Professor Messer

Professor Messer's

CompTIA A+

220 -1002 Core 2

Course Notes

James "Professor" Messer

Professor Messer's CompTIA 220-1002 Core 2 A+ Course Notes

James "Professor" Messer

http://www.ProfessorMesser.com

Professor Messer's CompTIA 220-1002 Core 2 A+ Course Notes
Written by James "Professor" Messer

http://www.ProfessorMesser.com

First Edition: September 2018

Trademark Acknowledgments

Warning and Disclaimer
This book is designed to provide information about the CompTIA 220-1002 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 220-1001 and the 220-1002 exams. You must pass both exams to earn your CompTIA A+ certification. This book provides a set of notes for the 220-1002 Core 2 exam.

The 220-1002 Core 2 exam

The 220-1002 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 220-1002 exam domains:

Domain 1.0 - Operating Systems - 27%
Domain 2.0 - Security - 24%
Domain 3.0 - Software Troubleshooting - 26%
Domain 4.0 - Operational Procedures - 23%

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+
220-1002 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, hard drives, USB drives
- Operating system configuration and management tools

Microsoft Windows
- Major market presence
- Many different versions
  - Windows 10, Windows Server 2016
- 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

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

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

Operating system technologies
- 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

Windows on a mobile device
- Microsoft Windows 10
  - Fully-featured tablets
- Many different manufacturers
  - Touchscreen computer
  - Keyboards
  - Pen stylus
- Windows Mobile
  - No longer in active development
  - No support after December 2019

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, Mac OS X, and Linux with the Android SDK
  - Apps available from Google Play
  - Apps also available from third-party sites

1.1 - Operating Systems Overview (continued)

Apple iOS
- Apple iPhone and Apple iPad OS
- Based on Unix
- Closed-source - No access to source code
- Exclusive to Apple products
- iOS Apps
  - Apps are developed with iOS SDK on Mac OS X
  - Apps must be approved by Apple before release
  - Apps are available to users in the Apple App Store

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

Vendor-specific limitations
- End-of-life
  - Different companies set their own EOL policies
- Updating
  - iOS, Android, and Windows 10 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

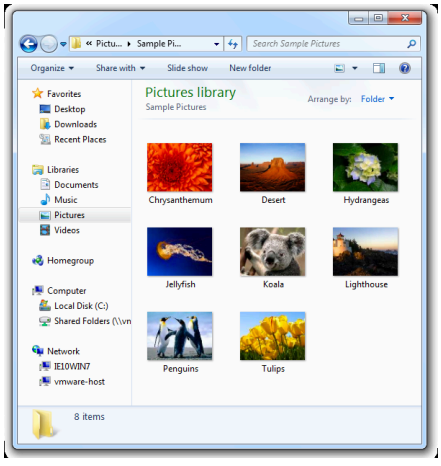
1.2 - An Overview of Windows 7

Windows 7
- Released October 22, 2009
  - Mainstream support ended January 13, 2005
  - Extended support until January 14, 2020
- Very similar to Windows Vista
  - Maintained the look and feel
  - Used the same hardware and software
  - Increased performance
- Updated features
  - Libraries, HomeGroup, pinned taskbar

Windows 7 Starter
- Built for netbooks
- No DVD playback or Windows Media Center, no Windows Aero, no Internet Connection Sharing (ICS), no IIS Web Server
- No enterprise technologies
  - No Domain connection, BitLocker, EFS, etc.
- Only a 32-bit version, maximum of 2 GB of RAM

Windows 7 Home Premium
- The consumer edition
  - DVD playback, Windows Aero, Internet Connection Sharing, IIS Web Server
- No enterprise technologies
  - No domain connection, BitLocker, EFS, etc.
- x64 version supports 16 GB of RAM and 2 processors

Windows 7 Ultimate
- Complete functionality
- Domain support, Remote Desktop, EFS
- All enterprise technologies, including BitLocker
- x64 version supports 192 GB of RAM
- Same features as Windows 7 Enterprise
  - But for the home user



Windows 7 Professional
- Same features as Home Premium
- Can connect to a Windows Domain
- Supports Remote Desktop Host and EFS
- Missing enterprise technologies - no BitLocker
- x64 version supports 192 GB of RAM

Windows 7 Enterprise
- Sold only with volume licenses
- Designed for very large organizations
- Multilingual User
- Interface packages

Windows 7

	Windows 7 Minimum Requirements (x86)	Windows 7 Minimum Requirements (x64)
Processor / CPU	1 GHz processor	
Memory	1 GB RAM	2 GB RAM
Free disk space	16 GB	20 GB
Video	DirectX 9 graphics device with WDDM 1.0 or higher driver	

Windows 7 Edition	DVD Playback	Aero	ICS	Domain Member	EFS	BitLocker	x86 RAM	x64 RAM
Starter	✖	✖	✖	✖	✖	✖	2 GB	N/A
Home Premium	✓	✓	✓	✖	✖	✖	4 GB	16 GB
Professional	✓	✓	✓	✓	✓	✖	4 GB	192 GB
Enterprise	✓	✓	✓	✓	✓	✓	4 GB	192 GB
Ultimate	✓	✓	✓	✓	✓	✓	4 GB	192 GB

Windows 8 and 8.1

	Windows 8/8.1 Minimum Requirements (x86)	Windows 8/8.1 Minimum Requirements (x64)
Processor / CPU	1 GHz processor with support for PAE, NX, and SSE2	
Memory	1 GB RAM	2 GB RAM
Free disk space	16 GB	20 GB
Video	Microsoft DirectX 9 graphics device with WDDM driver	

Windows 8/8.1 Edition	Windows Media Player	EFS	BitLocker	Domain Member	AppLocker	BranchCache	Max x86 RAM	Max x64 RAM
Core	✓	✖	✖	✖	✖	✖	4 GB	128 GB
Pro	✓	✓	✓	✓	✖	✖	4 GB	512 GB
Enterprise	✓	✓	✓	✓	✓	✓	4 GB	512 GB

Windows 10

	Windows 10 Minimum Requirements (x86)	Windows 10 Minimum Requirements (x64)
Processor / CPU	1 GHz processor with support for PAE, NX, and SSE2	
Memory	1 GB RAM	2 GB RAM
Free disk space	16 GB	20 GB
Video	Microsoft DirectX 9 graphics device with WDDM driver	

Windows 10 Edition	Hyper-V	BitLocker	Domain Member	AppLocker	BranchCache	Max x86 RAM	Max x64 RAM
Home	✖	✖	✖	✖	✖	4 GB	128 GB
Pro	✓	✓	✓	✖	✖	4 GB	2048 GB
Education/ Enterprise	✓	✓	✓	✓	✓	4 GB	2048 GB

1.2 - An Overview of Windows 8 and 8.1

Windows 8 and 8.1

- Windows 8
  - Available October 26, 2012
  - New user interface - no traditional “Start” button
- Windows 8.1
  - Released October 17, 2013
  - A free update to Windows 8 - not an upgrade
- Mainstream support ended January 9, 2018
  - Extended support ends January 10, 2023

Windows 8/8.1 Core

- A basic version for the home - x86 and x64 versions
- Microsoft account integration
  - Login to your computer and all of your services
- Windows Defender
  - Integrated anti-virus and anti-malware
- Windows Media Player
  - Play audio CD and DVDs

Windows 8/8.1 Pro

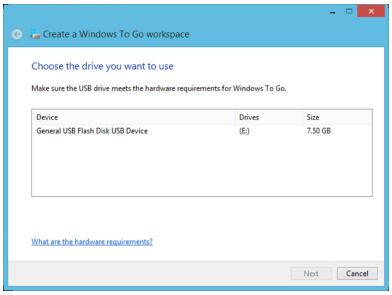
- The professional version
  - Similar to Windows 7 Professional / Ultimate
- Full support for BitLocker and EFS
  - Full-disk and file-level encryption
- Join a Windows Domain
  - Support for IT management
- Group Policy support
  - Centralized management of Windows devices

Windows 8/8.1 Enterprise

- Available to “Software Assurance” customers
  - Large volume licenses
- Adds enterprise features
  - AppLocker
  - Windows To Go
  - DirectAccess
  - BranchCache

Windows 8/8.1 processor requirements

- PAE (Physical Address Extension)
  - 32-bit processors can use more than
  - 4 GB of physical memory
- NX (NX Processor Bit)
  - Protect against malicious software
- SSE2 (Streaming SIMD Extensions 2)
  - A standard processor instruction set
  - Used by third-party applications and drivers



1.2 - An Overview of Windows 10

Windows 10
- Released on July 29, 2015
  - We skipped Windows 9
- A single platform
  - Desktops, laptops, tablets, phones, all-in-one devices
- Upgrades were free for the first year
  - From Windows 7 and Windows 8.1
- Microsoft calls Windows 10 a "service"
  - Periodic updates to the OS
  - Instead of completely new versions

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 Education and Enterprise
- Very similar features in both
  - Minor features differences
  - 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 customization

Windows 10 processor requirements
- Same requirements as Windows 8/8.1
- PAE (Physical Address Extension)
  - 32-bit processors can use more than
  - 4 GB of physical memory
- NX (NX Processor Bit)
  - Protect against malicious software
- SSE2 (Streaming SIMD Extensions 2)
  - A standard processor instruction set
  - Used by third-party applications and drivers

1.2 - Windows in the Enterprise

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
- Distributed architecture
  - Many servers
  - Not suitable for home use
- Everything documented in one place
  - User accounts, servers, volumes, printers
- Many different uses
  - Authentication
  - Centralized management

BitLocker and EFS
- Data confidentiality
  - Encrypt important information
- Encrypting File System
  - 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

Media Center
- Video, music, and television portal
  - Perfect for watching at home
  - Record shows from a TV tuner
  - Play music
  - Watch DVDs
- The center of your home entertainment center
  - Cable companies and other technologies were strong competition
- Discontinued by Microsoft
  - Not officially available in Windows 10

1.2 - Windows in the Enterprise (continued)

BranchCache
- Caching for branch offices
  - Without additional hardware or external services
  - Conserve bandwidth over slower links
- Seamless to the end-user
  - Same protocols
  - Same network connection
  - Same authentication methods
  - Activates when round-trip latency exceeds 80 milliseconds

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 - Installing Operating Systems

Boot methods
- USB storage
  - USB must be bootable
  - Computer must support booting from USB
- CD-ROM and DVD-ROM
  - A common media
- PXE ("Pixie") - Preboot eXecution Environment
  - Perform a remote network installation
  - Computer must support booting with PXE
- NetBoot
  - Apple technology to boot Macs from the network
  - Similar concept to PXE
  - Boot methods
- Solid state drives / hard drives
  - Store many OS installation files
- External / hot swappable drive
  - Some external drives can mount an ISO (DVD-ROM image)
  - Boot from USB
- Internal hard drive
  - Install and boot from separate drive
  - Create and boot from new partition

Types of installations
- Unattended installation
  - Answer Windows questions in a file (unattend.xml)
  - No installation interruptions
- In-place upgrade
  - Maintain existing applications and data
- Clean install
  - Wipe the slate clean and reinstall
  - Migration tool can help
- Image
  - Deploy an clone on every computer
  - Types of installations
- Repair installation
  - Fix problems with the Windows OS
  - Does not modify user files
- Multiboot
  - Run two or more operating systems from a single computer
- Recovery partition
  - Hidden partition with installation files
- Refresh / restore
  - Windows 8/10 feature to clean things up
  - Requires a recovery partition

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

MBR partition style
- MBR (Master Boot Record)
  - The old standby, with all of the old limitations
- 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

GPT partition style
- GPT (GUID Partition Table)
  - Globally Unique Identifier
  - The latest partition format standard
- Requires a UEFI BIOS
  - Can have up to
  - 128 primary partitions
- No need for extended partitions or logical drives

1.3 - 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
  - You'll probably have one partition
- BE CAREFUL!
  - Serious potential for data loss
  - This is not an everyday occurrence

Storage types
- Layered on top of the partition and file system
  - A Windows thing
- Basic disk storage
  - Available in DOS and Windows versions
  - Primary/extended partitions, logical drives
  - Basic disk partitions can't span separate physical disks
- Dynamic disk storage
  - Available in all modern Windows versions
  - Span multiple disks to create a large volume
  - Split data across physical disks (striping)
  - Duplicate data across physical disks (mirroring)
  - Not all Windows versions support all capabilities

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

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

NTFS and CDFS
- NTFS – NT File System
  - Extensive improvements over FAT32
  - Quotas, file compression, encryption, symbolic links, large file support, security, recoverability
- CDFS - Compact Disk File System
  - ISO 9660 standard
  - All operating systems can read the CD

Other file systems
- ext3
  - Third extended file system
  - Commonly used by the Linux OS
- ext4
  - Fourth extended file system
  - An update to ext3
  - Commonly seen in Linux and Android OS
- NFS
  - Network File System
  - Access files across the network as if they were local
  - NFS clients available across many operating systems
- HFS+ / HFS Plus
  - Hierarchical File System
  - Also called Mac OS Extended
  - Replaced by Apple File System (AFPS) in macOS High Sierra (10.13)
- Swap partition
  - Memory management
  - Frees memory by moving unused pages onto disk
  - Copies back to RAM when needed
  - Usually a fast drive or SSD

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 in Windows 7, 8/8.1, and 10
  - 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

Other considerations
- Load alternate third party drivers when necessary
  - Disk controller drivers, etc.
- Workgroup vs. Domain setup
  - Home vs. business
- Time/date/region/language settings
  - Where are you?
- Driver installation, software and windows updates
  - Load video drivers, install apps, update the OS
- Factory recovery partition
  - This can help you later

1.3 - Installing and Upgrading Windows

Prepare the boot drive
- Know your drive
  - Is there data on the drive?
  - Has the drive been formatted?
  - What partitions are on the drive?
- Backup any old data - You may need that back someday
- 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
  - Windows 10 Upgrade Checker
- Plan for installation questions
  - Drive/partition configuration, license keys, etc.
- Application compatibility - Check with the app developer

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
  - Get up and running quickly
- Seamless and fast
  - Run from the DVD-ROM or USB flash

Upgrading from Windows 8.1
- Keep Windows settings, personal files, and applications
- Must upgrade to a similar Edition
- You cannot upgrade directly from Windows 8 to Windows 10

Upgrading from Windows 7
- Keep Windows settings, personal files, and applications
- Must upgrade to a similar Edition

Upgrade methods
- In-place
  - Upgrade the existing OS
  - Keeps all applications, documentations, 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

Upgrading to Windows 10
- Upgrade from the Windows 10 installation media
  - Downloadable versions are available from Microsoft
  - Includes a media creation tool
- You cannot upgrade x86 to x64
  - Or x64 to x86
  - Applies to all Windows versions
  - You'll have to migrate instead

Post-installation
- Does it work?
  - If it doesn't boot, there are bigger problems
  - Some testing is useful for unknown hardware configurations
- Additional installations
  - Service packs
  - Security patches
  - Security applications
  - Driver updates
  - Application updates

	Windows 10 Home	Windows 10 Pro	Windows 10 Enterprise
Windows 8.1 Core	Upgrade	Upgrade	Install
Windows 8.1 Professional	Install	Upgrade	Upgrade
Windows 8.1 Enterprise	Install	Install	Upgrade

	Windows 10 Home	Windows 10 Pro	Windows 10 Enterprise
Windows 7 Starter	Upgrade	Upgrade	Install
Windows 7 Home Basic	Upgrade	Upgrade	Install
Windows 7 Home Premium	Upgrade	Upgrade	Install
Windows 7 Professional	Install	Upgrade	Upgrade
Windows 7 Ultimate	Install	Upgrade	Install
Windows 7 Enterprise	Install	Install	Upgrade

1.4 - Microsoft 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**

File management
- **dir**
  - List files and directories
- **cd**
  - Change working directory
  - Use backslash **** to specify volume or folder name
- **..**
  - Two dots/periods
  - The folder above the current folder

shutdown
- Shutdown a computer
  - And optionally restart
- **shutdown /s /t nn**
  - Wait nn seconds, then shutdown
- **shutdown /r /t nn**
  - Shutdown and restart after nn seconds
- **shutdown /a**
  - Abort the countdown!

dism
- Deployment Image Servicing and Management tool
  - Manage Windows Imaging Format (WIM) files
- Make changes to your image with DISM
  - Get information about an image
  - Update applications
  - Manage drivers
  - Manage updates
  - Mount an image
- All command-line based
  - Many different options
  - Easy to automate

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

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

DiskPart
- Manage disk configurations
  - **diskpart** - start the DiskPart command interpreter

TaskList and TaskKill
- Manage tasks from the command line
  - No Task Manager required!
- **tasklist**
  - Displays a list of currently running processes
  - Local or remote machine
- **taskkill**
  - Terminate tasks by process id (PID) or image name
  - **TASKKILL /IM notepad.exe**
  - **TASKKILL /PID 1234 /T**

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:professor /force**
- **gpresult**
  - Verify policy settings for a computer or user
  - **gpresult /r**
  - **gpresult** /user sgc/professor /v

Format
- Formats a disk for use with Windows
  - **format c:**

Copy
- Copy files from one location to another
- **copy (/a, /v, /y)**
- **/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 7, 8.1, and 10

1.4 - Network Command Line Tools

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?
- Written by Mike Muuss in 1983
  - The sound made by sonar
  - Not an acronym for Packet INternet Groper

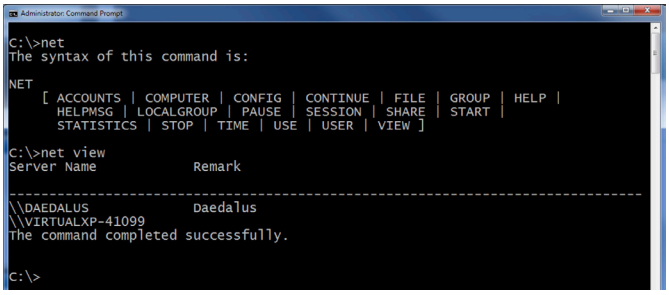
tracert
- Determine the route a packet takes to a destination
  - Map the entire path
- Takes advantage of ICMP Time to Live Exceeded message
  - The time in TTL refers to hops, not seconds or minutes
  - TTL=1 is the first router, TTL=2 is the second router, etc.
- Not all devices will reply with ICMP 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, Mac OS, etc.
- IOS devices send UDP datagrams over port 33434
  - The port number can be changed with extended options
  - The mechanics of traceroute

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

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**



1.5 - Windows Administrative Tools

Computer Management
- A pre-built Microsoft Management Console
  - A predefined mix of plugins
  - Control Panel / Administrative Tools
  - **mmc.exe**
- A handy starting point
  - Events
  - User accounts
  - Storage management
  - Services
  - And more!

Device Manager
- The OS doesn't know how to talk directly to most hardware
- Device drivers are hardware specific and operating system specific
  - Windows 7 device drivers may not necessarily work in Windows 10
- Technical Support FAQ
  - "Have you updated the drivers?"
- Computer Management or **devmgmt.msc**

1.5 - Windows Administrative Tools (continued)

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

Local Security Policy
- Big companies have big security policies
  - Managed through Active Directory Group Policies
- Stand-alone computers aren't managed through AD
  - You need local policies
- Not available in Home editions
  - Available in Professional / Pro, Ultimate, Enterprise

Performance Monitor
- Gather long-term statistics
  - Control Panel / Administrative Tools
- 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

Services
- Background process
  - No user interaction
  - File indexing, anti-virus, network browsing, etc.
- Useful when troubleshooting the startup process
  - Many services startup automatically
- Command-line control
  - `net start`, `net stop`
- Control Panel / Administrative Tools / Services
  - `services.msc`

Task Scheduler
- Schedule an application or batch file
  - Plan your future
- Includes predefined schedules - Click and go
- Organize - Manage with folders
- Control Panel / Administrative Tools / Task Scheduler

Component Services
- Microsoft COM+
  - Component Object Model
- Distributed applications
  - Designed for the enterprise
- Manage COM+ apps
  - Device COM+ Management
  - Event Viewer
  - Services

ODBC Data Sources
- ODBC - Open Database Connectivity
- Application independence
  - Database and OS doesn't matter
- Configure in Control Panel / Administrative Tools
  - Users probably won't need this

Print Management
- Control Panel / Administrative Tools / Print Management
- Manage printers
  - Share printers from one central console
- Add and manage printer drivers
  - Central management of
  - 32-bit and 64-bit drivers

Memory diagnostics
- Is your memory working?
  - I don't remember
- May be notified automatically
  - Or launched manually
- Multiple passes
  - Try to find the bad chip/module
  - Control Panel / Administrative Tools

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

1.5 - Windows Firewall with Advanced Security

Windows Firewall
- Integrated into the operating system
- Control Panel / Windows Firewall
- Windows Firewall with Advanced Security
  - Click "Advanced settings"
- Fundamental firewall rules
- Based on applications
  - No detailed control
- No scope
  - All traffic applies
- No connection security rules

Windows Firewall with Advanced Security
- Inbound rules
- Outbound rules
- Connection security rules
- Granular
  - Program, port, predefined services, custom
- Custom
  - Program, protocol/port, scope, action, profile

1.5 - System Configuration

System Configuration (`msconfig`)
- Manage boot processes, startup, services, etc.
  - One-stop shop
- Control Panel / Administrative Tools
  - `msconfig.exe`

General tab
- Control the startup process
  - Normal, Diagnostic, Selective
- Normal startup
  - Nothing to see here, go about your business
- Diagnostic startup
  - Similar to Safe Mode, but not quite the same
- Selective startup
  - You decide what to load

Boot tab
- Control the boot location
  - Multiple locations and operating systems
- Advanced options
  - Number of processors, maximum memory, etc.
- Boot options
  - Safe boot, remove the GUI, create a log file, base video, OS boot information (shows drivers as they load), set timeout for booting

Services tab
- Enable and disable Windows services
  - Determine what starts during boot
- Easier to manage than the Services applet
  - Click/unclick
- Useful for trial and error
  - It may take many reboots to find your problem

Startup tab
- Manage which programs start with a Windows login
  - Easily toggle on and off
- Multiple reboots
  - You'll find it
- A popular feature
  - Has moved to the Task Manager in Windows 8/8.1/10

Tools tab
- Easy access to popular administrative tools
  - UAC settings, System Information, Computer Management, etc.
- Faster than searching through menus or typing
  - A static (but comprehensive) list

1.5 - 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*
- Enhancements since Windows 7
  - More information and features

Applications
- Lists user-interactive applications in use
  - Apps on the desktop
- Administratively control apps
  - End task, start new task
- Combined with the Processes tab in Windows 8/8.1/10

Processes
- View all running processes
  - Interactive and system tray apps
  - View services and processes from other accounts
- Manage the view
  - Move columns, add metrics
- Later versions 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
- Newer versions include CPU, memory, disk, Bluetooth, and network in the Performance tab

Networking
- Network performance
  - Separate tab in Windows 7
  - Integrated into the Performance tab in Windows 8/8.1/10
- View utilization, link speeds, and interface connection state

Users
- Who is connected? What are they doing?
- Windows 7
  - User list, disconnect, logoff, send message
- Windows 8/8.1/10
  - Separate processes
  - Performance statistics

1.5 - Disk Management

Disk Management
- Manage disk operations
  - Individual computers and file servers
- Computer Management
  - Storage / Disk Management

Disk status
- Healthy
  - The volume is working normally
- Healthy (At Risk)
  - The volume has experienced I/O errors
  - Drive may be failing
- Initializing
  - Normal startup message
- Failed
  - Cannot be started automatically
  - The disk is damaged, or the file system is corrupted
- Failed redundancy
  - A drive has failed in a
  - RAID 1 or RAID 5 array
- Resynching
  - Mirrored (RAID 1) volume is synching data between the drives
- Regenerating
  - RAID 5 volume is recreating the data based on the parity data

Mounting drives
- Extend available storage space
  - Mount a separate storage device as a folder
- Mount in an empty folder
  - Instant storage space
  - Seamless to the user

Volume sizes
- Resize a volume
  - Shrink, extend
  - Right-click the volume
- Splitting
  - Shrink a volume
  - Format unallocated space

Storage spaces
- Storage for data centers, cloud infrastructures
  - Multiple tiers, administrative control
- Storage pool
  - A group of storage drives
  - Combine different storage devices into a single pool
  - Easy to add or remove space in the pool
- Storage space
  - Allocate virtual disks from available space in the pool
  - Includes options for mirroring and parity
  - Hot spare availability

1.5 - System Utilities

The Run line
- Start an application as a command
  - Instead of the graphical interface
- Use the run/search or command prompt
  - Specify options as part of the command

The Windows command line

`cmd`
- The "other" Windows
- Many options - The power under the hood

`regedit`
- The Windows Registry
  - 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

`services.msc`
- Control Panel / Administrative Tools / Services
- Useful when troubleshooting the startup process
- Control background applications
- Services can reveal dependencies between applications

`mmc`
- Build your own management framework
  - Choose from list of "snap-ins"
- Framework used for many built-in management tools

`mstsc`
- Microsoft Terminal Services Client
  - Remote Desktop Connection
- Access a desktop on another computer
  - Or connect to a Terminal Server
- Common for management
  - "Headless" servers

`Notepad`
- View and edit text files
  - You'll use a lot of text files
- Included with Windows
  - Almost any version

Explorer
- Windows Explorer / File Explorer (Windows 10)
  - File management
- View, copy, launch files
  - Granular control
- Easy access to network resources
  - Browse and view

1.5 - System Utilities (continued)

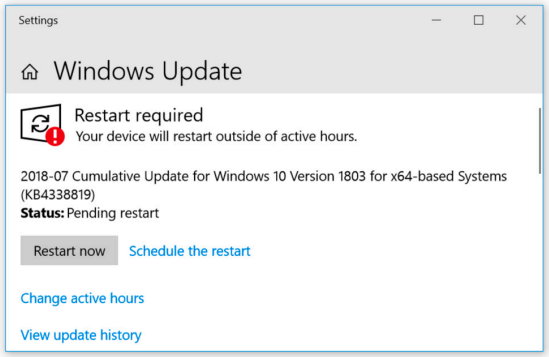
msinfo32
- Windows System Information
  - A wealth of knowledge
- Hardware Resources - Memory, DMA, IRQs, conflicts
- Components - Multimedia, display, input, network
- Software Environment - Drivers, print jobs, running tasks

dxdiag
- DirectX Diagnostic Tool
  - Manage your DirectX installation
- Multimedia API - 3D graphics, audio, and input options
- Also makes a very nice generic diagnostic tool
  - Not just for testing DirectX

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:**

System Restore
- Creates frequent restore points
  - Go back-in-time to correct problems
- F8 - Advanced Boot Options - Repair
- Windows 7/8/8.1/10: Control Panel / Recovery
- Doesn't guarantee recovery from viruses and spyware

Windows Update
- Keep your OS up to date - Security patches, bug fixes
- Automatic installation - Updates are always installed
- Download but wait for install - You control the time
- Check but don't download - Save bandwidth
- Never check - Don't do this



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
- Connections
  - VPN and proxy settings
- Programs
  - Default browser, plugins, etc.
- Advanced
  - Detailed configuration options (and reset!)

Display
- Resolution options
  - Important for LCD monitor native resolutions
- Color depth and Refresh rate
  - Advanced Settings, Adapter modes

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

Folder Options
- Manage Windows Explorer
  - Many options
- General
  - Windows, expand folders
- View
  - View hidden files, hide extensions
- Search
  - Indexing, search options, searching non-indexed areas

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

System Properties
- Computer information
  - Including version and edition
- Performance
  - Virtual memory
- Remote settings
  - Remote Assistance and Remote Desktop
- System protection
  - System Restore, select drives

1.6 - The Windows Control Panel (continued)

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

Power options
- Power plans - Customize power usage
- Sleep (standby)
  - Open apps are stored in memory
  - Save power, startup quickly
  - Switches to hibernate if power is low
- Hibernate
  - Open docs and apps are saved to disk
  - Common on laptops

Credential Manager
- Centralized management of web and Windows credentials
  - Each site can have a different username and password
- Add additional Windows credentials
  - Certificates

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

HomeGroup
- Easily share information
  - Windows 7 / Windows 8
  - No HomeGroup options on Windows 10
  - Documents, pictures, music, video
- A network for the home
  - Must be set to “Home” in Windows
- Enable HomeGroup
  - A single password for everyone

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

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

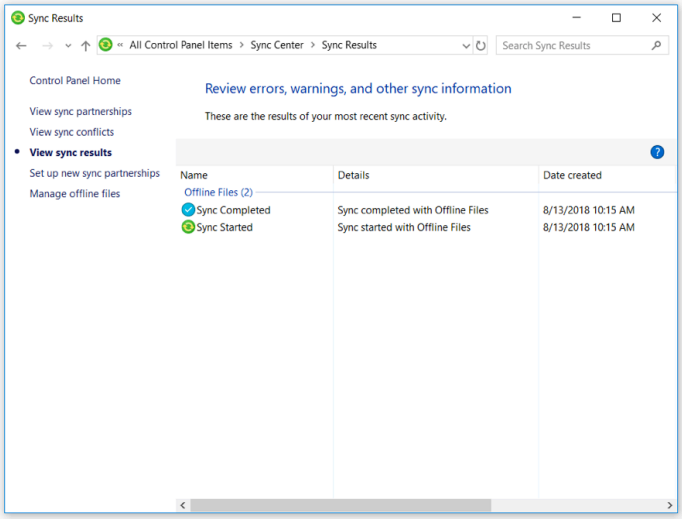
Troubleshooting
- Some problems can be easily fixed
  - Have you tried turning it off and on again?
- Automate some of the most common fixes
  - Categorized
- May require elevated account access
  - Enabling / disabling hardware and features

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

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

BitLocker
- Full disk encryption
  - The operating system and all files
- A TPM is recommended
  - Trusted Platform Module
  - Use a flash drive or password if there’s no TPM
- Seamless
  - Works in the background
  - You never know it’s there

Sync Center
- Make files available, even when you’re not online
  - Automatically sync when back online
  - Built-in sync conflict management
- Not available in Home editions
  - Needs offline file functionality
  - Only available in Pro and higher
- Mark files “Always available offline”



1.7 - 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

System requirements
- Drive space
  - Initial installation space requirement
  - Application use requirement
  - Some applications use a LOT of drive space after installation
- RAM
  - This would be above and beyond the OS requirements
  - Very dependent on the application
  - Consider all of the other running applications
- OS compatibility
  - Operating system (Windows, macOS, Linux)
  - Version of the OS

Installation methods
- Local installation
  - CD-ROM / DVD-ROM, Optical media, USB
  - Very compatible with most devices
  - Supports large installation programs
- Network-based
  - The default in most organizations
  - Applications are staged and deployed from a central server
  - Can be centrally managed

Local user permissions
- Folder/file access
  - Installation programs will be copying a lot of files
- The user needs permission to write application files to the storage drive
  - This may not be the default in an office
- May need to run as Administrator
  - Some applications will install additional drivers or services
  - Be careful when allowing this level of access!

Security 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

1.8 - HomeGroups, Workgroups, and Domains

Organizing network devices
- Windows HomeGroup
  - Share files, photos, video, etc. between all devices
  - Works on a single private network only
- Windows Workgroups
  - Logical groups of network devices
  - Each device is a standalone system, everyone is a peer
  - Single subnet
- Windows Domain
  - Business network
  - Centralized authentication and device access
  - Supports thousands of devices across many networks

HomeGroup
- Easily share information
  - Windows 7 / Windows 8/8.1
  - HomeGroup support was removed from Windows 10
  - Documents, pictures, music, video
- A network for the home
  - Must be set to "Home" in Windows
- Enable HomeGroup - A single password for everyone

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

Domains
- Central database
  - Active Directory Domain Services
  - Designed for the enterprise
- User accounts are managed centrally
  - Devices are added to the domain
- Manage all devices and users
  - Deploy software
  - Manage the operating system
- 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

1.8 - Windows Network Technologies

Network locations in Windows 7
- Automatically set security levels
  - You don't even have to remember
- Home
  - The network is trusted
- Work
  - You can see other devices, but can't join a HomeGroup
- Public
  - Airport, coffee shop
  - You are invisible

Network locations in Windows 8/8.1/10
- Private
  - Sharing and connect to devices
- Public
  - No sharing or connectivity
- Network and Internet Status
  - Change connection properties

Remote access
- Remote Assistance
  - Home editions
  - One-time remote access
  - Single-use password
  - Chat, diagnostics, NAT traversal
- Remote Desktop Connection
  - Non-Home editions
  - Ongoing access
  - Local authentication options
  - May require port forwarding

Proxy settings
- Change the traffic flow
  - An Internet go-between
- Control Panel / Internet Properties
- Define address and exceptions
  - Proxies don't work for everything

Network shares
- Make a folder available across the network
  - "Share" with others, view in Windows Explorer
- Assign (map) a drive letter to a share
  - Reconnect automatically
- Shares ending with a dollar sign ($) are "hidden"
  - Not a security feature
- Control Panel / Administrative Tools / Computer Management

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 x: \\sg-server\mission-reports

Printer shares
- Similar to sharing a folder
  - But it's a printer instead
- Windows Explorer
  - Add a printer

1.8 - Establishing 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 concentrators

VPN connections
- Built-in VPN client - Included with Windows
- 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

Dialup connections
- Modem connection - Standard phone lines
- Configuration
  - Authentication, Phone number
- Connect / Disconnect from network status icon

Wireless connections
- Network name - SSID (Service Set Identification)
- Security type - Encryption method
- Encryption type - TKIP, AES, Security key
- WPA2-Personal
  - Pre-shared key,
  - WPA2-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, Hotspot
- Requires third-party software
  - Each provider is different

1.8 - Configuring Windows Firewall

Enabling and disabling Windows 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 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 - Very broad
- Predefined exceptions
  - List of common exceptions
- Custom rule
  - Every firewall option

1.8 - Windows IP Address Configuration

How Windows gets an IP address

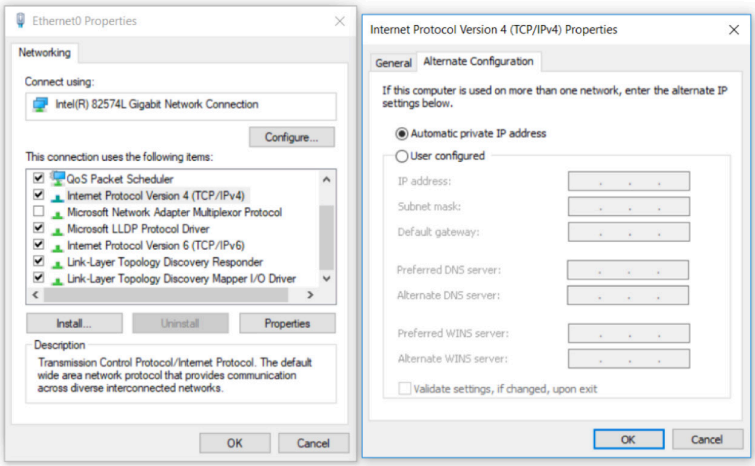
- DHCP (Dynamic Host Configuration Protocol)
  - Automatic IP addressing - This is the default
- APIPA (Automatic Private IP Addressing)
  - There's no static address or DHCP server
  - Communicate locally (link-local address)
  - Assigns 169.254.1.0 to 169.254.254.255
  - No Internet connectivity
- 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
  - Addresses can be dynamic or static
- Loopback address - 127.0.0.1 - It's always there!

A backup for the DHCP server

- Multiple DHCP servers should be configured 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



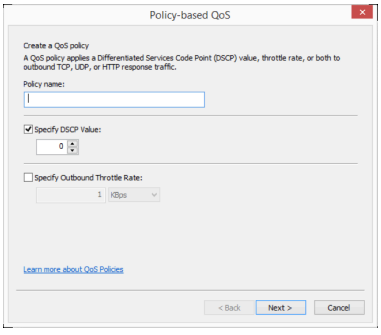
1.8 - Network Adapter Properties

Network adapter properties

- Link speed and duplex
  - Auto negotiation doesn't always negotiate
  - Both sides must match
- Wake on LAN
  - Computer sleeps until needed
  - Useful for late-night software updates

Quality of Service (QoS)

- Prioritize network traffic
  - Applications, VoIP, and Video
- Infrastructure must support QoS
  - Differentiated Services Code Points (DSCP) field in the IP header
  - IPv4 - Type of Service (ToS) field
  - IPv6 - Traffic Class octet
- Manage through Local Computer Policy or Group Policy
  - Computer Configuration / Windows Settings / Policy-based QoS



BIOS settings

- Enable/disable network adapters
  - On and off - Not much nuance

1.9 - Best Practices for macOS

Scheduled backups
- Time Machine - Included with Mac OS X
- Hourly backups - The past 24 hours
- Daily backups - The past month
- Weekly backups - All previous months
- Starts deleting oldest information when disk is full

Scheduled disk maintenance
- Disk Utility - Disk maintenance
- Rarely needed - No ongoing maintenance
- Verify disk
  - Every few months
  - Similar to Windows Check Disk

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

Driver/firmware updates
- Almost invisible in Mac OS X
  - Designed to be that way
- System Information - Detailed hardware list
- View only
  - No changes to settings
  - By design

Anti-virus/Anti-malware updates
- OS X 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 install base
- Automate your signature updates
  - New updates every hour / day

1.9 - macOS Tools

Time Machine backups
- Automatic and easy to use
  - Familiar Finder UI
- Dates along the right side
  - Files in the middle
- Mac OS takes snapshots if the Time Machine storage isn't available
  - You can restore from the snapshot

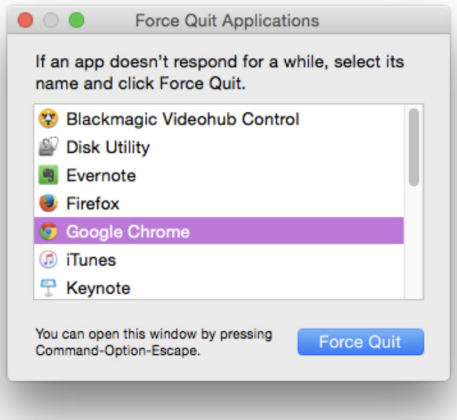
Image recovery
- Build a disk image in Disk Utility
  - Creates an Apple Disk Image (.dmg) file
- Mount on any Mac OS X system
  - Appears as a normal file system
  - Copy files from the image
- Use the restore feature in Disk utility
  - Restore a disk image to a volume

Disk Utility
- Manage disks and images
  - Resolve issues
- File system utilities
  - Verify and repair file systems
  - Erase disks
  - Modify partition details
  - Manage RAID arrays
  - Restore a disk image to a volume
- Create, convert, and resize images
  - Manage the image structure

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

Screen sharing
- Integrated into the operating system
  - Can also be viewed with VNC (Virtual Network Computing)
- Available devices appear in the Finder
  - Or access by IP address or name

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



1.9 - macOS Features

Mission Control and Spaces
- Quickly view everything that's running
  - Spread out the desktop into a viewable area
- 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 with 3DES
  - 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
  - Change the order of categories

iCloud
- Integrates Apple technologies - Mac OS, iOS
- 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

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

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

Remote Disk
- Use an optical drive from another computer
  - Becomes more important as time goes on
  - 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
- Utility available for Windows
  - Share a Windows CD or DVD drive

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

Boot Camp
- Dual-boot into Windows on Mac hardware
  - Not virtualization
- Requires Apple device drivers
  - Running Windows natively on
  - Apple's Intel CPU architecture
- Everything is managed through the Boot Camp Assistant
  - Builds a Boot Camp partition
  - Installs Windows OS and drivers

1.9 - Best Practices for Linux

Scheduled backups
- Many options
  - Command line and graphical
  - May be included with the distribution
- **`tar`**
  - Tape Archive
  - Easy to script into
  - a backup schedule
- **`rsync`**
  - Sync files between storage devices
  - Instant synchronization or scheduled

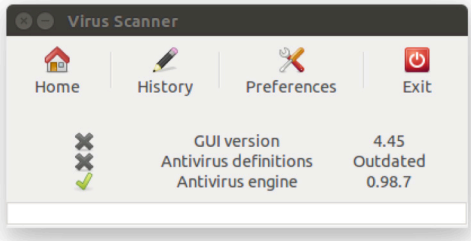
Scheduled disk maintenance
- Very little disk maintenance required
  - Space and resources
- Check file system
  - File systems can't be mounted
  - Done automatically every X number of reboots
  - Force after reboot by adding a file to the root
    - **`sudo touch /forcefsck`**
- Clean up log space
  - **`/var/log`**

1.9 - Best Practices for Linux (continued)

System updates
- Command line tools
  - **`apt-get`**, **`yum`**
- Graphical update managers
  - Software updater
- Patch management
  - Updates can be scheduled
  - Software center
  - The Linux "App Store"

Driver/firmware updates
- Many drivers are in the kernel
  - Updated when the kernel updates
- Additional drivers are managed with software updates or at the command line
  - Update those yourself

Anti-virus/Anti-malware updates
- Relatively few viruses and malware for Linux
  - Still important to keep updated
- ClamAV
  - Open source antivirus engine
- Same best practice as any other OS
  - Always update signature database
  - Always provide on-demand scanning



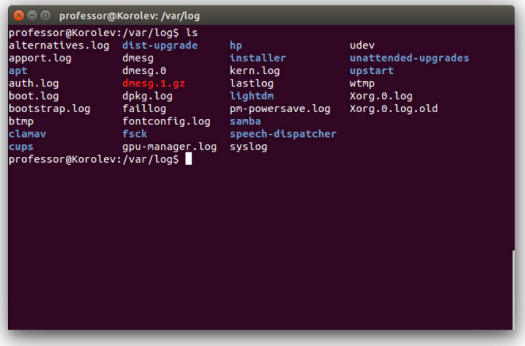
1.9 - Linux Tools

Backups
- May be built-in to the Linux distribution
  - Check with the documentation
- Graphical interface - Backup and restore, Scheduling
- Command-line options - **`rsync`**
- There are many different options
  - That's the beauty (and challenge) of Linux

Image recovery
- Not as many options as Windows
  - But still some good ones
- **`dd`** is built-in to Linux - And very powerful
- Other 3rd-party utilities can image drives
  - GNU Parted, Clonezilla

Disk maintenance
- Linux doesn't require a lot of maintenance
  - You probably already know this
- Clean up log space - All logs are stored in **`/var/log`**
- File system check
  - Done automatically every X number of reboots
  - Force after reboot by adding a file to the root
  - **`sudo touch /forcefsck`**

Terminal
- Command line access to the operating system
  - Common to manage in Linux
- OS maintenance - Run scripts, manage files
  - Configure OS and application settings



Screen sharing
- Screen access to remote devices
  - Manage from your desk
- Many options - Like most of Linux
- May be included with your distribution
  - UltraVNC, Remmina

1.9 - Basic Linux Commands

Linux commands
- The command line - Terminal, XTerm, or similar
- Commands are similar in both Linux and Mac OS
  - 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
  - I'm using Ubuntu in a virtual machine
- 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)

1.9 - Basic Linux Commands (continued)

grep
- Find text in a file
  - Search through many files at a time
  - **grep PATTERN [FILE]**
  - **> grep failed auth.log**

cd
- Change current directory
  - Nearly identical to Windows command line
  - Forward slashes instead of backward
- **cd <directory>**
  - **> cd /var/log**

shutdown
- Shut the system down
  - Safely turn off the computer in software
  - Similar to the Windows shutdown command
- **sudo shutdown 2**
  - Shuts down and turns off the computer in two minutes
- **sudo shutdown -r 2**
  - Shuts down and reboots in two minutes
  - Important when you're not on site
- **Ctrl-C** to cancel

pwd vs. passwd
- **pwd**
  - Print Working Directory
  - Displays the current working directory path
  - Useful when changing directories often
- **passwd**
  - Change a user account password
  - Yours or another
  - **passwd [username]**

mv
- Move a file
  - 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**

mkdir
- Make a directory
  - Create a folder for file storage
- **mkdir DIRECTORY**
  - **> mkdir notes**

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

#	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	– – –

chown
- Change file owner and group
  - Modify file settings
- **sudo chown [OWNER:GROUP] file**
  - **> sudo chown professor script.sh**

iwconfig / ifconfig
- **iwconfig**
  - View or change wireless network configuration
  - essid, frequency/channel, mode, rate, etc.
  - Requires some knowledge of the wireless network
  - **iwconfig eth0 essid studio-wireless**
- **ifconfig**
  - View or configure a network interface and IP configuration
  - **ifconfig** eth0

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**

1.9 - Basic Linux Commands (continued)

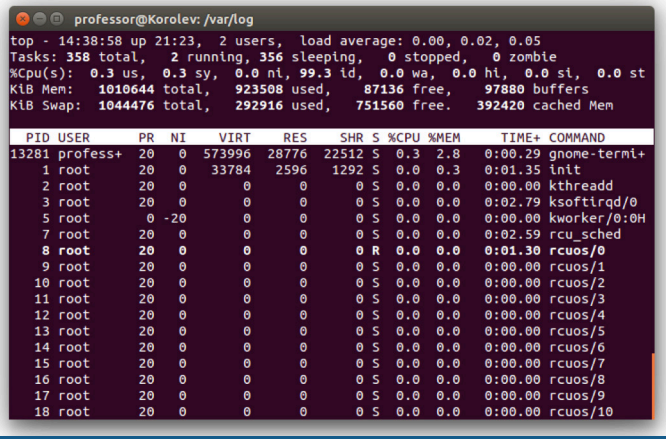
su / sudo
- Some command require elevated rights
  - There are some things normal users can't do
- **su**
  - Become super user
  - Or change to a different user
  - You continue to be that user until you exit
- **sudo**
  - Execute a command as the super user
  - Or as a different user ID
  - Only that command executes as the super user

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

vi
- Visual mode editor
  - Full screen editing with copy, paste, and more
- **vi FILE**
  - **> vi script.sh**
- Insert text
  - **i <text>**
  - Exit insert mode with **Esc**
- Save (write) the file and quit vi
  - **:wq**

dd
- Convert and copy a file
  - Backup and restore an entire partition
  - **> dd if=<source file name> of=<target file name> [Options]**
  - Creating a disk image
  - **> dd if=/dev/sda of=/tmp/sda-image.img**
  - Restoring from an image
  - **> dd if=/tmp/sda-image.img of=/dev/sda**

Closing programs
- Use terminal - **sudo** for proper permissions
- **killall**
  - **sudo killall firefox**
- **xkill**
  - Graphical kill
- **kill <pid>**



2.1 - Physical Security

Mantraps
- 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

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

Tokens and cards
- Smart card
  - Integrates with devices
  - May require a PIN
- USB token
  - Certificate is on the USB device
- Hardware or software tokens
  - Generates pseudo-random authentication codes
- Your phone
  - SMS a code to your phone

Guards and access lists
- Security guard
  - Physical protection
  - 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

2.1 - Physical Security (continued)

Biometrics
- Biometric authentication
  - Fingerprint, iris, voiceprint
- 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

Cable locks
- Temporary security
  - Connect your hardware to something solid
- Cable works almost anywhere
  - Useful when mobile
- Most devices have a standard connector
  - Reinforced notch
- Not designed for long-term protection
  - Those cables are pretty thin

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

USB locks
- Prevent access to a USB port
  - Physical lock inside of the interface
- A secondary security option after disabling the interface in BIOS and/or operating system
  - There's always a way around security controls
- Relatively simple locks
  - Defense in depth

Privacy filters
- 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

2.2 - Logical Security

Active Directory
- Centralized management
  - Windows Domain Services
  - Limit and control access
- Login script
  - Map network drives
  - Update security software signatures
  - Update application software
- Group Policy/Updates
  - Define specific policies
  - Password complexity
  - Login restrictions
- Organizational Units
  - Structure Active Directory
  - Can be based on the company (locations, departments)
- Home Folder
  - Assign a network share as the user's home
  - `\\server1\users\professormesser`
- Folder redirection
  - Instead of a local folder, redirect to the server
  - Store the Documents folder on `\\server1`
  - Access files from anywhere

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 single user devices

Port security
- Prevent unauthorized users from connecting to a switch interface
  - Alert or disable the port
- Based on the source MAC address
  - Even if forwarded from elsewhere
- Each port has its own config
  - Unique rules for every interface

Port security example
- Configure a maximum number of source MAC addresses on an interface
  - You decide how many is too many
  - You can also configure specific MAC addresses
- The switch monitors the number of unique MAC addresses
  - Maintains a list of every source MAC address
- Once you exceed the maximum, port security activates
  - Default is to disable the interface

MAC filtering
- Media Access Control - The "hardware" address
- Limit access through the physical hardware address
  - Keeps the neighbors out
  - Additional administration with visitors
- Easy to find MAC addresses through wireless LAN analysis
  - MAC addresses can be spoofed
- Security through obscurity

Smart cards
- Must have physical card to provide digital access
  - A digital certificate
- Multiple factors
  - Card with PIN or fingerprint

Certificate-based authentication
- Smart card
  - Private key is on the card
- PIV (Personal Identity Verification) card
  - US Federal Government smart card
  - Picture and identification information
- CAC (Common Access Card)
  - US Department of Defense smart card
  - Picture and identification
- IEEE 802.1X
  - Gain access to the network using a certificate
  - On-device storage or separate physical device

Anti-virus and anti-malware
- Anti-malware software runs on the computer
  - Each device manages its own protection
- Updates must be completed on all devices
  - This becomes a scaling issue
- Large organizations need enterprise management
  - Track updates, push updates, confirm updates, manage engine updates
- Mobility adds to the challenge
  - Need additional management

Host-based firewalls
- "Personal" firewalls
  - Software-based
- Included in many operating systems
  - 3rd-party solutions also available
- Stops unauthorized network access
  - "Stateful" firewall
  - Blocks traffic by application
- Windows Firewall
  - Filters traffic by port number and application

Network-based firewalls
- Filters traffic by port number
  - HTTP is 80, SSH is 22
  - Next-generation firewalls can identify the application
- Can encrypt traffic into/out of the network
  - Protect your traffic between sites
- Can proxy traffic
  - A common security technique
- Most firewalls can be layer 3 devices (routers)
  - Usually sits on the ingress/egress of the network

User authentication
- Identifier
  - Something unique
  - In Windows, every account has a Security Identifier (SID)
- Credentials
  - The information used to authenticate the user
  - Password, smart card, PIN code, etc.
- Profile
  - Information stored about the user
  - Name, contact information, group memberships, etc.

Strong passwords
- Weak passwords can be difficult to protect against
  - Interactive brute force
  - Hashed passwords can be brute forced offline
- Passwords need complexity and constant refresh
  - Reduce the chance of a brute force
  - Reduce the scope if a password is found
- Annual password analysis from SplashData
  - Examines leaked password files
- Pretty much what you'd expect
  - #1: 123456, #2: password, #3: 12345, #4: 12345678, #5: qwerty

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
- Can be inexpensive
  - Free smartphone applications
  - Software-based token generator

Software tokens
- Pseudo-random number generator
  - Can't guess it
  - Changes constantly
- Saves money
  - Free smartphone applications
  - No separate device to lose

Directory permissions
- NTFS permissions
  - Much more granular than FAT
  - Lock down access
  - Prevent accidental modification or deletion
  - Some information shouldn't be seen
- User permissions
  - Everyone isn't an Administrator
  - Assign proper rights and permissions
  - This may be an involved audit

2.2 - Logical Security (continued)

VPN concentrator
- Virtual Private Network
  - Encrypt (private) data traversing a public network
- Concentrator
  - Encryption/decryption access device
- Many deployment options
  - Specialized cryptographic hardware
  - Software-based options available
- Used with client software - Sometimes built into the OS

Data Loss Prevention (DLP)
- Where's your data?
  - Social Security numbers, credit card numbers, medical records
- Stop the data before the bad guys get it
  - Data "leakage"
- So many sources, so many destinations
  - Often requires multiple solutions in different places

Access Control Lists (ACLs)
- Used to allow or deny traffic
  - Also used for NAT, QoS, etc.
- Defined on the ingress or egress of an interface
  - Often on a router or switch
  - Incoming or outgoing
- 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?
  - Following the traffic flow

Email filtering
- Unsolicited email
  - Stop it at the gateway before it reaches the user
  - On-site or cloud-based
- Scan and block malicious software
  - Executables, known vulnerabilities
  - Phishing attempts
  - Other unwanted content

Trust/untrusted software sources
- Consider the source
  - May not have access to the code
  - Even then, may not have the time to audit
- Trusted sources
  - Internal applications
  - Well-known publishers
  - Digitally-signed applications
- Untrusted sources
  - Applications from third-party sites
  - Links from an email
  - Pop-up/drive-by downloads

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

2.3 - Wireless Security

Wireless encryption
- All wireless computers are radio transmitters and receivers
  - Anyone can listen in
- Solution: Encrypt the data
  - Everyone gets the password
  - Or their own password
- Only people with the password can transmit and listen
  - WPA and WPA2

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
  - Run on existing hardware
- WPA: RC4 with TKIP (Temporal Key Integrity Protocol)
  - Initialization Vector (IV) is larger and an encrypted hash
  - Every packet gets a unique 128-bit encryption key

Temporal Key Integrity Protocol
- Mixed the keys
  - Combines the secret root key with the IV
- Adds a sequence counter
  - Prevents replay attacks
- Implements a 64-bit Message Integrity Check
  - Protects against tampering
- TKIP has it's own set of vulnerabilities
  - Deprecated in the 802.11-2012 standard

WPA2 and CCMP
- WPA2 certification began in 2004
  - AES (Advanced Encryption Standard) replaced RC4
  - CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) replaced TKIP
- CCMP block cipher mode
  - Uses AES for data confidentiality
  - 128-bit key and a 128-bit block size
  - Requires additional computing resources
- CCMP security services
  - Data confidentiality (AES), authentication, and access control

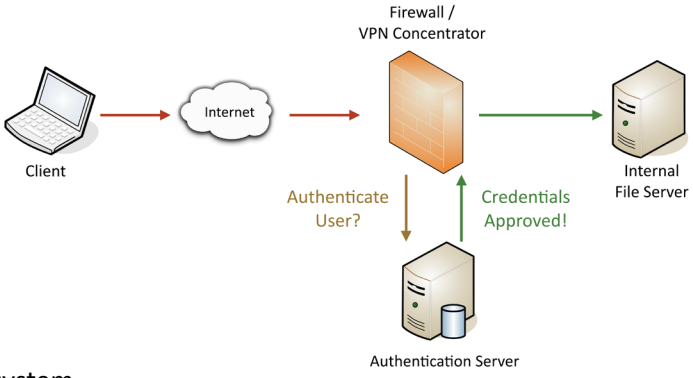
2.3 - Wireless Security (continued)

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

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 operating system

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

Gaining access



2.4 - Types of Malware

Ransomware
- The bad guys want your money
  - They'll take your computer in the meantime
- May be a fake ransom
  - Locks your computer "by the police"
- The ransom may be avoided
  - A security professional may be able to remove these kinds of malware

Crypto-malware
- New generation of ransomware
  - 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

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

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

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

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

2.4 - Types of Malware (continued)

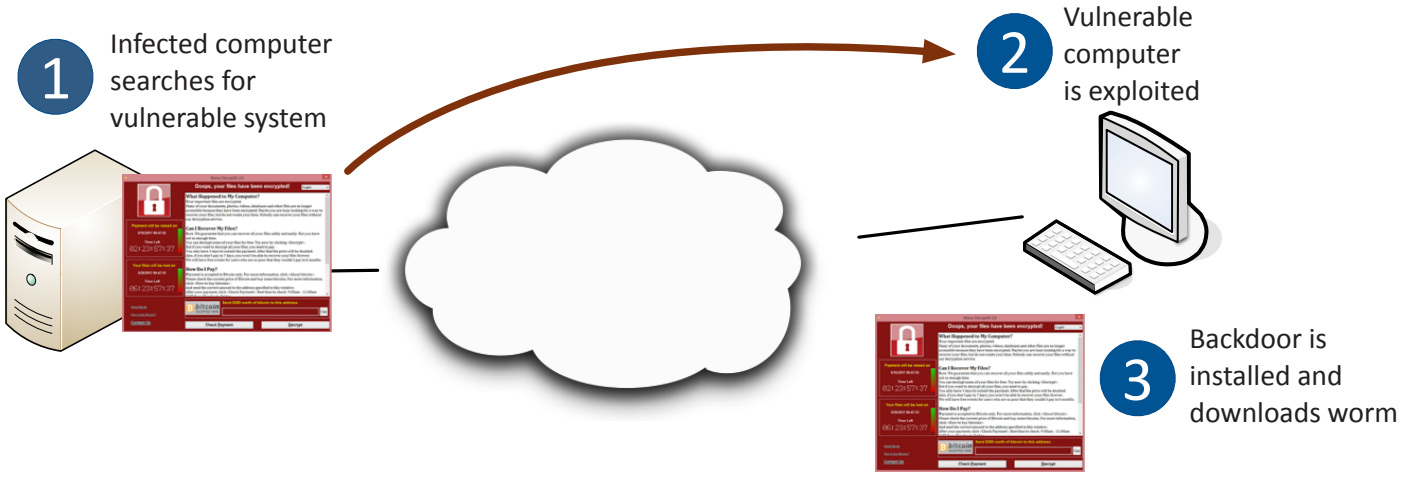
Virus
- Malware that can reproduce itself
  - It doesn't need you to click anything
  - It needs you to execute a program
- Reproduces through file systems or the network
  - Just running a program can spread a virus
- May or may not cause problems
  - Some viruses are invisible, some are annoying
-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

Virus types
- Program viruses
  - It's part of the application
- Boot sector viruses
  - Who needs an OS?
- Script viruses
  - Operating system and browser-based
- Macro viruses
  - Common in Microsoft Office

Worms
- Malware that self-replicates
  - Doesn't need you to do anything
  - Uses the network as a transmission medium
  - Self-propagates and spreads quickly
- Worms are pretty bad things
  - Can take over many systems very quickly
- Firewalls and IDS/IPS can mitigate many worm infestations
  - Doesn't help much once the worm gets inside

Botnets
- Robot networks
  - Skynet is self-aware
- Once your machine is infected, it becomes a bot
  - You may not even know
- How does it get on your computer?
  - Trojan Horse (I just saw a funny video of you! Click here.) or you run a program or click an ad you THOUGHT was legit, but...
  - OS or application vulnerability
- A day in the life of a bot
  - Sit around. Check in with the mother ship. Wait for instructions.

Worm infection and transmission



2.4 - Anti-Malware Tools

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

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
- Windows 7 - System Recovery Options / Command Prompt
  - Boot from installation media
  - Or select from F8 Advanced Boot Menu
- Windows 8/8.1/10
  - Troubleshoot / Advanced Options / Command Prompt
  - Boot from installation media

2.4 - Anti-Malware Tools (continued)

Backup / restore
- Always have a backup
  - This is the best insurance policy ever
- Image backup built into Windows
  - In Windows 8/10 it's called
  - Backup and Restore (Windows 7)
- This is the only way to be 100% sure that malware has been removed
  - Seriously. Cleaning isn't 100%.

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

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

Secure DNS services
- External/Hosted DNS service
  - Provides additional security services
- Real-time domain blocking
  - Sites containing malware are not resolvable
- Block harmful websites
  - Phishing sites, parked domains
- Secure platforms - Avoid DNS cache poisoning attacks

2.5 - Social Engineering Attacks

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

Social engineering principles
- Authority
  - The social engineer is in charge
  - I'm calling from the help desk/office of the CEO/police
- Intimidation
  - There will be bad things if you don't help
  - If you don't help me, the payroll checks won't be processed
- Consensus / Social proof
  - Convince based on what's normally expected
  - Your co-worker Jill did this for me last week
- Scarcity
  - The situation will not be this way for long
  - Must make the change before time expires
- Urgency
  - Works alongside scarcity
  - Act quickly, don't think
- Familiarity / Liking
  - Someone you know, we have common friends
- Trust
  - Someone who is safe
  - I'm from IT, and I'm here to help

Phishing
- Social engineering with a touch of spoofing
  - Often delivered by spam, IM, etc.
  - Very remarkable when well done
- Don't be fooled - Check the URL
- Usually there's something not quite right
  - Spelling, fonts, graphics
- Vishing is done over the phone
  - Fake security checks or bank updates

Spear phishing
- Phishing with inside information
  - Makes the attack more believable
  - Spear phishing the CEO is "whaling"
- April 2011 - Epsilon
  - Less than 3,000 email addresses attacked
  - 100% of email operations staff
  - Downloaded anti-virus disabler, keylogger, and remote admin tool
- April 2011 - Oak Ridge National Laboratory
  - Email from the "Human Resources Department"
  - 530 employees targeted, 57 people clicked, 2 were infected
  - Data downloaded, servers infected with malware

Impersonation
- Pretend to be someone you aren't
- 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
- Throw tons of technical details around
- Be a buddy - How about those Cubs?

2.5 - Social Engineering Attacks (continued)

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
  - Coffee shops
- Surf from afar
  - Binoculars / Telescopes
  - Easy in the big city
  - Webcam monitoring

Tailgating
- Use someone else to gain access to a building
  - Not an accident
- Johnny Long / No Tech Hacking
  - Blend in with clothing
  - 3rd-party with a legitimate reason
  - Temporarily take up smoking
  - I still prefer bringing doughnuts
- Once inside, there's little to stop you
  - Most security stops at the border

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

Is it legal to dive in a dumpster?
- I am not a lawyer.
- In the United States, it's legal
  - Unless there's a local restriction
- If it's in the trash, it's open season
  - Nobody owns it
- Dumpsters on private property or "No Trespassing" signs may be restricted
  - You can't break the law to get to the rubbish
- Questions? Talk to a legal professional.

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 - 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 the developer
- Bad guys 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)
  - http://cve.mitre.org/

2.5 - Zero-day Attacks (continued)

Zero-day vulnerabilities

- March 2017
  - CVE-2017-0199 - Microsoft Office/WordPad Remote Code
  - Execution Vulnerability w/Windows API
  - Open a Microsoft Office or WordPad file
  - SophosLabs documented attacks in the wild since November 2016
- June 2017
  - CVE-2017-8543 | Windows Search
  - Remote Code Execution Vulnerability
  - Send a specially crafted SMB message to the Search service
  - Install programs, view/change/delete data, create new user accounts

2.5 - Man-in-the-Middle

Man -in- the-middle

- How can a bad guy watch without you knowing?
  - Man-in-the-middle
- Redirects your traffic
  - Then passes it on to the destination
  - You never know your traffic was redirected
- ARP poisoning - ARP has no security

Mitigating man-in-the-middle

- Use encrypted protocols
  - HTTPS, SSH
- Communicate over a secure channel
  - Client-based VPN
- Use encrypted wireless networks
  - Avoid insecure networks
  - Public WiFi, Hotels

2.5 - Brute Force Attacks

The password file

- Different across operating systems
  - Different hash methods

Brute force

- The password is the key
  - Secret phrase
  - Stored hash
- 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

- People use common words as passwords
  - You can find them in the dictionary
- If you're using brute force, you should start with the easy ones
  - 123456, password, ninja, football
- Many common wordlists available on the 'net
  - Some are customized by language or line of work
- This will catch the low-hanging fruit
  - You'll need some smarter attacks for the smarter people

Rainbow tables

- An optimized, pre-built set of hashes
  - Doesn't need to contain every hash
  - The calculations have already been done
- Remarkable speed increase
  - Especially with longer password lengths
- Need different tables for different hashing methods
  - Windows is different than MySQL
- Rainbow tables won't work with salted hashes
  - Additional random value added to the original hash

2.5 - Spoofing

Spoofing

- Pretend to be something you aren't
  - Fake web server, fake DNS server, etc.
- Email address spoofing
  - The sending address of an email isn't really the sender
- Caller ID spoofing
  - The incoming call information is completely fake
- Man-in-the-middle attacks
  - The person in the middle of the conversation pretends to be both endpoints

MAC spoofing

- Your Ethernet device has a MAC address
  - A unique burned-in address
  - Most drivers allow you to change this
- Changing the MAC address can be legitimate
  - Internet provider expects a certain MAC address
  - Certain applications require a particular MAC address
- It might not be legitimate
  - Circumvent MAC-based ACLs
  - Fake-out a wireless address filter
- Very difficult to detect
  - How do you know it's not the original device?

2.5 - Spoofing (continued)

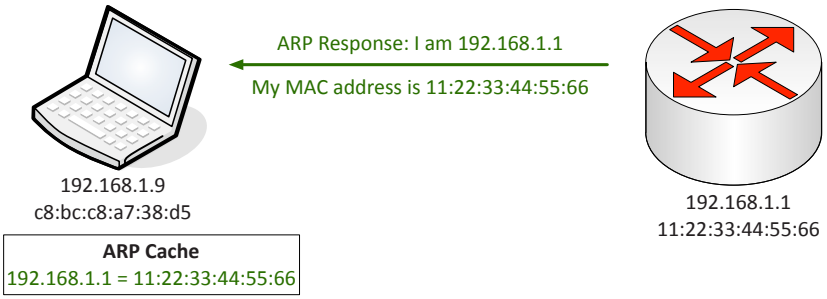
IP address spoofing

- Take someone else's IP address
  - Actual device
  - Pretend to be somewhere you are not
- Can be legitimate
  - Load balancing
  - Load testing
- May not be legitimate
  - ARP poisoning
  - DNS amplification / DDoS
- Easier to identify than MAC address spoofing
  - Apply rules to prevent invalid traffic, enable switch security

1

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

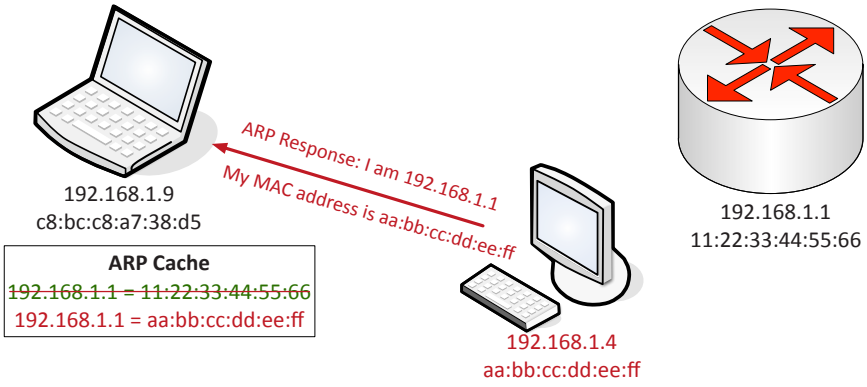
The ARP response is cached on the local device.



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 - Non-compliant Systems

Non-compliant systems

- A constant challenge
  - There are always changes and updates
- Standard operating environments (SOE)
  - A set of tested and approved 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

2.6 - Windows Security Settings

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

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

2.6 - Windows Security Settings

Shared files and folders
- Administrative shares
  - Hidden shares (i.e., C$) created during installation
  - Local shares are created by users
- System files and folders
  - C$ - \
  - ADMIN$ - \Windows
  - PRINT$ - Printers folder
- Computer Management / Shared Folders
  - `net share`

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

User authentication
- Authentication
  - Prove you are the valid account holder
  - Username / Password
  - Perhaps additional credentials
- Single sign-on (SSO)
  - Windows Domain
  - Provide credentials one time
  - No additional pop-ups or interruptions
  - Managed through Kerberos

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 *Ctrl-Shift-Enter*)

BitLocker
- Encrypt an entire volume
  - Not just a single file
  - Protects all of your data, including the OS
- 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 filesystem level
  - On NTFS
- OS support
  - 7 Professional, Enterprise and Ultimate
  - 8 and 8.1 Pro and Enterprise
  - 10 Pro, Enterprise, and Education
- Uses password and username to encrypt the key
  - Administrative resets will cause EFS files to be inaccessible

2.7 - Workstation Security Best Practices

Password complexity and length
- Make your password strong
  - No single words
  - No obvious passwords
  - What's the name of your dog?
  - Mix upper and lower case
  - Use special characters
  - Don't replace a o with a 0, t with a 7
- A strong password is at least 8 characters
  - Consider a phrase or set of words
- Set password expiration, require change
  - System remembers password history, requires unique passwords

Password expiration and recovery
- All passwords should expire
  - Change every 30 days, 60 days, 90 days
- Critical systems might change more frequently
  - Every 15 days or every week
- The recovery process should not be trivial!
  - Some organizations have a very formal process

Desktop security
- Require a screensaver password
  - Integrate with login credentials
  - Can be administratively enforced
  - Automatically lock after a timeout
- Disable autorun
  - autorun.inf in Vista
  - No Autorun in Windows 7, 8/8.1, or 10
  - Disabled through the registry
- Consider changing AutoPlay
  - Get the latest security patches
  - Updates to autorun.inf and AutoPlay

Password best practices
- Changing 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 or automated logins

2.7 - Workstation Security Best Practices (continued)

Restricting user permissions
- 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

Disabling 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 usernames
  - User:admin Password:admin
  - Helps with brute-force attacks

Account lockout and disablement
- Too many bad passwords will cause a lockout
  - This should be normal for most users
  - This can cause big issues for service accounts
  - You might want this
- Disable user accounts
  - Part of the normal change process
  - You don't want to delete accounts
  - At least not initially

Active Directory
- Windows networks can be centrally managed
  - Active Directory Domain Services (AD DS)
- Create and delete accounts
  - Add users to the domain
  - Remove user accounts
- Reset passwords and unlock accounts
  - I forgot it. Again.
- Disable accounts
  - Off-boarding or security processes

Data encryption
- Full-disk encryption
  - Encrypt the entire drive
- Filesystem 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

Patch and update management
- Keep OS and applications updated
  - Security and stability improvements
- Built-in to the operating system
  - Updates are deployed as available
  - Deployment may be managed internally
- Many applications include their own updater
  - Check for updates when starting
- Always stay up to date
  - Security vulnerabilities are exploited quickly

2.8 - Securing Mobile Devices

Screen locks
- Restrict access to the device
- You're going to leave it somewhere
- Fingerprint - Built-in fingerprint reader
- Face Unlock - Face recognition
- Swipe - Choose a pattern
- Passcode - Choose a PIN or add complexity
- Failed attempts
  - iOS: Erase everything after 10 failed attempts
  - Android: Lock the device and require a Google login

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

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
- Windows Phone
  - Closed environment
- Apps run in a "sandbox"
  - You control what data an app can view

2.8 - Securing Mobile Devices (continued)

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

Biometric authentication
- Multi-factor authentication
  - More than one factor
  - Passcode, password, swipe pattern
  - Fingerprint, face, iris
- A phone is always with you
  - And you're a good source of data
- We're just figuring this out
  - Biometrics have a long way to go
  - Use as many factors as necessary

Authenticator apps
- Pseudo-random token generators
  - A useful authentication factor
- Carry around physical token devices
  - Where are my keys again?
- You're carrying your phone around
  - And it's pretty powerful

Full device encryption
- Encrypt all device data
  - Phone keeps the key
- iOS 8 and later
  - Personal data is encrypted with your passcode
- Android - Full device encryption can be turned on

Trusted vs. untrusted sources
- Once malware is on a phone, it has a huge amount of access
  - Don't install APK files from an untrusted source
- iOS
  - All apps are curated by Apple
- Android
  - Apps can be downloaded from
  - Google Play or sideloaded
  - This is where problems can occur

Firewalls
- Mobile phones don't include a firewall
  - Most activity is 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
- 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 and Disposal

Physical destruction
- Shredder
  - Heavy machinery
  - Complete destruction
- Drill / Hammer
  - Quick and easy
  - Platters, all the way through
- Electromagnetic (degaussing)
  - Remove the magnetic field
  - Destroys the drive data and the electronics
- Incineration
  - Fire hot.

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

Disk formatting
- Low-level formatting
  - Provided at the factory - Not possible by 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
  - Windows Vista and later
  - Can't recover the data

Hard drive security
- 2009 UK university study of 300 hard drives from eBay and computer fairs
  - 34% had personal data, corporate information, sensitive information
  - Launch procedures for a ground-to-air missile system
- File level overwriting - Sdelete – Windows Sysinternals
- Whole drive wipe secure data removal
  - DBAN - Darik's Boot and Nuke
- Physical drive destruction
  - One-off or industrial removal and destroy

2.10 - Securing a SOHO Network

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

Wireless encryption
- All wireless computers are radio transmitters and receivers
  - Anyone can listen in
- Solution: Encrypt the data
  - Everyone gets the password
- Only people with the password can transmit and listen
  - WPA2 encryption

Power level controls
- Usually a wireless configuration
  - Set it as low as you can
- How low is low?
  - This might require some additional study
- Consider the receiver
  - High-gain antennas can hear a lot
  - Location, location, location

Using WPS
- Wi-Fi Protected Setup
  - Originally called Wi-Fi Simple Config
- Allows "easy" setup of a mobile device
  - A passphrase can be complicated to a novice
- Different ways to connect
  - PIN configured on access point must be entered on the mobile device
  - Push a button on the access point
  - Near-field communication - Bring the mobile device close to the access point
  - USB method - no longer used

The WPS hack
- December 2011 - WPS has a design flaw
  - It was built wrong from the beginning
- PIN is an eight-digit number
  - Really seven digits and a checksum
  - Seven digits, 10,000,000 possible combinations
- The WPS process validates each half of the PIN
  - First half, 4 digits. Second half, 3 digits.
  - First half, 10,000 possibilities.
  - Second half, 1,000 possibilities
- It takes about four hours to go through all of them
  - Most devices now include a lockout function

Default usernames and 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 WAP or router
  - *http://www.routerpasswords.com*

MAC address filtering
- Media Access Control
  - The "hardware" address
- Limit access through the physical hardware address
  - Keeps the neighbors out
  - Additional administration with visitors
- Easy to find working MAC addresses through wireless LAN analysis
  - MAC addresses can be spoofed
  - Free open-source software
- Security through obscurity

IP addressing
- DHCP (automatic) IP addressing vs. manual IP addressing
- IP addresses are easy to see in an unencrypted network
- If the encryption is broken, the IP addresses will be obvious
- Configuring a static IP address is not a security technique
  - Security through obscurity

SOHO firewalls
- Small office / home office appliances
  - Generally has reduced throughput requirements
- Usually includes multiple functions
  - Wireless access point, router, firewall, content filter
- May not provide advanced capabilities
  - Dynamic routing
  - Remote support
  - Install the latest software
- Update and upgrade the firmware
  - Firewalls, routers, switches, etc.

Firewall settings
- Inbound traffic
  - Extensive filtering and firewall rules
  - Allow only required traffic
  - Configure port forwarding to map TCP/UDP ports to a device
  - Consider building a DMZ
- Outbound traffic
  - Blacklist - Allow all, stop only unwanted traffic
  - Whitelist - Block all, only allow certain traffic types

2.10 - Securing a SOHO Network (continued)

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

Content filtering
- Control traffic based on data within the content
  - Data in the packets
- 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 security
- Physical access
  - A relatively easy hack
  - Highly secure data centers
- Door access
  - Lock and key
  - Electronic keyless
- Biometric
  - Eyeballs and fingers
- The process
  - Documented
  - Well established

3.1 - Troubleshooting Windows

Slow system 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 bad guys

Limited connectivity
- Limited or no connectivity: The connection has limited or no connectivity. You might be unable to access the Internet or some network resources. The connection is limited
- Local issues
  - Wireless signal, disconnected cable
  - Check IP address configuration
  - Reboot
- External issues
  - Wireless router rebooted/turned off
  - Ping your default gateway and external IP

Boot errors
- Can't find operating system
  - OS missing
- Boot loader replaced or changed
  - Multiple OSes 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
- Missing operating system
  - Boot Configuration Data (BCD) may be incorrect
  - Run Startup Repair or manually configure BCD store
- Boots to Safe Mode
  - Windows is not starting normally
  - Run Startup Repair

Application crashes
- 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

Bluescreens and spontaneous 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

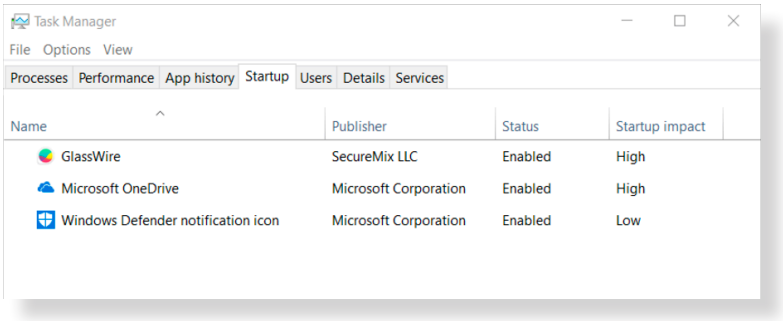
3.1 - Troubleshooting Windows (continued)

Black screen
- No login dialog, no desktop
  - Driver corruption, OS file corruption
- Start in VGA mode
  - F8 for startup options
- Run SFC - System File Checker
  - Run from recovery console
- Update driver in Safe Mode
  - Download from known good source
- Repair/Refresh or recover from backup

Testing the printer
- Print or scan a test page
  - Built into Windows
  - Not the application
- Use diagnostic tools
  - Web-based utilities
    - Built into the printer
  - Vendor specific
    - Download from the web site
  - Generic
    - Available in LiveCD form

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

Slow boot
- Boot process hangs or takes longer than normal
  - No activity, no drive lights
- Manage the startup apps
  - Control what loads during the boot process
- Task Manager
  - Startup tab
  - Startup impact, Right-click / Disable
- Disable everything
  - Load them back one at a time



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

3.1 - Troubleshooting Solutions

Defragmentation
- Moves file fragments so they are contiguous
  - Sharing a common border
  - Improves read and write time
  - Only applicable to spinning hard drives
- Graphical version in the drive properties
  - Command line: **`defrag`**
- Weekly schedule with *Control Panel / Administrative Tools / Task Scheduler*

Reboot
- Have you tried turning it off and on again?
  - There's a reason it works
- Bug in your router software
  - Reboot the router
- Application is using too many resources
  - Stops the app
- Memory leak slowly consumes all available RAM
  - Clears the RAM and starts again

Kill tasks
- Instead of rebooting, find the problem
  - And kill it
- Task Manager - Processes tab
- Sort by resource - CPU, memory, disk, network
- Right-click to end task
  - Trial and error

Restart services
- Services
  - Applications that run in the background
  - No user interaction
- Similar issues as a normal process
  - Resource utilization
  - Memory leaks
  - Crashes
- View status in Task Manager
  - Services tab
  - Right-click to start, stop, or restart

Update network settings
- One configuration mismatch can cause significant network slowdowns
  - Speed
  - Duplex
- Most auto negotiations work fine
  - Until they don't
- Driver may not show the negotiated value
  - Filter through the Event Viewer
- Device should match the switch
  - Both sides should be identical

Reimage or reload OS
- Windows is big
  - And complex
- Spend time trying to find the needle
  - Or simply build a new haystack
- Many organizations have prebuilt images
  - Don't waste time researching issues
- Windows includes a reset option
  - *Settings / Update & Security / Recovery*

Roll back
- Restore points
  - Rewind to an earlier point in time
  - Time travel without erasing your work
- Application updates
  - Restore point created automatically during application installations
- Device Drivers
  - These can break Windows
  - Roll back from the
  - Windows start menu (F8)

Update and patch
- Windows Update
  - Centralized OS and driver updates
- Lots of flexibility
  - Change active hours
  - Manage metered connections
- Applications must be patched
  - Security issues don't stop at the OS
  - Download from the publisher

Repair application
- Application issues
  - Problems with the application files or configurations
- Each application has its own repair process
  - Fix missing files
  - Replace corrupted files
  - Fix application shortcuts
  - Repair registry entries
  - Update or reconfigure drivers

Update boot order
- Try to boot from a USB drive
  - Doesn't even try
- The BIOS determines which physical device will be used during boot
  - And in which order
- Each BIOS is a bit different
  - The configuration is in there somewhere
- It's an easy one to miss
  - Usually the first thing to check

Disable startup services / apps
- It's difficult to tell what application might be a problem child
  - Much of the underlying OS operations are hidden from view
- Trial and error
  - Disable all startup apps and services
  - Or disable one at a time
  - This might take quite a few restarts
- Manage startup processes
  - *Task Manager, Control Panel / Administrative Tools / Services*

Safe Mode - Windows 7 and 8/8.1
- Press F8 on boot
  - Advanced Boot Options
- Safe Mode
  - Only the necessary drivers to get started
- Safe Mode with Networking
  - Includes drivers for network connectivity
- Safe Mode with Command Prompt
  - No Windows Explorer – quick and dirty
- Enable low-resolution (VGA Mode)
  - Recover from bad video driver installations

Safe Mode - Windows 10
- F8 probably won't work
  - Windows Fast Startup prevents a complete shutdown
- From the Windows desktop
  - Hold down shift when clicking Restart
  - *Settings / Update & Security / Recovery / Advanced startup / Restart now*
  - System Configuration (**msconfig**)

Rebuild Windows profiles
- Profiles can become corrupted
  - The User Profile Service failed the logon. User Profile cannot be loaded.
- If a profile doesn't exist, it's recreated
  - We're going to delete the profile and force the rebuilding process
- It's not as easy as copying a file
  - Backups, registry modifications
- Login with domain admin
- Rename the \Users\name folder
- Export the user's registry
- Delete the registry entry
- Restart the computer

3.1 - Troubleshooting Solutions (continued)

Deleting Windows profiles
- Login to the computer with Domain Administrator rights
- Rename the *Users**name* folder
  - This will save important files
- Backup the user's registry
  - *HKLM**SOFTWARE**Microsoft**Windows NT**CurrentVersion**ProfileList*
  - Right-click / Export
- Delete the registry entry - You have a backup
- Restart the computer

Reconstructing Windows profiles
- Login to the computer with the user account
  - The profile will be rebuilt
  - This will recreate the \Users\name folder
- Login as Domain Administrator
  - Copy over any important files from the old profile
- Do not copy the entire profile
  - Corrupted files might exist in the old profile

3.2 - Troubleshooting Security Issues

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 and check pop-up block feature
- Scan for malware
  - Consider a cleaning
  - Rebuild from scratch or known good backup to guarantee removal

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

Browser security alerts
- 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)

Malware network symptoms
- 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

Malware OS symptoms
- 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

System lock up
- Completely stops
  - Check Caps Lock and Num Lock status lights
- May still be able to terminate bad apps
  - Windows and Linux Task Manager (*Ctrl-Alt-Del / Task Manager*)
  - Mac OS X Force Quit (*Command-Option-Esc*)
- Check logs when restarting
  - May have some clues about what's happening
- May be a security issue
  - Perform a virus/malware scan
- Perform a hardware diagnostic
  - System issues can be a factor

Application crashes
- 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

3.2 - Troubleshooting Security Issues (continued)

Virus alerts and hoaxes
- Rogue antivirus
  - 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

Email security
- Spam - Unsolicited email messages, advertisements, phishing attacks, spread viruses
  - Spam filters can be helpful
- Hijacked email
  - Infected computers can become email spammers
  - You receive odd replies from other users
  - You receive bounce messages from unknown email addresses

System / application log errors
- Many errors go undetected
  - The details are in the log
- It may take some work to find them
  - Filter and research
- Find security issues
  - Improper logins
  - Unexpected application use
  - Failed login attempts

3.3 - Removing Malware

1. Identify 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
- Disable System Protection
  - No reason to save an infected config
- Delete all restore points
  - Remove all infection locations

4a. Remediate: Update anti-virus
- Signature and engine updates
  - The engine
  - The guts of the machine
  - 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

4b. Remediate: Scan and remove
- Microsoft, Symantec, McAfee
  - The big anti-virus apps
- Malwarebytes Anti-Malware - Malware-specific
- Stand-alone removal apps
  - Check with your anti-virus company
- There's really no way to know if it's really gone
  - Delete and rebuild

4b. Remediate: Scan and remove
- 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

5. 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

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

7. 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

3.4 - Troubleshooting Mobile Apps

Dim display
- Difficult to see the details, even in low light
- Check the brightness setting
  - iOS: Settings / Display and brightness
  - Android: Settings / Display / Brightness level
- Replace the bad display - backlight issue

Wireless connectivity
- Intermittent connectivity
  - Move closer to access point
  - Try a different access point
- No wireless 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

Cannot broadcast to monitor
- Broadcast to a TV
  - Apple TV, Xbox, Playstation, Chromecast, etc.
- Check app requirements
  - Every broadcast device is different
- All devices must be on the same wireless network
  - Can't mix your private and guest network
- Signal strength is important
  - Between phone and television
  - Between television and the Internet

Non-responsive touchscreen
- Touchscreen completely black or touchscreen not responding to input
- Apple iOS restart
  - Hold power button, slide to power off, press power button
  - Hold down power button and Home button for 10 seconds
- Android device restart
  - Remove battery, put back in, power on
  - Hold down power and volume down until restart
  - Some phones have different key combinations

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

Unable to decrypt email
- Built-in to corporate email systems - Outlook
- Each user has a private key
  - You can't decrypt without the key
- Install individual private keys on every mobile device
  - Use a Mobile Device Manager (MDM)

Short battery life
- Bad reception - Always searching for signal
- Disable unnecessary features
  - 802.11 wireless, Bluetooth, GPS
- Check application battery usage
  - iPhone: Settings/General/Usage
  - Android: Settings/Battery
- Aging battery - There's only so many recharges

Overheating
- Phone will automatically shut down to avoid damage
- Charging/discharging the battery, CPU usage, display light
- Check app usage - Some apps can use a lot of CPU
- Avoid direct sunlight - Quickly overheats

Frozen system
- Nothing works - No screen or button response
- Soft reset - Hold power down and turn off
- Hard reset
  - iOS: Hold power and home button for 10 seconds
  - Android: Combinations of power, home, and volume
- Ongoing problems may require a factory reset

No sound from speakers
- No sound from a particular app
  - Check volume settings - Both app and phone settings
  - Bad software / delete and reload
  - Try headphones
- Sound starts but then stops
  - Dueling apps / keep app in foreground
- No speaker sound from any app (no alarm, no music, no audio)
  - Load latest software
  - Factory reset

Inaccurate touch screen response
- Screen responds incorrectly or is unresponsive
- Close apps - Low memory can cause resource contention
- Perform a soft reset, unless a hard reset is required
- May require a hardware fix
  - Replace the digitizer / reseat cables

System lockout
- Too many incorrect unlock attempts
- iOS: Erases the phone after 10 failed attempts
- Android: Locks or wipes the phone after failed attempts

App log errors
- Most log information is hidden
  - You'll need developer tools to view it
- A wealth of information
  - If you can decipher it
  - This might take a bit of research
- Viewing logs
  - iOS - Xcode
  - Android - Logcat

3.5 - Troubleshooting Mobile Device Security

Signal drop / weak signal
- Drops and weak signals prevent traffic flows
- Make sure you're connecting to a trusted WiFi network
  - Use a VPN if you're not
  - Never trust a public WiFi Hotspot
  - Tether with your own device
- Run a speed test
  - Cell tower analyzer and test

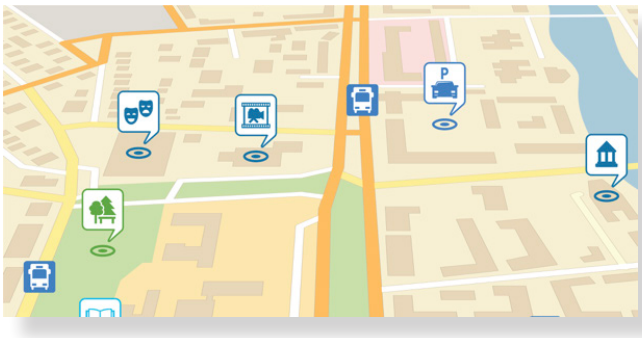
Power drain
- Power drains faster than normal
  - Heavy application use
  - Increased network activity
  - High resource utilization
- Check application before install
  - Use an App scanner
  - Force stop running apps
- Run anti-malware
  - Check for malicious activity
- Perform a clean install
  - Factory reset, reinstall apps

Slow data speeds
- Unusual network activity
  - Unintended WiFi connections
  - Data transmission over limit
- Check your network connection
  - Run a WiFi analyzer
  - Are you on a trusted WiFi network?
- Check network speed
  - Run speed check / cell tower analyzer
- Examine running apps for unusual activity
  - Large file transfers, constant activity

Unintended Bluetooth pairing
- Connect with a device that isn't yours
  - This isn't a good idea
- Remove the Bluetooth device
  - You would have to re-pair to access again
- Disable Bluetooth radio
  - No Bluetooth communication at all
- Run an anti-malware scan
  - Make sure there are no malicious apps

Leaked information
- 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 iTunes/iCloud/Apple Configurator, Google Sync, Microsoft OneDrive

Unauthorized location tracking
- Real-time tracking information and historical tracking details
  - This should be as protected as your other data
- Run an anti-malware scan
  - Malicious apps can capture many data points
- Check apps with an offline app scanner
  - Get some insight into what's running
- Perform a factory reset
  - Restore from a known-good backup



Unauthorized camera / microphone use
- Third-party app captures intimate information
  - Ethical and legal issues
- Run an anti-malware scan
  - Try to identify the source of the breach
- Confirm that loaded apps are legitimate
  - Check with a third-party scanner
- Factory refresh
  - Completely reset and start from the beginning

4.1 - Documentation Best Practices

Internal operating procedures
- Organizations have different business objectives
  - Processes and procedures
- Operational procedures
  - Downtime notifications
  - Facilities issues
- Software upgrades
  - Testing, change control
- Documentation is the key
  - Everyone can review and understand the policies

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

4.1 - Documentation Best Practices (continued)

Network topology diagrams
- Describes the network layout
  - May be a logical diagram
  - Can include physical rack locations

Incident response: Documentation
- Security policy
  - An ongoing challenge
- Documentation must be available
  - No questions
- Documentation always changes
  - Constant updating
  - Have a process in place
  - Use the wiki model

Compliance
- Meeting the standards of laws, policies, and regulations
- A healthy catalog of rules
  - Across many aspects of business and life
  - Many are industry-specific or situational
- Penalties
  - Fines
  - Loss of employment
  - Incarceration
- Scope
  - Domestic and international requirements

Regulatory
- Sarbanes-Oxley Act (SOX)
  - The Public Company Accounting Reform and Investor Protection Act of 2002
- The Health Insurance Portability and Accountability Act (HIPAA)
  - Extensive healthcare standards for storage, use, and transmission of health care information
- The Gramm-Leach-Bliley Act of 1999 (GLBA)
  - Disclosure of privacy information from financial institutions

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

Password policy
- Passwords should be complex, and all passwords should expire
  - Change every 30 days, 60 days, 90 days
- Critical systems might change more frequently
  - Every 15 days or every week
- The recovery process should not be trivial!
  - Some organizations have a very formal process

Account lockout and disablement
- Too many bad passwords will cause a lockout
  - This should be normal for most users
  - This can cause big issues for service accounts
  - You might want this
- Disable accounts
  - Part of the normal change process
  - You don't want to delete accounts
  - At least not initially

Inventory management
- A record of every asset
  - Routers, switches, cables, fiber modules, etc.
- Financial records, audits, depreciation
  - Make/model, configuration, purchase date, etc.
- Tag the asset
  - Barcode, RFID, visible tracking number

4.2 - Change Management

Change management
- Change control
  - A formal process for managing change
  - Avoid downtime, confusion, and mistakes
- Nothing changes without the process
  - Determine the scope of the change
  - Analyze the risk associated with the change
  - Create a plan
  - Get end-user approval
  - Present the proposal to the change control board
  - Have a backout plan if the change doesn't work
  - Document the changes

Scope 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?
  - No impact, or hours of downtime

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 vulnerability, application unavailability, or unexpected downtime to other services

4.2 - Change Management (continued)

Plan for change
- What's it take to make the change?
  - Detailed information
  - Describe a technical process to other technical people
- Others can help identify unforeseen risk
  - A complete picture
- Scheduling
  - Time of day, day of week
  - Include completion timeframes

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

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

Backout 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
  - Always have backups

Document changes
- Something changed
  - Everyone needs to know
- Help desk documentation
  - Version numbers, network diagram, new server names
- Track changes over time
  - Cross-reference against help desk tickets
- Track before and after statistics
  - Better or worse?

4.3 - Disaster Recovery

Backup strategies
- Image level
  - Bare metal backup using images
  - Operating system volume snapshots or hypervisor snapshots
  - Recover the entire system at once
  - Make an exact copy somewhere else
- File level
  - Copy individual files to a backup
  - May not necessarily store all system files
  - May need to rebuild the OS and then perform a file restore

Critical application backups
- Application software
  - Often distributed across multiple servers
- Application data
  - Databases, other data storage
- Location of data
  - Local and cloud-based
- All of these are needed when restoring
  - They all work together

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

UPS
- Uninterruptible Power Supply
  - Short-term backup power
  - Blackouts, brownouts, surges
- UPS types
  - Offline/Standby UPS
  - Line-interactive UPS
  - On-line/Double-conversion UPS
- Features
  - Auto shutdown, battery capacity, outlets, phone line suppression

4.3 - Disaster Recovery (continued)

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

Cloud storage
- Data is available anywhere, anytime, on any device
  - If you have a network, you have your data
- Advantages over local backups
  - No tape drives to manage
  - No offsite storage processing
- Disadvantages over local backups
  - Data is not under your direct control
  - Strong encryption mechanisms are critical

Account recovery options
- Apps won't work if users can't login
  - Your Windows Domain will most likely be the foundation of your recovery efforts
- Consider other authentication requirements
  - Multi-factor authentication validation
  - Additional authentication databases
  - RADIUS, TACACS
- Another good reason for centralized administration
  - No local accounts

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 an electrical ground
  - This is not a way to prevent ESD

Handling toxic waste
- Batteries
  - Uninterruptible Power Supplies
  - Dispose at your local hazardous waste facility
- CRTs
  - Cathode ray tubes - there's a few of those left
  - Glass contains lead
  - 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

Mobile device disposal
- Wipe your data, if possible
  - This isn't always an option
- Manufacturer or phone service provider may have a recycling program or an upgrade program
- Dispose at a local hazardous waste facility
  - Do not throw in the trash

Personal safety
- Remove jewelry
  - And name badge neck straps
  - Or use breakaway straps
- 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
- Cable management
  - Avoid trip hazards
  - Use cable ties or velcro
- Safety goggles
  - Useful when working with chemicals
  - Printer repair, toner, batteries
- Air filter mask
  - Dusty computers
  - Printer toner

Local 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

4.4 - 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 a good idea. Really.
  - Do not connect yourself to an electrical ground!
- Try not to touch components directly
  - Card edges only

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 grounded mat for standing or sitting
- Anti-static bag
  - Safely move or ship components

Anti-static strap

4.5 - Environmental Impacts

Disposal procedures
- Read your Material Safety Data Sheets (MSDS)
  - United States Department of Labor,
  - Occupational Safety and Health Administration (OSHA)
  - http://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

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

UPS
- Uninterruptible Power Supply
  - Backup power
  - Blackouts, brownouts, 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

4.5 - Environmental Impacts (continued)

Protection from airborne particles
- Enclosures
  - Protect computers on a manufacturing floor
  - Protect from dust, oil, smoke
- Air filters and masks
  - Protect against airborne particles
  - Dust in computer cases, laser printer toner

Dust and debris
- Cleaning
  - Neutral detergents
  - No ammonia-based cleaning liquids
  - Avoid isopropyl alcohol
- Vacuum
  - Use a “computer” vacuum - Maintain ventilation
- Compressed air pump
  - Try not to use compressed air in a can

Local government regulations
- Environmental regulations
  - May have very specific controls
- The obvious
  - Hazardous waste
  - Batteries
  - Computer components
- The not-as-obvious
  - Paper disposal

4.6 - Privacy, Licensing, and Policies

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

Incident response: Documentation
- Security policy
  - An ongoing challenge
- Documentation must be available
  - No questions
- Documentation always changes
  - Constant updating
  - Have a process in place
  - Use the wiki model

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
  - Digital signatures

Licensing / EULA
- Closed source / Commercial
  - Source code is private
  - End user gets compiled executable
- Free and Open Source (FOSS)
  - Source code is freely available
  - End user can compile their own executable
- End User Licensing Agreement
  - Determines how the software can be used
- Digital Rights Management (DRM)
  - Used to manage the use of software

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
- Enterprise license
  - Per-seat purchase / Site license
  - The software may be installed everywhere
  - Annual renewals

PII - Personally identifiable information
- 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
- July 2015 - U.S. Office of Personnel Management (OPM)
  - Compromised personal identifiable information
  - Personnel file information; name, SSN, date of birth, job assignments, etc.
  - Approximately 21.5 million people affected

PCI DSS
- 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

4.6 - Privacy, Licensing, and Policies (continued)

GDPR - General Data Protection Regulation

- European Union regulation
  - Data protection and privacy for individuals in the EU
  - Name, address, photo, email address, bank details, posts on social networking websites, medical information, a computer's IP address, etc.
- Controls export of personal data
  - Users can decide where their data goes
- Gives individuals control of their personal data
  - A right to be forgotten
- Site privacy policy
  - Details all of the privacy rights for a user

PHI - Protected Health Information

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

Policies and best practices

- Policies
  - General IT guidelines
  - Determines how technology should be used
  - Provides processes for handling important technology decisions
- Security best practices
  - Some security techniques are accepted standards
  - Covers both processes and technologies
  - You need a firewall
  - What happens if there's a breach?

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

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

4.7 - Professionalism

Maintain 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 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

Don't minimize problems
- Technical issues can be traumatic
  - Often money and/or jobs on the line
- Even the smallest problems can seem huge
  - Especially when things aren't working
- Part technician, part counselor
  - Computers don't have problems
  - People have problems

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

4.8 - Scripting

Scripting and 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

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 8/8.1 and 10
- 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

4.8 - Scripting (continued)

Shell script
- Scripting the Unix/Linux shell
  - Automate and extend the command line
  - .sh file extension

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

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

Scripting basics
- Variables
  - Associate a name with an area of memory
  - x=1. y=x+7. Therefore, y=8.
  - pi=3.14
  - greeting="Hello and welcome."
- String data types
  - Some text
- Integer data types
  - Perform numerical calculations
- Loops
  - Perform a process over and over
  - Loop one time
  - Loop until something happens
- Comments
  - Annotate the code
  - There never seems to be enough of this

Environment variables
- Describes the operating system environment
  - Scripts use these to make decisions
- Common environment variables
  - Location of the Windows installation
  - The search path
  - The name of the computer
  - The drive letter and path of the user's home directory

```
#!/bin/sh
// Add the first input string
INPUT_STRING=hello
// Keep looping if the string isn't equal to bye
while [ "$INPUT_STRING" != "bye" ]
do
  echo "Please type something in (bye to quit)"
  read INPUT_STRING
  echo "You typed: $INPUT_STRING"
done
```

4.9 - Remote Access Technologies

RDP (Remote Desktop Protocol)
- Share a desktop from a remote location over tcp/3389
- Remote Desktop Services on many Windows versions
- Can connect to an entire desktop or just an application
- Clients for Windows, MacOS, Linux, Unix, iPhone, and others

Telnet
- Telnet – Telecommunication Network - tcp/23
  - Login to devices remotely
  - Console access
  - Unencrypted communication
  - Not the best choice for production systems

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

Third-party tools
- VNC (Virtual Network Computing)
  - Remote Frame Buffer (RFB) protocol
  - Clients for many operating systems
  - Many are open source
- Commercial solutions
  - TeamViewer, LogMeIn, etc.
- Screen sharing
  - Control the desktop
- File sharing
  - Transfer files between devices

Security considerations
- Microsoft Remote Desktop
  - An open port 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


Professor
Messer