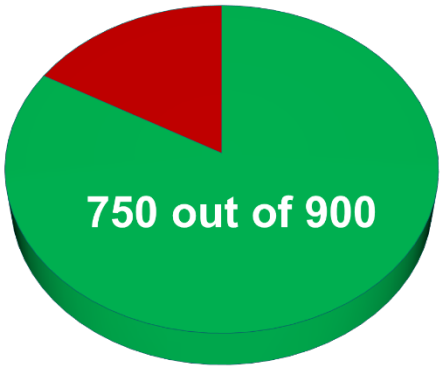
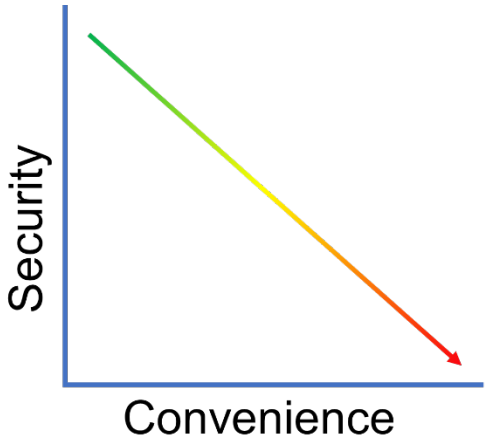
Overview of Security

- **Welcome**
  - **Domains (SYO-501)**
    - Threats, Attacks, and Vulnerabilities (21%)
    - Technologies and Tools (22%)
    - Architecture and Design (15%)
    - Identity and Access Management (16%)
    - Risk Management (14%)
    - Cryptography and PKI (12%)
  - **90 minutes to answer up to 90 questions**
  - **Minimum to Pass**



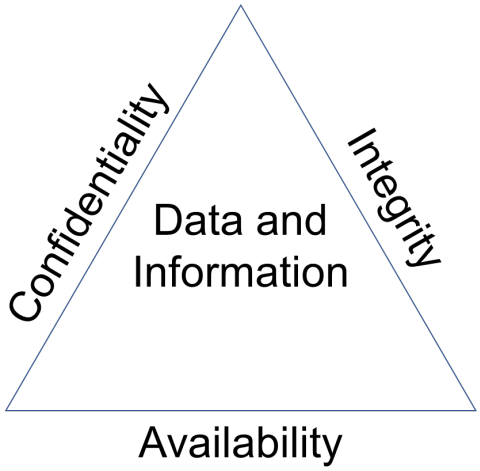
- **Overview of Security**



  - **Information Security**
    - Act of protecting data and information from unauthorized access, unlawful modification and disruption, disclosure, corruption, and destruction
  - **Information Systems Security**
    - Act of protecting the systems that hold and process our critical data

- **Basics and Fundamentals**

- **CIA Triad**



  - **Confidentiality**
    - Information has not been disclosed to unauthorized people
  - **Integrity**
    - Information has not been modified or altered without proper authorization
  - **Availability**
    - Information is able to be stored, accessed, or protected at all times

- **AAA of Security**
  - **Authentication**
    - When a person's identity is established with proof and confirmed by a system
      - Something you know
      - Something you are
      - Something you have
      - Something you do
      - Somewhere you are
  - **Authorization**
    - Occurs when a user is given access to a certain piece of data or certain areas of a building
  - **Accounting**
    - Tracking of data, computer usage, and network resources
    - Non-repudiation occurs when you have proof that someone has taken an action

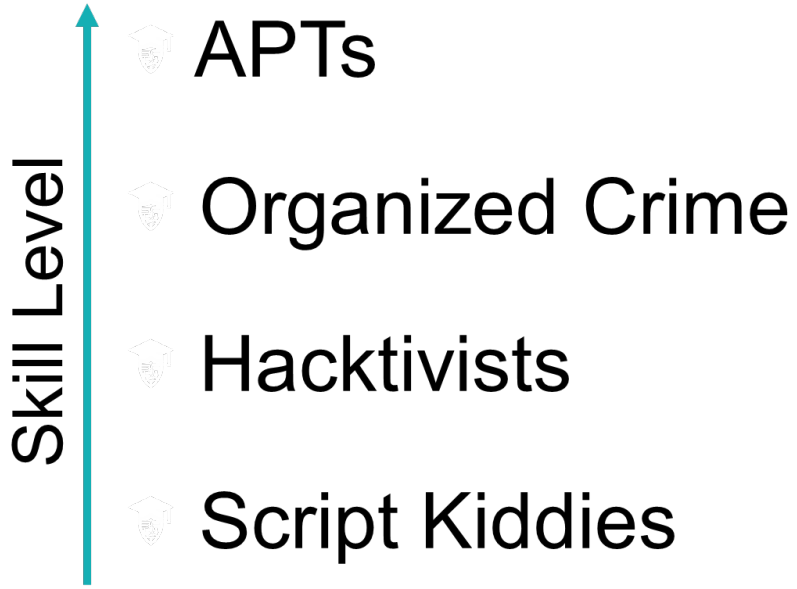
- Security Threats
  - **Malware**
    - Short-hand term for malicious software
  - **Unauthorized Access**
    - Occurs when access to computer resources and data occurs without the consent of the owner
  - **System Failure**
    - Occurs when a computer crashes or an individual application fails
  - **Social Engineering**
    - Act of manipulating users into revealing confidential information or performing other detrimental actions

- Mitigating Threats
  - Physical Controls
    - Alarm systems, locks, surveillance cameras, identification cards, and security guards
  - Technical Controls
    - Smart cards, encryption, access control lists (ACLs), intrusion detection systems, and network authentication
  - Administrative Controls
    - Policies, procedures, security awareness training, contingency planning, and disaster recovery plans
    - User training is the most cost-effective security control to use

- Hackers
  - Five Types of Hackers
    - White Hats
      - Non-malicious hackers who attempt to break into a company's systems at their request
    - Black Hats
      - Malicious hackers who break into computer systems and networks without authorization or permission
    - Gray Hats
      - Hackers without any affiliation to a company who attempt to break into a company's network but risk the law by doing so
    - Blue Hats
      - Hackers who attempt to hack into a network with permission of the company but are not employed by the company
    - Elite
      - Hackers who find and exploit vulnerabilities before anyone else does

        - 1 in 10,000 are elite
    - Script kiddies have limited skill and only run other people's exploits and tools

- **Threat Actors**
    - **Script Kiddies**
        - Hackers with little to no skill who only use the tools and exploits written by others
    - **Hacktivists**
        - Hackers who are driven by a cause like social change, political agendas, or terrorism
    - **Organized Crime**
        - Hackers who are part of a crime group that is well-funded and highly sophisticated
    - **Advanced Persistent Threats**
        - Highly trained and funded groups of hackers (often by nation states) with covert and open-source intelligence at their disposal



Malware

- **Malware**
  - **Malware**
    - Software designed to infiltrate a computer system and possibly damage it without the user's knowledge or consent
      - Viruses
      - Worms
      - Trojan horses
      - Ransomware
      - Spyware
      - Rootkits
      - Spam

- **Viruses**
  - **Virus**
    - Malicious code that runs on a machine without the user's knowledge and infects the computer when executed
    - Viruses require a user action in order to reproduce and spread
      - Boot sector
        - Boot sector viruses are stored in the first sector of a hard drive and are loaded into memory upon boot up
      - Macro
        - Virus embedded into a document and is executed when the document is
          opened by the user
      - Program
        - Program viruses infect an executable or application
      - Multipartite
        - Virus that combines boot and program viruses to first attach itself to the boot sector and system files before attacking other files on the computer
      - Encrypted
      - Polymorphic
        - Advanced version of an encrypted virus that changes itself every time it is executed by altering the decryption module to avoid detection

- Metamorphic
  - Virus that is able to rewrite itself entirely before it attempts to infect a file (advanced version of polymorphic virus)
- Stealth
- Armored
  - Armored viruses have a layer of protection to confuse a program or person analyzing it
- Hoax

- **Worms**
  - **Worm**
    - Malicious software, like a virus, but is able to replicate itself without user interaction
    - Worms self-replicate and spread without a user's consent or action
    - Worms can cause disruption to normal network traffic and computing activities
    - Example
      - 2009: 9-15 million computers infected with conficker

- **Trojans**
  - **Trojan Horse**
    - Malicious software that is disguised as a piece of harmless or desirable software
      - Trojans perform desired functions and malicious functions
  - **Remote Access Trojan (RAT)**
    - Provides the attacker with remote control of a victim computer and is the most commonly used type of Trojan

- **Ransomware**
  - **Ransomware**
    - Malware that restricts access to a victim's computer system until a ransom is received
    - Ransomware uses a vulnerability in your software to gain access and then encrypts your files
    - Example
      - $17 million: SamSam cost the City of Atlanta

- **Spyware**
  - **Spyware**
    - Malware that secretly gathers information about the user without their consent
    - Captures keystrokes made by the victim and takes screenshots that are sent to the attacker
  - **Adware**
    - Displays advertisements based upon its spying on you
  - **Grayware**
    - Software that isn't benign nor malicious and tends to behave improperly without serious consequences

- **Rootkits**
  - **Rootkit**
    - Software designed to gain administrative level control over a system without detection
    - DLL injection is commonly used by rootkits to maintain their persistent control
  - **DLL Injection**
    - Malicious code is inserted into a running process on a Windows machine by taking advantage of Dynamic Link Libraries that are loaded at runtime
  - **Driver Manipulation**
    - An attack that relies on compromising the kernel-mode device drivers that operate at a privileged or system level
    - A shim is placed between two components to intercept calls and redirect them
  - **Rootkits are activated before booting the operating system and are difficult to detect**

- **Spam**
  - **Spam**
    - Activity that abuses electronic messaging systems, most commonly through email
    - Spammers often exploit a company's open mail relays to send their messages
    - CAN-SPAM Act of 2003

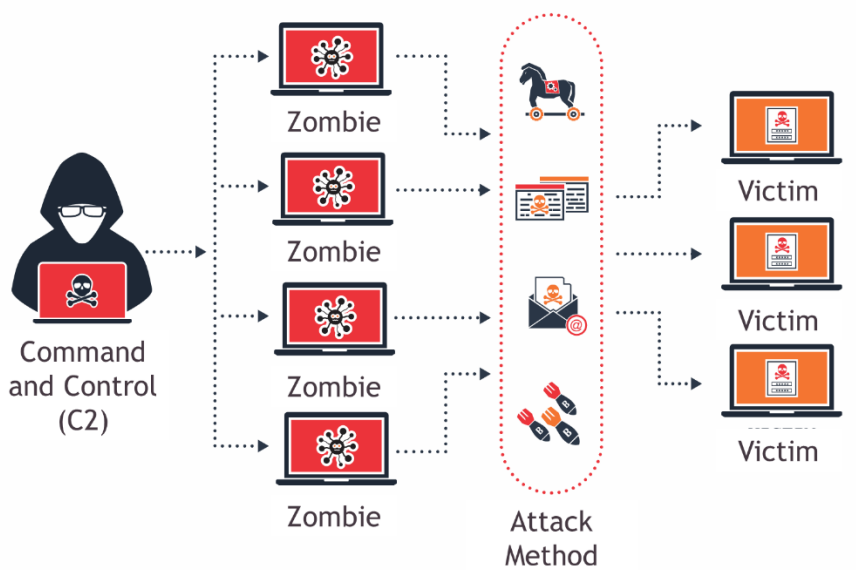
- **Summary of Malware**
  - **Virus**
    - Code that infects a computer when a file is opened or executed
  - **Worm**
    - Acts like a virus but can self-replicate
  - **Trojan**
    - Appears to do a desired function but also does something malicious
  - **Ransomware**
    - Takes control of your computer or data unless you pay
  - **Spyware**
    - Software that collects your information without your consent
  - **Rootkit**
    - Gains administrative control of your system by targeting boot loader or kernel
  - **Spam**
    - Abuse of electronic messaging systems

Malware Infections

- **Malware Infection**
  - **Threat Vector**
    - Method used by an attacker to access a victim's machine
  - **Attack Vector**
    - Method used by an attacker to gain access to a victim's machine in order to infect it with malware

- **Common Delivery Methods**
  - **Malware infections usually start within software, messaging, and media**
  - **Watering Holes**
    - Malware is placed on a website that you know your potential victims will access

- **Botnets and Zombies**
  - **Botnet**
    - A collection of compromised computers under the control of a master node



- Botnets can be utilized in other processor intensive functions and activities

- **Active Interception & Privilege Escalation**
  - **Active Interception**
    - Occurs when a computer is placed between the sender and receiver and is able to capture or modify the traffic between them

  - **Privilege Escalation**
    - Occurs when you are able to exploit a design flaw or bug in a system to gain access to resources that a normal user isn't able to access

- **Backdoors and Logic Bombs**
  - **Backdoors are used to bypass normal security and authentication functions**
  - **Remote Access Trojan (RAT) is placed by an attacker to maintain persistent access**
  - **Logic Bomb**
    - Malicious code that has been inserted inside a program and will execute only when certain conditions have been met
  - **Easter Egg**
    - Non-malicious code that when invoked, displays an insider joke, hidden message, or secret feature
  - **Logic bombs and Easter eggs should not be used according to secure coding standards**

- **Symptoms of Infection**
  - **Your computer might have been infected if it begins to act strangely**
    - Hard drives, files, or applications are not accessible anymore
    - Strange noises occur
    - Unusual error messages
    - Display looks strange
    - Jumbled printouts
    - Double file extensions are being displayed, such as textfile.txt.exe
    - New files and folders have been created or files and folders are missing/corrupted
    - System Restore will not function

- **Removing Malware**
  - **Identify symptoms of a malware infection**
  - **Quarantine the infected systems**
  - **Disable System Restore (if using a Windows machine)**
  - **Remediate the infected system**
  - **Schedule automatic updates and scans**
  - **Enable System Restore and create a new restore point**
  - **Provide end user security awareness training**
  - **If a boot sector virus is suspected, reboot the computer from an external device and scan it**

- **Preventing Malware**
  - **Viruses**
  - **Worms**
  - **Trojans**
  - **Ransomware**
  - **Spyware**
  - **Rootkits**
  - **Spam**
  - **Worms, Trojans, and Ransomware are best detected with anti-malware solutions**
  - **Scanners can detect a file containing a rootkit before it is installed…**
  - **…removal of a rootkit is difficult and the best plan is to reimage the machine**
  - **Verify your email servers aren't configured as open mail relays or SMTP open relays**
  - **Remove email addresses from website**
  - **Use whitelists and blacklists**
  - **Train and educate end users**

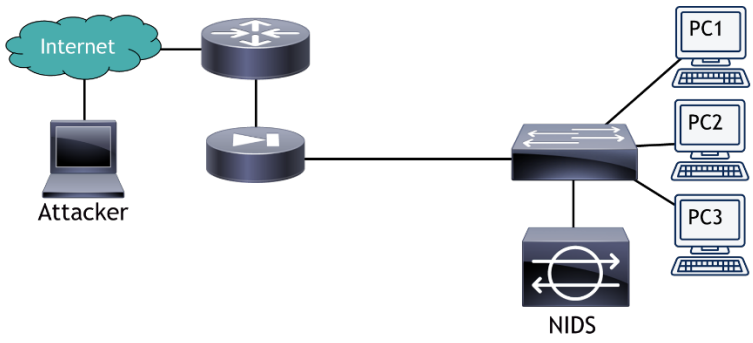
- Update your anti-malware software automatically and scan your computer
- Update and patch the operating system and applications regularly
- Educate and train end users on safe Internet surfing practices

Security Applications and Devices

- **Software Firewalls**
  - **Personal Firewalls**
    - Software application that protects a single computer from unwanted Internet traffic
    - Host-based firewalls
    - Windows Firewall (Windows)
    - PF and IPFW (OS X)
    - iptables (Linux)
  - **Many anti-malware suites also contain software firewalls**

- **IDS**
  - **Intrusion Detection System**
    - Device or software application that monitors a system or network and analyzes the data passing through it in order to identify an incident or attack
    - HIDS
      - Host-based IDS

    - NIDS
      - Network-based IDS



  - **Signature, Policy, and Anomaly-based detection methods**
    - Signature-based
      - A specific string of bytes triggers an alert
    - Policy-based

        - Relies on specific declaration of the security policy (i.e., 'No Telnet Authorized')
    - Anomaly-based
        - Analyzes the current traffic against an established baseline and triggers an alert if outside the statistical average
- **Types of Alerts**
    - True positive
        - Malicious activity is identified as an attack
    - False positive
        - Legitimate activity is identified as an attack
    - True negative
        - Legitimate activity is identified as legitimate traffic
    - False negative
        - Malicious activity is identified as legitimate traffic
- **IDS can only alert and log suspicious activity…**
- **IPS can also stop malicious activity from being executed**
- **HIDS logs are used to recreate the events after an attack has occurred**

- **Pop-up Blockers**
    - **Most web-browsers have the ability to block JavaScript created pop-ups**
    - **Users may enable pop-ups because they are required for a website to function**
    - **Malicious attackers could purchase ads (pay per click) through various networks**
    - **Content Filters**
        - Blocking of external files containing JavaScript, images, or web pages from loading in a browser
    - **Ensure your browser and its extensions are updated regularly**

- **Data Loss Prevention**
    - **Data Loss Prevention (DLP)**
        - Monitors the data of a system while in use, in transit, or at rest to detect attempts to steal the data
        - Software or hardware solutions
        - Endpoint DLP System
            - Software-based client that monitors the data in use on a computer and can stop a file transfer or alert an admin of the occurrence
        - Network DLP System
            - Software or hardware-based solution that is installed on the perimeter of the network to detect data in transit

        - Storage DLP System
            - Software installed on servers in the datacenter to inspect the data at rest
        - Cloud DLP System
            - Cloud software as a service that protects data being stored in cloud services

- **Securing the BIOS**
    - **Basic Input Output System**
        - Firmware that provides the computer instructions for how to accept input and send output
        - Unified Extensible Firmware Interface (UEFI)
        - BIOS and UEFI are used interchangeable in this lesson
    - **1. Flash the BIOS**
    - **2. Use a BIOS password**
    - **3. Configure the BIOS boot order**
    - **4. Disable the external ports and devices**
    - **5. Enable the secure boot option**

- **Securing Storage Devices**
    - **Removable media comes in many different formats**
        - You should always encrypt files on removable media
    - **Removable media controls**
        - Technical limitations placed on a system in regards to the utilization of USB storage devices and other removable media
        - Create administrative controls such as policies
    - **Network Attached Storage (NAS)**
        - Storage devices that connect directly to your organization's network
        - NAS systems often implement RAID arrays to ensure high availability
    - **Storage Area Network (SAN)**
        - Network designed specifically to perform block storage functions that may consist of NAS devices
        - 1. Use data encryption
        - 2. Use proper authentication
        - 3. Log NAS access

- **Disk Encryption**
    - **Encryption scrambles data into unreadable information**
    - **Self-Encrypting Drive (SED)**

        - Storage device that performs whole disk encryption by using embedded hardware
    - **Encryption software is most commonly used**
        - FileVault
        - BitLocker
    - **Trusted Platform Module (TPM)**
        - Chip residing on the motherboard that contains an encryption key
        - If your motherboard doesn't have TPM, you can use an external USB drive as a key
    - **Advanced Encryption Standard**
        - Symmetric key encryption that supports 128-bit and 256-bit keys
    - **Encryption adds security but has lower performance**
    - **Hardware Security Module (HSM)**
        - Physical devices that act as a secure cryptoprocessor during the encryption process

Mobile Device Security

- **Mobile Device Security**
- **Securing Wireless Devices**
  - **WiFi Protected Access 2 (WPA2) is the highest level of wireless security**
  - **AES**
    - Advanced Encryption Standard
  - **Bluetooth pairing creates a shared link key to encrypt the connection**
  - **Wired devices are almost always more secure than wireless ones**

- **Mobile Malware**
  - **Ensure your mobile device is patched and updated**
  - **Only install apps from the official App Store or Play Store**
  - **Do not jailbreak/root device**
  - **Don't use custom firmware or a custom ROM**
  - **Only load official store apps**
  - **Always update your phone's operating system**

- **SIM Cloning & ID Theft**
  - **Subscriber Identity Module (SIM)**
    - Integrated circuit that securely stores the international mobile subscriber identity (IMSI) number and its related key
  - **SIM Cloning**
    - Allows two phones to utilize the same service and allows an attacker to gain access to the phone's data
    - SIM v1 cards were easy to clone but newer SIM v2 cards are much harder
    - Be careful with where you post phone numbers

- **Bluetooth Attacks**
  - **Bluejacking**
    - Sending of unsolicited messages to Bluetooth-enabled devices
  - **Bluesnarfing**
    - Unauthorized access of information from a wireless device over a Bluetooth connection
  - **Bluejacking sends information to a device**
  - **Bluesnarfing takes information from a device**

- **Mobile Device Theft**
  - **Always ensure your device is backed up**
  - **Don't try to recover your device alone if it is stolen**

  - **Remote Lock**
    - Requires a PIN or password before someone can use the device
  - **Remote Wipe**
    - Remotely erases the contents of the device to ensure the information is not recovered by the thief

- **Security of Apps**
  - **Only install apps from the official mobile stores**
  - **TLS**
    - Transport Layer Security
  - **Mobile Device Management**
    - Centralized software solution that allows system administrators to create and enforce policies across its mobile devices
  - **Turn location services off to ensure privacy**
  - **Geotagging**
    - Embedding of the geolocation coordinates into a piece of data (i.e., a photo)
  - **Geotagging should be considered when developing your organization's security policies**

- **Bring Your Own Device**
  - **BYOD introduces a lot of security issues to consider**
  - **Storage Segmentation**
    - Creating a clear separation between personal and company data on a single device
  - **Mobile Device Management**
    - Centralized software solution for remote administration and configuration of mobile devices
  - **CYOD**
    - Choose Your Own Device
  - **MDM can prevent certain applications from being installed on the device**
  - **Ensure your organization has a good security policy for mobile devices**

- **Hardening Mobile Devices**
  - **1. Update your device to the latest version of the software**
  - **2. Install AntiVirus**
  - **3. Train users on proper security and use of the device**
  - **4. Only install apps from the official mobile stores**
  - **5. Do not root or jailbreak your devices**
  - **6. Only use v2 SIM cards with your devices**

- **7. Turn off all unnecessary features**
- **8. Turn on encryption for voice and data**
- **9. Use strong passwords or biometrics**
- **10. Don’t allow BYOD**
- **Ensure your organization has a good security policy for mobile devices**

Hardening

- **Hardening**
  - **Hardening**
    - Act of configuring an operating system securely by updating it, creating rules and policies to govern it, and removing unnecessary applications and services
  - **We are not guaranteed security, but we can minimize the risk…**
  - **Mitigate risk by minimizing vulnerabilities to reduce exposure to threats**

- **Unnecessary Applications**
  - **Least Functionality**
    - Process of configuring workstation or server to only provide essential applications and services
  - **Personal computers often accumulate unnecessary programs over time**
  - **Utilize a secure baseline image when adding new computers**
  - **SCCM**
    - Microsoft's System Center Configuration Management

- **Restricting Applications**
  - **Application Whitelist**
    - Only applications that are on the list are allowed to be run by the operating system while all other applications are blocked
  - **Application Blacklist**
    - Any application placed on the list will be prevented from running while all others will be permitted to run
  - **Whitelisting and blacklisting can be centrally managed**

- **Unnecessary Services**
  - **Any services that are unneeded should be disabled in the OS**

- **Trusted Operating Systems**
  - **Trusted Operating System (TOS)**
    - An operating system that meets the requirements set forth by government and has multilevel security
    - Windows 7 (and newer)
    - Mac OS X 10.6 (and newer)
    - FreeBSD (TrustedBSD)
    - Red Hat Enterprise Server
  - **You need to identify the current version and build prior to updating a system**

- **Updates and Patches**
  - **Patches**
    - A single problem-fixing piece of software for an operating system or application
  - **Hotfix**
    - A single problem-fixing piece of software for an operating system or application
  - **Patches and Hotfixes are now used interchangeably by most manufacturers**
  - **Categories of Updates**
    - Security Update
      - Software code that is issued for a product-specific security-related vulnerability
    - Critical Update
      - Software code for a specific problem addressing a critical, non-security bug in the software
    - Service Pack
      - A tested, cumulative grouping of patches, hotfixes, security updates, critical updates, and possibly some feature or design changes
    - Windows Update
      - Recommended update to fix a noncritical problem that users have found, as well as to provide additional features or capabilities
    - Driver Update
      - Updated device driver to fix a security issue or add a feature to a supported piece of hardware
    - Windows 10 uses the Windows Update program (wuapp.exe) to manage updates

- **Patch Management**
  - **Patch Management**
    - Process of planning, testing, implementing, and auditing of software patches
    - Planning
    - Testing
    - Implementing
    - Auditing
  - **Verify it is compatible with your systems and plan for how you will test and deploy it**
  - **Always test a patch prior to automating its deployment**
  - **Manually or automatically deploy the patch to all your clients to implement it**

- **Large organizations centrally manage updates through an update server**
- **Disable the wuauserv service to prevent Windows Update from running automatically**
- **It is important to audit the client's status after patch deployment**
- **Linux and OSX also have built-in patch management systems**

- **Group Policies**
  - **Group Policy**
    - A set of rules or policies that can be applied to a set of users or computer accounts within the operating system
    - Access the Group Policy Editor by opening the Run prompt and enter gpedit
    - Password complexity
    - Account lockout policy
    - Software restrictions
    - Application restrictions
  - **Active Directory domain controllers have a more advanced Group Policy Editor**
  - **Security Template**
    - A group of policies that can be loaded through one procedure
  - **Group Policy objectives (GPOs) aid in the hardening of the operating system**
  - **Baselining**
    - Process of measuring changes in the network, hardware, and software environment
    - A baseline establishes what is normal so you can find deviations

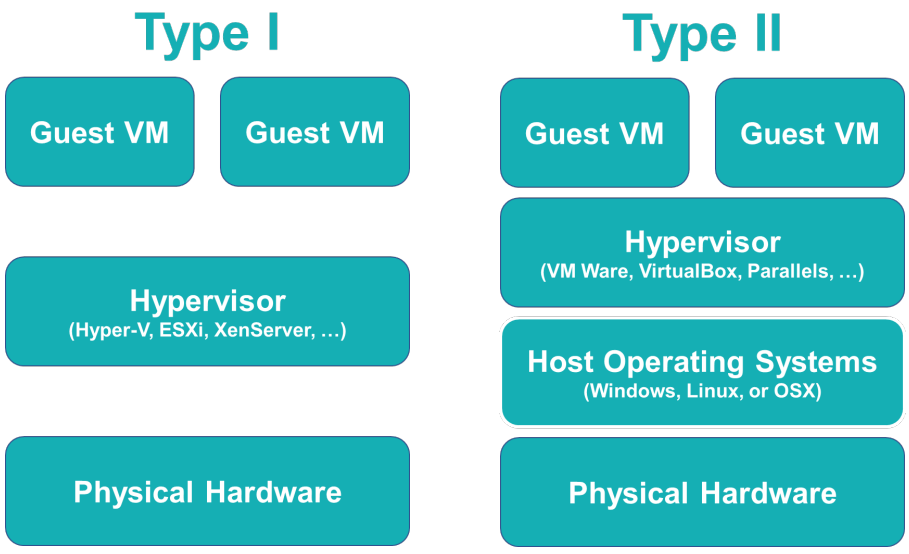
- **File Systems and Hard Drives**
  - **Level of security of a system is affected by its file system type**
    - NTFS
    - FAT32
    - ext4
    - HFS+
    - APFS
  - **Windows systems can utilize NTFS or FAT32**
  - **NTFS**
    - New Technology File System is the default file system format for Windows and is more secure because it supports logging, encryption, larger partition sizes, and larger file sizes than FAT32
  - **Linux systems should use ext4 and OSX should use the APFS**
  - **All hard drives will eventually fail**
    - 1. Remove temporary files by using Disk Cleanup
    - 2. Periodic system file checks

- 3. Defragment your disk drive
- 4. Back up your data
- 5. Use and practice restoration techniques

Virtualization

- **Virtualization**
  - **Virtualization**
    - Creation of a virtual resource
  - **A virtual machine is a container for an emulated computer that runs an entire operating system**
  - **VM Types**
    - System Virtual Machine
      - Complete platform designed to replace an entire physical computer and includes a full desktop/server operating system
    - Processor Virtual Machine
      - Designed to only run a single process or application like a virtualized web browser or a simple web server
  - **Virtualization continues to rise in order to reduce the physical requirements for data centers**

- **Hypervisors**
  - **Hypervisor**
    - Manages the distribution of the physical resources of a host machine (server) to the virtual machines being run (guests)



        - Type I (bare metal) hypervisors are more efficient than Type II
    - **Container-based**
        - Application Containerization
            - A single operating system kernel is shared across multiple virtual machines but each virtual machine receives its own user space for programs and data
            - Containerization allows for rapid and efficient deployment of distributed applications
    - **Docker**
    - **Parallels Virtuozzo**
    - **OpenVZ**

- **Threats to VMs**
    - **VMs are separated from other VMs by default**
    - **VM Escape**
        - An attack that allows an attacker to break out of a normally isolated VM by interacting directly with the hypervisor
        - Elasticity allows for scaling up or down to meet user demands
    - **Data Remnants**
        - Contents of a virtual machine that exist as deleted files on a cloud-based server after deprovisioning of a virtual machine
    - **Privilege Elevation**
        - Occurs when a user is able to grant themselves the ability to run functions as a higher-level user
    - **Live migration occurs when a VM is moved from one physical server to another over the network**

- **Securing VMs**
    - **Uses many of the same security measures as a physical server**
        - Limit connectivity between the virtual machine and the host
        - Remove any unnecessary pieces of virtual hardware from the virtual machine
        - Using proper patch management is important to keeping your guest's operating system secure
    - **Virtualization Sprawl**
        - Occurs when virtual machines are created, used, and deployed without proper management or oversight by the system admins

Application Security

- **Application Security**

- **Web Browser Security**
  - **Ensure your web browser is up-to-date with patches…**
    - …but don't adopt the newest browser immediately
  - **Which web browser should I use?**
  - **General Security for Web Browsers**
    - 1. Implement Policies
      - Create and implement web browsing policies as an administrative control or technical control
    - 2. Train Your Users
      - User training will prevent many issues inside your organization
    - 3. Use Proxy & Content Filter
      - Proxies cache the website to reduce requests and bandwidth usage
      - Content filters can be used to blacklist specific websites or entire categories of sites
    - 4. Prevent Malicious Code
      - Configure your browsers to prevent ActiveX controls, Java applets, JavaScript, Flash, and other active content

- **Web Browser Concerns**
  - **Cookies**
    - Text files placed on a client's computer to store information about the user's browsing habits, credentials, and other data
  - **Locally Shared Object (LSO)**
    - Also known as Flash cookies, they are stored in your Windows user profile under the Flash folder inside of your AppData folder
  - **Add-Ons**
    - Smaller browser extensions and plugins that provide additional functionality to the browser
  - **Advanced Security Options**
    - Browser configuration and settings for numerous options such as SSL/TLS settings, local storage/cache size, browsing history, and much more

- **Securing Applications**
  - **Use passwords to protect the contents of your documents**

- **Digital signatures and digital certificates are used by MS Outlook for email security**
- **User Account Control**
  - Prevents unauthorized access and avoid user error in the form of accidental changes

Secure Software Development

- **Software Development**
  - **SDLC**
    - Software Development Life Cycle
    - SDLC is an organized process of developing a secure application throughout the life of the project

SDLC Phases

- Planning and Analysis
- Software/Systems Design
- Implementation
- Testing
- Integration
- Deployment
- Maintenance

- **Agile**
  - Software development is performed in time-boxed or small increments to allow more adaptivity to change
- **DevOps**
  - Software development and information technology operations

- **SDLC Principles**
  - **Developers should always remember confidentiality, integrity, and availability**
    - Confidentiality
      - Ensures that only authorized users can access the data
    - Integrity
      - Ensures that the data is not modified or altered without permission
    - Availability
      - Ensuring that data is available to authorized users when it is needed
  - **Threat modeling helps prioritize vulnerability identification and patching**
  - **Least Privilege**
    - Users and processes should be run using the least amount of access necessary to perform a given function
  - **Defense in Depth**
    - Layering of security controls is more effective and secure than relying on a single control
  - **Never Trust User Input**
    - Any input that is received from a user should undergo input validation prior to allowing it to be utilized by an application
  - **Minimize Attack Surface**
    - Reduce the amount of code used by a program, eliminate unneeded functionality, and require authentication prior to running additional plugins
  - **Create Secure Defaults**
    - Default installations should include secure configurations instead of requiring an administrator or user to add in additional security
  - **Authenticity and Integrity**
    - Applications should be deployed using code signing to ensure the program is not changed inadvertently or maliciously prior to delivery to an end user
  - **Fail Securely**
    - Applications should be coded to properly conduct error handling for exceptions in order to fail securely instead of crashing

- **Fix Security Issues**
  - If a vulnerability is identified then it should be quickly and correctly patched to remove the vulnerability
- **Rely on Trusted SDKs**
  - SDKs must come from trusted source to ensure no malicious code is being added

- **Testing Methods**
  - **System Testing**
    - Black-box Testing
      - Occurs when a tester is not provided with any information about the system or program prior to conducting the test
    - White-box Testing
      - Occurs when a tester is provided full details of a system including the source code, diagrams, and user credentials in order to conduct the test

- **Structured Exception Handling (SEH)**
  - Provides control over what the application should do when faced with a runtime or syntax error
- **Programs should use input validation when taking data from users**
  - Input Validation
    - Applications verify that information received from a user matches a specific format or range of values
  - Example

```
get  $ssn

if ($ssn >=000-00-0000 and
   $ssn <= 999-99-9999)

  then [do function]

  else [conduct error handling]
```

- **Static Analysis**
  - Source code of an application is reviewed manually or with automatic tools without running the code
- **Dynamic Analysis**
  - Analysis and testing of a program occurs while it is being executed or run
- **Fuzzing**
  - Injection of randomized data into a software program in an attempt to find system failures, memory leaks, error handling issues, and improper input validation

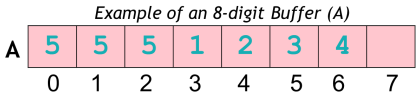
- **Software Vulnerabilities and Exploits**
  - **Backdoors**
    - Code placed in computer programs to bypass normal authentication and other security mechanisms
    - Backdoors are a poor coding practice and should not be utilized
  - **Directory Traversal**
    - Method of accessing unauthorized directories by moving through the directory structure on a remote server

- **Arbitrary Code Execution**
  - Occurs when an attacker is able to execute or run commands on a victim computer
- **Remote Code Execution (RCE)**
  - Occurs when an attacker is able to execute or run commands on a remote computer
- **Zero Day**
  - Attack against a vulnerability that is unknown to the original developer or manufacturer

- **Buffer Overflows**
  - **Buffer Overflow**
    - Occurs when a process stores data outside the memory range allocated by the developer
  - **Buffer**
    - A temporary storage area that a program uses to store data
    - Over 85% of data breaches were caused by a buffer overflow
  - **Example**

Phone Number

555-1234

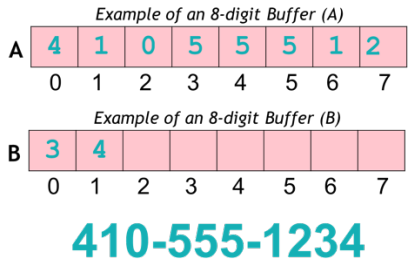


555-1234

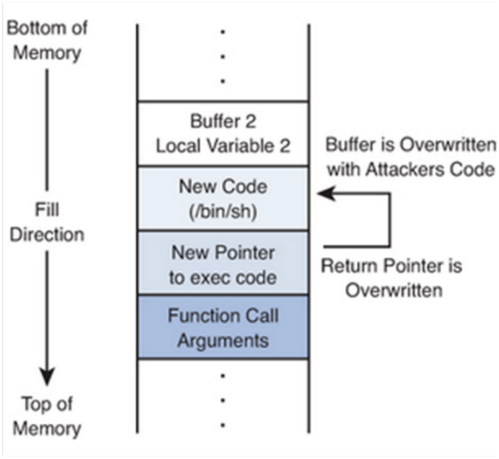
What happens if we try to enter a number that is too long?

Phone Number

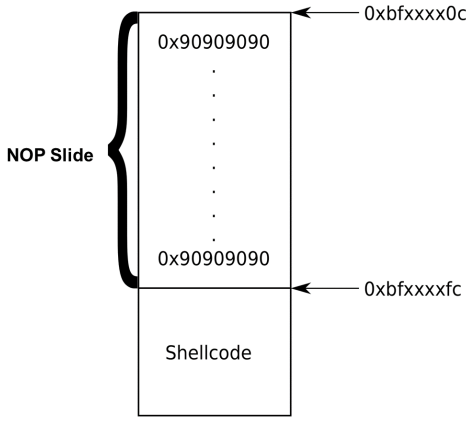
410-555-1234



- **Let's get technical…**
  - Stack
    - Reserved area of memory where the program saves the return address when a function call instruction is received



  - "Smash the Stack"
    - Occurs when an attacker fills up the buffer with NOP so that the return address may hit a NOP and continue on until it finds the attacker's code to run

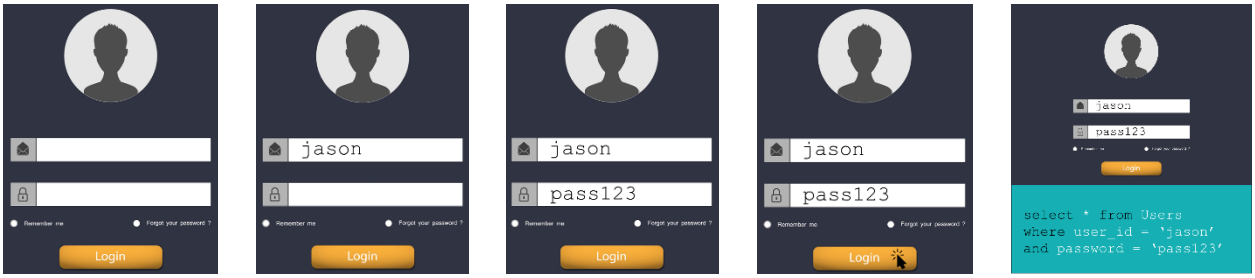


        - Address Space Layout Randomization
            - Method used by programmers to randomly arrange the different address spaces used by a program or process to prevent buffer overflow exploits
    - ***Buffer overflows attempt to put more data into memory than it is designed to hold***

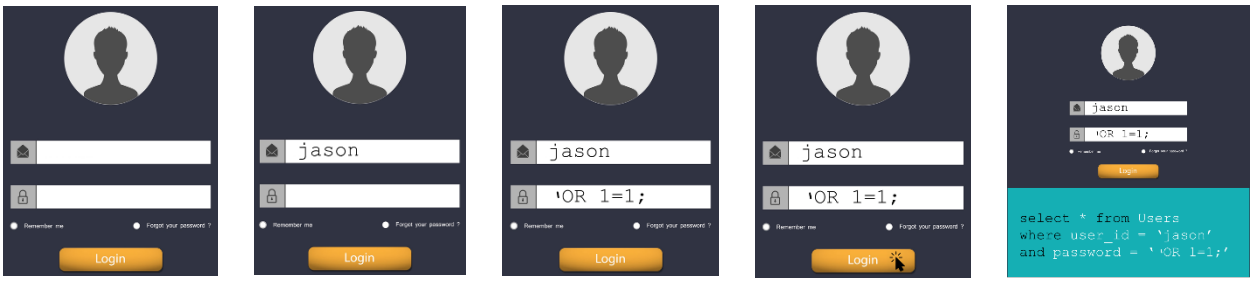
- **XSS and XSRF**
    - **Cross-Site Scripting (XSS)**
        - Occurs when an attacker embeds malicious scripting commands on a trusted website
        - Stored/Persistent
            - Attempts to get data provided by the attacker to be saved on the web server by the victim
        - Reflected
            - Attempts to have a non-persistent effect activated by a victim clicking a link on the site
        - DOM-based
            - Attempt to exploit the victim's web browser
        - Prevent XSS with output encoding and proper input validation
    - **Cross-Site Request Forgery (XSRF/CSRF)**
        - Occurs when an attacker forces a user to execute actions on a web server for which they are already authenticated
        - Prevent XSRF with tokens, encryption, XML file scanning, and cookie verification

- **SQL Injection**
    - **SQL Injection**
        - Attack consisting of the insertion or injection of an SQL query via input data from the client to a web application
    - **Injection Attack**
        - Insertion of additional information or code through data input from a client to an application
            - SQL
            - HTML
            - XML
            - LDAP
        - Most common type is an SQL injection

- **How does a normal SQL request work?**



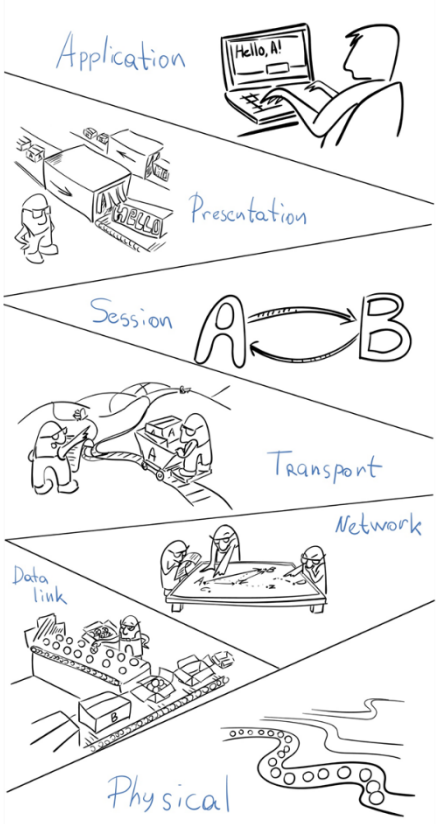
- **How does an SQL injection work?**



  - SQL injection is prevented through input validation and using least privilege when accessing a database
  - If you see ` OR 1=1; on the exam, it's an SQL injection

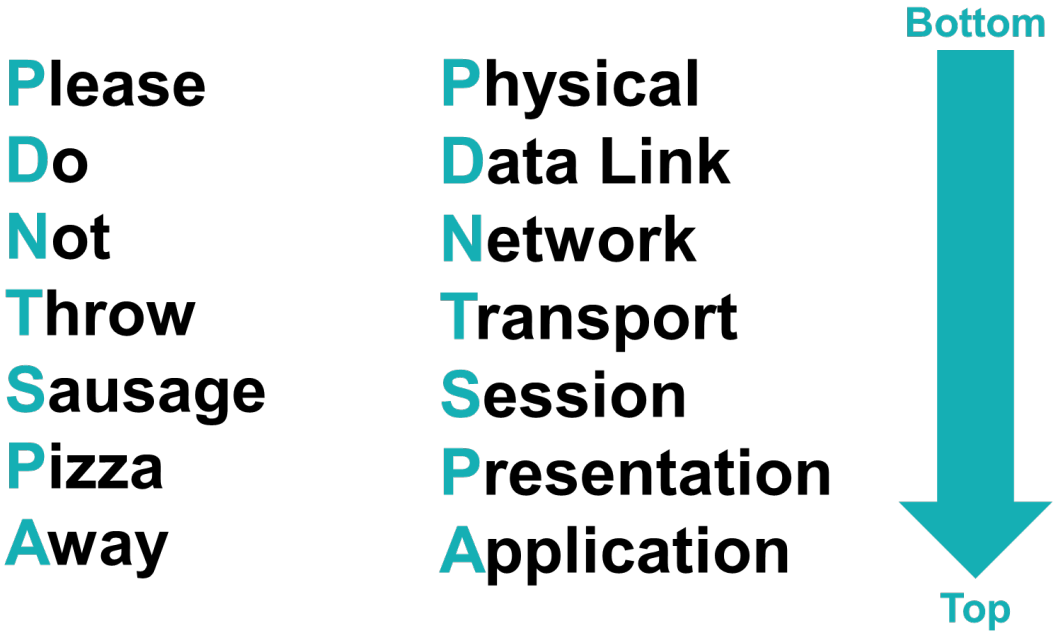
Network Design

- **Network Security**
  - **OSI Model**



  - **If you never learned network fundamentals, go back and review**

- **OSI Model**
  - **OSI Model**
    - Used to explain network communications between a host and remote device over a LAN or WAN



- **Physical Layer**
  - Represents the actual network cables and radio waves used to carry data over a network
  - Bits
- **Data Link Layer**
  - Describes how a connection is established, maintained, and transferred over the physical layer and uses physical addressing (MAC addresses)
  - Frames
- **Network Layer**
  - Uses logical address to route or switch information between hosts, the network, and the internetworks
  - Packets
- **Transport Layer**
  - Manages and ensures transmission of the packets occurs from a host to a destination using either TCP or UDP
  - Segments (TCP) or Datagrams (UDP)
- **Session Layer**
  - Manages the establishment, termination, and synchronization of a session over the network
- **Presentation Layer**
  - Translates the information into a format that the sender and receiver both understand

- **Application Layer**
  - Layer from which the message is created, formed, and originated
  - Consists of high-level protocols like HTTP, SMTP, and FTP

- **Switches**
  - **Switches are the combined evolution of hubs and bridges**
  - **MAC Flooding**
    - Attempt to overwhelm the limited switch memory set aside to store the MAC addresses for each port
    - Switches can fail-open when flooded and begin to act like a hub
  - **MAC Spoofing**
    - Occurs when an attacker masks their own MAC address to pretend they have the MAC address of another device
    - MAC Spoofing is often combined with an ARP spoofing attack
    - Limit static MAC addresses accepted
    - Limit duration of time for ARP entry on hosts
    - Conduct ARP inspection
  - **Physical Tampering**
    - Physical tampering occurs when an attacker attempts to gain physical access

- **Routers**
  - **Routers operate at Layer 3**
  - **Routers**
    - Used to connect two or more networks to form an internetwork
    - Routers rely on a packet's IP Addresses to determine the proper destination
    - Once on the network, it conducts an ARP request to find final destination
  - **Access Control List**
    - An ordered set of rules that a router uses to decide whether to permit or deny traffic based upon given characteristics
    - IP Spoofing is used to trick a router's ACL

- **Network Zones**
  - **Any traffic you wish to keep confidential crossing the internet should use a VPN**
  - **De-Militarized Zone (DMZ)**
    - Focused on providing controlled access to publicly available servers that are hosted within your organizational network

        - Sub-zones can be created to provide additional protection for some servers
    - **Extranet**
        - Specialized type of DMZ that is created for your partner organizations to access over a wide area network
    - **Intranets are used when only one company is involved**

- **Network Access Control**
    - **Network Access Control (NAC)**
        - Security technique in which devices are scanned to determine its current state prior to being allowed access onto a given network
        - If a device fails the inspection, it is placed into digital quarantine
    - **Persistent Agents**
        - A piece of software that is installed on the device requesting access to the network
    - **Non-Persistent Agents**
        - Uses a piece of software that scans the device remotely or is installed and subsequently removed after the scan
    - **NAC can be used as a hardware or software solution**
    - **IEEE 802.1x standard is used in port-based NAC**

- **VLANs**
    - **Segment the network**
    - **Reduce collisions**
    - **Organize the network**
    - **Boost performance**
    - **Increase security**
    - **Switch Spoofing**
        - Attacker configures their device to pretend it is a switch and uses it to negotiate a trunk link to break out of a VLAN
    - **Double Tagging**
        - Attacker adds an additional VLAN tag to create an outer and inner tag
        - Prevent double tagging by moving all ports out of the default VLAN group

- **Subnetting**
    - **Subnetting**
        - Act of creating subnetworks logically through the manipulation of IP addresses
        - Efficient use of IP addresses
        - Reduced broadcast traffic

        - Reduced collisions
        - Compartmentalized
    - **Subnet's policies and monitoring can aid in the security of your network**

- **Network Address Translation**
    - **Network Address Translation (NAT)**
        - Process of changing an IP address while it transits across a router
        - Using NAT can help us hide our network IPs
    - **Port Address Translation (PAT)**
        - Router keeps track of requests from internal hosts by assigning them random high number ports for each request
    - **Class A**
        - 10.0.0.0 to 10.255.255.255
    - **Class B**
        - 172.16.0.0 to 172.31.255.255
    - **Class C**
        - 192.168.0.0 to 192.168.255.255

- **Telephony**
    - **Telephony**
        - Term used to describe devices that provide voice communication to users
    - **Modem**
        - A device that could modulate digital information into an analog signal for transmission over a standard dial-up phone line
    - **War Dialing**
        - Protect dial-up resources by using the callback feature
    - **Public Branch Exchange (PBX)**
        - Internal phone system used in large organizations
    - **Voice Over Internet Protocol (VoIP)**
        - Digital phone service provided by software or hardware devices over a data network
    - **Quality of Service (QoS)**

Perimeter Security

- **Perimeter Security**
  - **Perimeter Security**
    - Security devices focused on the boundary between the LAN and the WAN in your organization's network
    - Perimeter security relies on several different devices

- **Firewalls**
  - **Firewalls screen traffic between two portions of a network**
    - Software
    - Hardware
    - Embedded
  - **Packet Filtering**
    - Inspects each packet passing through the firewall and accepts or rejects it based on the rules
    - Stateless Packet Filtering
    - Stateful packet filtering tracks the requests leaving the network
  - **NAT Filtering**
    - Filters traffic based upon the ports being utilized and type of connection (TCP or UDP)
  - **Application-layer gateway conducts an in-depth inspection based upon the application being used**
  - **Circuit-Level gateway**
    - Operates at the session layer and only inspects the traffic during the establishment of the initial session over TCP or UDP
  - **MAC Filtering**
  - **Explicit Allow**
    - Traffic is allowed to enter or leave the network because there is an ACL rule that specifically allows it
    - Example: allow TCP 10.0.0.2 any port 80
  - **Explicit Deny**
    - Traffic is denied the ability to enter or leave the network because there is an ACL rule that specifically denies it
    - Example: deny TCP any any port 23
  - **Implicit Deny**
    - Traffic is denied the ability to enter or leave the network because there is no specific rule that allows it
    - Example: deny TCP any any port any
  - **Most operate at Layer 3 (blocking IP addresses) and Layer 4 (blocking ports)**

- **Web Application Firewall**
  - Firewall installed to protect your server by inspecting traffic being sent to a web application
  - A WAF can prevent a XSS or SQL injection

- **Proxy Server**
  - **Proxy Server**
    - A device that acts as a middle man between a device and a remote server
    - IP Proxy
      - IP Proxy is used to secure a network by keeping its machines anonymous during web browsing
    - Caching Proxy
      - Attempts to serve client requests by delivering content from itself without actually contacting the remote server
      - Disable Proxy Auto-Configuration (PAC) files for security
    - Internet Content Filter
      - Used in organizations to prevent users from accessing prohibited websites and other content
    - Web Security Gateway
      - A go-between device that scans for viruses, filters unwanted content, and performs data loss prevention functions

- **Honeypots and Honeynets**
  - **Honeypots and honeynets are used to attract and trap potential attackers**
  - **Honeypot**
    - A single computer (or file, group of files, or IP range) that might be attractive to an attacker
  - **Honeynet**
    - A group of computers, servers, or networks used to attract an attacker
  - **Honeypots are normally used in security research**

- **Data Loss Prevention**
  - **Data Loss Prevention**
    - Systems designed to protect data by conducting content inspection of data being sent out of the network
    - Also called Information Leak Protection (ILP) or Extrusion Prevention Systems (EPS)
    - DLP is used to ensure your private data remains secure

- **NIDS vs NIPS**
  - **Network Intrusion Detection Systems**
    - Attempts to detect, log, and alert on malicious network activities
    - NIDS use promiscuous mode to see all network traffic on a segment
  - **Network Intrusion Prevention Systems**
    - Attempts to remove, detain, or redirect malicious traffic
    - NIPS should be installed in-line of the network traffic flow
    - Should a NIPS fail open or fail shut?
    - NIPS can also perform functions as a protocol analyzer

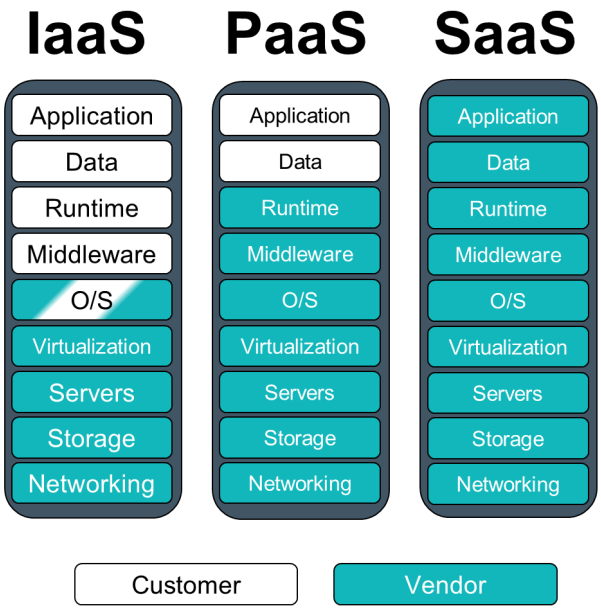
- **Unified Threat Management**
  - **Relying on a firewall is not enough**
  - **Unified Threat Management**
    - Combination of network security devices and technologies to provide more defense in depth within a single device
    - UTM may include a firewall, NIDS/NIPS, content filter, anti-malware, DLP, and VPN
    - UTM is also known as a Next Generation Firewall (NGFW)

Cloud Security

- **Cloud Computing**
  - **Cloud Computing**
    - A way of offering on-demand services that extend the traditional capabilities of a computer or network
    - Cloud computing relies on virtualization to gain efficiencies and cost savings
  - **Hyperconvergence allows providers to fully integrate the storage, network, and servers**
  - **Virtual Desktop Infrastructure (VDI)**
    - VDI allows a cloud provider to offer a full desktop operating system to an end user from a centralized server
  - **Secure Enclaves and Secure Volumes**

- **Cloud Types**
  - **Public Cloud**
    - A service provider makes resources available to the end users over the Internet
  - **Private Cloud**
    - A company creates its own cloud environment that only it can utilize as an internal enterprise resource
    - A private cloud should be chosen when security is more important than cost
  - **Hybrid**
  - **Community Cloud**
    - Resources and costs are shared among several different organizations who have common service needs

- **As a Service**
  - **Software as a Service (SaaS)**
    - Provides all the hardware, operating system, software, and applications needed for a complete service to be delivered
  - **Infrastructure as a Service (IaaS)**
    - Provides all the hardware, operating system, and backend software needed in order to develop your own software or service
  - **Platform as a Service (PaaS)**
    - Provides your organization with the hardware and software needed for a specific service to operate



- **Security as a Service (SECaaS)**
  - Provides your organization with various types of security services without the need to maintain a cybersecurity staff
  - Anti-malware solutions were one of the first SECaaS products
- **Some solutions may not scan all the files on your system**
- **Cloud-based vulnerability scans can better provide the attacker's perspective**
- **Your vulnerability data may be stored on the cloud provider's server**
- **Sandboxing**
  - Utilizes separate virtual networks to allow security professionals to test suspicious or malicious files
- **Data Loss Prevention (DLP)**
- **Continuous Monitoring**
- **Access Control**
- **Identity Management**
- **Business Continuity**
- **Disaster Recovery**

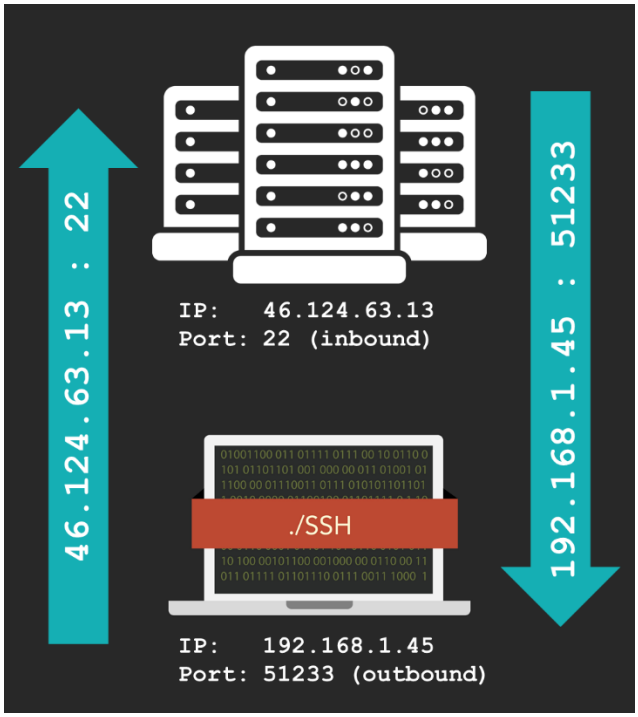
- **Cloud Security**
  - **Collocated data can become a security risk**
  - **Configure, manage, and audit user access to virtualized servers**
  - **Utilizing the cloud securely requires good security policies**
  - **Data remnants may be left behind after deprovisioning**

- **Defending Servers**
  - **File Servers**
    - Servers are used to store, transfer, migrate, synchronize, and archive files for your organization
  - **Email servers are a frequent target of attacks for the data they hold**
  - **Web servers should be placed in your DMZ**
  - **FTP Server**
    - A specialized type of file server that is used to host files for distribution across the web
    - FTP servers should be configured to require TLS connections
  - **Domain Controller**
    - A server that acts as a central repository of all the user accounts and their associated passwords for the network
  - **Active Directory is targeted for privileged escalation and lateral movement**

Network Attacks

- **Network Attacks**
  - **Denial of Service**
  - **Spoofing**
  - **Hijacking**
  - **Replay**
  - **Transitive Attacks**
  - **DNS attacks**
  - **ARP Poisoning**
  - **Ports and protocols will be tested on the Security+ exam**

- **Ports and Protocols**
  - **Port**
    - A logical communication endpoint that exists on a computer or server
  - **Inbound Port**
    - A logical communication opening on a server that is listening for a connection from a client
  - **Outbound Port**
    - A logical communication opening created on a client in order to call out to a server that is listening for a connection



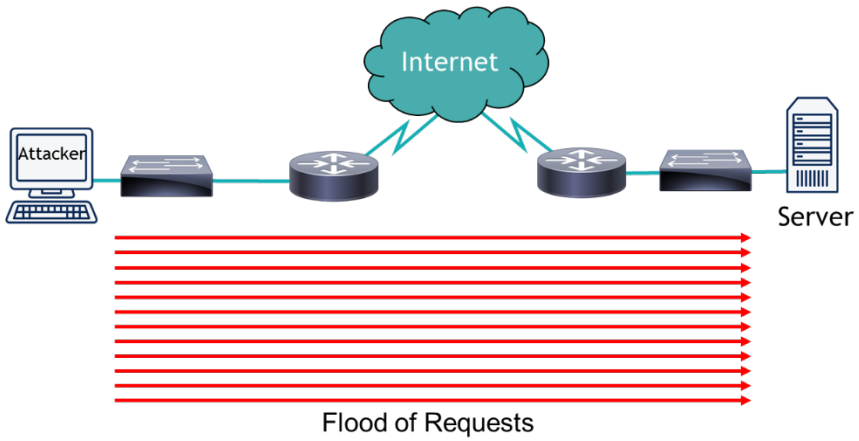
- **Ports can be any number between 0 and 65,535**
- **Well-Known Ports**
  - Ports 0 to 1023 are considered well-known and are assigned by the Internet Assigned Numbers Authority (IANA)
- **Registered Ports**
  - Ports 1024 to 49,151 are considered registered and are usually assigned to proprietary protocols
- **Dynamic or Private Ports**
  - Ports 49,152 to 65,535 can be used by any application without being registered with IANA

- **Memorization of Ports**
  - **65,536 ports are available for use**

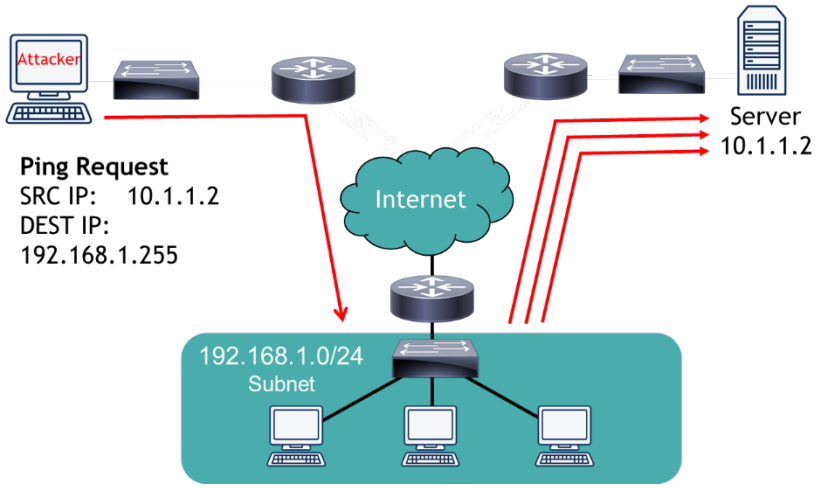
21 TCP	FTP	File Transfer Protocol is used to transfer files from host to host
22 TCP/UDP	SSH, SCP, SFTP	Secure Shell is used to remotely administer network devices and systems. SCP is used for secure copy and SFTP for secure FTP.
23 TCP/UDP	Telnet	Unencrypted method to remotely administer network devices (should not be used)
25 TCP	SMTP	Simple Mail Transfer Protocol is used to send email over the Internet
53 TCP/UDP	DNS	Domain Name Service is used to resolve hostnames to IPs and IPs to hostnames
69 UDP	TFTP	Trivial FTP is used as a simplified version of FTP to put a file on a remote host, or get a file from a remote host
80 TCP	HTTP	Hyper Text Transfer Protocol is used to transmit web page data to a client for unsecured web browsing
88 TCP/UDP	Kerberos	Used for network authentication using a system of tickets within a Windows domain
110 TCP	POP3	Post Office Protocol v3 is used to receive email from a mail server
119 TCP	NNTP	Network News Transfer Protocol is used to transport Usenet articles
135 TCP/UDP	RPC/DCOM-scm	Remote Procedure Call is used to located DCOM ports request a service from a program on another computer on the network
137-139 TCP/UDP	NetBIOS	NetBIOS is used to conduct name querying, sending of data, and other functions over a NetBIOS connection
143 TCP	IMAP	Internet Message Access Protocol is used to receive email from a mail server with more features than POP3
161 UDP	SNMP	Simple Network Management Protocol is used to remotely monitor network devices
162 TCP/UDP	SNMPTRAP	Used to send Trap and InformRequests to the SNMP Manager on a network
389 TCP/UDP	LDAP	Lightweight Directory Access Protocol is used to maintain directories of users and other objects
443 TCP	HTTPS	Hyper Text Transfer Protocol Secure is used to transmit web page data to a client over an SSL/TLS-encrypted connection
445 TCP	SMB	Server Message Block is used to provide shared access to files and other resources on a network
465/587 TCP	SMTP with SSL/TLS	Simple Mail Transfer Protocol used to send email over the Internet with an SSL and TLS secured connection
514 UDP	Syslog	Syslog is used to conduct computer message logging, especially for routers and firewall logs
636 TCP/UDP	LDAP SSL/TLS	LDAP is used to maintain directories of users and other objects over an encrypted SSL/TLS connection
860 TCP	iSCSI	iSCSI is used for linking data storage facilities over IP
989/990 TCP	FTPS	File Transfer Protocol Secure is used to transfer files from host to host over an encrypted connection
993 TCP	IMAP4 with SSL/TLS	Internet Message Access Protocol is used to receive email from a mail server over an SSL/TLS-encrypted connection
995 TCP	POP3 (SSL/TLS)	Post Office Protocol v3 is used to receive email from a mail server using an SSL/TLS-encrypted connection
1433 TCP	Ms-sql-s	Microsoft SQL server is used to receive SQL database queries from clients
1645/1646 UDP	RADIUS (alternative)	Remote Authentication Dial-In User Service is used for authentication and authorization (1645) and accounting (1646)
1701 UDP	L2TP	Layer 2 Tunnel Protocol is used as an underlying VPN protocol but has no inherent security
1723 TCP/UDP	PPTP	Point-to-Point Tunneling Protocol is an underlying VPN protocol with built-in security
1812/1813 UDP	RADIUS	Remote Authentication Dial-In User Service is used for authentication and authorization (1812) and accounting (1813)
3225 TCP/UDP	FCIP	Fibre Channel IP is used to encapsulate Fibre Channel frames within TCP/IP packets
3260 TCP	iSCSI Target	iSCSI Target is as the listening port for iSCSI-targeted devices when linking data storage facilities over IP
3389 TCP/UDP	RDP	Remote Desktop Protocol is used to remotely view and control other Windows systems via a Graphical User Interface
3868 TCP	Diameter	A more advanced AAA protocol that is a replacement for RADIUS
6514 TCP	Syslog over TLS	It is used to conduct computer message logging, especially for routers and firewall logs, over a TLS-encrypted connection

- **Unnecessary Ports**
  - **65,536 ports available**
  - **35 ports to memorize**
  - **Unnecessary Port**
    - Any port that is associated with a service or function that is non-essential to the operation of your computer or network
  - **Any open port represents a possible vulnerability that might be exposed**
  - **Inbound Port**
    - A logical communication opening on a server that is listening for a connection from a client
  - **C:\ net stop *service***
  - **# sudo stop *service***

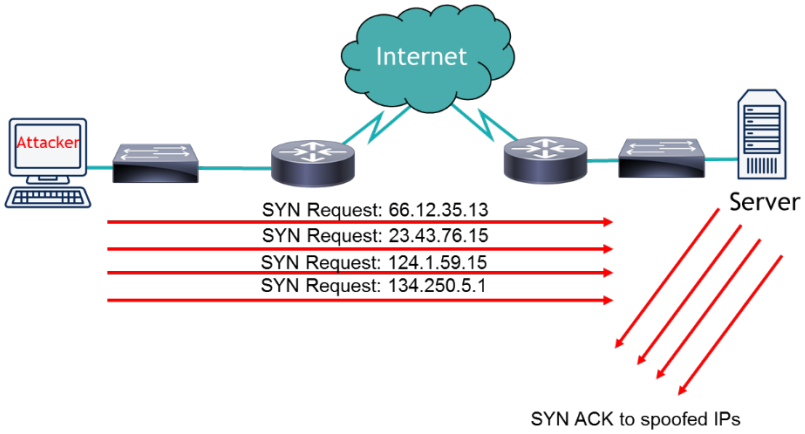
- **Denial of Service**
  - **Denial of Service (DoS)**
    - Term used to describe many different types of attacks which attempt to make a computer or server's resources unavailable
      - Flood Attacks
      - Ping of Death
      - Teardrop Attack
      - Permanent DoS
      - Fork Bomb
  - **Flood Attack**
    - A specialized type of DoS which attempts to send more packets to a single server or host than they can handle



- **Ping Flood**
  - An attacker attempts to flood the server by sending too many ICMP echo request packets (which are known as pings)
- **Smurf Attack**
  - Attacker sends a ping to subnet broadcast address and devices reply to spoofed IP (victim server), using up bandwidth and processing



- **Fraggle Attack**
  - Attacker sends a UDP echo packet to port 7 (ECHO) and port 19 (CHARGEN) to flood a server with UDP packets
- **SYN Flood**
  - Variant on a Denial of Service (DOS) attack where attacker initiates multiple TCP sessions but never completes the 3-way handshake



  - Flood guards, time outs, and an IPS can prevent SYN Floods

  - **XMAS Attack**
    - A specialized network scan that sets the FIN, PSH, and URG flags set and can cause a device to crash or reboot
  - **Ping of Death**
    - An attack that sends an oversized and malformed packet to another computer or server
  - **Teardrop Attack**
    - Attack that breaks apart packets into IP fragments, modifies them with overlapping and oversized payloads, and sends them to a victim machine
  - **Permanent Denial of Service**
    - Attack which exploits a security flaw to permanently break a networking device by reflashing its firmware
  - **Fork Bomb**
    - Attack that creates a large number of processes to use up the available processing power of a computer

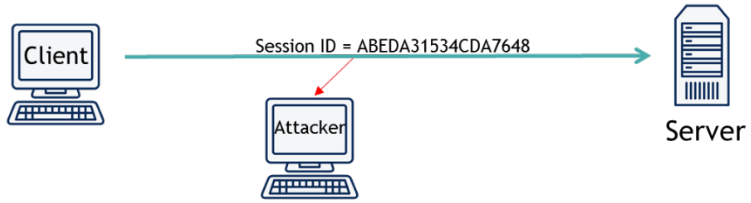
- **DDoS**
  - **Distributed Denial of Service (DDoS)**
    - A group of compromised systems attack simultaneously a single target to create a Denial of Service (DOS)
  - **DNS Amplification**
    - Attack which relies on the large amount of DNS information that is sent in response to a spoofed query on behalf of the victimized server

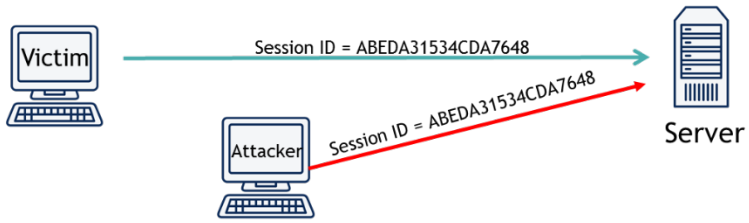
- **Stopping a DDoS**
  - **GitHub suffered a 1.35 Tbps DDoS**
  - **Blackholing or Sinkholing**
    - Identifies any attacking IP addresses and routes all their traffic to a non-existent server through the null interface
  - **An IPS can prevent a small-scale DDoS**
  - **Specialized security services cloud providers can stop DDoS attacks**

- **Spoofing**
  - **Spoofing**
    - Occurs when an attacker masquerades as another person by falsifying their identity
    - Anything that uniquely identifies a user or system can be spoofed
    - Proper authentication is used to detect and prevent spoofing

- **Hijacking**

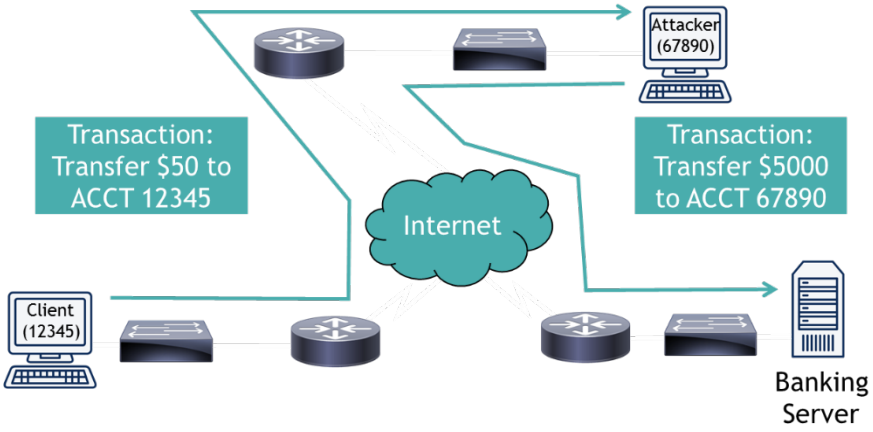
- **Hijacking**
  - Exploitation of a computer session in an attempt to gain unauthorized access to data, services, or other resources on a computer or server
  - Session theft
  - TCP/IP hijacking
  - Blind hijacking
  - Clickjacking
  - Man-in-the-Middle
  - Man-in-the-Browser
  - Watering hole
  - Cross-site scripting
- **Session Theft**
  - Attacker guesses the session ID for a web session, enabling them to take over the already authorized session of the client





- **TCP/IP Hijacking**
  - Occurs when an attacker takes over a TCP session between two computers without the need of a cookie or other host access
- **Blind Hijacking**
  - Occurs when an attacker blindly injects data into the communication stream without being able to see if it is successful or not
- **Clickjacking**
  - Attack that uses multiple transparent layers to trick a user into clicking on a button or link on a page when they were intending to click on the actual page
- **Man-in-the-Middle (MITM)**

- Attack that causes data to flow through the attacker's computer where they can intercept or manipulate the data



  - **Man-in-the-Browser (MITB)**
    - Occurs when a Trojan infects a vulnerable web browser and modifies the web pages or transactions being done within the browser
  - **Watering Hole**
    - Occurs when malware is placed on a website that the attacker knows his potential victims will access

- **Replay Attack**
  - **Replay Attack**
    - Network-based attack where a valid data transmission is fraudulently or malicious rebroadcast, repeated, or delayed
    - Multi-factor authentication can help prevent successful replay attacks

- **Transitive Attacks**
  - **Transitive Attacks aren't really an attack but more of a conceptual method**

A = B = C

Transitive Property

  - **When security is sacrificed in favor of more efficient operations, additional risk exists**

- **DNS Attacks**

- **DNS Poisoning**
  - Occurs when the name resolution information is modified in the DNS server's cache
  - If the cache is poisoned, then the user can be redirected to a malicious website
- **Unauthorized Zone Transfer**
  - Occurs when an attacker requests replication of the DNS information to their systems for use in planning future attacks
- **Altered Hosts File**
  - Occurs when an attacker modifies the host file to have the client bypass the DNS server and redirects them to an incorrect or malicious website
  - Windows stores the hosts file in the following directory:

    \%systemroot%\system 32\drivers\etc
- **Pharming**
  - Occurs when an attacker redirects one website's traffic to another website that is bogus or malicious
- **Domain Name Kiting**
  - Attack that exploits a process in the registration process for a domain name that keeps the domain name in limbo and cannot be registered by an authenticated buyer

- **ARP Poisoning**
  - **ARP Poisoning**
    - Attack that exploits the IP address to MAC resolution in a network to steal, modify, or redirect frames within the local area network
    - Allows an attacker to essentially take over any sessions within the LAN
    - ARP Poisoning is prevented by VLAN segmentation and DHCP snooping

Securing Networks

- **Securing Networks**
  - **Wired and wireless networks are vulnerable to attacks**

- **Securing Network Devices**
  - **Network devices include switches, routers, firewalls, and more**
  - **Default Accounts**
    - A user or administrator-level account that is installed on a device by the manufacturer during production
  - **Weak Passwords**
    - A password should be long, strong, and complex. This should require at least 14 characters with a mix of uppercase, lowercase, numbers, and special characters
      - password
      - PaSSworD
      - Pa55w0rd
      - P@$5w0rd
  - **Privilege Escalation**
    - Occurs when a user is able to gain the rights of another user or administrator
    - Vertical Privilege Escalation
    - Horizontal Privilege Escalation
  - **Backdoor**
    - A way of bypassing normal authentication in a system
  - **An IPS, proper firewall configs, network segmentation, and firmware updates are the keys to having network security**

- **Securing Network Media**
  - **Network Media**
    - Copper, fiber optic, and coaxial cabling used as the connectivity method in a wired network
  - **Electromagnetic Interference (EMI)**
    - A disturbance that can affect electrical circuits, devices, and cables due to radiation or electromagnetic conduction
    - EMI can be caused by TVs, microwaves, cordless phones, motors, and other devices
    - Shielding the cables (STP) or the source can minimize EMI

- **Radio Frequency Interference (RFI)**
  - A disturbance that can affect electrical circuits, devices, and cables due to AM/FM transmissions or cell towers
  - RFI causes more problems for wireless networks
- **Crosstalk**
  - Occurs when a signal transmitted on one copper wire creates an undesired effect on another wire
  - UTP is commonly used more often than STP
- **Data Emanation**
  - The electromagnetic field generated by a network cable or device when transmitting
  - A Faraday cage can be installed to prevent a room from emanating
  - Split the wires of a twisted-pair connection
- **Protected Distribution System (PDS)**
  - Secured system of cable management to ensure that the wired network remains free from eavesdropping, tapping, data emanations, and other threats

- **Securing WiFi Devices**
  - **Service Set Identifier (SSID)**
    - Uniquely identifies the network and is the name of the WAP used by the clients
    - Disable the SSID broadcast in the exam
  - **Rogue Access Point**
    - An unauthorized WAP or Wireless Router that allows access to the secure network
  - **Evil Twin**
    - A rogue, counterfeit, and unauthorized WAP with the same SSID as your valid one

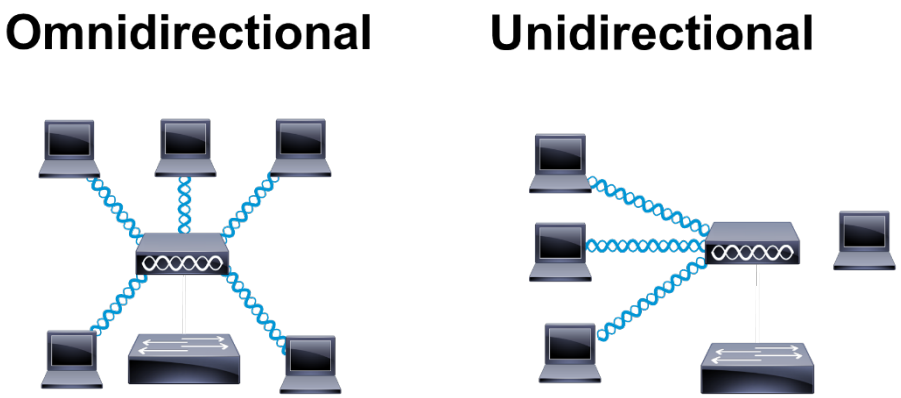
- **Wireless Encryption**
  - **Encryption of data in transit is paramount to security**
  - **Pre-Shared Key**
    - Same encryption key is used by the access point and the client
  - **Wired Equivalent Privacy**
    - Original 802.11 wireless security standard that claims to be as secure as a wired network
    - WEP's weakness is its 24-bit IV (Initialization Vector)
  - **WiFi Protected Access (WPA)**
    - Replacement for WEP which uses TKIP, Message Integrity Check (MIC), and RC4 encryption

        - WPA was flawed, so it was replaced by WPA2
    - **WiFi Protected Access version 2 (WPA2)**
        - 802.11i standard to provide better wireless security featuring AES with a 128-bit key, CCMP, and integrity checking
        - WPA2 is considered the best wireless encryption available

If you are asked about…	Look for the answer with…
Open	No security or protection provided
WEP	IV
WPA	TKIP and RC4
WPA2	CCMP and AES

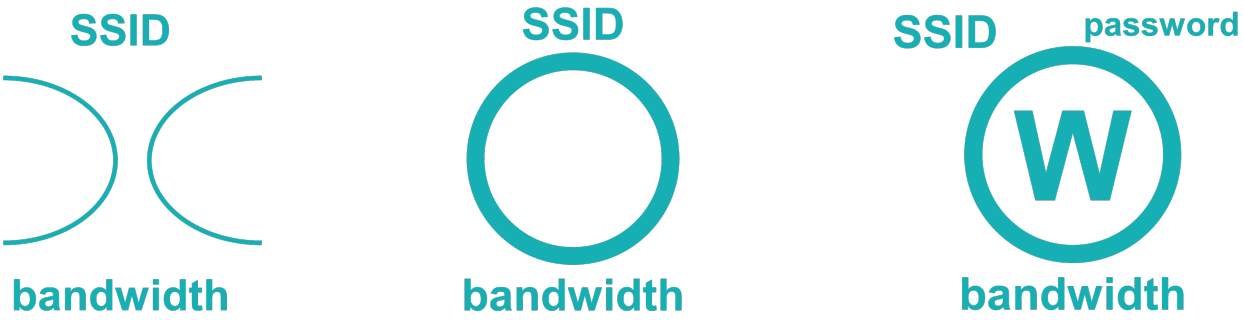
    - **If we make operations easier, then security is reduced**
    - **WiFi Protected Setup (WPS)**
        - Automated encryption setup for wireless networks at a push of a button, but is severely flawed and vulnerable
        - Always disable WPS
    - **Encryption and VPNs are always a good idea**

- **Wireless Access Points**
    - **Wireless security also relies upon proper WAP placement**



- **Wireless B, G, and N use a 2.4 GHz signal**
- **Wireless A, N, and AC use a 5.0 GHz signal**
- **2.4 GHz signals can travel further than 5 GHz**
- **Jamming**
  - Intentional radio frequency interference targeting your wireless network to cause a denial of service condition
  - Wireless site survey software and spectrum analyzers can help identify jamming and interference
- **AP Isolation**
  - Creates network segment for each client when it connects to prevent them from communicating with other clients on the network

- **Wireless Attacks**
  - **War Driving**
    - Act of searching for wireless networks by driving around until you find them
    - Attackers can use wireless survey or open source attack tools
  - **War Chalking**
    - Act of physically drawing symbols in public places to denote the open, closed, and protected networks in range



    - War chalking digitally is becoming more commonplace
  - **IV Attack**
    - Occurs when an attacker observes the operation of a cipher being used with several different keys and finds a mathematical relationship between those keys to determine the clear text data
    - This happened with WEP and makes it easy to crack
  - **WiFi Disassociation Attack**
    - Attack that targets an individual client connected to a network, forces it offline by deauthenticating it, and then captures the handshake when it reconnects

        - Used as part of an attack on WPA/WPA2
    - **Brute Force Attack**
        - Occurs when an attacker continually guesses a password until the correct one is found
        - Brute force will always find the password…eventually!

- **Other Wireless Technologies**
    - **Bluejacking**
        - Sending of unsolicited messages to Bluetooth-enabled devices such as mobile phones and tablets
    - **Bluesnarfing**
        - Unauthorized access of information from a wireless device through a Bluetooth connection
    - **Bluejacking sends information**
    - **Bluesnarfing takes information**
    - **Don't allow Bluetooth devices to use default PINs for pairing**
    - **Radio Frequency Identification (RFID)**
        - Devices that use a radio frequency signal to transmit identifying information about the device or token holder
        - RFID can operate from 10 cm to 200 meters depending on the device
    - **Near Field Communication (NFC)**
        - Allows two devices to transmit information when they are within close range through automated pairing and transmission
        - NFC devices are operated within 4 cm from each other

Physical Security

- **Physical Security**
  - **If an attacker can physically touch your devices, they can own your devices**

- **Surveillance**
  - **Closed Circuit TV (CCTV)**
  - **Pan Tilt Zoom (PTZ)**

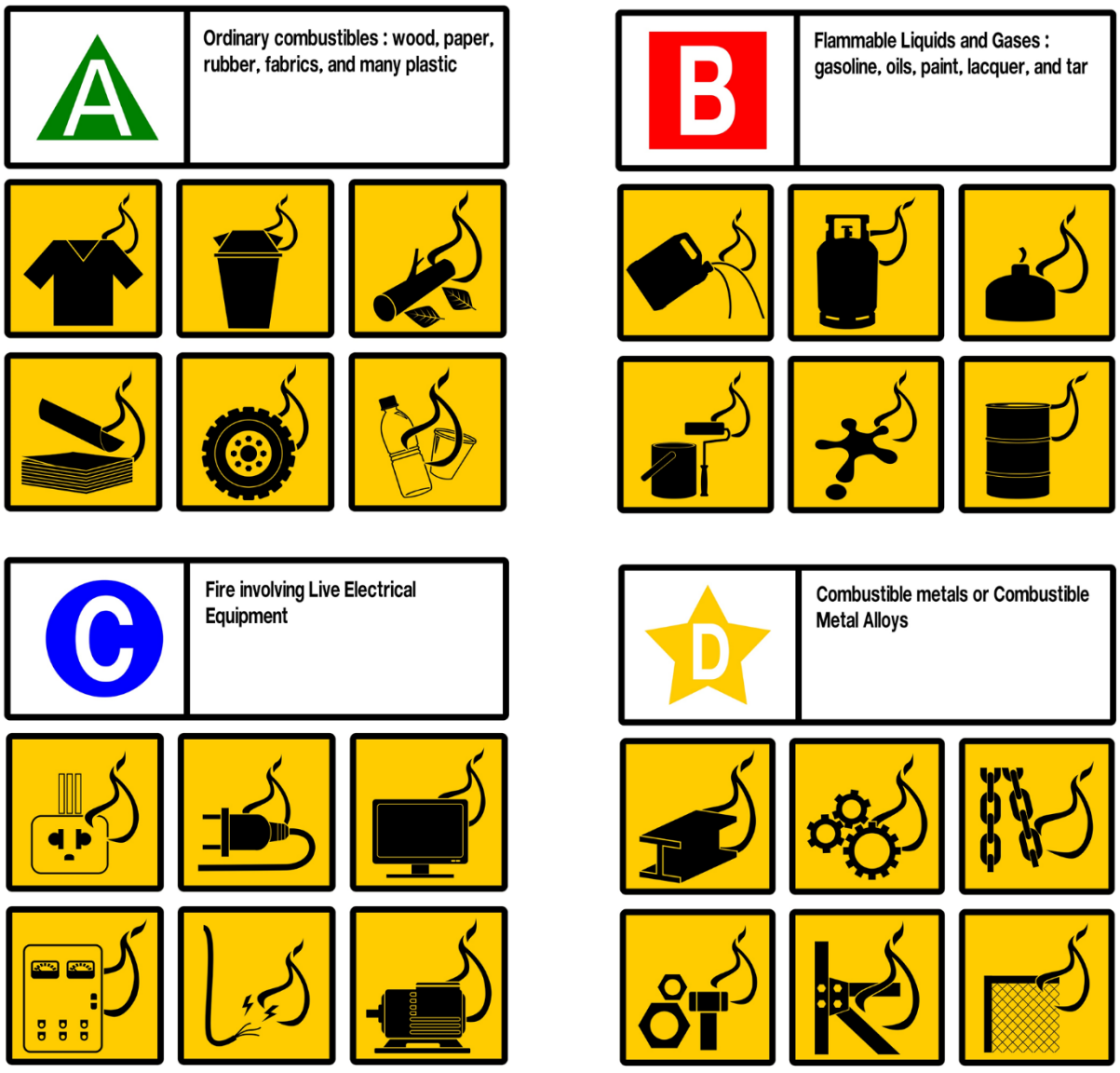
- **Door Locks**
  - **Door locks can use keys, pins, wireless signals, or biometrics**
  - **Mantrap**
    - Area between two doorways that holds people until they are identified and authenticated

- **Biometric Readers**
  - **Biometrics**
    - Relies on the physical characteristics of a person to identify them
    - Biometrics is considered “something you are”
  - **False Acceptance Rate (FAR)**
    - Rate that a system authenticates a user as authorized or valid when they should not have been granted access to the system
  - **False Rejection Rate (FRR)**
    - Rate that a system denies a user as authorized or valid when they should have been granted access to the system
  - **Crossover Error Rate (CER)**
    - An equal error rate (ERR) where the false acceptance rate and false rejection rate are equal
    - CER measures the effectiveness of a biometric system

Facilities Security

- **Facility Security**

- **Fire Suppression**
  - **Fire Suppression**
    - Process of controlling and/or extinguishing fires to protect an organization's employees, data, equipment, and buildings
  - **Handheld**
    - Class A, B, C, D, K



- **Sprinklers**
  - Wet Pipe Sprinkler System
    - Pipes are filled with water all the way to the sprinkler head and are just waiting for the bulb to be melted or broken
  - Dry Pipe Sprinkler System
    - Pipes are filled with pressurized air and only push water into the pipes when needed to combat the fire
  - A pre-action sprinkler system will activate when heat or smoke is detected
- **Special Hazard Protection**
  - Clean Agent System
    - Fire suppression system that relies upon gas (HALON, FM-200, or CO2) instead of water to extinguish a fire
- **If you hear a loud alarm in the server room… GET OUT!**

- **HVAC**
  - **HVAC**
    - Heating, Ventilation, and Air Conditioning
  - **Humidity should be kept around 40%**
  - **HVAC systems may be connected to ICS and SCADA networks**

- **Shielding**
  - **Shielded Twisted Pair (STP) adds a layer of shielding inside the cable**
  - **Faraday Cage**

        - Shielding installed around an entire room that prevents electromagnetic energy and radio frequencies from entering or leaving the room
    - **TEMPEST**
        - U.S. Government standards for the level of shielding required in a building to ensure emissions and interference cannot enter or exit the facility
        - TEMPEST facilities are also resistant to EMPs (electromagnetic pulses)

- **Vehicles**
    - **Controller Area Network (CAN)**
        - Connects all of a car's systems together in order for them to communicate effectively
    - **Air Gap**
        - A method of isolating an entity to effectively separate it from everything else
    - **Your security policies must consider the company's vehicles**

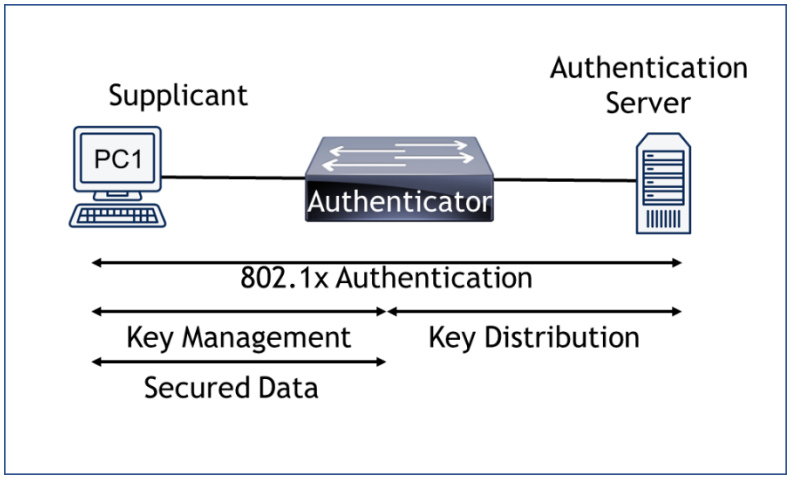
Authentication

- **Authentication**
  - **Multi-factor Authentication**
    - Use of two or more authentication factors to prove a user's identity
      - Knowledge
      - Ownership
      - Characteristic
      - Location
      - Action
    - Username and password are only considered single-factor authentication
  - **One-Time Passwords**
    - Time-based One Time Password (TOTP)
      - A password is computed from a shared secret and current time
    - HMAC-based One Time Password (HOTP)
      - A password is computed from a shared secret and is synchronized between the client and the server

- **Authentication Models**
  - **Context-aware Authentication**
    - Process to check the user's or system's attributed or characteristics prior to allowing it to connect
    - Restrict authentication based on the time of day or location
  - **Single Sign-On (SSO)**
    - A default user profile for each user is created and linked with all of the resources needed
    - Compromised SSO credentials cause a big breach in security
  - **Federated Identity Management (FIdM)**
    - A single identity is created for a user and shared with all of the organizations in a federation
    - Cross-Certification
      - Utilizes a web of trust between organizations where each one certifies others in the federation
    - Trusted Third-Party
      - Organizations are able to place their trust in a single third-party (also called the bridge model)
      - Trusted third-party model is more efficient than a cross certification or web of trust model
    - Security Assertion Markup Language (SAML)
      - Attestation model built upon XML used to share federated identity management information between systems

        - OpenID
            - An open standard and decentralized protocol that is used to authenticate users in a federated identity management system
            - User logs into an Identity Provider (IP) and uses their account at Relying Parties (RP)
            - OpenID is easier to implement than SAML
            - SAML is more efficient than OpenID

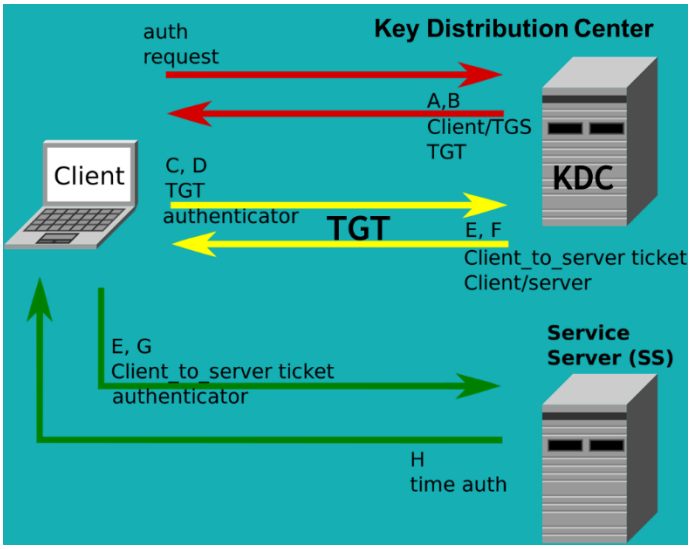
- **802.1x**
    - **802.1x**
        - Standardized framework used for port-based authentication on wired and wireless networks
        - RADIUS
        - TACACS+



        - 802.1x can prevent rogue devices
    - **Extensible Authentication Protocol (EAP)**
        - A framework of protocols that allows for numerous methods of authentication including passwords, digital certificates, and public key infrastructure
        - EAP-MD5 uses simple passwords for its challenge-authentication
        - EAP-TLS uses digital certificates for mutual authentication
        - EAP-TTLS uses a server-side digital certificate and a client-side password for mutual authentication

- **EAP-FAST**
  - Provides flexible authentication via secure tunneling (FAST) by using a protected access credential instead of a certificate for mutual authentication
- **Protected EAP (PEAP)**
  - Supports mutual authentication by using server certificates and Microsoft's Active Directory to authenticate a client's password
- **LEAP is proprietary to Cisco-based networks**

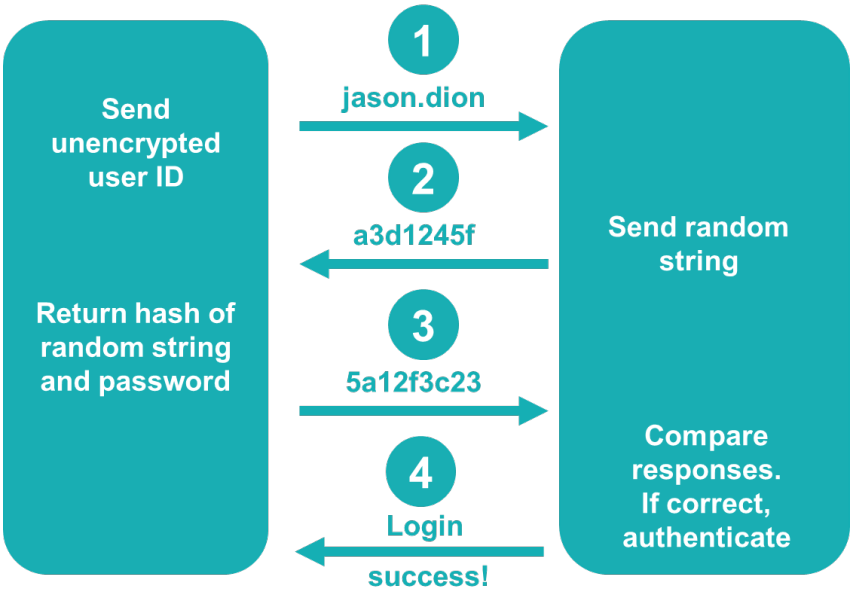
- **LDAP and Kerberos**
  - **Lightweight Directory Access Protocol (LDAP)**
    - A database used to centralize information about clients and objects on the network
    - Unencrypted
      - Port 389
    - Encrypted
      - Port 636
    - Active Directory is Microsoft's version
  - **Kerberos**
    - An authentication protocol used by Windows to provide for two-way (mutual) authentication using a system of tickets



    - Kerberos
      - Port 88
    - A domain controller can be a single point of failure for Kerberos

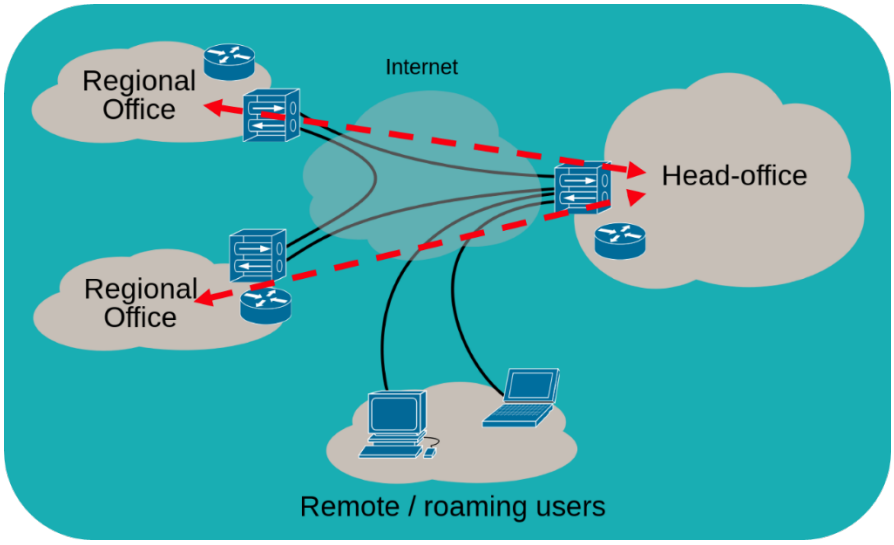
- **Remote Desktop Services**
  - **Remote Desktop Protocol (RDP)**
    - Microsoft's proprietary protocol that allows administrators and users to remotely connect to another computer via a GUI
    - RDP doesn't provide authentication natively
  - **Virtual Network Computing (VNC)**
    - Cross-platform version of the Remote Desktop Protocol for remote user GUI access
    - VNC requires a client, server, and protocol be configured
  - **RDP**
    - Port 3389
  - **VNC**
    - Port 5900

- **Remote Access Services**
  - **Password Authentication Protocol (PAP)**
    - Used to provide authentication but is not considered secure since it transmits the login credentials unencrypted (in the clear)
  - **Challenge Handshake Authentication Protocol (CHAP)**
    - Used to provide authentication by using the user's password to encrypt a challenge string of random numbers



    - Microsoft's version of CHAP is MS-CHAP
  - **PAP and CHAP used mostly with dial-up**

- **VPN**
  - **Virtual Private Network (VPN)**
    - Allows end users to create a tunnel over an untrusted network and connect remotely and securely back into the enterprise network
    - Client-to-Site VPN or Remote Access VPN



  - **VPN Concentrator**
    - Specialized hardware device that allows for hundreds of simultaneous VPN connections for remote workers
  - **Split Tunneling**
    - A remote worker's machine diverts internal traffic over the VPN but external traffic over their own internet connection
    - Prevent split tunneling through proper configuration and network segmentation

- **RADIUS and TACACS+**
  - **Remote Authentication Dial-In User Service (RADIUS)**
    - Provides centralized administration of dial-up, VPN, and wireless authentication services for 802.1x and the Extensible Authentication Protocol (EAP)
    - RADIUS operates at the application layer

AAA

**Authentication,
Authorization,
and Accounting**

Authentication	**Authentication**
Port 1812	**Port 1645**
Authorization	**Authorization**
Port 1813	**Port 1646**
(Standard Ports)	(Proprietary Variation)

- **Cisco's TACACS+ is a proprietary version of RADIUS**

TACACS+

Port 49 (TCP)

- **Authentication Summary**
  - **802.1x**
    - IEEE standard that defines Port-based Network Access Control (PNAC) and is a data link layer authentication technology used to connected devices to a wired or wireless LAN
  - **LDAP**
    - Application layer protocol for accessing and modifying directory services data (Active Directory uses it)
  - **Kerberos**
    - Authentication protocol used in Windows to identify clients to a sever using mutual authentication (Uses tickets)

- **Remote Access Services (RAS)**
  - Service that enables dial-up and VPN connections to occur from remote clients
- **Challenge Handshake Protocol (CHAP)**
  - Authentication scheme that is used in dial-up connections
- **RADIUS**
  - Centralization administration system for dial-up, VPN, and wireless authentication that uses either ports 1812/1813 (UDP) or 1645/1646 (UDP)
- **TACACS+**
  - Cisco's proprietary version of RADIUS that provides separate authentication and authorization functions over port 49 (TCP)

Access Control

- **Access Control**
  - **Access Control**
    - Methods used to secure data and information by verifying a user has permissions to read, write, delete, or otherwise modify it
  - **Access Control Models**
    - Discretionary Access Control (DAC)
      - The access control policy is determined by the owner
      - DAC is used commonly
      - 1. Every object in a system must have an owner
      - 2. Each owner determines access rights and permissions for each object
    - Mandatory Access Control (MAC)
      - An access control policy where the computer system determines the access control for an object
      - The owner chooses the permissions in DAC but in MAC, the computer does
      - MAC relies on security labels being assigned to every user (called a subject) and every file/folder/device or network connection (called an object)
      - Data labels create trust levels for all subjects and objects
      - To access something, you need to meet the minimum level and have a “need-to-know”
      - MAC is implemented through the Rule-based and the Lattice-based access control methods
    - Rule-based Access Control
      - Label-based access control that defines whether access should be granted or denied to objects by comparing the object label and the subject label
    - Lattice-based Access Control
      - Utilizes complex mathematics to create sets of objects and subjects to define how they interact
      - Mandatory Access Control is a feature in FreeBSD & SELinux
      - Only in high security systems due to its complex configuration
    - Role-Based Access Control (RBAC)
      - An access model that is controlled by the system (like MAC) but utilizes a set of permissions instead of a single data label to define the permission level

        - Power Users is a role-based permission
    - Attribute-Based Access Control (ABAC)
        - An access model that is dynamic and context-aware using IF-THEN statements
        - If Jason is in HR, then give him access to \\fileserver\HR

- **Best Practices**
    - **Best Practices**
        - The access control policy is determined by the owner
        - Best Practices for Access Control
    - **Implicit Deny**
        - All access to a resource should be denied by default and only be allowed when explicitly stated
    - **Least Privilege**
        - Users are only given the lowest level of access needed to perform their job functions
        - Does everyone in the company need to know employee salary data?
    - **Separation of Duties**
        - Requires more than one person to conduct a sensitive task or operation
        - Separation of duties can be implemented by a single user with a user and admin account
    - **Job Rotation**
        - Occurs when users are cycled through various jobs to learn the overall operations better, reduce their boredom, enhance their skill level, and most importantly, increase our security
        - Job rotation helps the employee become more well-rounded and learn new skills
        - Job rotation also helps the organization identify theft, fraud, and abuse of position

- **Users and Groups**
    - **Computers can have multiple users and groups**
        - 1. Right-click on an empty area in the Users folder of ADUC and select Create New User
        - 2. Create a new user within the Organizational Unit (OU) within Active Directory
    - **User Rights**
        - Permissions assigned to a given user
    - **Groups**
        - Collection of users based on common attributes (generally work roles)

- **Permissions in Windows**
  - Permissions are broken down into Read, Write, and Execute inside Linux
    - Full Control
    - Modify
    - Read & Execute
    - List Folder Contents
    - Read
    - Write
  - Permissions are assigned to Owners (U), Groups (G), and All Users (O or A)
- **chmod**
  - Program in Linux that is used to change the permissions or rights of a file or folder using a shorthand number system
- **R (Read) = 4**
  W (Write) = 2
  X (Execute) = 1
- **# chmod 760 filename**
  7 = Owner can RWX
  6 = Group can RW
  0 = All Users (no access)
- **777 allows everyone to Read, Write, and Execute**
- **Privilege Creep**
  - Occurs when a user gets additional permission over time as they rotate through different positions or roles
  - Privilege creep violates the principles of least privilege
- **User Access Recertification**
  - Process where each user's rights and permissions are revalidated to ensure they are correct
    - Hired
    - Fired
    - Promoted

- **Permissions**
  - **Permissions are inherited by default from the parent when a new folder is created**
  - **Any permissions added/removed from the parent folder will pass to the child by default too!**
  - **Propagation**
    - Occurs when permissions are passed to a subfolder from the parent through inheritance

- **Use Groups for roles and do not assign users directly to a folder's permissions**
- **Review Note: CompTIA A+**
- **If you copy a folder, then permissions are inherited from the parent folder it is copied into**
- **If you move a folder, then permissions are retained from its original permissions**

- **Usernames and Passwords**
  - **first.last@yourcompany.com**
  - **Strong Passwords**
    - Contain uppercase letters, lowercase letters, numbers, special characters, and at least 8 characters or more (preferably 14 or more)
    - 1. Always require the user to change the default password when the account is created
    - 2. Require that the password is changed frequently (every 90 days)
    - 3. Always change the default Administrator or Root password
    - 4. Disable the Guest account on your systems
    - 5. Enable CTRL+ALT+DEL for logging into the system
      - Turn this on in the Advanced tab of the User Accounts dialogue box
    - 6. Use good, strong policies in regards to your passwords

- **User Account Control**
  - **User Account Control (UAC)**
    - A security component in Windows that keeps every user in standard user mode instead of acting like an administrative user

      ** Only exception is the Administrator account **
    - 1. Eliminates unnecessary admin-level requests for Windows resources
    - 2. Reduces risk of malware using admin-level privileges to cause system issues
    - UAC can be disabled from the Control Panel

Risk Assessments

- **Risk Assessments**
  - **Risk Assessments**
    - A process used inside of risk management to identify how much risk exists in a given network or system
  - **Risk**
    - The probability that a threat will be realized
  - **Vulnerabilities**
    - Weaknesses in the design or implementation of a system
  - **Threat**
    - Any condition that could cause harm, loss, damage, or compromise to our information technology systems
    - Threats are external and beyond your control

    - What can we do about the threats we identified?
  - **Risk management is used to minimize the likelihood of a negative outcome from occurring**
    - Risk Avoidance
      - A strategy that requires stopping the activity that has risk or choosing a less risky alternative
    - Risk Transfer
      - A strategy that passes the risk to a third party
    - Risk Mitigation
      - A strategy that seeks to minimize the risk to an acceptable level
    - Risk Acceptance
      - A strategy that seeks to accept the current level of risk and the costs associated with it if the risk were realized

        - Residual Risk
            - The risk remaining after trying to avoid, transfer, or mitigate the risk
    - **Identify assets**
    - **Identify vulnerabilities**
    - **Identify threats**
    - **Identify the impact**

- **Qualitative Risk**
    - **Qualitative analysis uses intuition, experience, and other methods to assign a relative value to risk**
    - **Experience is critical in qualitative analysis**

- **Quantitative Risk**
    - **Quantitative analysis uses numerical and monetary values to calculate risk**
    - **Quantitative analysis can calculate a direct cost for each risk**
    - **Magnitude of Impact**
        - An estimation of the amount of damage that a negative risk might achieve
        - Single Loss Expectancy (SLE)
            - Cost associated with the realization of each individualized threat that occurs

Asset Value x Exposure Factor

SLE = AV x EF

SLE = $10,000 x 20%

SLE = $2,000

        - Annualized Rate of Occurrence (ARO)
            - Number of times per year that a threat is realized
        - Annualized Loss Expectancy (ALE)
            - Expected cost of a realized threat over a given year

ALE = SLE x ARO

ALE = SLE x ARO **ALE = SLE x ARO**

ALE = $2,000 x 3 **ALE = $2,000 x 0.5**

ALE = $6,000 **ALE = $1,000**

- **If it costs $200,000 to build a server room that never loses power, then it would take 33 years to recover the building costs instead of losing power 3x year!**
- **Hybrid approaches that combine quantitative and qualitative analysis are commonly used**

- **Methodologies**
  - **Security Assessments**
    - Verify that the organization's security posture is designed and configured properly to help thwart different types of attacks
    - Assessments might be required by contracts, regulations, or laws
    - Assessments may be active or passive
      - Active Assessments
        - Utilize more intrusive techniques like scanning, hands-on testing, and probing of the network to determine vulnerabilities
      - Passive Assessments
        - Utilize open source information, the passive collection and analysis of the network data, and other unobtrusive methods without making direct contact with the targeted systems
        - Passive techniques are limited in the amount of detail they find

- **Security Controls**
  - **Security Controls**
    - Methods implemented to mitigate a particular risk
  - **Security controls are categorized as physical, technical, or administrative**
    - Physical Controls
      - Any security measures that are designed to deter or prevent unauthorized access to sensitive information or the systems that contain it

        - Technical Controls
            - Safeguards and countermeasures used to avoid, detect, counteract, or minimize security risks to our systems and information
        - Administrative Controls
            - Focused on changing the behavior of people instead of removing the actual risk involved
    - **NIST categories are management, operational, and technical**
        - Management Controls
            - Security controls that are focused on decision-making and the management of risk
        - Operational Controls
            - Focused on the things done by people
        - Technical Controls
            - Logical controls that are put into a system to help secure it
    - **Preventative, Detective, or Corrective controls**
        - Preventative Controls
            - Security controls that are installed before an event happens and are designed to prevent something from occurring
        - Detective Controls
            - Used during the event to find out whether something bad might be happening
        - Corrective Controls
            - Used after an event occurs
    - **A single control can be categorized into multiple types or categories**
    - **Compensating Control**
        - Used whenever you can't meet the requirement for a normal control
        - Residual risk not covered by a compensating control is an accepted risk

- **Vulnerability Management**
    - **Vulnerability Assessment**
        - Seeks to identify any issues in a network, application, database, or other systems prior to it being used that might compromise the system
        - Defines, identifies, and classifies vulnerabilities within a system
    - **Vulnerability Management**
        - Practice of finding and mitigating the vulnerabilities in computers and networks
    - **These 3 questions can help to scope your assessments**
        - 1. What is the value of the information?
        - 2. What is the threat your system is facing?

        - 3. What is the mitigation that could be deployed?
    - **Nessus, Qualysguard, and AlienVault are used for vulnerability assessments**
        - 1. Define the desired state of security
        - 2. Create a baseline
        - 3. Prioritize the vulnerabilities
        - 4. Mitigate vulnerabilities
        - 5. Monitor the network and systems
    - **Scan, Patch, Scan, …**

- **Penetration Testing**
    - **Penetration tests look at a network's vulnerabilities from the outside**
    - **Metasploit and CANVAS are commonly used**
    - **Get permission and document info**
    - **Conduct reconnaissance**
    - **Enumerate the targets**
    - **Exploit the targets**
    - **Document the results**
    - **Vulnerability Assessment**
        - Seeks to identify any issues in a network, application, database, or other systems prior to it being used that might compromise the system
    - **Pivot**
        - Occurs when an attacker moves onto another workstation or user account
    - **Persistence**
        - Ability of an attacker to maintain a foothold inside the compromised network
    - **A pentester can also simulate an insider threat**

- **OVAL**
    - **Open Vulnerability and Assessment Language (OVAL)**
        - A standard designed to regulate the transfer of secure public information across networks and the Internet utilizing any security tools and services available
        - OVAL is comprised of a language and an interpreter
    - **OVAL Language**
        - An XML schema used to define and describe the information being created by OVAL to be shared among the various programs and tools
    - **OVAL Interpreter**
        - A reference developed to ensure the information passed around by these programs complies with the OVAL schemas and definitions used by the OVAL language

- **Vulnerability Assessments**
  - **Vulnerability Assessment**
    - Baselining of the network to assess the current security state of computers, servers, network devices, and the entire network in general
    - Network Mapping
      - Discovery and documentation of physical and logical connectivity that exists in the network
      - Commercial and free network mapping software is available
    - Vulnerability Scanning
      - A technique that identifies threats on the network without exploiting them
      - Banner Grabbing
        - A technique used to gain information about servers and inventory the systems or services
      - Nessus and Qualysguard are commercial vulnerability scanners
    - Network Sniffing
      - The process of finding and investigating other computers on the network by analyzing the network traffic or capturing the packets being sent
      - Network sniffer, packet sniffing, and protocol analyzer can all conduct packet capture
      - Protocol Analyzer
        - Software tool that allows for the capture, reassembly, and analysis of packets from the network
    - Password Analysis
      - A tool used to test the strength of your passwords to ensure your password policies
        are being followed
      - **Password Cracker**
        - Uses comparative analysis
          to break passwords and systematically continues guessing until the password
          is determined
        - Cain & Abel and John the Ripper
      - **Password Guessing**
        - Occurs when a weak password is simply figured out by a person
      - **Dictionary Attack**
        - Method where a program attempts to guess the password by using a list of possible passwords

- **Brute-Force Attack**
  - Method where a program attempts to try every possible combination until it
    cracks the password
- Increasing complexity exponentially increases the time required to brute-force a password
- **Cryptanalysis Attack**
  - Comparing a precomputed encrypted password to a value in a lookup table
- **Rainbow Table**
  - List of precomputed valued used to more quickly break a password since values don't have to be calculated for each password being guessed
- **Rubber Hose Attack**
  - Attempt to crack a password by threating or causing a person physical harm in order to make them tell you the password

Monitoring and Auditing

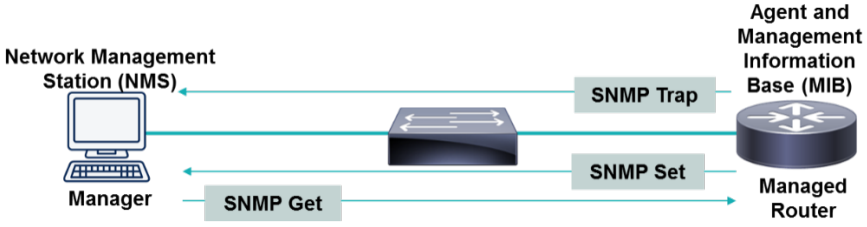
- **Monitoring Types**
  - **Signature-based**
    - Network traffic is analyzed for predetermined attack patterns
  - **Anomaly-based**
    - A baseline is established and any network traffic that is outside of the baseline is evaluated
  - **Behavior-based**
    - Activity is evaluated based on the previous behavior of applications, executables, and the operating system in comparison to the current activity of the system
  - **Methods may be combined into a hybrid approach in some IDS/IPS systems**

- **Performance Baselining**
  - **Baselining**
    - Process of measuring changes in networking, hardware, software, and applications
  - **Baseline Reporting**
    - Documenting and reporting on the changes in a baseline
  - **Security Posture**

        - Risk level to which a system or other technology element is exposed
    - **Perfmon.exe is the Windows program for Performance Monitor**

- **Protocol Analyzers**
    - **Protocol analyzers are used to capture and analyze network traffic**
    - **Promiscuous Mode**
        - Network adapter is able to capture all of the packets on the network, regardless of the destination MAC address of the frames carrying them
    - **Non-promiscuous Mode**
        - Network adapter can only capture the packets directly addressed to itself
    - **To capture the most information, you need to be in promiscuous mode**
    - **Port Mirroring**
        - One or more switch ports are configured to forward all of their packets to another port on the switch
    - **If you cannot configure a SPAN port, then you can use a network tap**
        - Network Tap
            - A physical device that allows you to intercept the traffic between two points on the network

- **SNMP**
    - **Simple Network Management Protocol (SNMP)**
        - A TCP/IP protocol that aids in monitoring network-attached devices and computers
        - SNMP is incorporated into a network management and monitoring system
    - **Managed Devices**
        - Computers and other network-attached devices monitored through the use of agents by a network management system
    - **Agents**
        - Software that is loaded on a managed device to redirect information to the network management system
    - **Network Management System (NMS)**
        - Software running on one or more servers to control the monitoring of network-attached devices and computers



- **SNMP v1/v2 are insecure due to the use of community strings to access a device**
- **SNMP v3**
  - Version of SNMP that provides integrity, authentication, and encryption of the messages being sent over the network
- **Management should be conducted on an out-of-band network to increase security**

- **Auditing**
  - **Auditing**
    - A technical assessment conducted on applications, systems, or networks
    - Auditing is a detective control
      - Security logs
      - ACLs
      - User rights/permissions
      - Group policies (GPOs)
      - Vulnerability scans
      - Written organizational policies
      - Interviewing personnel
    - Software tools are also used to help conduct audits

- **Logging**
  - **Logs**
    - Data files that contain the accounting and audit trail for actions performed by a user on a computer or network
  - **Security, System, and Application logs should be audited on a Windows system**
    - Security Logs
      - Logs the events such as successful and unsuccessful user logins to the system
    - System Logs
      - Logs the events such as a system shutdown and driver failures
    - Application Logs
      - Logs the events for the operating system and third-party applications
  - **To consolidate all the logs into a single repository, you can use SYSLOG**
    - SYSLOG
      - A standardized format used for computer message logging that allows for the separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them

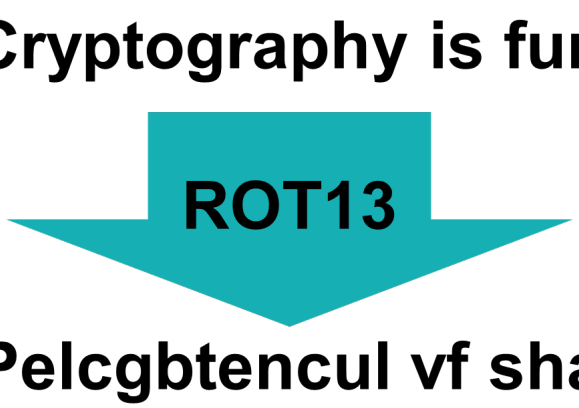
- SYSLOG uses port 514 over UDP

- **Log Files**
  - **Log files are important to your ability to reconstruct an event after it occurs**
  - **Log File Maintenance**
    - Actions taken to ensure the proper creation and storage of a log file, such as the proper configuration, saving, back up, security, and encryption of the log files
    - Log files should be saved to a different partition or an external server
  - **Overwrite Events**
    - When a maximum log size is reached, the system can begin overwriting the oldest events in the log files to make room
  - **Logs should be archived and backed up to ensure they are available when required**
  - **Write Once Read Many (WORM)**
    - Technology like a DVD-R that allows data to be written only once but read unlimited times

- **SIEM**
  - **Security Information and Event Management (SIEM)**
    - Combines security event management and security information management systems into one tool
  - **A SIEM performs data aggregation and correlation**
    - Data Aggregation
      - Combines data from various network devices, servers, and applications from across the enterprise network
    - Data Correlation
      - Automatically looks for common attributes of events across the monitored portions of the network
  - **SIEMs may also perform regulatory audits and forensic analysis functions**

Cryptography

- **Cryptography**
  - **Cryptography**
    - The practice and study of writing and solving codes in order to hide the true meaning of information
  - **Encryption**
    - Process of converting ordinary information (plaintext) into an unintelligible form (ciphertext)
    - Encryption protects data at rest, data in transit, or data in use
      - Data at Rest
        - Inactive data that is archived, such as data resident on a hard disk drive
      - Data in Transit
        - Data crossing the network or data that resides in a computer's memory
      - Data in Use
        - Data that is undergoing constant change



    - Encryption strength comes from the key, not the algorithm
        - Key
            - The essential piece of information that determines the output of a cipher

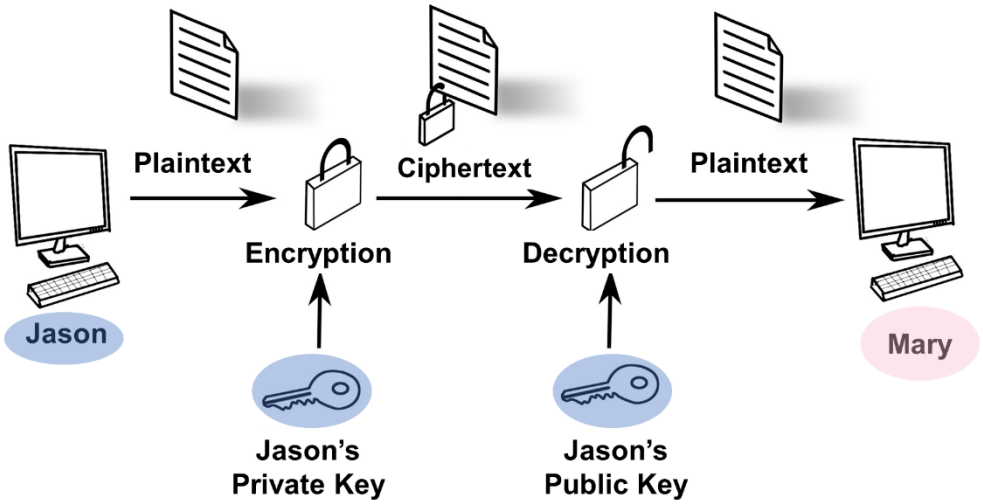
- **Symmetric vs Asymmetric**
    - **Symmetric Algorithm (Private Key)**
        - Encryption algorithm in which both the sender and the receiver must know the same secret using a privately-held key
        - Confidentiality can be assured with symmetric encryption
        - Key distribution can be challenging with symmetric encryption
        - Symmetric Algorithms
            - DES, 3DES, IDEA, AES, Blowfish, Twofish, RC4, RC5, RC6
    - **Asymmetric Encryption (Public Key)**
        - Encryption algorithm where different keys are used to encrypt and decrypt the data
        - Asymmetric Algorithms
            - Diffie-Hellman, RSA, and ECC
    - **Symmetric is 100-1000x faster than asymmetric**
    - **Hybrid Implementation**
        - Utilizes asymmetric encryption to securely transfer a private key that can then be used with symmetric encryption
    - **Stream Cipher**
        - Utilizes a keystream generator to encrypt data bit by bit using a mathematical XOR function to create the ciphertext
    - **Block Cipher**
        - Breaks the input into fixed-length blocks of data and performs the encryption on each block
        - Block ciphers are easier to implement through a software solution

- **Symmetric Algorithms**
  - **Symmetric Algorithms**
    - DES, 3DES, IDEA, AES, Blowfish, Twofish, RC4, RC5, RC6
  - **Data Encryption Standard (DES)**
    - Encryption algorithm which breaks the input into 64-bit blocks and uses transposition and substitution to create ciphertext using an effective key strength of only 56-bits
    - DES used to be the standard for encryption
  - **Triple DES (3DES)**
    - Encryption algorithm which uses three separate symmetric keys to encrypt, decrypt, then encrypt the plaintext into ciphertext in order to increase the strength of DES
  - **International Data Encryption Algorithm (IDEA)**
    - Symmetric block cipher which uses 64-bit blocks to encrypt plaintext into ciphertext
  - **Advanced Encryption Standard (AES)**
    - Symmetric block cipher that uses 128-bit, 192-bit, or 256-bit blocks and a matching encryption key size to encrypt plaintext into ciphertext
    - AES is the standard for encrypting sensitive U.S. Government data
  - **Blowfish**
    - Symmetric block cipher that uses 64-bit blocks and a variable length encryption key to encrypt plaintext into ciphertext
  - **Twofish**
    - Symmetric block cipher that replaced blowfish and uses 128-bit blocks and a 128-bit, 192-bit, or 256-bit encryption key to encrypt plaintext into ciphertext
  - **Rivest Cipher (RC4)**
    - Symmetric stream cipher using a variable key size from 40-bits to 2048-bits that is used in SSL and WEP
  - **Rivest Cipher (RC5)**
    - Symmetric block cipher with a key size up to 2048-bits
  - **Rivest Cipher (RC6)**
    - Symmetric block cipher that was introduced as a replacement for DES but AES was chosen instead
  - **Exam Tips**
    - RC4 is the only stream cipher covered

- **Public Key Cryptography**
  - **Asymmetric algorithms are also known as Public Key Cryptography**
    - Confidentiality

- Integrity
- Authentication
- Non-repudiation

Using Public Key Cryptography to ensure non-repudiation



- Organizations want both confidentiality and non-repudiation

  - **Digital Signature**
    - A hash digest of a message encrypted with the sender's private key to let the recipient know the document was created and sent by the person claiming to have sent it
  - **PKI**
    - Public Key Infrastructure
  - **Exam Tips**
    - Asymmetric encryption is also known as public key cryptography
    - Two keys are used in public key cryptography

- **Asymmetric Algorithms**
  - **Asymmetric Algorithms**
    - Diffie-Hellman, RSA, and ECC
  - **Diffie-Hellman (DH)**
    - Used to conduct key exchanges and secure key distribution over an unsecure network
    - Diffie-Hellman is used for the establishment of a VPN tunnel using IPSec
  - **RSA (Rivest, Shamir, and Adleman)**
    - Asymmetric algorithm that relies on the mathematical difficulty of factoring large prime numbers

        - RSA is widely used for key exchange, encryption, and digital signatures
        - RSA can use key sizes of 1024-bits to 4096-bits
    - **Elliptic Curve Cryptography (ECC)**
        - Algorithm that is based upon the algebraic structure of elliptic curves over finite fields to define the keys
        - ECC with a 256-bit key is just as secure as RSA with a 2048-bit key
        - ECDH
            - Elliptic Curve Diffie-Hellman
        - ECDHE
            - Elliptic Curve Diffie-Hellman Ephemeral
        - ECDSA
            - Elliptic Curve Digital Signature Algorithm
        - ECC is most commonly used for mobile devices and low-power computing device

- **Pretty Good Privacy**
    - **Pretty Good Privacy (PGP)**
        - An encryption program used for signing, encrypting, and decrypting emails
        - The IDEA algorithm is used by PGP
    - **Symmetric functions use 128-bit or higher keys and the asymmetric functions use 512-bit to 2048-bit key sizes**
    - **GNU Privacy Guard (GPG)**
        - A newer and updated version of the PGP encryption suite that uses AES for its symmetric encryption functions
        - GPG has cross-platform availability

- **Key Management**
    - **Key Management**
        - Refers to how an organization will generate, exchange, store, and use encryption keys
    - **The strength of an encryption system lies in the key strength**
    - **Keys must be securely stored**
    - **Periodically change your keys**

- **One-Time Pad**
    - **One-Time Pad**
        - A stream cipher that encrypts plaintext information with a secret random key that is the same length as the plaintext input
    - **There are no such thing as truly random numbers in computers**

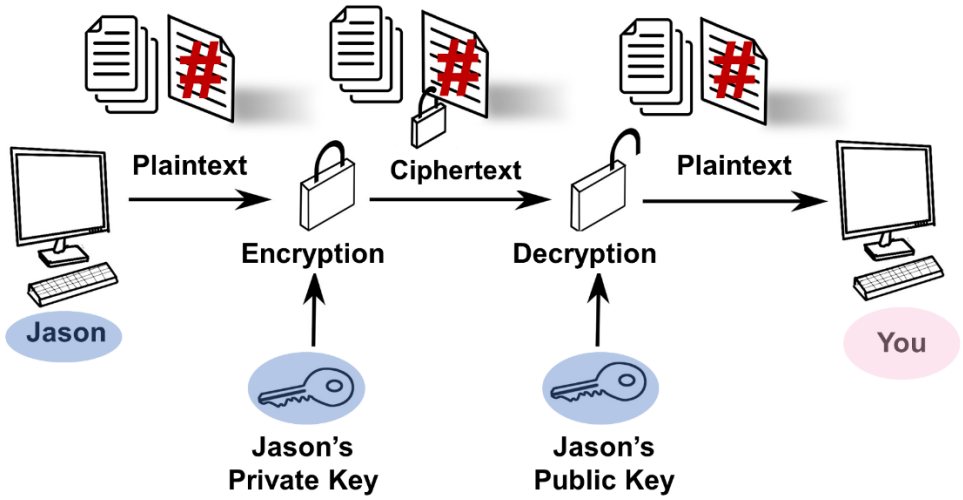
- **Pseudo-Random Number Generator (PRNG)**
  - A simulated random number stream generated by a computer that is used in cryptography, video games, and more
- **One-time pads are not commonly used**

- **Steganography**
  - **Steganography**
    - The science and art of hiding messages within other messages
    - Steganography is a form of obfuscation, not encryption

- **Hashing**
  - **Hashing**
    - A one-way cryptographic function which takes an input and produces a unique message digest
  - **Message Digest 5 (MD5)**
    - Algorithm that creates a fixed-length 128-bit hash value unique to the input file
  - **Collision**
    - Condition that occurs when two different files create the same hash digest
  - **Secure Hash Algorithm (SHA-1)**
    - Algorithm that creates a fixed-length 160-bit hash value unique to the input file
  - **Secure Hash Algorithm (SHA-2)**
    - Family of algorithms that includes SHA-224, SHA-256, SHA-348, and SHA-512
  - **Secure Hash Algorithm (SHA-3)**
    - Family of algorithms that creates hash digests between 224-bits and 512-bits
  - **RACE Integrity Primitive Evaluation Message Digest (RIPEMD)**
    - An open-source hash algorithm that creates a unique 160-bit, 256-bit, or 320-bit message digest for each input file
  - **Hash-based Message Authentication Code (HMAC)**
    - Uses a hash algorithm to create a level of assurance as to the integrity and authenticity of a given message or file
    - HMAC-MD5
    - HMAC-SHA1
    - HMAC-SHA256

- **Digital signatures prevent collisions from being used to spoof the integrity of a message**

Using digital signatures to prevent spoofing of a message's integrity

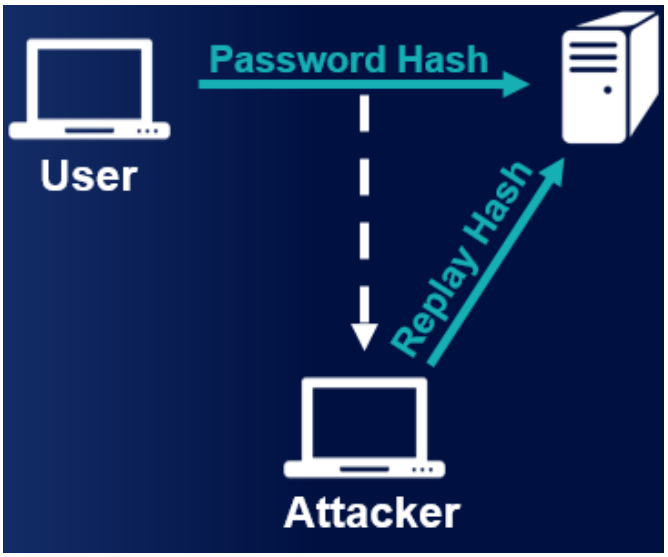


- **Digital signatures use either DSA, RSA, ECDSA, or SHA**

- **Code Signing**
  - Uses digital signatures to provide an assurance that the software code has not been modified after it was submitted by the developer
- **LANMAN (LM Hash)**
  - Original version of password hashing used by Windows that uses DES and is limited to 14 characters
- **NT LAN Manager Hash (NTLM Hash)**
  - Replacement for LM Hash that uses RC4 and was released with Windows NT 3.1 in 1993
- **NTLMv2 Hash**
  - Replacement for NTLM Hash that uses HMAC-MD5 and is considered difficult to crack
  - NTLMv2 is used when you do not have a domain with Kerberos for authentication
- **Exam Tips**
  - Instantly match integrity and hashing on the exam
  - MD5 and SHA are the most common hash functions used

- **Hashing Attacks**
  - **Pass the Hash**

- A technique that allows an attacker to authenticate to a remote server or service by using the underlying NTLM or LM hash instead of requiring the associated plaintext password



- Pass the Hash is difficult to defend against

- Mimikatz
  - A penetration testing tool used to automate the harvesting of hashes and conducting the Pass the Hash attack
- Only use a trusted OS
- Patch/update workstations
- Use multifactor authentication
- Use least privilege

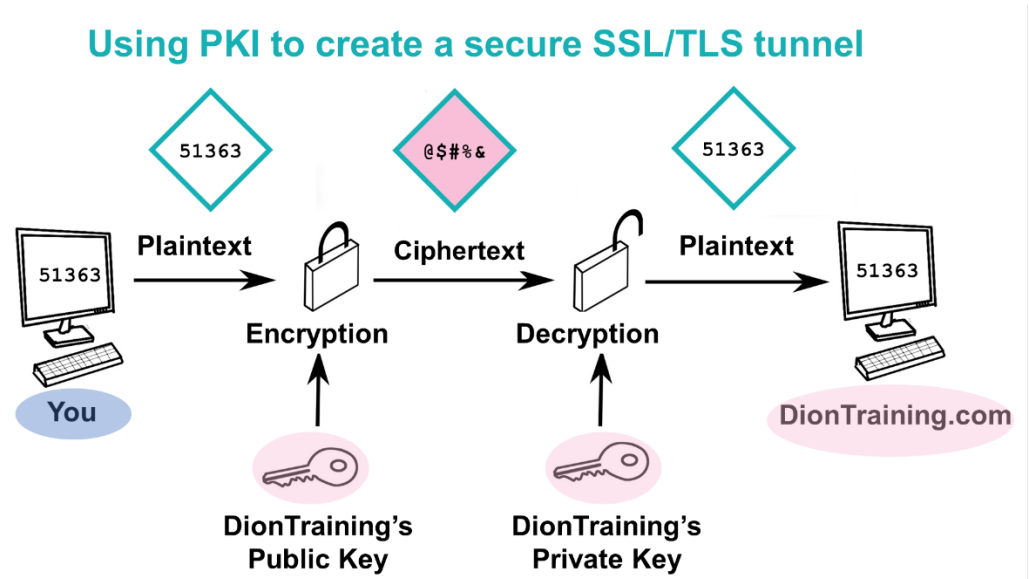
- **Birthday Attack**
  - Technique used by an attacker to find two different messages that have the same identical hash digest
  - 99% chance of finding a matching birthday in a 57-person group
  - 50% chance of finding a matching birthday in a 23-person group
  - Collision
    - Occurs when two different inputs to a hash create an identical hash digest output

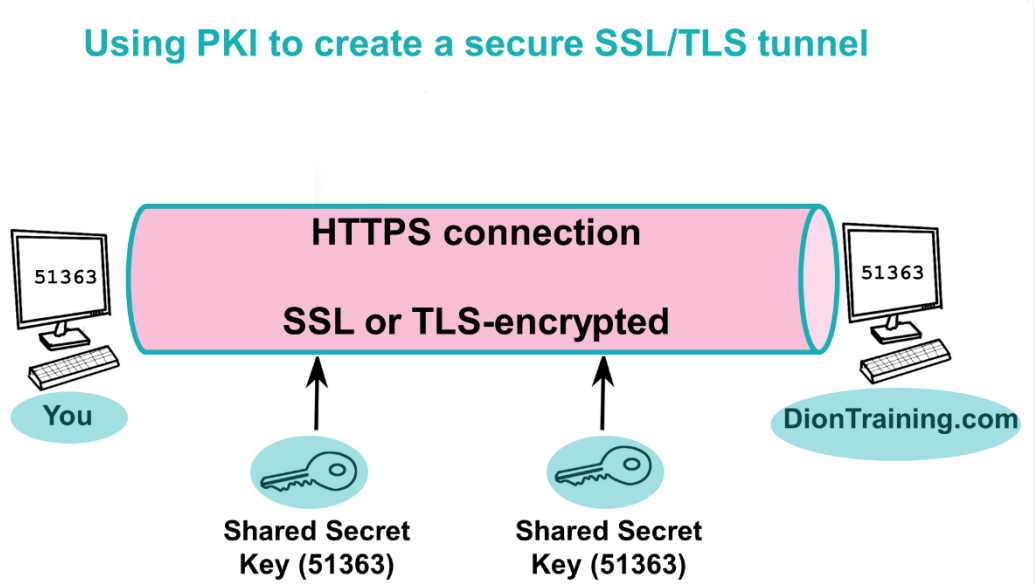
- **Increasing Hash Security**
  - **Key Stretching**

        - A technique that is used to mitigate a weaker key by increasing the time needed to crack it
        - WPA, WPA2, PGP, bcrypt, and other algorithms utilize key stretching
    - **Salting**
        - Adding random data into a one-way cryptographic hash to help protect against password cracking techniques
        - A “nonce” is used to prevent password reuse

Public Key Infrastructure

- **Public Key Infrastructure**
    - **Public Key Infrastructure (PKI)**
        - An entire system of hardware, software, policies, procedures, and people that is based on asymmetric encryption





  - **PKI and public key encryption are related but they are not the same thing**
  - **PKI is the entire system and just uses public key cryptography to function**
- **Digital Certificates**
  - **Certificates**
    - Digitally-signed electronic documents that bind a public key with a user's identity
  - **X.509**
    - Standard used PKI for digital certificates and contains the owner/user's information and the certificate authority's information

- **Wildcard Certificates**
  - Allow all of the subdomains to use the same public key certificate and have it displayed as valid
  - Wildcard certificates are easier to manage
- **Subject Alternative Name (SAN)**
  - Allows a certificate owner to specify additional domains and IP addresses to be supported
- **Single-sided certificates only require the server to be validated**
  - Dual-sided certificates require both the server and the user to be validated
- **X.690 uses BER, CER, and DER for encoding**
- **Basic Encoding Rules (BER)**
  - The original ruleset governing the encoding of data structures for certificates where several different encoding types can be utilized
- **Canonical Encoding Rules (CER)**
  - A restricted version of the BER that only allows the use of only one encoding type
- **Distinguished Encoding Rules (DER)**
  - Restricted version of the BER which allows one encoding type and has more restrictive rules for length, character strings, and how elements of a digital certificate are stored in X.509
- **PEM**
- **CER**
- **CRT**
- **KEY**
- **P12**
- **PFX**
- **P7B**
- **Privacy-enhanced Electronic Mail**
  - .pem, .cer, .crt, or .key
- **Public Key Cryptographic System #12 (PKCS#12)**
  - .p12
- **Personal Information Exchange**
  - .pfx
- **Public Key Cryptographic Systems #7 (PKCS#7)**
  - .p7b
- **Remember, these file types are associated with PKI**

- **Certificate Authorities**
  - **Registration Authority**

        - Used to verify information about a user prior to requesting that a certificate authority issue the certificate
    - **Certificate Authority**
        - The entity that issues certificates to a user
        - Verisign, Digisign, and many others act as Root CA
    - **Certificate Revocation List (CRL)**
        - An online list of digital certificates that the certificate authority has revoked
    - **Online Certificate Status Protocol (OCSP)**
        - A protocol that allows you to determine the revocation status of a digital certificate using its serial number
    - **OCSP Stapling**
        - Allows the certificate holder to get the OCSP record from the server at regular intervals and include it as part of the SSL or TLS handshake
    - **Public Key Pinning**
        - Allows an HTTPS website to resist impersonation attacks by presenting a set of trusted public keys to the user's web browser as part of the HTTP header
    - **Key Escrow and Key Recovery Agent**
        - Key Escrow
            - Occurs when a secure copy of a user's private key is held in case the user accidently loses their key
        - Key Recovery Agent
            - A specialized type of software that allows the restoration of a lost or corrupted key to be performed
    - **All of a CA's certificates must be revoked if it is compromised**

- **Web of Trust**
    - **Web of Trust**
        - A decentralized trust model that addresses issues associated with the public authentication of public keys within a CA-based PKI system
        - A peer-to-peer model
        - Certificates are created as self-signed certificates
        - Pretty Good Privacy (PGP) is a web of trust

Security Protocols

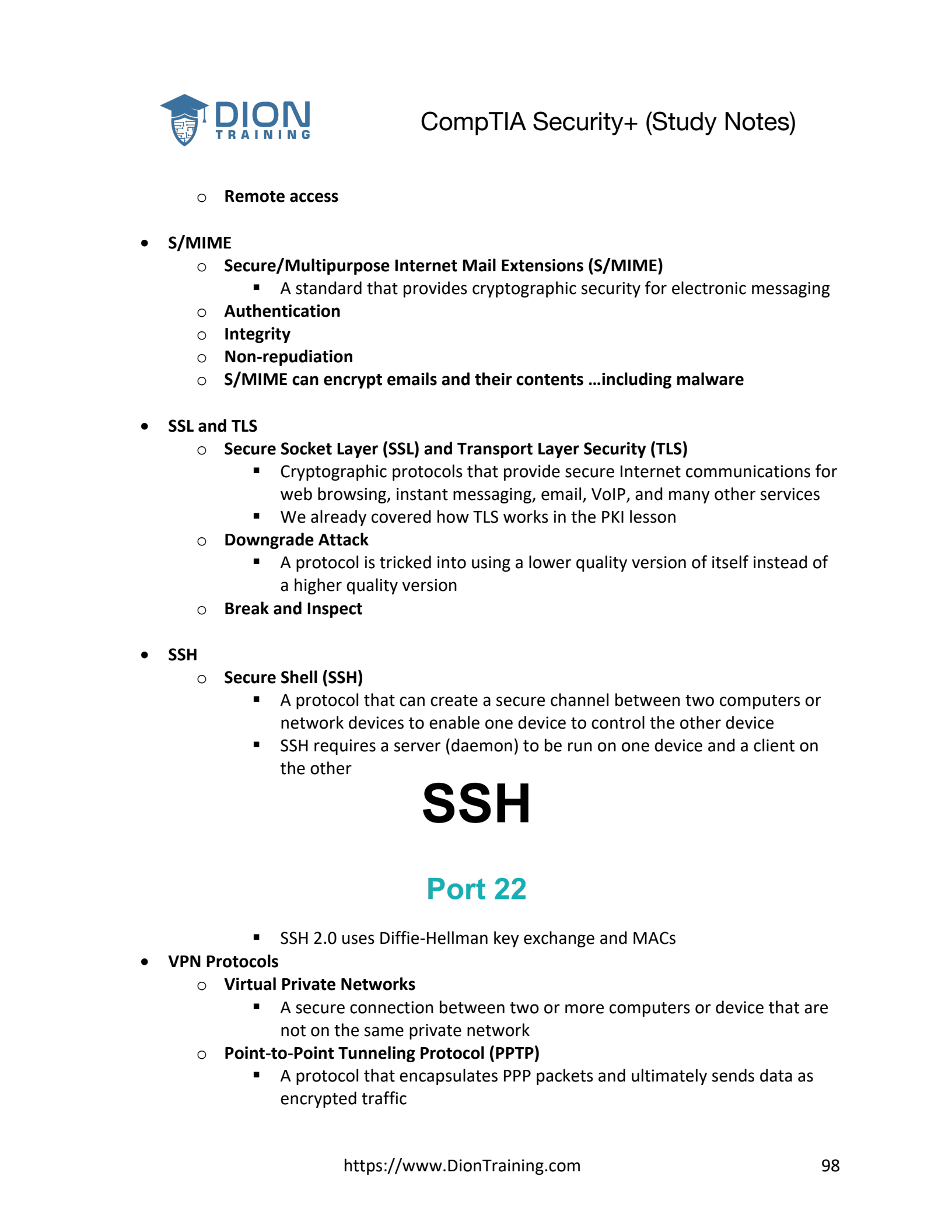
- **Security Protocols**
    - **Emails**
    - **Websites**
    - **Remote control**

- **Remote access**

- **S/MIME**
  - **Secure/Multipurpose Internet Mail Extensions (S/MIME)**
    - A standard that provides cryptographic security for electronic messaging
  - **Authentication**
  - **Integrity**
  - **Non-repudiation**
  - **S/MIME can encrypt emails and their contents …including malware**

- **SSL and TLS**
  - **Secure Socket Layer (SSL) and Transport Layer Security (TLS)**
    - Cryptographic protocols that provide secure Internet communications for web browsing, instant messaging, email, VoIP, and many other services
    - We already covered how TLS works in the PKI lesson
  - **Downgrade Attack**
    - A protocol is tricked into using a lower quality version of itself instead of a higher quality version
  - **Break and Inspect**

- **SSH**
  - **Secure Shell (SSH)**
    - A protocol that can create a secure channel between two computers or network devices to enable one device to control the other device
    - SSH requires a server (daemon) to be run on one device and a client on the other



    - SSH 2.0 uses Diffie-Hellman key exchange and MACs
- **VPN Protocols**
  - **Virtual Private Networks**
    - A secure connection between two or more computers or device that are not on the same private network
  - **Point-to-Point Tunneling Protocol (PPTP)**
    - A protocol that encapsulates PPP packets and ultimately sends data as encrypted traffic

PPTP

Port 1723

    - PPTP can use CHAP-based authentication, making it vulnerable to attacks
- **Layer 2 Tunneling Protocol (L2TP)**
    - A connection between two or more computers or device that are not on the same private network
    - L2TP is usually paired with IPSec to provide security

L2TP

Port 1701

- **IPSec**
    - A TCP/IP protocol that authenticates and encrypts IP packets and effectively securing communications between computers and devices using this protocol
    - IPSec provides confidentiality (encryption), integrity (hashing), and authentication (key exchange)
- **Internet Key Exchange (IKE)**
    - Method used by IPSec to create a secure tunnel by encrypting the connection between authenticated peers
- **Main**
- **Aggressive**
- **Quick**
- **Security Association (SA)**
    - Establishment of secure connections and shared security information using certificates or cryptographic keys
- **Authentication Header (AH)**
    - Protocol used in IPSec that provides integrity and authentication
- **Encapsulating Security Payload (ESP)**
    - Provides integrity, confidentiality, and authenticity of packets by encapsulating and encrypting them
    - Transport Mode

        - Host-to-host transport mode only uses encryption of the payload of an IP packet but not its header
        - Transport mode is used for transmission between hosts on a private network
    - Tunnel Mode
        - A network tunnel is created which encrypts the entire IP packet (payload and header)
        - Tunnel mode is commonly used for transmission between networks

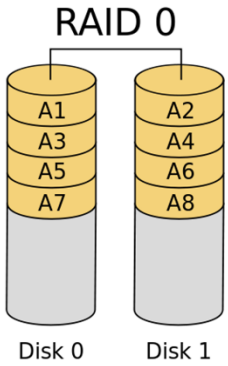
Planning for the Worst

- **Planning for the Worst**
    - **Redundancy usually refers to when you have something extra or unnecessary**
    - **Redundancy helps ensure fault-tolerance to continue operations**
    - **Single Point of Failure**
        - The individual elements, objects, or parts of a system that would cause the whole system to fail if they were to fail

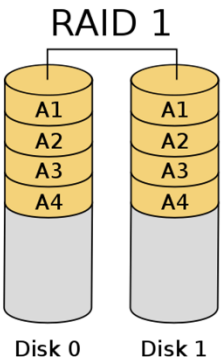
- **Redundant Power**
  - **Redundant Power Supply**
    - An enclosure that provides two or more complete power supplies
    - A redundant power supply mitigates a single point of failure
  - **Surge**
    - An unexpected increase in the amount of voltage provided
  - **Spike**
    - A short transient in voltage that can be due to a short circuit, tripped circuit breaker, power outage, or lightning strike
  - **Sag**
    - An unexpected decrease in the amount of voltage provided
  - **Brownout**
    - Occurs when the voltage drops low enough that it typically causes the lights to dim and can cause a computer to shut off
  - **Blackout**
    - Occurs when there is a total loss of power for a prolonged period

- **Backup Power**
  - **Uninterruptible Power Supply (UPS)**
    - Combines the functionality of a surge protector with that of a battery backup
  - **Backup Generator**
    - An emergency power system used when there is an outage of the regular electric grid power
    - Portable gas-engine
    - Permanently installed
    - Battery-inverter
  - **How do you decide which to use?**

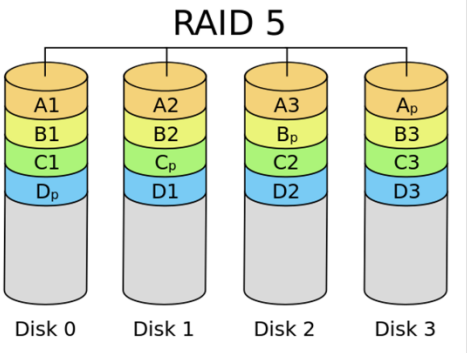
- **Data Redundancy**
  - **Redundant Array of Independent Disks (RAID)**
    - Allows the combination of multiple physical hard disks into a single logical hard disk drive that is recognized by the operating system
  - **RAID 0**
    - Provides data striping across multiple disks to increase performance



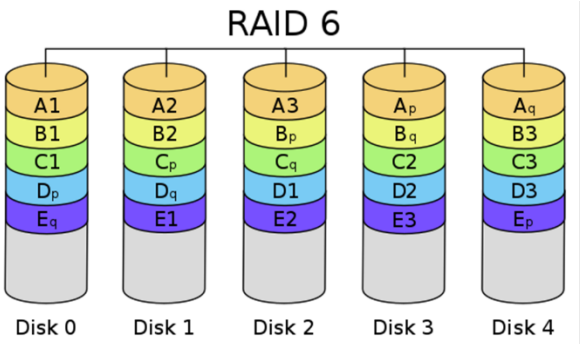
- **RAID 1**
  - Provides redundancy by mirroring the data identically on two hard disks



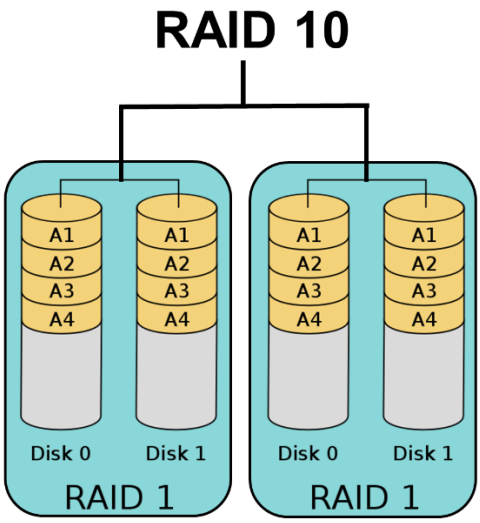
- **RAID 5**
  - Provides redundancy by striping data and parity data across the disk drives



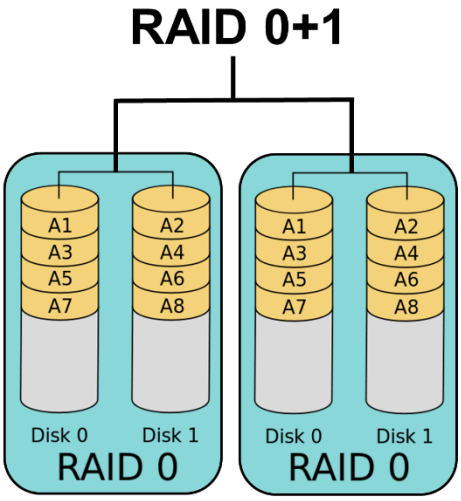
- **RAID 6**
  - Provides redundancy by striping and double parity data across the disk drives



- **RAID 10**
  - Creates a striped RAID of two mirrored RAIDs (combines RAID 1 & RAID 0)



- **Fault-resistant RAID**
  - Protects against the loss of the array's data if a single disk fails (RAID 1 or RAID 5)
- **Fault-tolerant RAID**
  - Protects against the loss of the array's data if a single component fails (RAID 1, RAID 5, RAID 6)
- **Disaster-tolerant RAID**
  - Provides two independent zones with full access to the data (RAID 10)



  - **RAIDs provide redundancy and high-availability**

- **Network Redundancy**
  - **Focused on ensuring that the network remains up**
  - **Redundant Internet connections**

- **Server Redundancy**
  - **Cluster**
    - Two or more servers working together to perform a particular job function
  - **Failover Cluster**
    - A secondary server can take over the function when the primary one fails
  - **Load-balancing Cluster**
    - Servers are clustered in order to share resources such as CPU, RAM, and hard disks

- **Redundant Sites**
  - **Hot Site**
    - A near duplicate of the original site of the organization that can be up and running within minutes
  - **Warm Site**
    - A site that has computers, phones, and servers but they might require some configuration before users can start working
  - **Cold Site**
    - A site that has tables, chairs, bathrooms, and possibly some technical items like phones and network cabling

- **How do you choose the type of site?**

- **Data Backup**
  - **Maintaining a good backup is crucial to disaster recovery**
  - **Full Backup**
    - All of the contents of a drive are backed up
  - **Incremental Backup**
    - Only conducts a backup of the contents of a drive that have changed since the last full or incremental backup
  - **Differential Backup**
    - Only conducts a backup of the contents of a drive that has changed since the last full backup

Day	Type
Sunday	Full
Monday	Differential
Tuesday	Differential
Wednesday	Failure
Thursday	
Friday	

Day	Type
Sunday	Full
Monday	Incremental
Tuesday	Incremental
Wednesday	Incremental
Thursday	Incremental
Friday	Failure

    - Differential backups take more time to create but less time to restore

- **Tape Rotation**
  - **10 Tape Rotation**
    - Each tape is used once per day for two weeks and then the entire set is reused
  - **Grandfather-Father-Son**
    - Three sets of backup tapes are defined as the son (daily), the father (weekly), and the grandfather (monthly**)**
  - **Towers of Hanoi**
    - Three sets of backup tapes (like the grandfather-father-son) that are rotated in a more complex system

Day	I	II	III
1	A		
2		B	
3	A		
4			C
5	A		
6		B	
7	A		

    - **Snapshot Backup**
        - Type of backup primarily used to capture the entire operating system image including all applications and data
        - Snapshots are also commonly used with virtualized systems

- **Disaster Recovery Planning**
    - **Disaster Recovery Planning**
        - The development of an organized and in-depth plan for problems that could affect the access of data or the organization's building
            - Fire
            - Flood
            - Long-term Power Loss
            - Theft or Attack
            - Loss of Building
    - **Disaster Recovery Plan (DRP) should be written down**
        - Contact Information
        - Impact Determination
        - Recovery Plan
        - Business Continuity Plan (BCP)
        - Copies of Agreements
        - Disaster Recovery Exercises
        - List of Critical Systems and Data

Social Engineering

- **Social Engineering**
  - **Social Engineering**
    - Manipulates a user into revealing confidential information that are detrimental to that user or the security of our systems

- **Insider Threat**
  - **Most dangerous threat to organizational security**
  - **Insider Threat**
    - A person who works for or with your organization but has ulterior motives
    - Employees who steal your information are insider threats
    - Data Loss Prevention systems can be used to help identify insider threats

- **Phishing**
  - **Phishing**
    - An attempt to fraudulently obtain information from a user (usually by email)
  - **Smishing**
    - Phishing conducted over text messaging (SMS)
  - **Vishing**
    - Phishing conducted over voice and phone calls
  - **Pharming**
    - Phishing attempt to trick a user to access a different or fake website (usually by modifying hosts file)
  - **Phishing is a more specific type of social engineering**
  - **Phishing is a generic category with specific techniques**

- **More Social Engineering**
  - **Diversion Theft**
    - When a thief attempts to take responsibility for a shipment by diverting the delivery to a nearby location
  - **Hoax**
    - Attempt at deceiving people into believing that something is false when it is true (or vice versa)
  - **Shoulder Surfing**
    - When a person uses direct observation to obtain authentication information

- **Eavesdropping**
  - When a person uses direct observation to “listen” in to a conversation
- **Dumpster Diving**
  - When a person scavenges for private information in garbage containers
- **Baiting**
  - When a malicious individual leaves malware-infected removable media such as a USB drive or optical disc lying around in plain view
- **Piggybacking**
  - When an unauthorized person tags along with an authorized person to gain entry to a restricted area
- **Watering Hole Attack**
  - When an attacker figures out where users like to go, and places malware to gain access to your organization

- **User Education**
  - **Never share authentication information**
  - **Clean Desk Policy**
    - Policy where all employees must put away everything from their desk at the end of the day into locked drawers and cabinets
  - **Train users how to encrypt emails and data**
  - **Follow organizational data handling and disposal policies**

Policies and Procedures

- **Policies and Procedures**
  - **Governance provides a comprehensive security management framework**
  - **Policies**
    - Defines the role of security in an organization and establishes the desired end state of the security program
    - Policies are very broad
  - **Organizational Policies**
    - Provide general direction and goals, a framework to meet the business goals, and define the roles, responsibilities, and terms
  - **System-Specific Policies**
    - Address the security needs of a specific technology, application, network, or computer system
  - **Issue-Specific Policies**
    - Built to address a specific security issue, such as email privacy, employee termination procedures, or other specific issues
  - **Policies may be regulatory, advisory, or informative**
  - **Standards are used to implement a policy in an organization**
  - **Baseline**
    - Created as reference points which are documented for use as a method of comparison during an analysis conducted in the future
  - **Guidelines are used to recommend actions**
  - **Procedures**
    - Detailed step-by-step instructions that are created to ensure personnel can perform a given action
  - **Exam Tip**
    - Policies are generic
    - Procedures are specific

- **Data Classifications**
  - **Data Classification**
    - Category based on the value to the organization and the sensitivity of the information if it were to be disclosed
  - **Sensitive Data**
    - Any information that can result in a loss of security, or loss of advantage to a company, if accessed by unauthorized persons
  - **Commercial businesses and the government use different classification systems**

- **Commercial Classifications**
  - Public Data
    - Has no impact to the company if released and is often posted in the open-source environment
    - Sensitive data might have a minimal impact if released
  - Private Data
    - Contains data that should only be used within the organization
  - Confidential Data
    - Highest classification level that contains items such as trade secrets, intellectual property data, source code, and other types that would seriously affect the business if disclosed
- **Government Classifications**
  - Unclassified data can be released to the public
  - Sensitive but Unclassified
    - Items that wouldn't hurt national security if released but could impact those whose data is contained in it
  - Confidential Data
    - Data that could seriously affect the government if unauthorized disclosure were to happen
  - Secret Data
    - Data that could seriously damage national security if disclosed
  - Top Secret Data
    - Data that could gravely damage national security if it were known to those who are not authorized for this level of information
- **Data should not be stored forever**

- **PII and PHI**
  - **It is your responsibility to protect the data collected**
  - **Personal Identifiable Information (PII)**
    - A piece of data that can be used either by itself or in combination with some other pieces of data to identify a single person
      - Full Name
      - Driver's License
      - Date of Birth
      - Place of Birth
      - Biometric Data
      - Financial Account Numbers
      - Email Addresses
      - Social Media Usernames
    - Verify with your legal team what is considered PII

- **Privacy Act of 1974**
  - Affects U.S. government computer systems that collects, stores, uses, or disseminates personally identifiable information
- **Health Insurance Portability and Accountability Act (HIPAA)**
  - Affects healthcare providers, facilities, insurance companies, and medical data clearing houses
- **Sarbanes-Oxley (SOX)**
  - Affects publicly-traded U.S. corporations and requires certain accounting methods and financial reporting requirements
- **Gramm-Leach-Bliley Act (GLBA)**
  - Affects banks, mortgage companies, loan offices, insurance companies, investment companies, and credit card providers
- **Federal Information Security Management (FISMA) Act of 2002**
  - Requires each agency to develop, document, and implement an agency-wide information systems security program to protect their data
- **Payment Card Industry Data Security Standard (PCI DSS) is a contractual obligation**
- **Help America Vote Act (HAVA) of 2002**
  - Provides regulations that govern the security, confidentiality, and integrity of the personal information collected, stored, or processed during the election and voting process
- **SB 1386 requires any business that stores personal data to disclose a breach**

- **Security Policies**
  - **Privacy policies govern the labeling and handling of data**
  - **Acceptable Use Policy**
    - Defines the rules that restrict how a computer, network, or other systems may be used
  - **Change Management Policy**
    - Defines the structured way of changing the state of a computer system, network, or IT procedure
  - **Separation of Duties is a preventative type of administrative control**
  - **Job Rotation**
    - Different users are trained to perform the tasks of the same position to help prevent and identify fraud that could occur if only one employee had the job
  - **Onboarding and Offboarding Policy**
    - Dictates what type of things need to be done when an employee is hired, fired, or quits
    - Terminated employees are often not cooperative

  - **Due Diligence**
    - Ensuring that IT infrastructure risks are known and managed properly
  - **Due Care**
    - Mitigation actions that an organization takes to defend against the risks that have been uncovered during due diligence
  - **Due Process**
    - A legal term that refers to how an organization must respect and safeguard personnel's rights
    - Due process protects citizens from their government and companies from lawsuits

- **User Education**
  - **Security Awareness Training**
    - Used to reinforce to users the importance of their help in securing the organization's valuable resources
    - User security awareness training has the best return on investment
  - **Security Training**
    - Used to teach the organization's personnel the skills they need to perform their job in a more secure manner
  - **Security education is generalized training (like Security+)**
  - **Specialized training may be developed too**

- **Vendor Relationships**
  - **Non-Disclosure Agreement (NDA)**
    - Agreement between two parties that defines what data is considered confidential and cannot be shared outside of the relationship
    - NDAs are a binding contract
  - **Memorandum of Understanding (MOU)**
    - A non-binding agreement between two or more organizations to detail an intended common line of action
    - MOUs can be between multiple organizations
  - **Service-Level Agreement (SLA)**
    - An agreement concerned with the ability to support and respond to problems within a given timeframe and continuing to provide the agreed upon level of service to the user
    - SLA may promise 99.999% uptime
  - **Interconnection Security Agreement (ISA)**
    - An agreement for the owners and operators of the IT systems to document what technical requirements each organization must meet

- **Business Partnership Agreement (BPA)**
  - Conducted between two business partners that establishes the conditions of their relationship
  - A BPA can also include security requirements

- **Disposal Policies**
  - **Asset disposal occurs whenever a system is no longer needed**
  - **Degaussing**
    - Exposes the hard drive to a powerful magnetic field which in turn causes previously-written data to be wiped from the drive
  - **Purging (Sanitizing)**
    - Act of removing data in such a way that it cannot be reconstructed using any known forensic techniques
  - **Clearing**
    - Removal of data with a certain amount of assurance that it cannot be reconstructed
  - **Data remnants are a big security concern**
  - **Possible reuse of the device will influence the disposal method**
    - 1. Define which equipment will be disposed of
    - 2. Determine a storage location until disposal
    - 3. Analyze equipment to determine disposal – reuse, resell, or destruction
    - 4. Sanitize the device and remove all its data
    - 5. Throw away, recycle, or resell the device

- **Incident Response Procedures**
  - **Our systems will never be 100% secure**
  - **Incident Response**
    - A set of procedures that an investigator follows when examining a computer security incident
  - **Incident Management Program**
    - Program consisting of the monitoring and detection of security events on a computer network and the execution of proper responses to those security events
    - Preparation
    - Identification
      - Process of recognizing whether an event that occurs should be classified as an incident
    - Containment
      - Containment is focused on isolating the incident

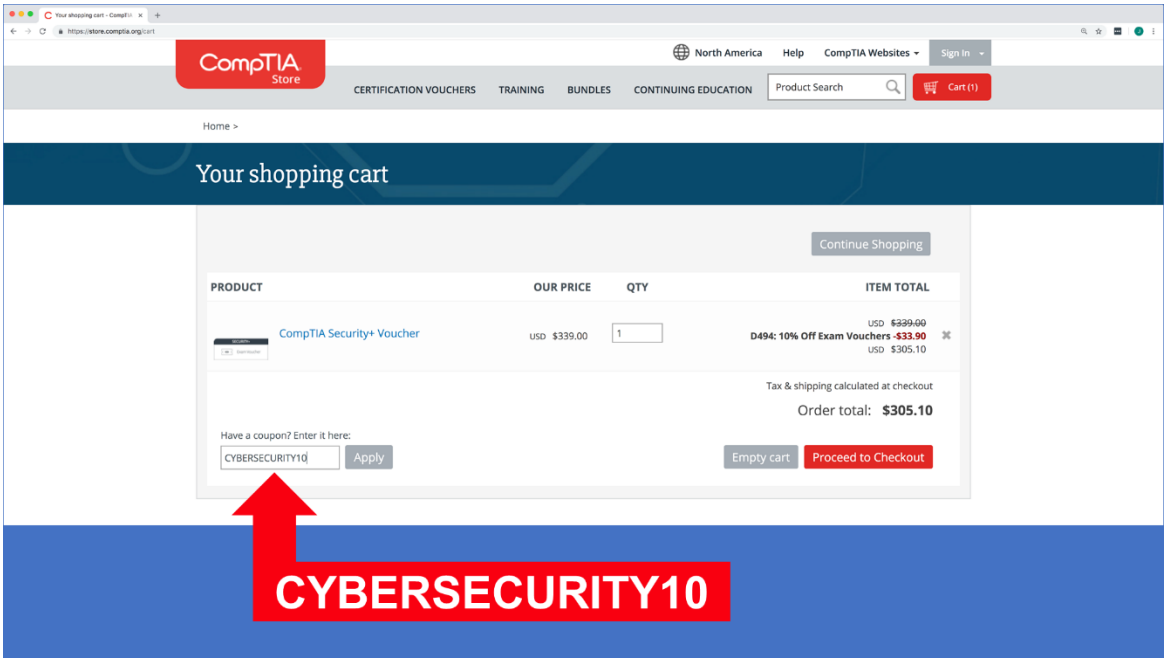
        - Eradication
        - Recovery
            - Focused on data restoration, system repair, and re-enabling any servers or networks taken offline during the incident response
        - Lessons Learned

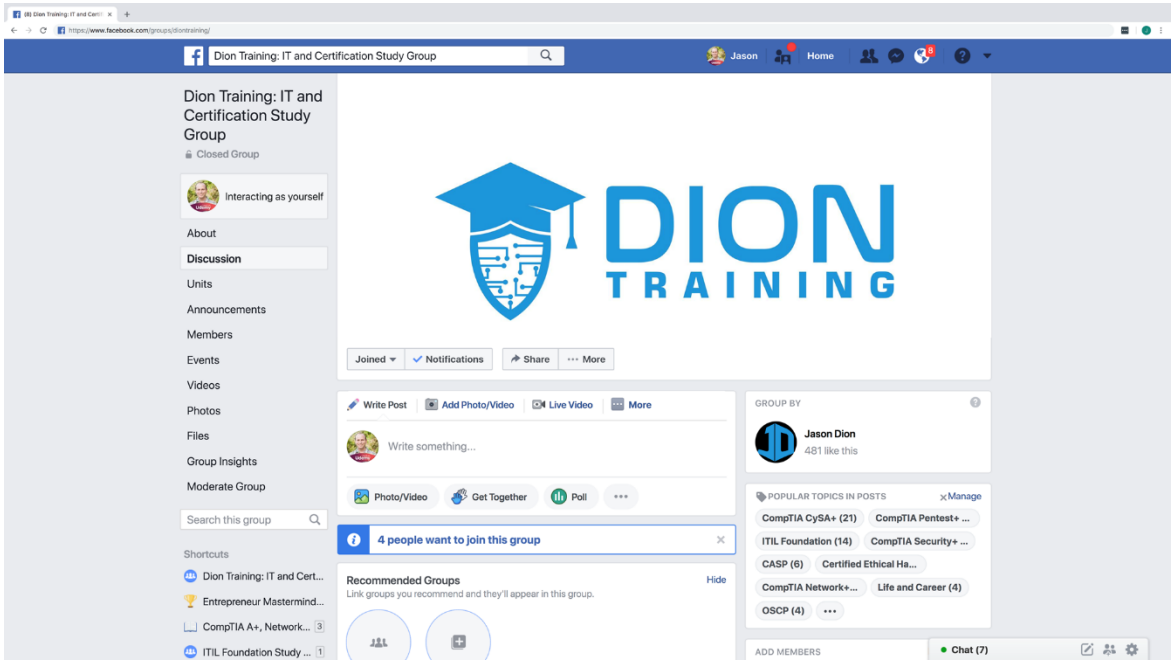
- **Data Collection Procedures**
    - **Create a forensic disk image of the data as evidence**
        - Capture and hash system images
        - Analyze data with tools
        - Capture screenshots
        - Review network traffic and logs
        - Capture video
        - Consider Order of Volatility
        - Take statements
        - Review licensing and documentation
        - Track man-hours and expenses
    - **FTK and EnCase are popular forensic tools**

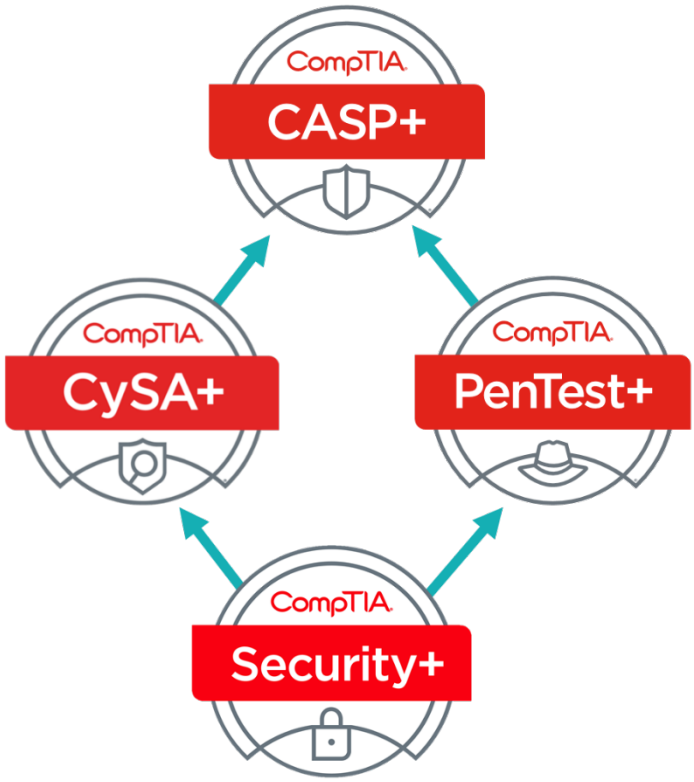
- **IT Security Frameworks**
    - **Sherwood Applied Business Security Architecture (SABSA) is a risk-driven architecture**
    - **Control Objectives for Information and Related Technology (COBIT)**
        - A security framework that divides IT into four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate
    - **NIST SP 800-53 is a security control framework developed by the Dept. of Commerce**
    - **ISO 27000**
    - **ITIL is the de facto standard for IT service management**
        - Being able to discuss ITIL will help in your job interviews

Conclusion

- **Conclusion**
  - **We learned all the information in a more practical order**
  - **Domains (SYO-501)**
    - 1. Threats, Attacks, and Vulnerabilities (21%)
    - 2. Technologies and Tools (22%)
    - 3. Architecture and Design (15%)
    - 4. Identity and Access Management (16%)
    - 5. Risk Management (14%)
    - 6. Cryptography and PKI (12%)
  - **Let's get you certified on your first attempt!**
  - **You can take it at any PearsonVue testing center worldwide**




Dion Training: IT and Certification Study Group
Jason
Home
Dion Training: IT and Certification Study Group
Closed Group
Interacting as yourself
About
Discussion
Units
Announcements
Members
Events
Videos
Photos
Files
Group Insights
Moderate Group
Search this group
Shortcuts
Dion Training: IT and Cert...
Entrepreneur Mastermind...
CompTIA A+, Network...
ITIL Foundation Study ...
DION TRAINING
Joined
Notifications
Share
More
Write Post
Add Photo/Video
Live Video
More
Write something...
Photo/Video
Get Together
Poll
4 people want to join this group
Recommended Groups
Hide
Link groups you recommend and they'll appear in this group.
GROUP BY
Jason Dion
481 like this
POPULAR TOPICS IN POSTS
Manage
CompTIA CySA+ (21)
CompTIA Pentest+ ...
ITIL Foundation (14)
CompTIA Security+ ...
CASP (6)
Certified Ethical Ha...
CompTIA Network+...
Life and Career (4)
OSCP (4)
ADD MEMBERS
Chat (7)


CompTIA
CASP+
CompTIA
CySA+
CompTIA
PenTest+
CompTIA
Security+

- **Exam Tricks**
  - **1. Use a Cheat Sheet**
  - **2. Skip the Simulations**
  - **3. Take a Guess**
  - **4. Pick the Best Time**
  - **5. Be Confident**

Let’s get you certified!