and all of the incremental backups



# 4.3 - Managing Backups (continued)

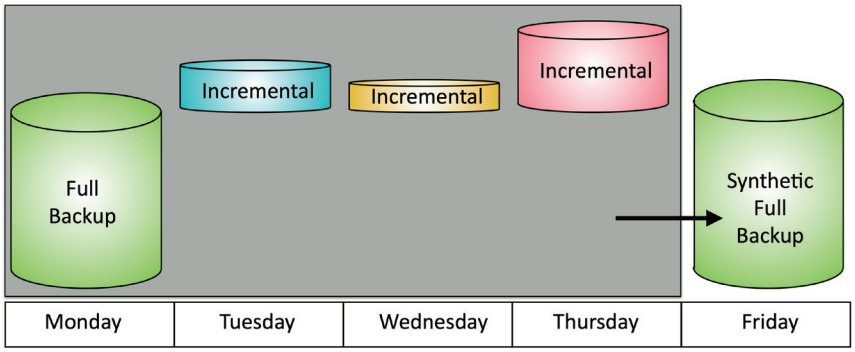
**Differential backup**

- A full backup is taken first
  - Subsequent backups contain data changed since the last full backup
  - These usually grow larger as data is changed
- A restoration requires the full backup and the last differential backup




**Synthetic backup**

- Create a full backup
  - Without actually performing a full backup
- Synthetic backup
  - The first full backup copies every file
  - Subsequent full backups are created from previous backups
- Can be faster and less bandwidth intensive
  - The advantage of a full backup
  - The efficiency of an incremental backup




| Type | Data Selection | Backup / Restore Time |
|---|---|---|
| Full | All selected data | High / Low<br>(one backup set) |
| Differential | All data modified<br>since the last full backup | Moderate / Moderate<br>(No more than 2 backup sets) |
| Incremental | New files and files modified<br>since the last backup | Low / High<br>(Multiple backup sets) |
| Synthetic | All selected data | Low / Low<br>(one backup set) |

**Backup testing**

- It's not enough to perform the backup
  - You have to be able to restore
- Disaster recovery testing
  - Simulate a disaster situation
  - Restore from backup
- Confirm the restoration
  - Test the restored application and data
- Perform periodic audits
  - Always have a good backup
  - Weekly, monthly, quarterly checks

**Recovery**

- Recovering from a backup
  - You've already tested this process
- In-place / overwrite
  - The original files are not viable
  - Replace files on the original system
  - Often used when reimaging
- Alternative location
  - There's always a concern with data loss
  - Restore to a separate system or drive
  - You won't lose anything on the original system

## 4.3 - Managing Backups (continued)

**On site vs. off site backups**
- On site backups
  - No Internet link required
  - Data is immediately available
  - Generally less expensive than off site
- Off site backups
  - Transfer data over Internet or WAN link
  - Data is available after a disaster
  - Restoration can be performed from anywhere
- Organizations often use both
  - More copies of the data
  - More options when restoring

**Grandfather-father-son (GFS)**
- Three separate backup rotations
  - For example, monthly, weekly, daily
- Twelve monthly full backups (grandfather)
  - A good choice for offsite storage
- Four (or five) weekly full backups (father)
  - Depends on which day of the month is selected
- Thirty-one daily incremental or differential backups (son)
  - Backup any daily changes

**GFS backup schedule**
- Choose a rotation
  - Every organization is different
- Grandfather
  - Last day of every month
- Father
  - Every Monday
- Son
  - Monday through Friday

**3-2-1 backup rule**
- A popular and effective backup strategy
  - For business or home use
- 3 copies of data should always be available
  - One primary copy and two backups
- 2 different types of media should be used
  - Local drive, tape backup, NAS
- 1 copy of the backup should be offsite
  - Offsite storage, cloud backup

## 4.4 - Managing Electrostatic Discharge

**What is electrostatic discharge?**
- Static electricity
  - Electricity that doesn't move
- Static electricity isn't harmful to computers
  - It's the discharge that gets them
- ESD can be very damaging to computer components
  - Silicon is very sensitive to high voltages
- Feel static discharge: ~3,500 volts
  - Damage an electronic component: 100 volts or less

**Controlling ESD**
- Humidity over 60% helps control ESD
  - Won't prevent all possible ESD
  - Keeping an air conditioned room at 60% humidity isn't very practical
- Use your hand to "self-ground"
  - Touch the exposed metal chassis before touching a component
  - You'll want to unplug the power connection
  - Always. Really.
- **Do not connect yourself to the ground of an electrical system!**

**Preventing static discharge**
- Anti-static strap
  - Connect your wrist to a metal part of the computer
- Anti-static pad
  - A workspace for the computer
- Anti-static mat
  - A mat for standing or sitting
- Anti-static bag
  - Safely move or ship components

**Component handling and storage**
- Try not to touch components directly
  - Card edges only
- Store in an HVAC regulated environment
  - Between 50 and 80 degrees Fahrenheit or 10 to 27 degrees Celsius
- Avoid high humidity
  - Silica gel packets can help control humidity
- Store in the original padded box
  - Bubble wrap can be a good alternative

## 4.4 - Safety Procedures

**WARNING**
- Power is dangerous
- **Remove all power sources before working**
- Don't touch ANYTHING if you aren't sure
- Replace entire power supply units
  – Don't repair internal components
- High voltage
  – Power supplies, displays, laser printers

**Equipment grounding**
- Most computer products connect to ground
  – Divert any electrical faults away from people
- Also applies to equipment racks
  – Large ground wire
- Don't remove the ground connection
  – It's there to protect you
- **Never connect yourself to the ground of an electrical system**
  – This is not a way to prevent ESD

**Cable management**
- Cables are unforgiving
  – Pay attention to their location
- Avoid trip hazards
  – Avoid cable runs across a floor
  – Secure and cover cables
- Use cable ties or velcro
  – A relatively permanent attachment

**Personal safety**
- Lifting technique
  – Lift with your legs, keep your back straight
  – Don't carry overweight items
  – You can get equipment to lift
- Electrical fire safety
  – Don't use water or foam
  – Use carbon dioxide, FM-200, or other dry chemicals
  – Remove the power source
- Safety goggles
  – Useful when working with chemicals
  – Printer repair, toner, batteries
- Air filter mask
  – Dusty computers
  – Printer toner

**Government regulations**
- Health and safety laws
  – Vary widely depending on your location
  – Keep the workplace hazard-free
- Building codes
  – Fire prevention, electrical codes
- Environmental regulation
  – High-tech waste disposal

## 4.5 - Environmental Impacts

**Disposal procedures**
- Read your Material Safety Data Sheets (MSDS)
  – United States Department of Labor,
  – Occupational Safety and Health Administration (OSHA)
  – https://www.osha.gov, Index page
- Provides information for all hazardous chemicals
  – Batteries, display devices / CRTs, chemical solvents and cans, toner and ink cartridges
- Sometimes abbreviated as Safety Data Sheet (SDS)
  – Different names in each country

**MSDS info**
- Product and company information
- Composition / ingredients
- Hazard information
- First aid measures
- Fire-fighting measures
- Accidental release / leaking
- Handling and Storage
- Much more

**Handling toxic waste**
- Batteries
  – Uninterruptible Power Supplies
  – Dispose at your local hazardous waste facility
- Toner
  – Recycle and reuse
  – Many printer manufacturers provide a return box
  – Some office supply companies will provide a discount for each cartridge
- Other devices and assets
  – Refer to the MSDS
  – Don't throw out without clear directions

**Room control**
- Temperature
  – Devices need constant cooling
  – So do humans
- Humidity level
  – High humidity promotes condensation
  – Low humidity promotes static discharges
  – 50% is a good number
- Proper ventilation
  – Computers generate heat
  – Don't put everything in a closet

## 4.5 - Environmental Impacts (continued)

**Battery backup**
- Uninterruptible Power Supply
  - Backup power
  - Power failures, under-voltage events, surges
- UPS types
  - Standby UPS, Line-interactive UPS, On-line UPS
- Features
  - Auto shutdown, battery capacity, outlets, phone line suppression

**Surge suppressor**
- Not all power is “clean”
  - Self-inflicted power spikes and noise
  - Storms, power grid changes
- Spikes are diverted to ground
- Noise filters remove line noise
  - Decibel (Db) levels at a specified frequency - Higher Db is better

**Surge suppressor specs**
- Joule ratings
  - Surge absorption
  - 200=good, 400=better
  - Look for over 600 joules of protection
- Surge amp ratings
  - Higher is better
- UL 1449 voltage let-through ratings
  - Ratings at 500, 400, and 330 volts
  - Lower is better

## 4.6 - Incident Response

**Incident response: Chain of custody**
- Control evidence - Maintain integrity
- Everyone who contacts the evidence
  - Avoid tampering, use hashes
- Label and catalog everything
  - Seal, store, and protect - Use digital signatures

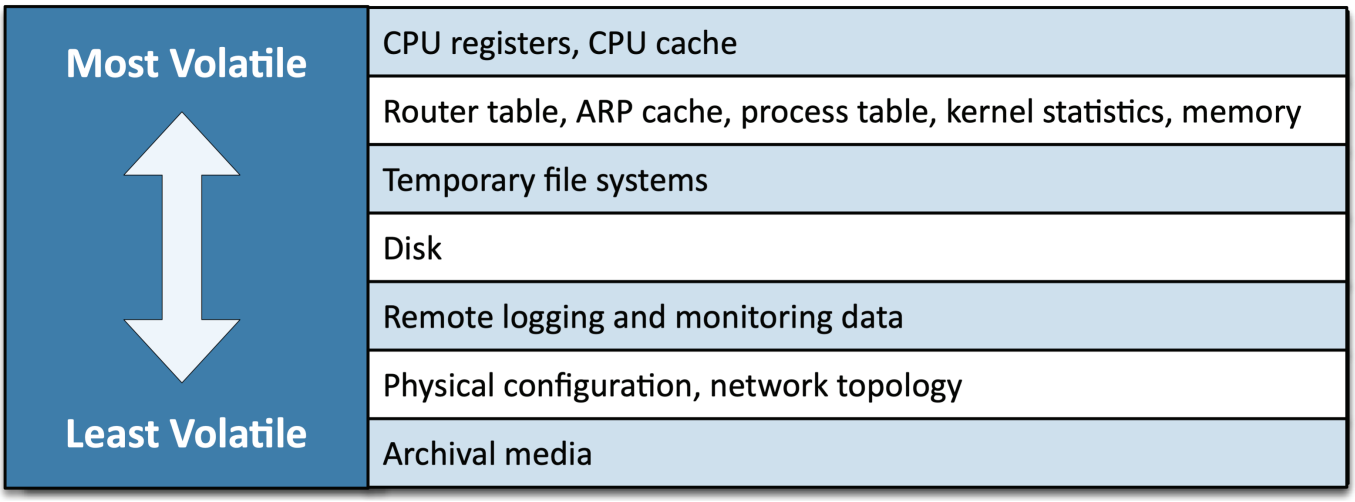
**Incident response: First response**
- Identify the issue - Logs, in person, monitoring data
- Report to proper channels
  - Don’t delay
  - May include internal management and law enforcement
- Collect and protect information relating to an event
  - Many different data sources and protection mechanisms

**Incident response: Copy of drive**
- Copy the contents of a disk - Bit-for-bit, byte-for-byte
- Remove the physical drive
  - Use a hardware write-blocker - Preserve the data
- Software imaging tools - Use a bootable device
- Use hashes for data integrity
  - Drive image is hashed to ensure that data has not been modified

**Incident response: Documentation**
- Document the findings
  - For Internal use, legal proceedings, etc.
- Summary information
  - Overview of the security event
- Detailed explanation of data acquisition
  - Step-by-step method of the process
- The findings - An analysis of the data
- Conclusion - Professional results, given the analysis

**Order of volatility**
- How long does data stick around?
  - Some media is much more volatile than others
  - Gather data in order from the most volatile to less volatile

**Order of volatility**



# 4.6 - Privacy, Licensing, and Policies

**Software licenses**
- Most software includes a license
  - Terms and conditions
  - Overall use, number of copies, and backup options
- Valid licenses
  - Per-seat or concurrent
- Non-expired licenses
  - Ongoing Subscriptions
  - Annual, three-year, etc.
  - Use the software until the expiration date

**Licenses**
- Personal license
  - Designed for the home user
  - Usually associated with a single device
  - Or small group of devices owned by the same person
  - Perpetual (one time) purchase
- Corporate use license
  - Per-seat purchase / Site license
  - The software may be installed everywhere
  - Annual renewals

**Open source license**
- Free and Open Source (FOSS)
  - Source code is freely available
  - End user can compile their own executable
- Closed source / Commercial
  - Source code is private
  - End user gets compiled executable
- End User Licensing Agreement (EULA)
  - Determines how the software can be used

**Non-disclosure agreement (NDA)**
- Confidentiality agreement between parties
  - Information in the agreement should not be disclosed
- Protects confidential information
  - Trade secrets
  - Business activities
  - Anything else listed in the NDA
- Unilateral or bilateral (or multilateral)
  - One-way NDA or mutual NDA
- Formal contract
  - Signatures are usually required

**Regulating credit card data**
- Payment Card Industry
  - Data Security Standard (PCI DSS)
  - A standard for protecting credit cards
- Six control objectives
  - Build and Maintain a Secure Network and Systems
  - Protect Cardholder Data
  - Maintain a Vulnerability Management Program
  - Implement Strong Access Control Measures
  - Regularly Monitor and Test Networks
  - Maintain an Information Security Policy

**Personal government-issued information**
- Used for government services and documentation
  - Social security number, driver license
- There may be restrictions on collecting or storing government information - Check your local regulations
- U.S. Office of Personnel Management (OPM)
  - Compromised personal identifiable information
  - Personnel file information; name, SSN, date of birth, job assignments, etc.
  - July 2015 - Affected ~21.5 million people

**PII - Personally identifiable information**
- Any data that can identify an individual
  - Part of your privacy policy - How will you handle PII?
- Not everyone realizes the importance of this data
  - It becomes a “normal” part of the day
  - It can be easy to forget its importance
- Attackers use PII to gain access or impersonate
  - Bank account information
  - Answer badly-written password-reset questions

**PHI - Protected Health Information**
- Health information associated with an individual
  - Health status, health care records, payments for health care, and much more
- Data between providers
  - Must maintain similar security requirements
- HIPAA regulations
  - Health Insurance Portability and Accountability Act of 1996

**Data retention requirements**
- Keep files that change frequently for version control
  - Files change often
  - Keep at least a week, perhaps more
- Recover from virus infection
  - Infection may not be identified immediately
  - May need to retain 30 days of backups
- Often legal requirements for data retention
  - Email storage may be required over years
  - Some industries must legally store certain data types
  - Different data types have different storage requirements
  - Corporate tax information, customer PII, tape backups, etc.

## 4.6 - Privacy, Licensing, and Policies (continued)

**Acceptable use policies (AUP)**
- What is acceptable use of company assets?
  - Detailed documentation
  - May be documented in the Rules of Behavior
- Covers many topics
  - Internet use, telephones, computers, mobile devices, etc.
- Used by an organization to limit legal liability
  - If someone is dismissed, these are the well-documented reasons why

**Splash screens**
- A message, logo, or graphic shown during startup or login
  - Can be used for branding or to require compliance
- Can be informational
  - Maintenance notifications or system changes
- May be required for legal or administrative purposes
  - Warnings about system misuse
  - Information about relying on application data

## 4.7 - Professionalism

**Professional appearance**
- Match the attire of the current environment
  - Everyone should feel comfortable about their dress
- Formal
  - Some organizations have specific requirements
- Business casual
  - A more relaxed style
- Find the right balance
  - Follow the organization's lead

**Avoid being judgmental**
- Cultural sensitivity
  - Use appropriate professional titles
- You're the teacher
  - Not the warden
  - Leave insults on the playground
- Make people smarter
  - They'll be better technologists
- You're going to make some BIG mistakes
  - Remember them.

**Be on time and avoid distractions**
- Don't allow interruptions
  - No personal calls, no texting, no Twitter
  - Don't talk to co-workers
- Apologize for delays and unintended distractions
  - Create an environment for conversation
  - In person
- Open and inviting
  - Candy bowl can be magical
  - On the phone
  - Quiet background, clear audio
  - Stay off the speakerphone

**Difficult situations**
- Technical problems can be stressful
- Don't argue or be defensive
  - Don't dismiss
  - Don't contradict
- Diffuse a difficult situation with listening and questions
  - Relationship-building
- Communicate
  - Even if there's no update
- Never take the situation to social media

**Maintain confidentiality**
- Privacy concerns
  - Sensitive information
  - Both professional and private
  - On the computer, desktop, or printer
- Professional responsibilities
  - IT professionals have access to a lot of corporate data
- Personal respect
  - Treat people as you would want to be treated

## 4.7 - Communication

**Communication skills**
- One of the most useful skills for the troubleshooter
- One of the most difficult skills to master
- A skilled communicator is incredibly marketable

**Avoid jargon**
- Abbreviations and TLAs - Three Letter Acronyms
- Avoid acronyms and slang - Be the translator
- Communicate in terms that everyone can understand
  - Normal conversation puts everyone at ease
  - Decisions are based on what you say
- These are the easiest problems to avoid

**Maintain a positive attitude**
- Positive tone of voice
  - Partner with your customer - Project confidence
- Problems can't always be fixed
  - Do your best - Provide helpful options
- Your attitude has a direct impact on the overall customer experience

**Avoid interrupting**
- But I know the answer!
- Why do we interrupt?
  - We want to solve problems quickly
  - We want to show how smart we are
- Actively listen, take notes
  - Build a relationship with the customer
  - They'll need help again someday
  - Don't miss a key piece of information
  - Especially useful on the phone
- This skill takes time to perfect
  - The better you are, the more time you'll save later

**Clarify customer statements**
- Ask pertinent questions
  - Drill-down into the details
  - Avoid an argument
  - Avoid being judgmental
- Repeat your understanding of the problem back to the customer
  - Did I understand you correctly?
- Keep an open mind
  - Ask clarifying questions, even if the issue seems obvious
  - Never make assumptions

**Setting expectations**
- Offer different options - Repair or replace
- Document everything - No room for questions
- Keep everyone informed
  - Even if the status is unchanged
- Follow up afterwards - Verify satisfaction

## 4.8 - Scripting Languages

**Scripting languages**
- Automate with the right tools
  - The script should match the requirement
- May be specific to a task or operating system
  - Your choices may already be limited
- You will probably learn more than one of these
  - An important skill for any technician

**Batch files**
- .bat file extension
  - Scripting for Windows at the command line
  - Legacy goes back to DOS and OS/2

**Windows PowerShell**
- Command line for system administrators
  - .ps1 file extension
  - Included with Windows 10 and 11
- Extend command-line functions
  - Uses cmdlets (command-lets)
  - PowerShell scripts and functions
  - Standalone executables
- Automate and integrate
  - System administration, Active Domain administration

**Microsoft Visual Basic Scripting Edition**
- VBScript
  - .vbs file extension
- General purpose scripting in Windows
  - Back-end web server scripting
  - Scripting on the Windows desktop
  - Scripting inside of Microsoft Office applications

**Shell script**
- Scripting the Unix/Linux shell
  - Automate and extend the command line
- Starts with a shebang or hash-bang #!
  - Often has a .sh file extension

**JavaScript**
- Scripting inside of your browser
  - .js file extension
- Adds interactivity to HTML and CSS
  - Used on almost every web site
- JavaScript is not Java
  - Different developers and origins
  - Very different use and implementation

**Python**
- General-purpose scripting language
  - .py file extension
- Popular in many technologies
  - Broad appeal and support

# 4.8 - Scripting Use Cases

**Basic automation**
- Automate tasks
  - You don't have to be there
  - Solve problems in your sleep
  - Monitor and resolve problems before they happen
- The need for speed
  - The script is as fast as the computer
  - No typing or delays
  - No human error
- Automate mundane tasks
  - You can do something more creative

**Restarting machines**
- Turning it off and back on again
  - An important task
- Application updates
  - Some apps require a system restart
- Security patches
  - Deploy overnight and reboot the system
- Troubleshooting
  - The once-a-day restart
  - You may not have physical access

**Remapping network drives**
- Shared network drives
  - The link between the user and their data
- A common task during startup
  - Login scripts provide the connection
- Automate software changes
  - Map a drive to the repository
- Add or move user data
  - Automate the process

**Application installations**
- Install applications automatically
  - Don't walk a flash drive to every computer
  - Many applications have an automated installation process
  - Scripting can turn this into a hands-off process
- On-demand or automatic installation scripts
  - Map the application installation drive
  - Install the application without user prompts
  - Disconnect the drive
  - Restart the system

**Automated backups**
- Usually performed at night or during off-hours
  - Get a copy of all important data
- Time consuming
  - File systems, network connections
- Script an automated backup process
  - Works while you sleep
  - Don't have to think about it

**Information gathering**
- Get specific information from a remote device
  - Monitoring and reporting
- Performance monitoring
  - Confirm proper operation of a device
- Inventory management
  - Check the hardware or software configuration
- Security and vulnerability checks
  - Check for certain application or library versions
  - Plan for the latest patches

**Initiating updates**
- Nothing ever stays the same
  - Constant changes and updates
- Operating systems
  - New features
  - Security patches
- Device drivers
  - Bug fixes
  - New hardware or OS support
- Applications
  - New version rollouts

**Other scripting considerations**
- Unintentionally introducing malware
  - Make sure you know what you're installing
- Inadvertently changing system settings
  - Test all updates
  - Track the file and registry changes
- Browser or system crashes
  - Mishandling of resources
  - A single character in a script can have unintended consequences
  - Always have a backup
  - Always test before deployment

# 4.9 - Remote Access

**Remote desktop connections**
- Share a desktop from a remote location
  - It's like you're right there
- RDP (Microsoft Remote Desktop Protocol)
  - Clients for Mac OS, Linux, and others as well
- VNC (Virtual Network Computing)
  - Remote Frame Buffer (RFB) protocol
  - Clients for many operating systems
  - Many are open source
- Commonly used for technical support
  - And for scammers

**Remote desktop security**
- Microsoft Remote Desktop
  - An open port of tcp/3389 is a big tell
  - Brute force attack is common
- Third-party remote desktops
  - Often secured with just a username and password
  - There's a LOT of username/password re-use
- Once you're in, you're in
  - The desktop is all yours
  - Easy to jump to other systems
  - Obtain personal information, bank details
  - Make purchases from the user's browser

**VPNs**
- Virtual Private Networks
  - Encrypted (private) data traversing a public network
- Concentrator
  - Encryption/decryption access device
  - Often integrated into a firewall
- Many deployment options
  - Specialized cryptographic hardware
  - Software-based options available
- Used with client software
  - Sometimes built into the OS

**VPN security**
- VPN data on the network is very secure
  - The best encryption technologies
- Authentication is critical
  - An attacker with the right credentials can gain access
- Almost always includes multi-factor authentication (MFA)
  - Require more than just a username and password

**SSH (Secure Shell)**
- Encrypted console communication - tcp/22
- Looks and acts the same as Telnet - tcp/23

**SSH security**
- The network traffic is encrypted
  - Nothing to see in the packets
- Authentication is a concern
  - SSH supports public/private key pair authentication
- Certain accounts should be disabled in SSH
  - For example, root
  - Consider removing all password-based authentication
- Limit access to SSH by IP address
  - Configure a local firewall or network filter

**RMM**
- Managed Service Providers (MSP)
  - Many customers and systems to monitor
  - Many different service levels
- Remote Monitoring and Management (RMM)
  - Manage a system from a remote location
- Many features
  - Patch operating systems
  - Remote login
  - Anomaly monitoring
  - Hardware/software inventory

**RMM security**
- A popular attack point
- The RMM has a great deal of information and control
- Access should be limited
  - Don't allow everyone to connect to the RMM service
- Auditing is important
  - Know who's connecting to which devices and what they're doing

**SPICE**
- Simple Protocol for Independent Computing Environments
  - View and control the remote display of a virtual machine
  - A more VM-centric remote desktop
- Helps manage virtual machines
  - Many different operating systems
  - One seamless remote control solution
- Feels like other remote desktops
  - Efficient graphics rendering
  - Fast response times
  - Folder and clipboard sharing

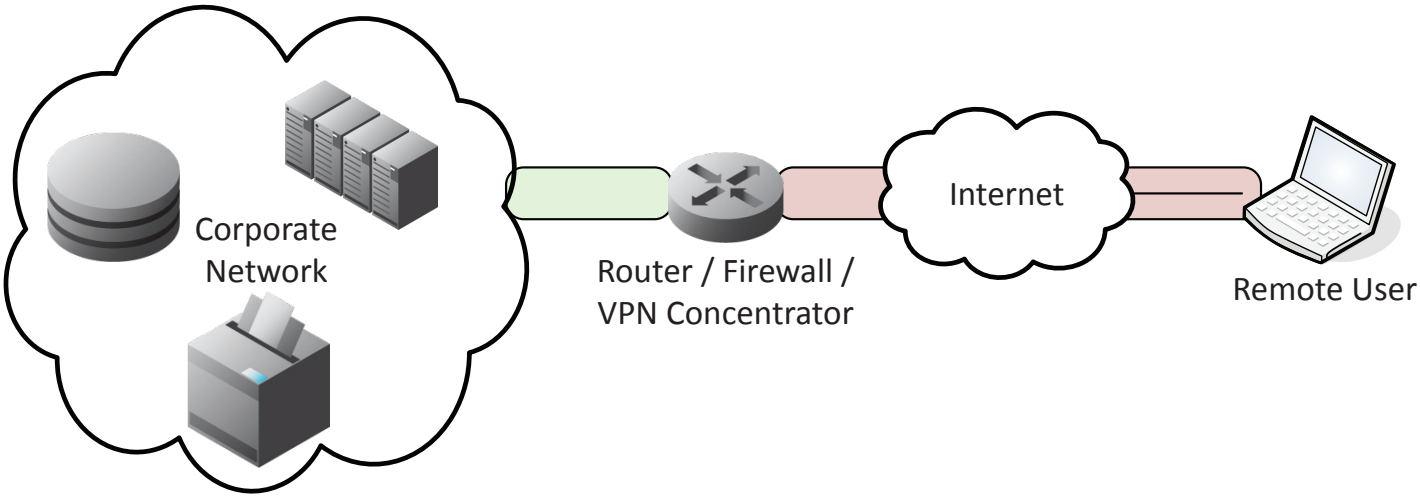
## 4.9 - Remote Access (continued)

**Windows Remote Management (WinRM)**
- Run command line commands and scripts on a remote Windows server
  - On by default on most modern Windows servers
- Administrator sends a script to a remote device
  - Secure communication and authentication required
- The script runs on the remote device
  - As if the administrator was local
- The resulting output is sent back to the requesting workstation
  - You didn't even have to leave your chair

**MSRA/Quick Assist security**
- No ongoing remote desktop service required
  - Avoids unintended access
  - No port forwarding
- Email with invitation details is always a concern
  - Consider using voice communication
- Perhaps a bit too easy to use
  - Social engineering can be an issue

**Third-party tools**
- Screen-sharing
  - See and control a remote device
  - GoToMyPC, TeamViewer
- Video-conferencing
  - Multi-user meetings with video and audio
  - Zoom, WebEx
- File transfer
  - Store and share documents in the cloud
  - Dropbox, Box.com, Google Drive
- Desktop management
  - Manage end-user devices and operating systems
  - Citrix Endpoint Management, ManageEngine Desktop Central

**Client-to-site VPN**
- On-demand access from a remote device
  - Software connects to a VPN concentrator
- Some software can be configured as always-on




## 4.10 - Managing AI

**Artificial Intelligence (AI)**
- Technology designed to meet or exceed human intelligence
  - Learn, infer, reason - a "thinking" computer
- Not a new concept
  - Decades in development
  - Lots of science fiction stories (now often science fact)
- A recent iteration is generative AI
  - Generating new content based on existing data
  - Text, audio, video (deepfakes)

**Application integration**
- AI is everywhere
  - Integrated into the apps we use every day
- Search engines
  - Search results are consolidated and summarized
  - Combines the results from multiple locations into a single view
- Email applications and services
  - Summarize email messages
- Graphics editors
  - Fill or remove image content with generative AI
  - Describe an image and it appears

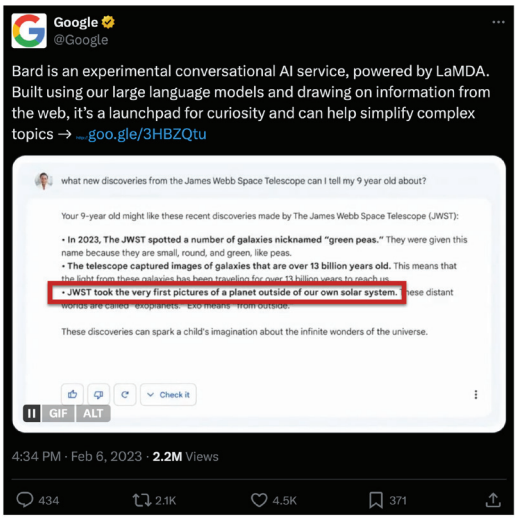
# 4.10 - Managing AI (continued)

**Appropriate AI use**
- Process large data repositories
  - Correlate diverse data types and identify trends
  - Look through terabytes of log files to identify potential security issues
- Automation
  - Identify issues and correct them without any human intervention
- Healthcare
  - Provide diagnostics, qualify drug interactions, ongoing monitoring
- Communication
  - Real-time language translation
  - Proofreading

**Inappropriate AI use**
- Fraud
  - Impersonating a real person
  - "Deep fake" audio and video
- Unethical shortcuts
  - The AI creates the application code
  - Graphical design is not human generated
- Plagiarism
  - Paraphrase existing works without proper citation

**AI bias**
- AI only knows what is it told
  - It can make the wrong conclusions
- Bias in the data
  - Healthcare data with an underrepresented ethnic or gender group
- Bias in the algorithms
  - The coding unknowingly creates a bias
- Amazon resume AI analysis for hiring
  - Based on 10 years of submitted resumes
  - Previous resumes used terms such as "executed" and "captured"
  - The AI was biased towards picking male CVs

**AI hallucinations**
- Misinterpretations of the data
  - A confidently incorrect AI
- Pictures containing a snout, a tail, and four legs, is a dog
  - A cloud appears to have a nose, tail, and four legs
  - The cloud is obviously a real dog
- Many, many examples of this
  - You've probably had some yourself
- Google and Microsoft introduces their new AI technologies, Google Bard and Microsoft Bing Chat
  - Both provided article summaries which had incorrect statements of fact
- Google introduces their new AI technology, Google Bard
  - The introductory post resulted in a hallucination
  - https://x.com/google/status/1622710355775393793




**AI accuracy**
- AI builds conclusions using models
  - Sometimes those models make bad predictions
- This is a common AI measurement
  - Get predictions from an AI
  - Compare those predictions to known test data
- Originality.ai AI Fact Checking Accuracy Study, August 2024
  - https://originality.ai/blog/ai-fact-checking-accuracy
  - Accuracy percentages:
  - Originality.ai: 72.3%, GPT-4: 64.9%, GPT-3.5: 58.6%,
  - CodeLlama-34b: 58.6%, Llama-2-70b: 55.2%, Llama-2-13b: 55.0%

**Private vs public AI**
- Public AI
  - Openly available on the Internet
  - ChatGPT, Google Gemini, Microsoft Copilot
- Private AI
  - An internal AI engine
  - Contains proprietary company data
  - An organization has complete control over the AI modeling
- Data security
  - Information added to the AI engine could be retrieved by others
  - Passwords, encryption keys, certificate details
  - Private AI sources can limit this breach
- Data source
  - Private data is specific to a single entity
  - Public data can be used by everyone
- Data privacy
  - Huge amounts of data; about YOU
  - AI knows where you live, your habits, your memberships
  - You're applying for a job; should the AI create a profile of you?

Continue your journey on
**ProfessorMesser.com:**


Professor Messer's Free
CompTIA A+ Training Courses

Monthly A+ Study Group Live Streams

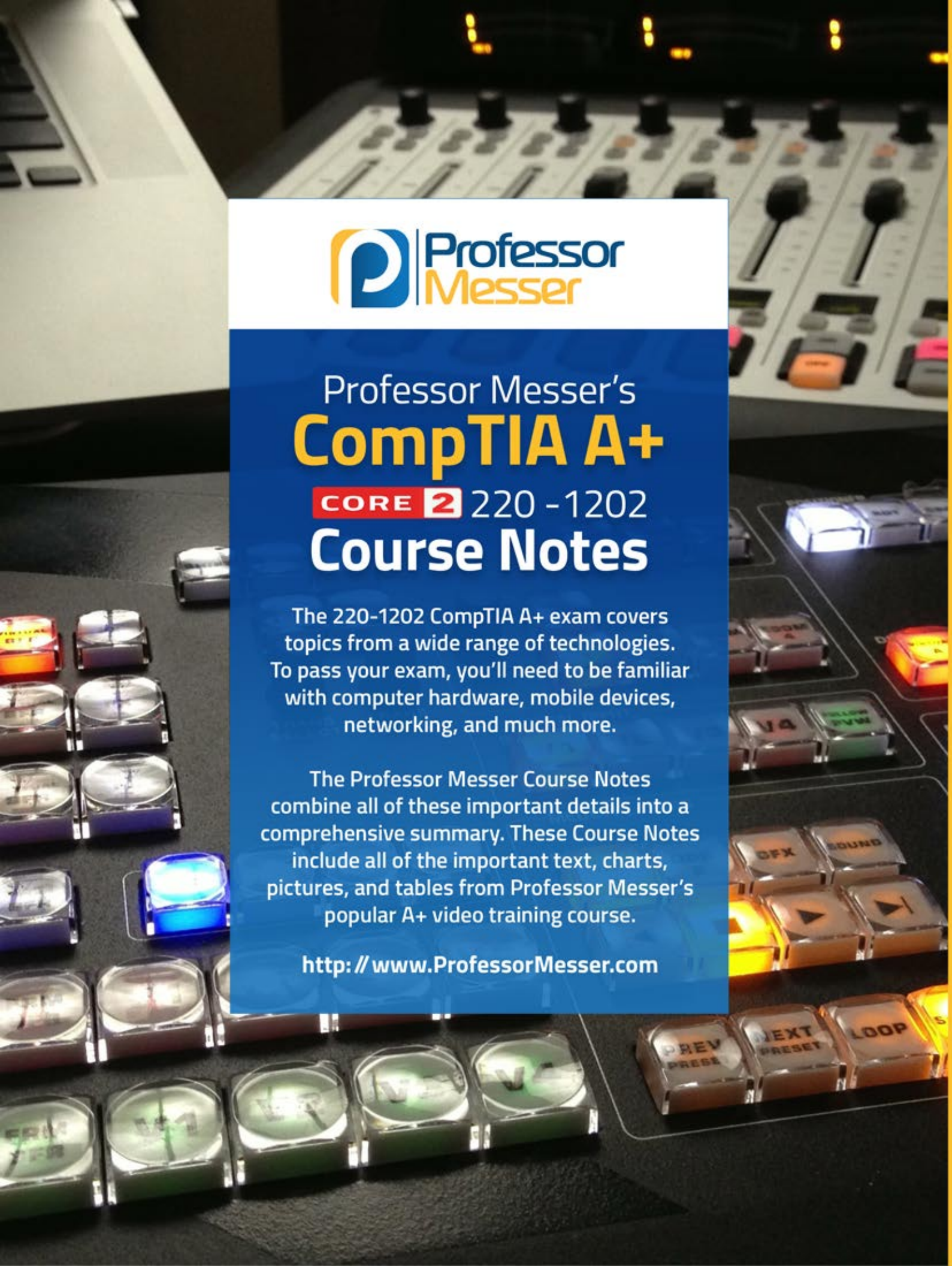
24 x 7 Live Discord Chat

Professor Messer's
CompTIA A+ Success Bundle

Voucher Discounts

Professor Messer

https://www.ProfessorMesser.com



Professor Messer

Professor Messer's

# CompTIA A+

CORE 2 220 -1202

# Course Notes

The 220-1202 CompTIA A+ exam covers topics from a wide range of technologies. To pass your exam, you'll need to be familiar with computer hardware, mobile devices, networking, and much more.

The Professor Messer Course Notes combine all of these important details into a comprehensive summary. These Course Notes include all of the important text, charts, pictures, and tables from Professor Messer's popular A+ video training course.

**http://www.ProfessorMesser.com**