Meyer's Security+ Video Notes

http://gcgapremium.com/501labs/

https://www.reddit.com/r/CompTIA/comments/a35pjg/just_passed_security_sy0501_heres_my_brain_dump/

Section 1: Risk Management

- **The CIA of Security** (Triad): Confidentiality, Integrity, Availability
    - **Confidentiality** - the goal of keeping data secret from anyone who doesn't have the need or the right to access that data
    - **Integrity** - everything stays in an unaltered state when stored, transmitted, and received. Also can be no unauthorized, modification, alteration, creation, or deletion of the data.
    - **Availability** - have to ensure that systems and data are available to authorize users when needed
- Also Important: Auditing & Accountability, and Non-Repudiation
    - **Auditing & Accountability** - Keeping track of what's going on and who's doing what, when, and where
    - **Non-Repudiation** - User can't deny that they have performed a particular action. A user can't deny of having made some form of communication
- **Threat Actors** - people and organizations who actually do the types of attacks
- **Attributes of threat actors:**
    - Internal/external: within organization or far of in another country
    - Level of sophistication: don't need to be overly sophisticated to cause damage
    - Funding: larger attacks requires lots of resources
    - Intent/motivation: what they are trying to achieve with an attack
    - **Open-Source Intelligence (OSINT):** Social media, online lookups
- **Types of Threat Actors:**
    - **Script Kiddies** - trivial attack knowledge, use premade tools and scripts, hardly any sophistication. Not very evil. Easily blocked.
    - **Hacktivist** - Some form of activism they want to pursue. Intent is motivation.
    - **Organized Crime** - smart groups of people working together usually motivation being to make money. Big Issue.
    - **Nation States/Advanced Persistent Threat (APT)** - Huge sophistication. Usually motivation is to acquire intelligence.
    - **Advanced Persistent Threat (APT)** - some form of threat and they stay there usually to spy and gather info
    - **Insiders** - Not always an employee, can be cleaning people, vendor, basically anyone who works within the infrastructure. Do they have access to information?
    - **Competitors** - looking to steal company secrets
- **Assets:** provide benefits to the organization.
- Can be any part of our infrastructure that we are worried about getting harmed. People, physical structures in a building, intangibles can be assets
- **Vulnerabilities:** Weakness to an asset to be exploited. Not changing default passwords, not locking important rooms in example

- **Threats:** A discovered action that exploits a vulnerability's potential to do harm to an asset. Someone accessing your network because they knew default password, stealing your server because door was unlocked, someone important quitting
- **Threat Agent:** person, entity or an event (weather) that initiates a threat.
- **Likelihood:** defines the level of certainty that something will happen. Often used as a percentage like what's the percentage of something happening in a year. **2 ways to measure while discussing risk.**
    - **Quantitative Likelihood** - using data like measurable metrics to assess risk and usually stated as a percentage.
    - **Qualitative Likelihood** - uses quality of things that are harder to measure such as customer experience. Usually measured in a high, medium, low scale i.e. to determine probability of risk through perceived impact
- **Impact:** actual harm caused by a threat.
    - Can be measured quantitative such as by cost, labor (man hrs), time caused by threat
    - Measured qualitative such as impact to customer service, reputation, unavailable resources caused by threat
- If an asset doesn't have a vulnerability or if there's no threat you don't have any risk
- **Risk = Threats x Vulnerability** (or Threats -> Vulnerability = Risk)
- **NIST (National Institute of Standards and Technologies)** has document called SP 800-30 listing all kinds of threats and vulnerabilities that the typical security person might be exposed to and everybody in the security world uses these documents as a starting place to be able to provide good risk management for their infrastructures.
- Threats exploit vulnerabilities to harm assets
- **Risk Identification/Assessment:** Catalog and define all of our assets
    - **Vulnerability Assessment** - determine what vulnerabilities can affect assets.
        - Can use NIST SP 800-37 but very broad
        - Common Vulnerabilities and Exposures Database - cve.mitre.org gives a lot more details on vulnerabilities
        - Nessus program gives very detailed info of system vulnerabilities
        - **Penetration (Pen) Testing -** Outside party tries to look for vulnerabilities to expose issues in infrastructure
    - **Threat Assessment** - define the threats that are applicable to your particular infrastructure
        - **Adversarial** - hacker or malicious software. Someone intentionally attacking your infrastructure
        - **Accidental** - someone who accidently or mistakenly causes an issue
        - **Structural** - Issue with equipment or software like breaking or malfunctioning
        - **Environmental** - Fires, earthquakes and other
    - Usually Vulnerability and Threat Assessment done together at the same time
- **Risk Response:** Actions to take to mitigate risks

    - **Mitigation** - effort to reduce impact of risk. Do something that will reduce impact of a particular risk. Like protecting a web server with a DMZ
    - **Risk Transference** - offload some of the likelihood, risk, and impact on a third party. Like using a cloud based web server service to offload the issues of hosting one
    - **Risk Acceptance** - Likelihood and impact of the risk is less than the cost of actually trying to mitigate that particular risk. You accept the risk and chose not to confront it. Like choosing not to defend against an asteroid
    - **Risk Avoidance** - Combination of likelihood and impact so high that simply don't want to deal with it. Like deciding not to store customer info in fear you might get hacked and lose info leading to a lawsuit
- **Frameworks:** a workflow, a methodology, an idea, of a process that helps you as a security professional deal with risk management
    - **NIST Risk Management Framework** Special Publication 800-37
    - **ISACA** Risk IT Framework
- Keep doing these processes over and over to manage risk
- CompTia defines risk assessment as how do we secure stuff
- **Risk Assessment Guides:**
    - **Benchmark** - Use threshold value to verify expected throughput or action
    - **Secure Configuration Guides** - Make sure configuration is done properly and securely
    - **Platform and Vendor Guides** (what CompTia is looking for) - Security tips, configuration guides given by hardware and software vendors
    - **Network Infrastructure Devices** - Guides for Routers, swtiches, WAPs, etc
    - **General Purpose Guides** - list of security controls you want to apply. Like NIST SP 800-123. Guides about different broad subjects
- **Security Controls:** 1) Protect our IT infrastructure from security problems or 2) Remediate problems if already had a problem with our security
    - Setting up things to protect our infrastructure
- Security guys understand, apply, monitor, and adjust security controls based on the needs of the infrastructure
- **Administrative Control (Management Control**): Control Actions towards IT security
    - Laws, policies, guidelines, best practices (what do people do)
- **Technical Control:** Control actions IT systems towards IT security
    - Computer stuff, firewalls, password links, authentication, encryption
- **Physical Control:** Control actions in the real world
    - Gates, guards, keys, man traps
- **Security Control Functions:**
    - **Deterrent** - deter the actor from attempting the threat. Stops them from even trying
    - **Preventative** - deters the actor from performing the threat. Stops them from doing it
    - **Detective** - recognizes an actor's threat and may or may not do something about it
    - **Corrective** - mitigates the impact of a manifested threat. Had an incident how will we fix it

    - **Compensating** - provides alternative or temp fixes to any of the above functions when we can't do them the way we want
- **Ex of Security controls:**
    - Background check - administrative, detective
    - Employee training - administrative, preventative
    - Firewall - technical, preventative
    - Backup - technical, corrective
    - Warning Sign - physical, deterrent
    - Fence - physical, preventative
    - Closed Circuit TV - physical, can be detective or deterrent
- **Interesting Security Controls:**
    - **Mandatory Vacation** - requires individuals to take vacations usually at different times of the year to detect fraud and unauthorized activity
    - **Job Rotation** - Switching people to take on different roles in case someone get sick or leaves, another can cover temp. Also avoid preferential treatment
    - **Multi-person Control** - more than one person required to complete an action to prevent a single person from doing something bad or ensuring that things are done the right way by having different people involved in the task
    - **Separation of Duties** (Admin control) - single individuals should not perform all critical or privileged duties across the board. Don't intermix security staff with finance staff
    - **Principle of Least Privilege** - users are granted only the level of privilege necessary for them to perform their job. Need to know basis.
- **Redundancy** - have applied some type of security control over and over again almost always in some form of layered fashion in case one fails. Ex putting anti malware in different places like on computer software, then IDS, and Firewall ACL
- **Diversity** - having different forms and types of security controls which is **defense in depth**. Like having a cable modem ISP and DSL line as backup
    - **Vendor Diversity** - using different vendors for technical controls
- Use a variety of physical, administrative, and technical controls for defense in depth
    - Ex to prevent employees from using Facebook can have a technical control by blocking FB through firewall and Administrative control by having policy of not using social media during working hours
- Redundancy is repeating the same controls at various intervals, while diversity is using a variety of controls in a random pattern
- **Governance:** the set of overarching rules that define how an organization and its personnel conduct themselves
- **IT security governance** influences how the organization conducts IT security and is defined by:
    - **Laws and Regulations** - HIPAA
    - **Standards** - 1) Gov standards (NIST in US; ISO in Europe); 2) Industry Standards (PCI-DSS(Payment Card Industry Data Security Standard)
    - **Best Practices** - best way to do stuff like Microsoft best practices

    - **Common Sense and Experience** - what has worked in the past and what sounds right
- **Polices:** Document that defines how we're going to do something **like Acceptable Use Policy (AUP)**
    - Broad in nature (we will always use strong passwords)
    - Used as directives (we will do this)
    - Define Roles and Responsibilities (We will always have Chief Info Sec Officer)
- **Organization Standards:** Define the acceptable level of performance of policy. More detailed than a policy
    - Ex. Password must be 12 characters alpha numeric and changed every 3 months
    - Some organizations will incorporate standards into policies
- Security controls come from the policies and standards so usually not a big list of security controls as a separate item
- **Procedures:** step by step process of how you do something. How we do the task.
- Governance at its core is making the right set of security controls for your organization
- **Guidelines:** Optional ideas that don't need to be clearly defined that tells us how to do something
- **Policies, Security Controls and Standards** help define and build procedures
- **Acceptable Use Policy (AUP):** most well know and usually has to be signed. Defines what a person can or can't do when using company assets
    - Personal use of the computer, where you store stuff. Usually is broad since can't predict every little thing you can't or shouldn't do
- **Data Sensitivity and Classification Policies:** define the importance or nature of the data
    - Applying labels like confidential
- **Access Control Policies:** How to get access to data and or resources
    - How to use passwords and authentication
    - What type of data do users have access to
    - Job title what you can and can't do
- **Password Policy:** (Can be snuck into another policy)
    - Password recovery, bad login, password retention, password reuse
- **Care and Use of Equipment:** Focus on how you maintain, borrow, deal with broken equipment
- **Privacy Policies:** Applied to customers and in house. What they will do with your privacy
    - How your data or data usage will be shared with other resources
- **Personnel Policies:** People that are dealing with our data. Has to do with the person
    - Background checks, security clearance
- Make sure to memorize all these Policies as CompTia is big on them
- **Framework:** Very important. List of big things you go to do to provide good IT security to your infrastructure and come from a variety of sources like:
    - **Regulatory, Non-Regulatory, National Standards, International Standards, Industry Specific Standards**
    - NIST SP800-37 - 1st go to for Sec Professionals who want to understand how to perform a risk management framework. Can be regulatory and national standard

    - ISACA IT Infrastructure - non regulatory
    - ISO 27000 - International people all over the world can use
- **NIST RISK Management Framework:**
    - **1) Categorize Information Systems** - understanding and categorize workflow, vendors, processes, etc
    - **2) Select Security Controls** - look at everything and select what works for your infrastructure
    - **3) Implement Security Controls** - Actually performing the security controls
    - **4) Assess Security Controls -** Verify that everything works the way it's supposed to. Done through sandbox
    - **5) Authorize Information Systems** - Who makes the decisions and accepts the risk of implementing the security controls
    - **6) Monitor Security Controls** - Watch the control to ensure it's doing what it was designed to do and make a judgment
        - The monitoring allows you to go back and adjust the other steps to improve the process
- **Quantitative Risk Calculation:**
    - **Asset Value (AV)** - the upfront cost of the asset plus the cost if it malfunctions and what the cot per day would be if it stop working and generating profit for the company
    - **Exposure Factor (EF)** - Percentage of an asset that's lost as the result of an incident.
        - Ex. water damage on a router could cause an exposure factor of 1 while damage to a server room could be .75 since not everything could have been damaged
    - **Single Loss Expectancy (SLE) = AV x EF** (for any one particular incident)
        - Router completely lost to flooding with AV of $5000 and an EF of 1 = SLE of $5000
- **Annualized Rate of Occurrence (ARO):** In a given year what are the chances of this particular incident taking place
- **Annualized Loss Expectancy (ALE) = SLE x ARO**
- **Mean Time to Repair (MTTR)** - Time asset takes to be repaired (things that can be repaired)
- **Mean Time to Failure (MTTF)** - Time an asset takes to fail (applied to things that can't be fixed)
- **Mean Time Between Failures (MTBF)** - Time between an asset failing, being repaired, and failing again (usually applied to something that can be repaired)
- **Business Impact Analysis (BIA):** the study and analysis of the impact on your organization
    - **1) Determine Mission Processes** - things done within the IT infrastructure to keep things going well that are mission essential. Like making sure internet is always up if you have a web server business
    - **2) Identification of Critical Systems** - certain pieces of equipment are important to keep the processes working. Like making sure cable modem and server is working properly
    - **3) Single Point-of-Failure** - avoid by using redundancy and defense in depth. Like having 2 ISPs and having backups

    - **4) Identify Resource Requirements** - what do I need for all these type of resources. Like for all these files we need a server
    - **5) Identify Recovery Priorities** - priorities for system resources like if everything goes down what are the priorities, the steps needed to run the best. Like make sure ISP is running, the server is working
- **Impact:** Things that can impact the company
    - **Monetary Loss**
    - **property** - tangible things like building, hardware
    - **People** - safety, life, make sure people aren't getting hurt
    - **Finance** - credit, cash flows, accounts receivable
    - **Reputation** - hard to measure in dollars. Privacy is a big killer of reputation
        - **Privacy Impact Assessment (PIA)** - impact if privacy being protected would get out in any way. What laws, regulations, obligations would run into.
        - **Privacy Threshold Assessment (PTA)** - an assessment to determine what, where, how are you storing data so usually PTAs are in-house
        - PDA and PTA are both done to understand what the impact of the loss of personal information can do to a particular business
- **Recovery Time Objective (RTO)** - min time necessary to restore a critical system to operation
    - And the max time a critical system can be down without substantial impact
- **Recovery Point Objective (RPO)** - Max amount of data that can be lost without substantial impact
- **Data Sensitivity/Labeling** - all the different data that we are in control of has a different amount of importance
    - **Public** - has no restrictions; within the public domain
    - **Confidential** - limited to authorized viewing as agreed on by the parties involved. (**Non Disclosure Agreement (NDA)**)
    - **Private** - Limited to only the individual to whom the info is shared to like SS #
        - **Personally Identifiable Information (PII)** - Name, address, phone and ss#
    - **Proprietary** - like private but at corporate level (info that gives company competitive advantage like soda formula)
    - **Protected Health Information (PHI)** - deals with the health of an individual like **Health Insurance Portability and Accountability Act (HIPAA)**. Usually includes some PII
- **Data Roles:** Who's in charge of a particular system
    - **Owner** - person who has legal responsibility so can be a corporation
    - **Steward/Custodian** - someone who's job is to maintain the day to day care of the accuracy and integrity of the data
    - **Privacy Officer** - Person who is in charge of ensuring data adheres to privacy policies and procedures
- **Data Users:** User roles
    - **Users** - assigned standard permission to complete task. How data functions and common problems. Just enough permissions to complete task

    - **Privileged Users** - Increase access and control relative to a user. See more data and have more control than a user
    - **Executive Users** - Makes strategic decisions. Set policy on data and incident response actions
    - **System Administrator** - will have complete control of data. In charge of the day to day manipulation and administration of that data set. Also one who sets permissions for users and privileged users
    - **Data Owner/System Owner** - People or Organizations who have legal ownership of the data set or system
- **Onboarding:** Bringing someone new into the organization like new hires or contractors, temp workers
    - Background checks, **Non Disclosure Agreement (NDA),** standard operating procedures, specialized issues, Rules of behavior (AUP), General Security Polices
    - Good to give refreshers and updates to keep things fresh
- **Offboarding:** processes of when someone leaves the company
    - Disable accounts - never delete account
    - Return credentials
    - Exit Interview - important for knowledge transfer to find out where data is stored, and other pertinent information
- **Personally Identifiable Information (PII**) - NIST SP 800-122 gives good detail
    - Full name, home address, email address, national ID # (SS#), passport #, vehicle registration #, driver's license #, face, fingerprints or handwriting, credit card #, digital identity, date of birth
- **Personnel Management Controls** - how we deal with what people do in terms of their work to be able to keep our infrastructure as secure as possible
    - **Mandatory vacations** - required usually 2 weeks in a row, dependency issues, makes fraud harder, prevents collusion
    - **Job Rotation** - redundancy and backup, makes fraud more difficult, allows for cross training
    - **Separation of Duties** - requires dual execution
- **Role-based Data Controls**
    - **System Owner** - management level role job is to maintain security of the system, defines a system admin, works with all data owners to ensure data security
    - **System Administrator** - Day-to-day admin of a system, implement security controls
    - **Data Owner** - person in charge of the system, defines the sensitivity of the data, defines the protection of the data, works with the system owner to protect data, defines access to the data
    - **User** - common folks, access and uses the assigned data responsibly, monitor and report security breaches
    - **Privileged User** - has special access to data beyond the typical user, usually a manager, works closely with system administrators to ensure data security

    - **Executive User** - Read only access to all the business data
- **Third Party agreements**: used when dealing with 3rd parties in many situations 4 common ones
- **Business Partners Agreement (BPA)** - Most generic doc of an agreement between parties to do business. BPAs are very common
    - **1) Primary Entities** - partners that are going to be working together
    - **2) Time Frame** - Ongoing, dissolution
    - **3) Financial Issues** - how much investment is each partner putting in
    - **4) Management** - Functions of those partners, when partners meet, and type of records keeping as well as the location of all partnership records
- **Service Level Agreement (SLA)** - agreement between entity getting service and service provider
    - **1) Service to be provided** -by whom, what, when
    - **2) Minimum (sometime max) up-time** - discuss penalties cost for not achieving these
    - **3) Response Time** - time service provider takes to rectify situation if there's an issue. Also who the contact is
    - **4) Start and End date** - of the service being offered
- **Interconnection Security Agreement (ISA)** - Got name from NIST 800-47. Quantify how 2 **government entities** can make data interconnections in a safe and secure way. **Technical document** so will not display who's in charge or costs
    - **1) Statement of Requirements** - Why, who are we connecting
    - **2) System Security Considerations** - What info is interconnecting; where is the info going; what services will be involved(http, email, etc); what encryption is needed
    - **3) Topological Drawing** - Show location connections and points, IP addresses, CSU/DSU, etc
    - **4) Signature Authority** - timeframe for this interconnection; scheduling technical and security reviews for that interconnection
- **Memorandum of Understanding/Agreement (MOU/A)** - used to **reinforce ISA. Not a contract**
    - **1) Purpose of the Interconnection** - why this happening
    - **2) Relevant Authorities** - who are the people in charge
    - **3) Specify the responsibilities** - define downtime, billing, legal issues
    - **4) Define the terms of the agreement** - cost
    - **5) Termination/Reauthorization** - on as needed basis
- BPAs and SLAs are used in the private sector
- ISAs and MOU/MOAs are used in the public sector

Section 2: Cryptography

- **Cryptography** is done to provide confidentiality through obfuscation and bringing it back to its original form
    - The practice of disguising information in a way that looks random
- **Obfuscation**: take something and hide it by changing it in a form that is unrecognizable to the casual outside observer
    - **Diffusion** - make something less visible and obvious
    - **Confusion** - stir up and scramble something to make it confusing
- **Encryption/Decryption** - creating cryptography through obfuscation and bring it back to its original form
- **Caesar Cipher**: Uses 2 sets of alphabet letters where the second set is rotated and used as **substitution** to create a cipher
    - ROT2 - Rotate the letters 2 times forward (ROT3 - turn 3 times)
    - Easy to crack with cryptanalysis
- **Cryptanalysis** - breaking encrypted codes
- **Vigenere Cipher**: Caesar Cipher using all the possible ROT values and a word key to make it more challenging to crack and uses classic cryptography components
    - Works great for letters but terrible for encrypting numbers, pictures, binary data
    - Also crackable
- **Classic Cryptography Components**: 1) **Algorithm**; 2) **Key for encryption**
- Need algorithm for binary data
- **Exclusive OR (XOR)** - used to encrypt binary
- **Kerchoffs's Principle** - As long as you don't know what the key is to an encryption, you can actually understand the algorithm completely. If you don't know how the lock works, then you can't test it to see if it actually works
- **Data at Rest** - Something stored on a hard media usually encrypted
- **Data in Transit** - data that's moving (issue is should this data be encrypted?)
- **Data in Process** - sitting in ram or CPU being used
- **Symmetric Encryption**: uses the same key to encrypt and decrypt a message
    - Issue is how to send key
    - **Session key** - used for an instance to encrypt/decrypt
    - **In-Band** - send the key with encrypted data (very risky)
    - **Out-of-Band** - send it directly like personally give (defeats the purpose of encryption)
    - The primary way to encrypt data despite its issues
    - **Ephemeral Key** - temporary key, provides perfect forward secrecy due to the temporary nature of the key
- **Asymmetric Encryption**: Uses a key pair known as a Public Key and a Private Key
    - **Public Key** - given to anybody. Usually used to encrypt data

    - **Private Key** - stored privately and safeguarded. Only used to decrypt
    - Used for sending a secure session symmetric key
    - Issue is its slow
- **Cryptosystem** - highly defined process that programs do to make cryptography work in the I.T. world
    - define key properties, communication requirements for the key exchange and the actions taken through encryption and decryption process
- **Algorithms**: 1) Have to be known to everyone 2) Have a key of different lengths and kept secret
- **Symmetric Key Algorithm** - uses the same key to encrypt and decrypt
    - **Symmetric Block Algorithm** - encrypts in block sizes
        - **Data Encryption Standard (DES)** - 1st open standard still. Block Cipher, 64-bit block size, 16 rounds, 56-bit key, hackable
        - **3Des** - Block Cipher, 64-bit block size, 16 rounds, 56 x 3 = 168-bit key, Repeats the process 3 times increasing key size
        - **Blowfish** - Block Cipher, 64-bit block size, 16 rounds, 32-448 bit key
        - **Advanced Encryption Standard (AES)** - Still unhackable and supported by NIST. Block Cipher, 128-bit block size, 10, 12, or 14 rounds, 128, 192, or 256 bit key
    - **Streaming Ciphers** - encrypts 1 bit at a time through the stream. Only 1 type
        - **RC4 (Rivest Cipher 4)** - 1 bit at a time, 1 Round, 40-2048 bit key
- **Electronic Code Book (ECB)** - Every block that's the same length and is encrypted with the same key has the same output so patterns start to appear and it's an issue with symmetric block encryption therefore don't use with symmetric encryption. Not used anymore
- **Block Modes** - used to obfuscate the data better. Encrypt something, and then use that to help encrypt the next thing so ends up like a chain
    - **Cipher Block Cleaning (CBC)** - Before encryption, uses an XOR against an **Initialization Vector (IV),** which is the same size as the blocks, then keep a copy to use for the next block causing data cipher to change
    - **Cipher Feedback (CFB)** - Encrypts IV and then take output and XOR to the first block and then use that for the next block
    - **Output Feedback** - Similar to CFB but uses same IV each time
    - **Counter (CTR)** - Uses nonce value plus counter value that continues to increment in binary then gets encrypted, then XOR. For the next block the counter gets incremented
- **Asymmetric Key Algorithms**: Use a key pair consisting of a public key to encrypt and a private key to decrypt
    - **RSA (Rivest-Shamir-Adleman)** - 1) Specifies how key pair is generated; 2) How public key will be sent to people
        - Takes 2 large prime numbers multiplied together to generate a semi prime number to use to generate initial key pair

        - Use at least 2048 bit key nowadays
    - **ECC (Elliptic Curve Cryptography**) - provide small keys but same robustness as large number RSA keys and faster going through encryprion/decryption process
        - Formula: y^2 = x^3 + ax + b to generate key pair
- **Diffie-Hellman**: Key Exchange Protocol. Uses asymmetric that provides methodology for 2 parties to come up with the same session key using modular arithmetic and without the overhead of RSA
    - Uses groups to increase effectiveness. Group 1 - 768-bit modulus; Group 2 - 1024-bit modulus…Group 21 521-bit elliptical curve
- **PGP (Pretty Good Privacy):** Invented for email encryption but has evolved for signing files, encrypt files, discs
    - Encryptor generates a random key to encrypt data, then encrypts the key using the receivers public key
    - Receiver then decrypts using private key to obtain random key which is then used to decrypt data
    - Uses PGP certificate and web of trust but now use PKI
    - PGP Certificates:
        - Symantec Corporation - Encrypts mass storage, signing, disk encryption, bitlocker, enterprise cloud solutions, not free so proprietary
        - Open PGP- Free, encrypted email (Proton Mail), PKI support, S/MIME
        - GPG (GNU Privacy Guard) - free toolset based on Open PGP. Does file and disk encryption
- **Hash**: Provides integrity when it comes to the CIA of security. It's an algorithm that provides a fixed value every time and if the data is changed in any way, the hash will be different
    - Hashes are 1 way, deterministic, and will produce the same result each time the source is hashed
    - Used for password storage on drives to verify, encryption
    - It doesn't matter how long the source data is, the hash will be the same exact size depending on the bit size
    - **MD5 (Message Digest 5)** - older, 128-bit hash. Issue will generate collisions meaning will generate same hash for 2 different sets of data making it prone to decipher. Not really used anymore
    - **Secure Hash Algorithm (SHA)** - Developed by NIS
        - **SHA-1** - 160-bit hash, prone to collisions, not really used anymore
        - **SHA-2** - Broken down into bit sizes ex. SHA-256 or SHA-512. No collisions detected yet
    - **RIPEMD (RACE Integrity Primitives Evaluation Message Digest)** - Not common, open standard, 128, 160, 256, 320 bit digests
- **HMAC (Hash Based Message Authentication Code):** HMAC provides message integrity and is based on standard hashes but also requires each side of the conversation to have the same key as it generates the hash using the key as well

    - Only way to get message is if someone has your key
- Freeformatter.com has HMAC generator
- **Steganography**: the process of taking data and hiding it in other data like hiding text in graphic images that may or may not be encrypted
- Image Steganography tool to embed text in images
- Problem with asymmetric encryption is the key exchange. How do you know where the public key came from and is it from the person you think it is
- **Digital Signature**: a hash to verify data and public key coming from the matching private key
    - Can take private key and encrypt a webpage, create a hash value for the encrypted web page and send that over with public key so that receiver can verify that public key came from that specific private key by encrypting site with public key and verifying that both hash values match
    - still can't fully verify that it really is coming from that specific website like spoofing or stealing another websites certificate, so **Certificate Authorities (CA)** or 3rd parties are used to check validity of digital signatures
- **Digital Certificate**: Document that encloses the public key, digital signature, and trusted 3rd party digital signature which can be sent to anyone
    - **3 Ways to do trust:**
        - **1) Unsigned Certificates** - generate your own certificates on your own without 3rd party. Usually used for in-house where people know each other so there's trust
        - **2) Web of Trust** - have a lot of people that trust each other that creates a web of mutually trusting peers. Issue requires a lot of work to administer and cannot really automate
        - **3) PKI (Public Key Infrastructure)** - based on the idea of a hierarchy with Certificate Authority (CA) with root servers at the top, in the middle Intermediate CAs to help take the load off the CAs, and at the bottom the users
- **Certificate Authority (CA)** - Very trusted organization that issues certificates. Usually large companies like Godaddy, Verisign and Thawte
    - At the top there is a root certificate system for a company that stores 1 root certificate that distributes certificates to intermediate systems so want root certificate protected so the users access the intermediate certificates through the certification path
- **PKI (Public Key Infrastructure):**
    - PKI is about trust, distribution, control, maintenance, and relocation when it comes to digital certificates
- **PKCS** - de facto standard for a lot of PKI systems
    - **PKCS-7** is a way to store certificates as individual files
    - **PKCS-12** stores the certificate and the private keys as a package

- **X.509** - PKI based on this standard that determines how to query a database if your far away and how to organize data in hierarchies to access on a timely basis
- Certificates usually already come with web browsers both root and intermediate and usually get updated with browsers
- Can export certificate for a backup but not done often
- **CRL (Certificate Revocation List)** - a path to quickly access URL to verify validity of certificates and react to bad certificates but take long to do as **not real time**
- **CSR (Certificate Signing Request)** - specially formatted encrypted message sent from an SSL digital certificate applicant to a CA. The CSR validates the information the CA requires to issue a certificate.
- **Online Certificate Status Protocol (OCSP)** - similar to CRL but **real time**
- Passwords are not stored on a hard drive, it just stores a hash of the password so password **attacks are typically trying to hack hashes**
    - 1) Have to get to list of hashed passwords
    - 2) Can't reverse hash, so do comparative attacks where hashes are generated and compared with stored hash to obtain password
- **Brute Force Attack** - attack where attempt different passwords to guess right one
    - Cain and Abel program used for brute force attack but outdated. Would input hash to try and guess password
    - The longer the password and more complex, the harder to crack in brute force attack
- **Dictionary Attack** - uses a text file that is filled with dictionary words which will be manipulated to try and guess password which speeds things up since people use words so it's easy to remember
- **Rainbow -Table Attack** - pre-generated index hash table. Massive huge files in the terabytes. Used for more challenging passwords
- Most good password storages manipulate the hash in some way to obfuscate and make it harder to crack like using Salt
- **Salt:** an arbitrary value added to data like a password and then hashed creating salted table which are a lot harder to crack
- **Key Stretching** - takes password and adds other values to generate a very complicated key that can then be hashed or passed through the internet. Currently uncrackable. 2 types:
    - **WPA** for wireless which uses key stretching technique PBKDF2 algorithm
    - **Bcrypt**

Section 3: Identity and Access Management

- **Identification, Authorization, Authentication**
  - I**dentification** proves who I am to the authenticating system
  - **Authentication** occurs when proving that I have rights to the system through passwords, smart cards, etc
  - **Authorization** means what rights do I have to the system
- **Authentication Factors**
  - **Something You Know:** Password, pin, captcha, security questions
  - **Something You Have:** Smart card, RSA key
  - **Something About You:** Biometrics like fingerprint scanner, retinal scanner, vein patterns, iris scanner, facial recognition
  - **Something You do:** Rhythm of typing, way you sign
  - **Somewhere You Are:** Credit cards can use to detect fraud by seeing your location
- **Federated Trust:** Can create authentication based on trust so if you're authenticated in one system, you no longer need to re-authenticate for other systems in the trusted network
- **Multifactor Authentication:** Use 2 or more different authentication factors like a password and fingerprint scanner
- **Authorization:** Defines what a particular person can do within a system
  - **Permissions** - what are the things that are assigned to you that you can use. They are assigned to resources
    - Administrator assigns permissions and usually users are put into groups when assigning permissions
  - **Rights/Privileges** - Assign to systems as a whole for instance can you login only locally or can you log in remotely. Can you change your username or password
- **Least Privileged Separation of Duties:** Are two authorization strategies
  - **Least Privileged** - give users/groups the least amount of privilege they need to get the job done
  - **Separation of Duties** - Making sure certain permissions are separated from certain job positions to avoid conflict of interest
- **Access Control List (ACL):** Define access. 3 types of authorization models
  - **Mandatory Access Control (MAC)** - used a labeling system for types of data one can access like confidential or top secret but ineffective
  - **Discretionary Access Control (DAC)** - Owner of the data defines who can access. Doesn't allow for roles
  - **Role-Based Access Control (RBAC)** - Access to resources is defined by a set of rules for a given role like Groups in Windows

- **ACL Implicit Deny** - unless you specifically allow something to happen, it's not going to happen so need to specify "permit" ex. 10 permit 192.168.1.35 0.0.0.255 any
- Good **Security Policy for password security**
    - **Complexity** - length and character requirements
    - **Expiration** - Reset and time triggers
    - **Password History** - Re-usage and retention
- **Windows Local Security Policy:** (can also do on other OS)
    - Can manage under "Password Policy" set password length, special char, etc
    - "Account Lockout Policy" set lockout duration, threshold, reset lockout counter
- **Group Policy Objects** - on Windows Directory allows you to set security policies on many devices under "Group Policy Management"
    - Can be applied to domains, individual sites, groups, organizational units
- **Linux File Permissions**
    - ls -l : shows list of files and begin with "rwx" which are the permission for that file
    - **First "rwx"** permissions for the **creator/owner**
    - **Second "rwx"** permissions for the **group**
    - **Third "rwx"** permissions for **everyone else**
    - **r = read:** allows you to open file; in directory view contents
    - **w = write:** allows to edit a file; in directory allows add or delete files
    - **x = execute:** allows you to run a file or script; directory allows to change directory and make current working directory
    - **chmod (Change Mode)** - command to change file or folder permissions
        - chmode o(for other)=(turn off all permissions)RunMe(name of exe/file)
            - or: chmode 770 RunMe
        - chmode g(for group)=rx(read and execute) RunMe(name of exe/file)
            - or: chmode 750 RunMe
        - chmode a(all or everybody)=rwx(read, write, execute) RunMe(name)
            - or: chmode 777 RunMe
    - sudo chown root RunMe (allows you to change the owner of a particular folder or file in this case change to "root" Also needs to run as admin so use "sudo")
    - sudo passwd (changes user password)
- **Windows File Permissions: NTFS Permissions** (not on FAT32)
    - Read and Execute - applies to .exe files and allows to run
    - Windows Best Practice allows you to create groups and then give permissions to those groups on a per folder basis
        - under "Folder Properties" then "Security" tab hit "Add" and enter Group name and then select permissions
    - **Inheritance** - Any permissions that you set for a folder will automatically transfer the NFTS permissions to new subfolders or new file within that folder
    - Creator of folder can setup permissions

    - **NFTS Permissions - Folder**
        - Full Control - anything you want
        - Modify - read, write and delete files and subfolders within that folder
        - Read/Execute - see contents of folders/subfolders and run programs
        - List Folder Contents - see content of folders/subfolders
        - Read - view contents and open data files
        - Write - write to files and create new files and folders
    - **NTFS Permissions - File**
        - Full Control - anything you want
        - Modify - read, write and delete the file
        - Read/Execute - open and run the file
        - Read - open the file
        - Write - open and write to the file
    - Deny is stronger than allow usually used to remove inheritance
    - Fat32 doesn't support NTFS permissions
    - Copying or moving from one drive to another will take on the NTSF properties of the destination drive so will not transfer permissions from original drive
    - Copying within the same drive will also lose NTSF properties of the original file
    - Moving within the same drive will keep the NTSF properties
- **Continuous Access Monitoring (CAM):** You should be monitoring 24/7 what your users are getting into to have an idea of what's going on within your infrastructure
    - Track log on/log off activity, and track of file access
- **Shared Accounts:** Bad thing and people being lazy
- **Multiple Accounts:** Sometimes a requirement
    - Use different user names and passwords
    - use different groups and monitor which users belong to which groups
    - Use least privilege - enough necessary to accomplish task
    - Monitor and log activity of users with multiple accounts
- **Default Accounts:** always change default/generic accounts and use dedicated service accounts
- **Authentication, Authorization, Accounting (AAA):** 2 ways to do it
    - **RADIUS** (Remote Authentication Dial-In User Service) - Designed to support dial-in networking
        - RADIUS server sitting inside network that can be active directory, user names&passwords, or connected to a database
        - RADIUS client which is a gateway between supplicant and server
        - RADIUS supplicant is user trying to get authenticated
        - RADIUS **used in wireless authentication**
        - Security Policy - RADIUS used for network access, **can use up to 4 UDP ports: 1812,1813,1645,1646**

        - Downside is it **doesn't really handle authorization** by itself. You're either in or you're out
    - **TACACS+** (Terminal Access Controller Access-Control System Plus) - form of AAA and **is very good at managing multiple devices**
        - **Takes care of Authorization really well** by defining what you can do
        - Decouples the authorization from the authentication
        - **Uses TCP port 49**
    - Both do Accounting really well through auditing for log files
- **Authentication Methods**
    - **Password Authentication Protocol (PAP)** - Oldest method. It sends username and password in the clear. Not secure
    - **Challenge-Handshake Authentication Protocol (CHAP)** - Old, first used in PC with some form of protection
        - Server and client have key stored, client sends request and server creates challenge message by creating hash with key and challenge message to authenticate so only hashes are sent. Still used in some situations
    - **NT LAN Manager (NTLM)** - Still used for basic stuff without domain controller. Currently at Version 2
        - Initiate handshake then each side generates challenge message and hashes with key that way each side challenges each other
    - **Kerberos** - **Only used authenticating to Windows domain controllers** but widespread popularity is high.
        - **Domain Controller (DC)** known as **Key Distribution Center (KDC)**
            - Has authentication service and ticket granting service
            - **Listen on TCP 88**
        - Client logs in and is given **Ticket Granting Ticket (TGT)** (aka SID (Security Identifier)) shows authenticated to the domain
        - **TGT is taken to DC Ticket Granting Service** and it knows what you're allowed to access with given logins **and generates Session Key**
        - **Session Key** allows access to a particular set of resources
    - **Security Assertion Markup Language (SAML)** - Not authentication but used for web applications to login into that app
    - **Lightweight Directory Access Protocol (LDAP)** - Not authentication but more of a structured language that allows one computer to go into somebody else's active directory and query it, update it, and other actions. Used a lot.
        - **TCP/UDP 389**
- **Windows Active Directory** (comes with Windows Server) used for **Single Sign-On (SSO)** in LANs
    - Computers within the same domain creates a trust situation or Federated System

- **SAML** - designed for web apps for single sign on for many devices in one instance
    - Have an Identity Provider for signing in that provides tokens to access different devices called Service Providers

Section 4: Tools of the Trade

- **Ping:** CMD prompt. Ex: >ping www.totalsem.com
  - >ping {url} -4 -pings with IPv4
  - >ping -t {url} -pings indefinitely (Don't need to use in Linux since default in Linux)
  - Use to check if DNS is working and resolving name to IP
  - Can I connect to somebody
  - Layer 3 issues allows to separate between IPv4 and IPv6
  - Check intermittent connection
- **Netstat:** know what sessions a particular host is running at any given moment
  - >netstat -n -Who am I talking to. -n displays ports
  - >netstat -a -Who's trying to talk to me. -a show me all open ports including the one's I'm not connected to. Can also do -a -n
  - **Shows all the network communications for host**
- **Tracert:** Allows you to trace the route from your network to external network
  - >tracert www.totalsem.com
  - If an issue on the first 2 routes, means you have an in-house problem since first route is your router and 2nd your ISP
  - If issue is a few routes later, than can be an issue with ISP so external and can't really do much to fix
  - **Maps out every router along the path to the destination**
  - Takes advantage of ICMP Time to Live (TTL) error message but some firewalls filter ICMP so might not return anything displaying "*"
- **ARP:** Run if suspect someone is messing with your switches like ARP poisoning
  - Resolves an Ethernet MAC address from an IP address
  - >arp -a -**use to view ARP cache (table)**
- **IPConfig** (ifconfig on Linux): Who am I and how am I configured. >ipconfig
  - **Gives you hardware and network information**
  - Have to know your network
  - >ipconfig /all -also shows MAC address
  - Shows DHCP issues
  - ip addr (linux) shows IP address and other info
- **NSlookup** (dig on Linux): Troubleshoot DNS issues. Has been shut down due to people exploiting tools
  - **Lookup information from DNS servers like Canonical names, IP addresses, cache timers, etc.**
  - >nslookup www.totalsem.com -Shows what DNS server using and what IP address for site entered
  - Query your DNS server to check if it's working

    - nslookup -> server 8.8.8.8 -changes DNS server to specified address
    - dig @8.8.8.8 {address or url} -changes DNS server on Linux
    - dig mx {url} -queries mail server
- **Netcat** (Linux): Does anything utility wise on Linux. **Can open and listen on ports** and it **can also open and act as a client on just about any port you** want
    - Read or write to the network
    - sudo netcat -l 231 -opens port 231 as a listening port
    - ncat 10.1.10.222 80 "enter" GET / HTTP/1.0 - gets info on web server
    - Can open port as a client which can be used in an aggressive fashion
    - Can be used to setup backdoor
- **Network Scanners**: sniff a network
    - Looking for open ports on various machines on network to either close and protect or exploit open ports
    - Network Inventory to see what devices are connected
    - Rogue Systems - systems that shouldn't be on the network
- **Nmap:** Need to install. Used for scanning networks, looking for attackers, inventorying of networks
    - **Network mapper, port scanner, OS scan, service scan**
    - >nmap -v -sn {local network} -v verbose output;
    - >nmap -v -A {url} -zero in on one particular computer
    - Nmap allows you to go in and query a system so you can then attack with something else
- **Zenmap:** GUI overlay that runs on top of Nmap
- Scanners usually set off IDSs since they're very noisy tools
- Advanced Port Scanner free tool that also scans networks
- **Protocol/Network Analyzers** allows you to monitor network traffic
- **Wireshark:** Free **Network Analyzer**.
    - Uses sniffer that grabs all the data going in and out of a particular interface
    - **Sniffer** will save into a file or make a live feed into the protocol analyzer
    - Protocol Analyzer reads data in displays it in a format we can look at
    - Very good at filtering data by services and protocols
    - Good at detecting rogue DHCP servers, ARP poisoning, broadcast storms
    - Issue misses a lot of incoming and outgoing traffic
- **TCP dump** (Linux only): Slim and works better than Wireshark at sniffing packets from a particular host (**Network Analyzer**)
    - Capture packets from the command line and allows to apply filters and view in real-time
    - Written in **pcap** format that can be sent to a program like Wireshark to analyze
    - sudo tcpdump -command to run

- **Simple Network Management Protocol (SNMP):** Tool which allows us to administer and manage network devices from hopefully a single source where we can do whatever we need to do
    - **Agent** - software built into a device from the factory that gives it the ability to do SNMP
        - Agent uses UDP 161, TLS UDP 10161
    - **Managed Device** - device capable of communication via SNMP
    - **SNMP Manager** - system that communicates with Managed Device
    - **Network Management Station (NMS)** - Device usually running some type of software or utility that's an SNMP tool
        - **NMS uses UDP 162, TLS UDP 10162**
    - **Management Information Base (MIB)** - database we query to talk to that particular device as different devices perform different tasks so have different MIBs. Also built in from the factory
    - Download command set that allows to query every particular device
    - **Get** - standard query consists of an NMS sending message to Managed Device and that device sends back a response like how many pages have been printed
    - **Trap** - Setup on the Managed Device that sends a trap message to the NMS when it hits a particular value like printer has low ink
    - **Walk (SNMPWalk)** - batch process of Gets to query multiple messages
    - **3 Versions of SNMP**
        - SNMP version 1 - Limited command set and does not support encryption
        - SNMP version 2 - Expanded command set and added basic encryption
        - SNMP version 3 - Added TLS encryption
    - 1 NMS can talk to all versions of SNMP so can have devices with different versions
    - An SNMP community is an organization of managed devices so can set a community of all Finance devices
    - **RO (Read Only)** - Cannot make changes
    - **RW (Read Write)** - Can make changes
    - Cacti is an open source NMS for graphing SNMP data but difficult to setup
    - Nagios, Zabbix and Spiceworks are other good NMSs
- Logs can be called Event Logs, Security Logs, etc
- **Non-Network Logs:** Logs events that happen on a host even though it's not connected to the network
    - **Operating System Events** - host starting, host shutdown, reboot, services starting, stopping, failing, OS updates
    - **App Events** - app installation, app starts, stops, crashes

    - **Security Events** - logons, logon successes and failures
    - Would have date, time, process/source, account, event number, event description
- **Network Logs:** Logs events that deals with the communication between the host and something on the network
    - **OS or System Level Events -** Remote logons (fail or not),
    - **Application Level Events** (big one on exam) - activity on web server, activity on a firewall
    - Date, time, source address (MAC, IP), destination (MAC, IP), description of what's happening
- **Decentralized Logging** - each device has its own place of storing log files so need to access each device to obtain logs
- **Centralized Logging** - Logs are centralized. 2 ways of doing it
    - 1) All devices send logs to a central repository. Can slow down network and drag system
    - 2) Use SNMP system which pulls info needed and generates graphs and charts
- **Monitoring as a Service (MaaS)** - 3rd party manages and maintains your logs

Section 5: Securing Individual Systems

- **Denial of Service (DoS) Attack:** Designed to deny service. 1 attacker
    - **Volumetric Attack** - overloading the system
        - **Ping Flood** - keep sending pings to overload the server
        - **UDP Flood** - sends strange UDP requests to different kinds of port to overwhelm server
    - **Protocol Attack** - Does something not normally accepted by the protocol to slow it down
        - **SYN Flood/TCP SYN Attack -** Continues to send SYN requests while ignoring SYN ACKS causing server to overload (most common form of attack)
    - **Application Attack** - Works within the application to keep it from responding it a timely fashion
        - **Slow Loris Attack** - Client initiates conversation but doesn't respond to server and continues to make requests without responding back so server continues to wait causing it to overload (can lower timeout value to prevent)
    - **Amplification Attack** - Smurf Attack sends ICMP packet, then spoofs website IP address to send out a broadcast into the network and then everyone responds back to the target causing it to overload
- **Distributed Denial of Service (DDoS) Attack**: Many computers attack a system using malware that generates a **BotNet** by turning infected computers into **Zombies** (Currently a big issue)
- **Spam:** Unsolicited email. Normally just an irritant
- **Phishing:** Spam that's trying to get info out of you. Can mimic a legitimate site
- **Spear Phishing:** Tries to get personal information out of you and is directed at you
- **Whale Phishing:** Targeting someone important like executive
- **Spim:** Receive spam via instant messaging
- **Vishing:** Unsolicited use of voice to get info out of you (huge fraud issue)
- **Clickjacking:** Gets you to click to activate malicious code on a website
- **Typo Squatting:** Take advantage of people mistyping URLs and leads you to a malicious site
- **Domain Hijacking:** Forgetting to renew your domain and someone buying it out and then blackmailing you to buy it back from them
- **Privilege Escalation/Elevation:** Getting enough power on a system to attack
- **Man In the Middle Attack(MTM):** 3rd party sneaking in between a conversation
    - Use the info to the 3rd party's advantage
    - Wireless man in the middle easy to do since wireless network is open unless you use encryption and or WPA/WPA2
    - Bluetooth susceptible but close proximity makes it difficult
    - NFC also susceptible but close proximity also issue for MIM
    - Wired MIM requires spoofing so system is tricked into thinking part of network or rerouting traffic to attacker

        - MAC Spoofing - trick the switch into thinking part of the connection
        - IP spoofing - trick router into thinking part of the network
    - **Ettercap** free program allows you to do spoofing called poisoning and also grab data for analyzing
    - Purpose of MIM is to gather data (user names, passwords, etc)
    - Can use Wireshark to grab data
    - **ARP Poisoning** - lies to the other systems confusing ARP cache (not the switch) so traffic is sent to attacking device thinking it has the correct IP
    - **DHCP Spoofing:** Poison the DNS by changing it with DHCP tool to spoof DNS servers and have request go to rouge DNS server that point user to a malicious site
    - MIM allows **Replay Attack** which allows to obtain username and password hash
    - **Downgrade Attack** - Convince web server to downgrade security by tricking it that client doesn't support the stronger security protocols
    - **Session Hijacking** - get in the middle of a live communication and inject something malicious
        - Firesheep allows to connect to wireless unencrypted connection and manipulate session
- **Man in the Browser (MITB) Attack:** Internet threat related to MIM where a proxy Trojan horse infects a web browser by taking advantage of to modify web pages, modify transaction content or insert additional transactions, all in a completely covert fashion invisible to both the user and host web application
- **Resiliency** is the ability of something to withstand a negative impact
- **System Resiliency:**
    - **Scalability** - we can add more resources to meet the demands
    - **Elasticity** - Be able to adapt to the demand by adding resources while demand is high and lowering resources as demand drops
    - **IaaS** and **SaaS** allows for scalability and elasticity
    - **Redundancy** - Have multiple instances of something in case one fails or to help distribute load
    - **Non-persistence** - Don’t make things permanent so can make changes
        - **Snapshot** - take the current state of something at a binary level and keep a copy of it
        - **Known State** - revert back to a known state like removing a windows update
        - **Rollback** - small part of the system like rolling back a driver or an application that lets you go back to a previous version
        - Run from live boot media
- **RAID** (Redundant Array of Independent Disks): Primary way that we provide security to our stored data systems. Use multiple hard drives that will work together to act as one hard drive to do one of two things.
    - **1) Provide some form of data integrity** if one drive dies and another one will take up for it

    - **2) Improve access** and in some cases we can actually do both at the same time
    - **RAID 0** (Striping) - Increase the speed you can get data but has **no data integrity**. Does this by dispersing data through multiple drives. Downside is if 1 drive fails, all data is lost
    - **RAID 1** (Mirroring) - Even number of drives where same data is saved on different drives. Doesn't change performance but **has data integrity**
    - **RAID 2-4** - Min of 3 drives. Disperses data between 2 drives and crates a mathematical formula called a parity on 3rd drive in case data is lost on 1 drive, it can recover it using the Dedicated Parity Drive
    - **RAID 5** - **Min of 3 drives.** Generates parity value and can be distributed to any drive so specific parity drive not needed. **Can lose 1 drive.**
    - **RAID 6** - **Min of 4 drives**. Makes 2 parity values so **can lose 2 drives** without issue
    - **Hybrid RAID** - Combines different RAID types
        - **RAID 01** (0+1) - Mirror of stripes. Min 4 drives. Send data to 2 sides and mirror it
        - **RAID 10** (1+0) - Stripe of mirrors. Min 4 drives. Stripe data
    - Most common RAID styles are 0,1,5,10
- **Proprietary Drives:**
    - **Synology hybrid RAID** - boxes build with drives accessed through web page
    - **Windows Storage Spaces**
- Different levels of RAID increase disk access and or they improve fault tolerance/data integrity
    - **Network Attached Storage (NAS):** File based sharing protocol specifically used for storing and accessing data. **Works at file level** and treats everything like network share
    - Runs over a standard network
    - Shows up as normal shares on network
    - FreeNAS free software to setup a NAS and SAN
    - Popular for small work groups
- **Storage Area Network (SAN): Provides block level storage**. No network shares provides fast powerful storage and basically adds a drive to your system
    - Runs on **Fibre Channel (FC)** which is its own network (not Ethernet) to move data very fast but very expensive. Requires **Host bus adaptor (HBA)** and fibre channel switch and controller
    - **iSCSI -** uses existing network and allows you to interconnect to different devices on top of your existing network working at the iSCSI block level
        - Uses an **iSCSI initiator** (OS to access drive) to find Targets (drive being used)
    - Allows you to **create an Extent** which lets you use whatever portions of a drive you want (can't do with NAS)
- **Removable Media Controls:** Harden Optical media like cds, dvds, bluray. Can configure in **Windows MMC** to limit optical media like not allowing executables to run
- **Data Execution Prevention (DEP):** Prevents the execution of programs in memory that aren't suppose to. Hardware issue that it fixes
- **Disabling Ports** - Done in BIOS. Disable things like legacy ports like serial ports, usb ports, etc
    - Turn off legacy non-active ports to avoid vulnerable entry point

- **Electromagnetic Interference (EMI):** aka electromagnetic pulse. Devices give off radiation
- **Radio Frequency Interference (RFI):** Radio range
- 1) Move stuff away or isolate to prevent
- 2) Shield devices from interference
- 3) Use separate circuits for other things that can cause interference like electric motors
- **Electrostatic Discharge (ESD):** Can destroy electronics so protect ourselves from transmitting
    - Use ESD wrist strap
- **Hardening a Host:** Strengthens the IT infrastructure
    - Disable unnecessary services, don't use default passwords especially in IoT, disable unnecessary user accounts
    - **Patch Management**
        - 1) Monitor - be on the lookout for patches; Might not get reminders so be on top of it through news, suppliers
        - 2) Test - Deploy in sandbox environment first
        - 3) Evaluate - determine if it's important enough
        - 4) Deploy Patch - scheduling issues
        - 5) Document - keep track of history
    - **Anti-Malware** - Training for users, procedures if malware is detected, Best practices, monitoring, IDS to detect threats to hosts, 3rd party anti-malware tools
    - **Host Firewalls** - work on an application level basis, white list or black list applications
- **Data Security:** Data integrity, speed/quick access, high availability
    - **RAID** - provides good integrity, good speed, is very affordable
    - **Clustering** - Have multiple computers doing the same job so if one goes down the other can take over. Downside is they have to be constantly updating and very expensive. Usually one doing the work and the others are more like a backup in case main one fails
    - **Load Balancing** - Clustered servers that have primary and backup share the workload so that one server doesn't get overloaded. Also pricey
    - **Virtualize the Servers** - If it fails, can bring back from a snapshot. Can do RAID, Clustering, and Load Balancing with virtual servers and cost effective
- **Disk Encryption:** encrypts the data that is stored on your mass storage but can slow systems down.
    - Use for mobile and portable devices like laptops, smart phones, tablets
    - Desktop systems with limited security
    - **TPM (Trusted Platform Module)** - chip burned into device that has public/private key where impossible to remove private key. Drive cannot be decrypted if not connected to TPM so activate at the system level
    - **PGP (Pretty Good Privacy):** encryption program that provides cryptographic privacy and authentication for data communication like files and email
    - **TrueCrpyt** - no longer exists but there are other that picked up where TrueCrypt left of
    - **BitLocker** for Win
    - **FileVault** for Mac

- **Full Disk Encryption (FDE):** Best security for mass storage. Windows use Bitlocker which uses TPM. Uses TPM so if hard drive is separated from motherboard, no way to retrieve data. Can **create a recovery key** in case motherboard is destroyed
- **Self-Encrypted Drive (SED)** - Self encrypted. Setup password first time it's used and will ask each time it's booted
- **Secure Boot** - TPM 2.0 has secure boot. Checks the quality of your system against attacks and malware
    - **Hardware Root of Trust** - Source that can always be trusted due to its strong cryptographic security
    - **Secure Supply Chain**
- **Hardware Security Module (HSM)** - Rare. Hardware who's only job is signing and can store keys where there's high traffic
- CompTIA's opinion of Secure OS:
    - **Server OS** - supports servers and made specifically for this purpose
        - Built in functionality and connections like DNS, DHCP, RAID, more CPUs, support and stronger hardware support. Ex. Windows Server
    - **Workstations** - Desktop Versions like Windows 10, MacOS, Ubuntu Linux
    - **Embedded Systems** - Appliances that usually have their own OS like routers (Cisco IOS), refrigerators, cameras
    - **Kiosk** - Usually touch screen that's very customized and specific to display things. Usually slimmed down versions of Linux with limited function
    - **Mobile OS** - Apple iOS and Android
    - On exam think about which one of these OS has the least amount of functionality but enough to do the job that it needs to do
    - OS can be setup to be a lot more secure named **Trusted Operating Systems**
- **Wired vs Wireless Peripherals:** difficult to create security problems with wired since need physical access to device.
- **Bluetooth** - messy technology with some vulnerabilities and not very secure
    - **Bluejacking** allowed any device to connect via Bluetooth and use it but uncommon now.
    - **Bluesnarfing** - connect to Bluetooth device to steal data but also obsolete
    - **Bluetooth classes:** Class1 = 328', Class2 = 33', Class 3 = 3"
        - Most mobile phones and headsets are class 2
- **WPS** - convenient but easily hackable so turn it off
- Hidden Wi-Fi - Plug **SD wireless** NICs onto devices with SD slots to access internet and can create WAP
- USB ports on displays and other devices can be compromised with tools like Rubber Duck that can compromise a system
- Avoid backdoors so avoid using apps that come with devices
- Turn off unneeded ports
- Patch Devices

- **Malware** -Software running on your system that you don't want and may or may not do something harmful
    - **Virus** - software that get's on your pc, attach to other files and would propagate to spread to other media and activate to perform actions like erasing files
    - **Adware** - programs that put ads usually web centric
    - **Spyware** - hides and can be tracking, stealing info, and sending it to attacker
    - **Trojan** - runs on system masked as something else but doing something malicious in the background
    - **RAT (Remote Access Trojan)** - Trojan that activates malicious intent from a remote location
    - **Ransomware/Cryptoware** - Locks your system until you pay attacker. Crypto encrypts your system and if you don't pay, data stays encrypted
    - **Logic Bomb** - malware triggered by an event like only go off if an admin removes your account
    - **Rootkit** - software that escalates privileges to execute other things on a computer. Difficult to detect and remove due to its root level privileges
    - **Backdoor** - software that has some intentionally derived way to get into something
    - **Polymorphic Malware** - changes itself to avoid being detected by anti malware that uses digital signatures to detect
    - **Armored Viruses** - make it hard to detect since it prevents reverse engineering by confusing with useless code written into it
    - **Keylogger** - Records keystrokes to collect info. Many malware install keyloggers. Can also be inserted via usb dongle
- **Host Based Firewall:** Fire wall installed on an individual host. Can filter based on filenames, applications, and ports. Use ACL
    - Are an implicit deny meaning they exclude everyone and you build white list
    - Output is ACL, Using leased privilege, and have whitelist to allow certain programs access internet
- **File Integrity Check** - verifies that a particular file is in good order and ready to run. File isn't corrupted, hasn't been tampered with, and version and date expected
    - **System File Checker** (>sfc /scannow) checks core files that make Win OS
        - Windows doesn’t hash files to check integrity, actually maintains a copy of individual files to use in case there's an issue
- **Software Management Tools:** Makes sure running right applications on your individual enterprise systems and keeping track of licenses and being standardized
- First line of defense is a firewall so usually routers will have firewall but firewalls are imperfect
- **Intrusion Detection System (IDS):** can be computer with specialized IDS software, or can be a device that's inside the network and watch for malicious intrusions inside the network and will send notification via email or text.
- **Intrusion Prevention System (IPS):** Active IDS which would act and notify router to block malicious content coming in

    - IPS is usually close to the edge of the network and does something to stop attack
- **A firewall filters, an IDS notifies, and an IPS acts to stop**
- **Automation** provides repetitive actions by giving the ability to do something specific every time with complete clock work
    - **Consistent** - does things the same way every time
    - **Ghost tool** that allows to take an image and restore it to multiple computers
    - Use **Template** restoration on a workstation and then user can customize after
    - **Continuous Monitoring** of network devices
    - **Automatic Updates** of Win OS
    - **Monitoring Application whitelists**
    - **Application development**
    - **PowerShell** is a built-in Windows tool to write custom-built scripts to automate tasks
- **Media Sanitization (Media Destruction):** 3 Types
    - **Clearing** - use some internal command within the mass storage device to remove data such as Erase command on CMD. Or format, delete. Data can still be recoverable
    - **Wiping** - Writes random 1s and 0s to drive to prevent data being recuperated while still allowing drive to be used
    - **Purge** - Do something externally to drive to make data go away and usually drive becomes unusable
        - **Dagausser** - which uses magnet to destroy data
        - **Crypto Erase** - encrypt drive and throw away the key making data unrecoverable
        - **Destroy** - Ruin the media where it's no longer functional like **burning, pulping** (soak it in water where ink gets removed), **shredding, pulverizing**

Section 6: The Basic LAN

- **Switches:** filter and forward data based on MAC addresses on Layer 2. Usually work automatically out of box
    - **VLAN** - Allows 1 broadcast domain split into many broadcast domains and split ports into different VLANs
        - Provides layer 2 separation of networks which is a good security feature
    - **Spanning Tree Protocol (STP)** - Flood Guarding by preventing loop floods
- **Routers:** filter and forward based on IP address or Layer 3. Spans, filters, and forwards IP addresses between different Network IDs
    - **Gateway Router** sits between LAN and Big Internet and **uses NAT (Network Address Translation)**
        - ISP gives 1 IP address to router and router converts into a private IP address range using NAT which then distributes to devices on LAN
- **Network Firewall:** commonly run on a gateway router to protect LAN from the internet and can forward and filter based on port numbers, IP addresses, URLs
- **Network Topology**: the actual organization of a network in terms of how is the data moving around
    - **LAN** - All devices connected to the same Broadcast Domain
    - **WAN** - Has at least 2 LANs connected via a Router
    - **MAN** - different WANs connected together within a city or town (still a WAN)
    - **Internet** - collection of WANs connected all over the world
- **TCP/IP** runs the internet but can also use without the internet
- **Intranet** - private network within an organization
- **Extranet** - allowing access to your private network to another entity like a vendor
- **Core Zone** of any network is a LAN that's physically connected via wire with 1 broadcast domain and devices connected to a switch
- **VLAN:** take one or more physical switches and chop it up into separate broadcast domains that would require a router for them to communicate with each other
- **DMZ (Demilitarized Zone):** Usage of 2 routers at each side with file, web, and or VPN servers inside. Gateway router connects to the internet with public IP address while the other connects to LAN with private IP addresses
    - Cloud Base tools have pretty much made DMZ obsolete but still on exam
- **Wireless Networks:** Use **Wireless Access Point (WAP)** via **802.11** to connect wireless devices to the network by connecting to WAP SSID. Can have separate VLAN for wireless clients
- **Guest Network:** separate VLAN design protected isolated zone used for guests that can be wired or wireless and firewall sits between LAN and Guest Network
- **Virtualization Zone** - create virtual machines within one computer. Can also have virtualized network

- **Airgap** - means disconnect. unplug different networks from each other to provide real isolation when a system is not connected to any other systems. Like having a separate Internet
- **Network Access Control:** Wireless Network, Remote Access, VPN. System acting as a gatekeeper that you need to get through some kind of authentication process that allows you to become part of that other network
    - **Point-to-Point Protocol (PPP)** - designed for dial-up networks, so not used anymore
        - Transport layer protocol that initiated connection, get address info, make connection.
        - Had basic authentication. **Password Authentication Protocol (PAP)** - passwords in the clear
        - **CHAP** (Challenge Handshake Authentication Protocol) - Better than PAP using a challenge that was hashed and wasn't in the clear
    - **Extensible Authentication Protocol (EAP)** - Current standard. developed as an extension to PPP, framework designed to run inside some transport layer protocol and just handles the authentication part
        - **EAP-MD5** - basically MSCHAP, that take passwords and hashes them into MD5 and exchanges them
        - **EAP-PSK** (Pre-Shared Key) - uses pre-determined symmetric keys. Similar to WPA/WPA2
        - **EAP-TLS** - Can handle an entire TLS. Needs server and client certificates
        - **EAP-TTLS** - Uses the TLS exchange method but only requires server certificates
    - **802.1X** - aka as EAP over Ethernet or 802.11. Full blown authentication standard that allows us to make connections between some type of client (supplicant) system and the network itself
        - Between them sits an authenticator (can be WAP, VPN concentrator, etc) that uses EAP to authenticate. Can also make a connection between the authenticator and an authentication server aka RADIUS
    - **LEAP** - Cisco's wireless high security standard. EAP with a password inside a TLS tunnel. Not good anymore. Replaced **by EAP-FAST**
    - **PEAP** - Microsoft's version of EAP before EAP came along. Like LEAP but not used since easily hackable
- **Network Firewalls Stateful vs. Stateless**
    - **Stateless blocks based on ACL and defined rules**. Will go ahead and filter, block and unblock stuff no matter what the situation. Blocks based on IP address, time of day, words that are coming in and stores rule in ACL
        - **Implicit Deny** - no one can do anything unless a rule allows
        - Block websites based on URL, block IP addresses, block services like FTP
        - Setup schedules, send you email of events
    - **Stateful** doesn't really have ACL. **Blocks based on behavior** more than rules. Monitors traffic and decides what it will do like if a lot of pings come into a system it will start blocking pings

    - **Web Application-based Firewall (WAF)** - designed to protect an application like web apps. Usually in front of web server
- **Proxy:** A box/piece of software running on a computer acts as an intermediary between two different devices having a session. Web Proxy is application specific (Web proxy, ftp proxy, VoIP proxy, etc) **2 kinds of Proxy Servers: Forward and Reverse**
    - **Forward** - Hides the client from the server. Client is aware of the proxy. Dedicated box/software in an organization common in schools
        - Client -> Proxy -> Firewall -> Internet -> Server
        - Provides cache, content filtering, can act as a firewall, can block parts of website, block adds
        - Have to setup manually all individual browsers to use web proxy
        - **Transparent Proxy** - don't need all this configuration stuff but has to be literally in the line between you and the Internet so that it can grab everything so nobody has a choice but to go through it
        - **Modern Forward Proxy (Open Proxy)** - used to hide yourself. Instead of going to web server, connect to proxy and proxy connects to web server masking IP address or using IP of another region to access region specific content
            - For privacy, can use a VPN to create encrypted tunnel so ISP doesn't know you're connecting to proxy
    - **Reverse** - Proxy hides the web server. Reverse Proxy servers protects the web server through high security, handle DOS attacks, load balancing, caching, encryption acceleration
- **Honeypots** - devices that are designed to emulate a host or a network to allow you to let the bad guys in and to be able to track what they're doing by logging everything
    - Sit out on the public network so usually put inside DMZ
    - Honeybot free honeypot software
- **Honeynet** - Emulates an entire network usually in virtual systems
- **Remote Desktop emulates** another desktop in that LAN network so anything done goes to the physical computer on the network not the remote computer
- **VPN (Virtual Private Network)** - directly connects into the network from a remote location and is fully functional. It's as if you connected directly to a switch via Ethernet
    - **Connection Options for VPN:** Lease your own line (very expensive), Use internet (downside is its public) so what to virtualize it
    - **VPN Tunnel** - a connection between two VPN Ends Points. On the network side can have Client using VPN software, router passing VPN traffic to client or VPN concentrator be end point
        - **Remote Access VPN** - **VPN Concentrator** uses public IP to connect with remote client but then concentrator will pass IP address that make it part of the network
            - **Full Tunnel** - usually want to avoid since if client tries to connect to the internet, will get routed through the LAN router taking much longer

            - **Split Tunnel** - VPN end point in tunnel recognizes type of traffic going through so only accepts traffic going to LAN in the tunnel speeding up performance dramatically
        - **Site to Site VPN** - Connect 2 or more LANs together via router, software or VPN concentrator so both LANs have same network
    - A VPN is much slower than being in the LAN
    - **VPN Setup Steps** - Protocol to set up tunnel; Protocol to handle authentication and encryption
    - **Point to Point Tunneling Protocol (PPTP)** - Old, uses PPP for tunnel and password only with basic encryption so not very secure
        - **TCP port 1723**
    - **Layer 2 Tunneling Protocol (L2TP)** - Cisco proprietary, similar to PPTP but uses L2TP tunnel and IPsec for encryption. Good and fast
        - **UDP ports 500, 4500**
    - **Pure IPsec** - uses IPsec for tunneling and encryption. Great for IPv6
        - **UDP ports 500, 4500**
    - **Secure Sockets Layer (SSL)/Transport Layer Security (TLS)** - Often works within a browser so client software not needed
        - **Uses TUN/TAP** (virtual network driver) for tunnel which build into any OS, and TLS for encryption
        - **TCP port 443**
    - **OpenVPN** - program that has unique tunnel with encryption based on SSL/TLS
        - **TCP port 1194**, but can easily be changed
- **IPsec:** works at the IP layer and it's a bunch of protocols that work together to have any to host create a secure connection with another host point to point with **2 modes (Transport and Tunnel)** that encapsulate data packets
    - **Authentication Header (AH)** - Only provides integrity. Provides integrity check and then inserts AH into TCP packet called **HMAC (Hash-Based Message Authentication Code)**
    - **Encapsulating Security Payloads (ESP)** - Uses encryption (DES, 3DES, AES) to encrypt payload and then adds AH header
    - Issue is there's too many formats like IPv4, NAT, IPv6 so can't use a simple IPsec standard
    - **Transport Mode** - would work great if everyone had the same IPv4 or v6 range or got rid of NAT so doesn't work in the real world
    - **Tunnel Mode** - Replaces IP address with a new one that can now be used in transport mode. But also can use ESP where original data with original IP is encrypted and then new IP and AH is added to the outside
    - **ISAKMP** - creates a **Security Association (SA)** between two hosts
    - **IPsec Protocol Suite**
        - Uses negotiation protocol **ISAKMP** which handles initial authentication through certificates, pre-shared keys, key exchange

    - IPsec used in VPNs via pure IPsec but more common is IPsec with L2TP crating a tunnel within a tunnel
    - IPec used with RADIUS/TCACAS+ to create tunnel between the two hosts to communicate securely
    - IPsec with IPv6 can have IPsec header information placed within an IP V-6 header
    - IPsec with unsecured protocols creating tunnels to encrypt info like telnet
- **Network Intrusion Detection System (NIDS):** Passive as it only detects intrusions and sends alert
    - Usually set up out-of-band on its own. (Can also be set in-band)
- **Network Intrusion Prevention System (NIPS):** Active since it detects and stops in one way or another. (Can be passive too if set out-of-band)
    - Usually set up in-band behind the firewall
    - Have ability to dynamically access router and block ports
    - Control devices to stop attacks
    - **Detection Methods**
        - **Behavioral/anomaly** - baseline on system so if surpassed baseline it will red flag
        - **Signature based** - similar to anti-malware
        - **Rule based** - similar to firewall ACL
        - **Heuristic** - most common today, combines anomaly and signature and learns over time. Some do combo of all 4
- **Network Tap** - sensors to monitor. Has 2 sets of connectors. 1 for in and 1 for out. Every packet going through Tap being logged and checked. Use for lots of traffic
- **Port Mirroring** - sends all traffic to a particular port
- **Collectors** - Used in enterprise networks. Computers whose job is to take all the data collected from all these sensors and store into a single database where it can be accessed from a single source
- **Correlation Engines** - Tool that does detection methods and deals with attacks for NIPS
- **Security Information and Event Management (SIEM):** Takes all the data that's being monitored and puts it together in a single package
    - **Aggregation** - grabbing data from different places and storing it
        - Time synchronization is important
        - Manage event duplication
        - **Normalization** - makes data more efficient so tools can work better
        - Logs - put logs together
        - **Write once, read many (WORM)**
    - **Correlation** - analyze data and report it in a meaningful way
        - Alerts like notification if something goes bad
        - Triggering so what sets an alert off such as exceeding threshold
    - Ex of SIEM software are Splunk (expensive but powerful), ArcSight, Elk (freeware and open source)

Section 7: Beyond the Basic LAN

- **802.11** infrastructure mode begins with a **Wireless Access Point (WAP)** connected to Ethernet
    - Uses **Radio Frequencies (RF)** to talk wirelessly and Ethernet to wired network
    - WAP has MAC address and broadcasts SSID to create **Basic Service Set Identifier (BSSID)**
    - Client sends request to BSSID and if open network, WAP authenticates and ads to Associated List listed by client's MAC address
    - **Extended Service Set Identifier (ESSID)** - multiple WAPs connected to a common Ethernet broadcast domain
    - 802.11 has no authentication or encryption
- **Wired Equivalent Privacy (WEP)** - **RC4 streaming protocol using Initialization Vector (IV),** shared key concept 64 or 128 bit. WEP can easily be hacked
- **802.11i** - Would use 802.1X authentication using a RADIUS server on wired network to get authenticated but would still allow pre-shared key with AES encryption however Industry could not handle 802.11i since many hardware was not compatible
- **Wireless Protected Access (WPA)** - WEP replaced with **TKIP (Temporal Key Integrity Protocol)** which still uses RC4 but improves issues with IV
- **WPA2** - basically what 802.11i was supposed to be. Can use RADIUS using 802.1X **or PSK (pre-shared key)** using AES encryption
- Cookie Cadger - program that looks out for anyone passing cookies since Session Cookies can expose user information since HTTP insecure and use a Replay Attack (aka SSL Stripping)
    - Use secure protocols on unsecure networks
    - Use https on web sites that collect info
    - Use VPN in non-secure environments
- **HTTP Strict Transport Security (HSTS)** - web server forces user to use https
- **Rogue Access Point** - unauthorized access point. Can be unintentional
    - **Evil Twin** - Intentional Rogue Access Point
    - **802.11 Jammer** - illegal in US that jams signal to cause DOS attack or jam channel so traffic gets redirected to evil twin creating MIM attack
    - **Deathentication Attack** - sends deauth commands that tells clients to get off network so they can connect to evil twin
- **Cracking WEP**: Oldest 802.11 security standard. Downside to WEP is IV susceptible to mathematical error causing IV Attack
    - **Aircrack -ng** - tool to grab WEP keys
    - Airmon -ng - shows what kind of network card
        - airmon-ng start {interface card}
    - airodump-ng wlan0mon (will show available SSIDs and MAC address, and channel)
    - airodump-ng -w dumpfile -c 6 --bssid {MAC address} wlan0mon (let it run for about 5 mins); ls - to see dumpfile files created
    - aircrack-ng dumpfile-01.cap - will provide WEP key

- WPA/WPA2 uses 4-way handshake - has weakness that can be exploited
- **Cracking WPA or WPA2** personal shared key
    - WPA is vulnerable to a dictionary attack
    - WPA grab those four way handshakes when people start to connect and using that we can derive the passwords by using a dictionary file
    - Use Airodump as well to find SSID and grab packets to find handshakes
        - airodump-ng -w wpafile -c 6 --bssid {MAC address} wlan0mon
    - aircrack -ng -a2 -w dictionary wpafile-01.cap
    - Works better with weak passwords so use, long complex private shared keys
- **Wi-Fi Protected Setup (WPS):** allows quick connection to network with a push of a button but unsecured and crackable
    - WPS Weakness is has only 8 digit key but only 7 digits (1 is used for cyclical redundancy check) used and key exchange happens with 4 bits processed first followed by the last 3 bits so can crack 4 bits easily then 3 bits
    - Some WPS AP can detect an attack and shut it off
    - **Reaver** - tool to crack WPS. Use airodump to scan for SSIDs
    - reaver -I wlan0mon -b {MAC address} -uses brute force attack but very slowly to not trigger auto shut off
    - **WPS Attack Prevention:**
        - Get Rid of old routers
        - Firmware updates
        - Upgrade to modern wireless router
- **Hardening 802.11 Networks:**
    - **Survey & Installation Issues** - Survey tools will find SSID, MAC addresses, bands, channels, and signals and document
        - Can have heatmap that shows signal strength
        - Kismet is a survey tool
    - **Maintaining Existing Wireless Network** - Good documentation, AP isolation which segments each device so they can't see each other
        - 802.1X makes a strong robust network that's basically uncrackable
        - Do scanning to survey network and find rogue devices
    - **Monitor Wireless network**
        - **Wireless Intrusion Detection System (WIDS)** - Monitors wireless radios, watches for rouge access points, knows MAC address for authorized equipment, watches working protocols
    - **Wireless Clients Hardening** - Can check SSID list on OS to see if there's rogue AP
- **Thick/Fat Client** - stand alone WAP that has to be configured separately
- **Thin Client** - Doesn't get configured through web page. Configured through a Controller
- **Controller** - allows you to configure multiple thin client WAPs at once
- Many WAPs can take external antennas to provide more signal
- **DBI** - Radio Frequency Signal Strength. Larger DBI is better

- **Antenna Types:**
  - **Omni** - Omni-directional antenna signal goes in all directions
  - **Dipole** - has 2 antennas built in having donut shaped signal. Great to cover a floor
  - **Directional** - shoots out a long beam. **Yagi** and **Parabolic** 2 types for long distance
  - **Patch** - Half of an omni great for shooting signal in 1 direction usually put on walls
- **Band Selection:** 802.11 has **2.4 or 5 GHz**. 5 is less crowded and has auto channel selection.
  - The wider the channel, the more throughput you get
- **Virtualization:** Virtualize everything that there is about a computer in a virtual room
  - Host System is a hardware device which virtualizes hardware from the host
  - Can have multiple virtual servers on one physical device
  - Virtual machines are saved as files, making for easy recovery
  - Hardware consolidation and reduces energy consumption
  - Easy for duplication
  - Handy for IT research
  - Emulation is different as software emulates hardware
- **Hypervisor** - **Virtual Machine Monitor (VMM)** manages VMs for us
  - **Type 1** - runs directly on top of hardware, independent of host OS
  - **Type 2** - runs on top of host OS
- **Cloud Based Virtualization:** Allows you to do **Infrastructure as a Service (IaaS)**
- **Virtualization Characteristics:**
  - Secure feature
  - Patch management
  - Centralized hardware maintenance
  - **Resilient** and **High Availability (HA)**
  - Great testing and sandboxing environment
  - **Network Separation** - can create virtual switch
  - **Snapshots** and **Backups**
- **Virtual Threats** - malware, bad patch management, etc
  - Cloud based VMs offer **Security as a Service (SECaaS)**
  - **VM Sprawl** - having too many clients with different VMs inside network can lose track
  - **VM Escape** - having a lot of Type 1 VM and bad guy being able to push out of VM and access real network
- **Virtualization Hardening:** remove remnant data, make good policies, define user privileges, patch everything
  - **Cloud Access Security Brokers (CASB)** - acts as an intermediary between your infrastructure and the cloud to make sure policies are controlled and watches out for malware
- **Containers:** Used in software development world. Uses **Docker** that runs isolated applications within host OS using host OS kernel. Can only see what's inside its container
  - Uses image which sits on hard drive and contains info

    - Self contained apps that can communicate with network resources that have been explicitly allowed
    - Can depend on each other, and can be configured to communicate with each other on a single host
    - Run a single program and all its dependencies end when the program exists
- **Infrastructure as a Service (IaaS):** Can create a virtualized infrastructure consisting of web servers, virtual switch, virtual router, public IP, firewall, etc
    - Don't need to worry about hardware going out, ISP going out, since everything is on the cloud at much lower costs
    - Enables you to quickly configure network resources hosted by someone else
    - Ex. Amazon AWS
- **Platform as a Service (PaaS):** Enables you to access a software development platform without the need to host it yourself or worry about hardware needed to run your applications
    - Ex. Heroku
- **Software as a Service (SaaS):** A subscription based license that gives you access to various programs and software so does away with optical media
    - Ex. Microsoft Office 365
    - Cloud storage, Google Docs, Google Maps can also be SaaS
- **Web App Deployment Methods:**
    - **On-Premise** - was the way a web application would be hosted by having to buy all the necessary hardware to make it work
    - **Hosted -** application would have a location with powerful hardware would allow you to bring a computer to host your web app or would rent you a computer
    - **Cloud** - modern way running virtualization where your app is hosted on the cloud
        - **Private Cloud** - Just within an organization
        - **Public Cloud** - Open for business where anyone can use
        - **Hybrid Cloud -** Some of it segregated as private, but also offer public hosting
        - **Community Cloud** - A few organization sharing a cloud
- **Virtual Desktop Environment (VDE)** - virtualizing the OS system which is a remotely controlled desktop. **Usually on the user end.**
- **Virtual Desktop Integration (VDI)** - the actual virtualized OS environment on the cloud. **What make it work.**
- **Static Host:** Intelligent device designed to do a specific task or process like many IoT, routers, etc
    - **Industrial Control Systems (ICS)** - **Heating, Ventilation, and Air Conditioning (HVAC)**
    - **Supervisory Control and Data Acquisition (SCADA)** - long range systems usually railroads or pipelines that require some kind of cellular connection
- **Securing Static Hosts:** Change default passwords, turn off unnecessary services, monitor security and firmware updates manually, Defense in Depth through network segmentation
- **Static Host For Exam:**
    - Treat static host like regular hosts at first
    - Use network segmentation and VPNs for SCADA to help protect static hosts

- **SATCOM (Satellite Communication)** - Were proprietary but now can have cell phone snap on
- **NFC (Near-Field Communication)** - allows data transfer but need very close proximity and there's no security
- **ANT/ANT+** - primarily for health monitors and currently no big security issues
- **Infrared** - most phones only transmit so really no security issues
- **USB OTG (On The GO)** - Make USB 2 way where can be ingoing and outgoing
- **Wi-Fi and Tethering:**
    - **WiFi Direct** - Adhoc Mode allows you to connect 2 devices easily but uses WPS
    - **Tethering** - Allows you to share your cellular WAN with another device **via cable**
    - **Wireless Tethering (Hotspots)** - share you internet connection wirelessly to another device by creating a WAP
- **Mobile Deployment Options:**
    - **Corporate Owned, Business Only (COBO)** - Company decides what to do with device and has full control. Popular with high security environments
    - **Corporate Owned, Personally Enabled (COPE)** - Everyone has the same device so learning curve can be an issue but can also use for some personal
    - **Chose Your Own Device (CYOD)** - User chooses from a list of approved devices so less of a learning curve
    - **Bring Your Own Device (BYOD)** - Users gets to choose device so very low learning curve but very heavy device management tools and mobile application management
- **Sideloading** - installing software that's not from an authorized 3rd party like Google Play or App Store. Dangerous since can't trust if app is from trusted source
- **Carrier Unlocking** - Removing carrier restrictions on a cellphone
- **Rooting an Android or Jailbreaking** an Apple gives root access - auto updates disabled, trouble accessing the "store", exposure to malware
- **Firmware OTA** (over the air) Updates - dispersed by people running OS like Apple for iPhone
- **Camera Use** - written policy we are monitoring all the things you do on camera
- **SMS/MMS** - What are people messaging, and how much as it can be expensive
- **External Media** - external storage device or extra SD card can result in unauthorized copying of data
- **Recording Mic/GPS tagging** - used when someone loses phone to locate
- **Payment Methods** - direct real time monitoring required
- **Mobile Device Management (MDM)** Tools: Allows control of device like what applications can be installed, what backgrounds you have, use of camera, etc
    - **Content Management** - app mgmt, databases, docs
    - **Geolocation** - know location of device
    - **Geofencing** - geolocation with geographic trigger
    - **Push Notification Services** - apps will push notifications you want
    - **Passwords and PINs required**, ability to recover passwords
    - **Biometrics** - fingerprints, facial recognition, vocal recognition, lock/unlock device, use to configure apps

    - **Screen Locks** - locked when not in use
    - **Remote Wipe** when device is lost
- **Mobile Application Management (MAM):** Allows management on certain important apps like versioning, updates, patches
    - **Context-Aware Authentication** - where are they right now, what OS using, what time of day trying to authenticate
    - **Storage Segmentation** - Dedicating a separate storage space for enterprise apps
    - **Full Device Encryption (FDE)** - encrypt entire device
    - **Containers** - separate personal content from work like having 2 phones in 1
- **Deterrent Physical Controls:** Designed to prevent bad guys from entering you physical infrastructure that they can see from the outside to prevent them from trying to access
    - Lighting, Signage, security guards
- **Preventative Physical Controls:** Fences, barricades (k ratings K4, k8, k12), mantrap, Air Gaps for cabling systems, VPN or VLANs, protected distribution systems, safe, locked cabinets, faraday cages to protect from EMI, locks, key management, cable locks, screen filters
- **Detective Physical Controls:** Detecting something bad happening in the physical world like alarms, Cameras, motion detectors, infrared detectors, Log Files
- **Compensating & Corrective Physical Controls:** Temp fixes when other controls are weakened like having a guard watch a gate that was broken
- **Heating, Ventilation, and Air Conditioning (HVAC):**
    - Office Environment - designed to be good for humans
    - Server Rooms - keep rack cool and running in 24/7 environment
    - Infrared Camera - thermal imagers that look for heat sources
    - Zone Based HVAC - allows to control temp in individual zones
    - Hot & Cold Aisles - Cool air comes from plenum that enter into Cold Aisles that push heat into hot aisles that push hot air up into warm aisles
    - **Contain System** - used today. Cold air comes up through the plenum but it's actually pulled out through the real racks themselves so concept of cold/warm aisles disappears because the air is all contained within the electronics itself
- **Securing HVAC:** Leave an Air Gap (no connectivity), or use VLAN for isolation, MAC filtering, remote monitoring can be an issue but necessary so secure it with VPN, etc
- **Fire Extinguisher Classes:**
    - A - ordinary solid combustibles like burning wood
    - B - Use for flammable liquids and gases (foam)
    - C - Designed for energized electrical equipment (powder)
    - D - Used for Combustible metals
    - K - Stands for kitchens used for oils and fats
- For server room or computer rooms class C would be used but can ruin electronics due to corrosive powder so now use **FM-200**
- Do not use water to put out electrical fire
- Halon was a good fire suppressant but not environmentally friendly so not used anymore

- **FM-200** material used today for suppressing fires in server room
- Seal off the server room, turn off the power

Section 8: Secure Protocols

- Everything on the Internet runs on top of TCP/IP
- Internet was not built with encryption in mind so took unencrypted applications and either completely rewrote them to make them encryption capable or invented protocols that we slid under unencrypted applications to make them secure
- **SSH Protocol:** SSH Applications have built in encryption. Connects on **TCP 22**
    - SSH Server usually passes certificate (key) first to client that will be used to make the initial key exchange (symmetric keys) to start session and send encrypted data
    - freeSSHd - free SSH server platform
    - PuTTy - client for different things like SSH, telnet client
- HHTP uses TLS protocol which acts as an intermediary between web page and web browser to do all the encryption known as **HTTPS**
- **TLS (Transport Layer Security)** - not an application but a protocol that's plugged into different types of applications. Originally designed for web sites but can do a lot more
- **OSI Model:** 1) Physical (cables, hubs); 2) Data Link (MAC, NIC, Switches); 3) Network (Logical Addresses, routers) ; 4) Transport (TCP/IP, assemble/disassemble packets); 5) Session (How session will be initiated); 6) Presentation (Encryption, convert data into formats); 7) Application (Smarts in the apps, app protocols, API)
- **TCP/IP Model:** 1) Network Interface (physical cabling, hardware, MAC); 2) Internet (routers, IP addressing); 3) Transport (TCP/UDP, assemble/disassemble, what it takes for data to get there); 4) Application (looks at applications as apps)
- **IP addressing:** IPv4 (32 bit address), IPv6 (128 bit address)
    - **IPv4 private address Ranges:**
        - 10.0.0.0 - 10.255.255.255
        - 172.16.0.0 - 172.31.255.255
        - 192.168.0.0 - 192.168.255.255
    - **IPv6 addresses**
        - Link local - FE80 (generated automatically by individual hosts)
        - Internet address - usually starts with 2000's range
- **NAT (Network Address Translation):** converts public IP addresses into private addresses
- **Transport Protocols:**
    - **TCP** - does most of the work on the internet. Connection oriented with lots of packets with **3 way handshake (SYN; SYN-ACK; ACK)**
    - **UDP** - Connectionless, fast
    - **ICMP** - supporting protocol, handles ARP, ping messages. 1 packet
- **Application Protocols:**
    - **HTTP - Port 80** unsecure websites (sometimes use 8080)
    - **HTTPS - Port 443** secure with SSH/TLS encryption
    - **Telnet - Port 23** unsecured form of remote connection

    - **SSH - Port 22** secure communication use instead of telnet
    - **FTP - Port 20,21** unsecured for file transfer
    - **FTP/SSH - Port 22**. Runs through SSH connection for secure file transfer
    - **FTPS - Port 990,20,21** added SSL/TLS security for secure file transfer
    - **SFTP (Secure File Transfer Protocol) - Port 22** for secure file transfer via SSH
    - **SCP (Secure Copy) Port 22** - primitive file transfer via SSH only moves files
    - **TFTP - UDP 69** only copy files
    - **NETbios - Port 137, 138, 139** used by windows for file transfer but outdate by SMB
    - **SMB (Server Message Block) - Port 445** Used for Windows for file transfer
    - **SMTP - port 25** for sending mail unsecured; **465, 587 secured**
    - **IMAP - port 143** newer allows sync unsecured; **993 secured**
    - **POP - port 110** doesn't sync unsecured; **995 secured**
    - **DNS - port 53** resolve website name to IP address
    - **DHCP - UDP 67/68** dynamic IP address resolution
    - **SNMP - Port 161/162** allows device reporting functions
    - **LDAP - Port 389** manage active directory
    - **RDP - Port 3389** Login to remote desktops
    - **SRTP** (Secure Real Time Transport Protocol) - Securely deliver audio/video
- **Secure Sockets Layer (SSL)** - Older protocol no longer secure so replaced by TLS but both do the same thing
- **SSL/TLS** - protocols that are designed to make secure connections between two points. Originally invented for websites, but now used all over the internet
    - Encryption (modify to symmetric encryption), key exchange, authentication (use RSA certificate), HMAC
- Using secure protocols is preferable when possible for hardening
- DNS is non-secure protocol
- **DNSSEC:** tool to force authentication of DNS servers by generating key pair and has upstream DNS servers sign them creating new DNS records for each zone to combat MIM attack
    - An authentication tool **not encryption**
    - Popular on public DNS servers like 8.8.8.8
- **SMTP secure (Port 465, 587)** uses TLS to connect client with SMTP server so data sent with authentication and encryption
- **IMAP/POP (Port 993/995)** secure uses smartTLS (an extension to imap/pop protocols) to connect to IMAP/POP server and create TLS encrypted tunnel
- **SSL Accelerator** - asymmetric encryption can burn through CPUs and overload web servers so SSL Accelerator Cards encrypt/decrypt SSL/TLS asymmetric encryption lightening the load on the servers
    - SSL Accelerator Appliance sits behind router for large web server enterprises
- **Load Balancer** - acts as a proxy taking all the incoming and outgoing traffic and distributes it between identical servers to lighten load. Can distribute based on DNS names, workload, and keep track of sessions

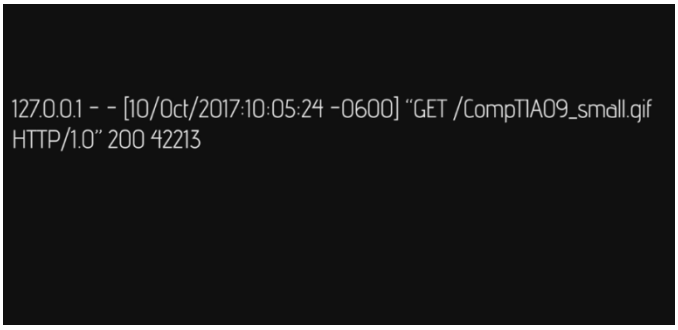
- **DDOS Mitigator** - Helps reduce effect of DDOS attack by rerouting traffic to other proxy servers hosted by companies like cloudfare and help divert bad traffic
- All these devices can be virtualized as well
- **Waterfall Model:** Requirements => Design => Implementation => Verification => Maintenance
- **Agile Model:** States water fall is not the way to do it. Agile is flexibility and being able to move and be able to move quickly with adjustments it needs to get that software out the door
    - Individuals and interactions are more important than processes and tools.
    - Working software is more important than comprehensive documentation.
    - Customer collaboration over contract negotiation.
    - Responding to change is better than just following a plan
    - **Sprint** - short amount of time and see what's achievable
    - **Scrum** - quick meetings to discuss goals and potential obstacles
- **DevOps:** the methodologies and tools that we allow for not only Development but also Operations. Work together to get product out the door
    - **Development**
        - **Plan** - plan out what you will do
        - **Create** - write the code, put it together
        - **Verify** - Let's test it, sandbox
        - **Package** - managerial approval
    - **Operations**
        - **Release** - how to get it out. Provisioning, scheduling
        - **Configuration** - types of configuration users need to deal with
        - **Monitor** - having any issues with security, tools, etc
        - **Cycle back to Plan** - plan to make changes, improvements, etc
- **Secure DevOps:**
    - Run security automation tools - like **Fuzzer** tools, static testers, intrusion detection
        - Always looking for vulnerabilities in code
    - **Change management/ version control** - since change will happen
        - Organization, authorization, documentation
        - Continuous integration
    - **Baselining** - critical security objectives like good encryption, input validation
    - Consider **Immutable Systems** - has interchangeable parts, embedded device, virtual machine
    - **Infrastructure as Code** - preset definition files
- **Compiled vs Runtime Code** - Compiler interprets written code so it can be executed. Most web apps are runtime meaning they can read highly refined code like javascript
- **Proper Error Handling** - App that recognizes error and gives notification of error. Bad error handling will have app accidently display internal information
- **Proper Input Validation** - Want app to validate what's being entered is correct and in proper format
- **Normalization** - want to avoid replication of data. Can use Indexing for efficiency

- **Stored Procedures** - Will check input validation from query and then send to database. This protects databases
- **Encryption/Code Signing** - don't want people messing with code so can digitally sign to make sure whoever receives knows it's in good order
- **Obfuscation** - Can use to compress spaces, get rid of unnecessary words in code and leaves only runtime code
- **Code reuse/dead code** - If you can reuse code do it / get rid of dead code as it can be exploited
- **Server-Side vs. Client-Side Execution** - If do too many things on client side putting a lot of onus and security on the individual client and sending a lot of code to the clients. Server side can put a lot of work on the server like encryption but usually better option.
- **Memory Management** - Issue more so on client side. Be careful with eating up memory, or leaking memory
- **Third Party Libraries and Software Development Kits** - Web apps use these. Can be security issues if these libraries are attacked
- **Data Exposure** - Job is to reduce data exposure by using aggressive encryption
- **Static Code Analyzers** - Look at code and try to find common errors coders tend to do. Not Running it, just reading it
- **Dynamic Code Analysis** - Run the code to look for logic errors, security holes, **fuzzing**. Check for memory leaks
- **Staging** - **Stress Test** by putting entire system under load to see how it performs within a **Sandbox**
- **Model Verification** - Is this doing what we visualized
- **Production** - Get the product out

Section 9: Testing Your Infrastructure

- **Vulnerability Assessment:** action we do to check for vulnerabilities in the systems by using vulnerability assessment tools to actually go about that process
- **Traceroute** - gives a lot of good info about the network like internal LAN is, public address, ISP
- **Port Scanners:**
    - **Advanced IP Scanner** - free tool. Allows you to see the system and displays NIC info, IP address, MAC address, System name
    - **Nmap** - network discovery tool but complex to use.
- **Vulnerability Assessment/Scanning:**
    - **Microsoft Baseline Security Analyzer (MBSA)** - refers to MS knowledge database to determine what vulnerabilities system may have
    - Nessus, Nexpose, OpenVAS (freeware). These tools use the **National Vulnerability Database** as a source
    - Enterprise ones can scan all your devices on your network
- **Vulnerability Scanning Assessments:** usually approved by management so get authorized
    - **Credential Vulnerability Assessment** - You have usernames and passwords that are part of the assessment so gives you more of an insider's edge
    - **Non - Credential Vulnerability Assessment** - Don't have usernames and passwords so more of an outsider so can see from different perspective
    - **Intrusive** - Finding vulnerabilities and exploiting them
    - **Non Intrusive** - Looking at the vulnerabilities but not taking action. Usually what's done
    - Job is to identify vulnerabilities
    - **Misconfigurations** can be vulnerabilities like using default IP addresses
    - **False Positives** - classifying something as a vulnerability when it's not
- **Compliance** - Have to follow compliance rules for certain actions like using PCIDSS Compliance Package to use credit cards
- **Social Engineering** - psychological manipulation of people into performing actions or divulging confidential information
    - People tricking people one way or another
    - **Social Engineering Principals:**
        - **Authority** - to impersonate or imply a position of authority
        - **Intimidation** - to frighten by threat
        - **Consensus** - To convince of a general group agreement
        - **Scarcity** - to describe a lack of something
        - **Familiarity** - to imply a closer relationship
        - **Trust** - to assure reliance on their honesty and integrity
        - **Urgency** - to call for immediate action
- **Social Engineering Attacks:** (Mike's own personal separation so not on exam)
    - **Physical Attacks** - 2 real people being face to face or very close like on the phone

    - **Virtual Attacks** - emails, websites
        - **Phishing** - emails that are used to steal personal information
        - **Spear Phishing** - phishing that is directed to a specific person or company
        - **Whaling** - Spear Phishing that targets senior management and executives
        - **Vishing** - uses the telephone system to get private information
        - **Hoax -** warns someone that something bad is happening when it's not
        - **Watering Hole Attack** - an attempt to infect websites that a group of end users would normally go to gain access to their information or network
- **Common Log Format (CLF):** standard type of logs that every single type of web server generates. And they're all generated in the same format.
    - 1st part usually host (the fully qualified domain name of the client, or its IP address)
    - -- is the Ident and Authuser but not really used anymore
    - Next is date and time
    - Then Request which line from the client enclosed in double quotes ("ex"). Data payload
    - Status - the 3 digit http status code returned to the client (200 means ok)
    - Last Bytes - The number of bytes in the object returned to the client, excluding all http headers



- **cPanel -** can phone home, send email, whenever something abnormal happens as a log file
- **Web Application Attacks:**
    - **Cross-site scripting (XSS)** - Tries to run a script from another site. Client-side script injected into trusted web sites
        - ex: '<script>source=http://evilsite</script>
    - **XML injections** - Tries to insert XML info that shouldn't be there altering the logic of the program. An attack technique used to manipulate or compromise the logic of an XML application or service
- **Injection Attacks:** Adds extra stuff into the input into an application that does potentially harmful things
    - **Code Injection** - add extra code to do stuff it isn't designed to do
    - **Command Injection** - Uses the app to get to the underlying OS
    - **SQL (Structured Query Language)** - complicated incredibly powerful queering language for SQL compliant databases
        - inner join; select from; insert into; are forms of SQL commands
    - **SQL Injection** - add SQL commands to access databases

    - **LDAP (Lightweight Directory Access Protocol)** - way to query directories. **Based on X.500**
        - Object in Directory: Distinguished Name (DN); Common Name (CN); Organizational Unit (OU); Domain Component (DC)
    - **LDAP Injections** - ex: ((cn=admin)(|(password=*))
- **Buffer Overflow:** Every time data is entered goes into a buffer. So entering too much data will cause buffer to crash
- **Integer Overflow:** Overflow of integers because value is too large
- Buffer and integer overflow attacks are inputs into app forms that exceed the max allowed bits
- **Penetration Test:** will try to actually grab data or exploit vulnerability
    - **Get Authorization** - define targets
        - Attack Model - what the attacker knows
            - **White Box** - attackers have extensive knowledge about the target, attackers usually more like trusted insiders, cheapest fastest type of attack
            - **Black Box** - attackers know nothing about the target, attackers are more like strangers, external hacking, potentially expensive and slow
            - **Grey Box** - somewhere between the two extremes
    - **Discover Vulnerabilities** - reconnaissance, get info, use vulnerability scanners
        - **Passive Discovery** - not putting your packets onto the target so uses external sources like whois lookup
        - **Semi-Passive Discovery** - putting packets onto target but not raising any alarms like Wireshark
        - **Active Discovery** - running tools and scanners that could alert IDS or block you
    - **Exploit Vulnerabilities** - grab usernames/passwords, take data from database, corrupt webpage
        - **Exploitation:**
            - **Banner Grabbing**
            - **Pivot** - uses the compromised system to attack other systems
            - **Persistence** - to connect again easily with your target with open timelines
            - **Privilege Escalation** - ability to gain elevated access to data and the network resources, gaining root access
        - Using **Metasploit (it's a framework).** Can run Armitage on top of Metasploit that helps run with the framework and is graphical
- **Race Conditions** - a device or system attempts to perform two or more operations at the same time, but because of the nature of the device or system, the operations must be done in the proper sequence in order to be done correctly
    - Race conditions exploit that small window of time between when a security control is applied and when the service is used. Usually these are very tricky and relatively difficult to pull off

- **Embedded Systems** - Immutable system that never changes. Issue is that tend to forget about them and they can be patched or anti-malware, firewall
- **Lack of Vendor Support** - Issue with hardware. Device or software can be obsolete or vendor completely out of business so can no longer patch or update. Might want to throw away and get something new
- **Weak Configuration** - default configuration, using old or outdated standards like WEP
- **Misconfiguration** - Have done something incorrect like didn't turn on a firewall
- **Improperly Configured Account** - isn't being provided the permissions it needs, or being given too many permissions. Can also be rights like access a system remotely
- **Vulnerable Business Processes** - storing non-essential info
- **Memory/Buffer Vulnerability:**
    - **Resource exhaustion** - get more of that resource, add more ram or stop what's causing the exhaustion to solve
    - **Memory Leak** - app not properly coded, might require recall or patch, need to dig up issue
    - **Integer Overflow, Buffer Overflow** - could allow bad actor to take control of a system
    - **Pointer Difference, DLL injection** - system is fine but sneaking behind a back door so don't have obvious performance symptoms so more nefarious.
        - Make sure you have robust code especially against input validation problems, have a good firewall, and watch system closely
- **System Sprawl** - Undocumented systems means outside the umbrella and might not be getting the appropriate updates and patches leaving the door open for vulnerabilities

Section 10: Dealing with Incidents

- **Incident Response:** Exam based on NIST 800-61 Computer Security Incident Handling Guide
    - **Preparation** - the big plan, who's doing what?, organize the types of incidents that might happen
        - **Reporting** - what reports go to whom, escalation
        - **Practice** scenarios
    - **Identification** - recognize what incident has occurred, reports from users, check the monitoring tools you use, watch alerts and logs, assess the impact, define who's involved
    - **Containment** - mitigate the damage, stop the attack, segregate the network, shutdown the system, turn off a service
    - **Eradication** - remove the malware, close off vulnerabilities, add new controls
    - **Recovery -** Restore from backups, pull from snapshots, hire replacement personnel, monitor to ensure good operations
    - **Documentation** - document the incident, what failed, what worked, generate a final report
- **Incident Response Plan:**
    - **CIRT (Cyber Incident Response Team)** - a group of people whose job is to respond to all incidents (full time, part-time or both) IT security team that understands forensics, IT Department, human resource, legal, public relations
    - **Document Incident types/category definitions** - Physical access, malware phishing, social engineering
    - **Roles and Responsibilities** - users, help desk, human resources, database manager, incident hotline, IR manager/officer, IR team
    - **Reporting Requirements/escalation** - Determining severity, based on severity have clear chain of escalation, informing law enforcement
    - **Practice** - annual or more frequently scenario drills
- **Digital Forensics:** the art, the science of collecting, storing, and quantifying digital evidence to be used as the result of some action that takes place now in our world
    - Incident Occurs in house
    - **Legal Hold** - must maintain all records requested
    - **Chain of Custody** - someone gathering evidence against somebody or something and **data must be of high integrity**. Process:
        - 1) Define the Evidence
        - 2) Document the collection method
        - 3) Date/time collected
        - 4) Person(s) handling the evidence
        - 5) Function of the person handling evidence
        - 6) All locations of the evidence
    - **Order of Volatility:**

        - **1) Memory** - CPU, caches, routing table, ARP table (can use programs like DumpIt or Volatility)
        - **2) Data on the Disc** - optical, flash drives, cache files, temp files, Write Blocker enabled tools
        - **3) Remotely Logged Data** - web site data, remote file server logs
        - **4) Backups** - trends, low volatility takes time to gather data
    - **Forensic Data Acquisition:**
        - Capture the system image (Write blocking tools)
        - Network traffic and logs
        - Capture Video - workstation, video and audio on system, security cameras, record time offset
        - Take hashes to show integrity of data
        - Take Screenshots - record date and time
        - Interview Witnesses
        - Track man hours - can have budget or insurance issues so track hours
- **Contingency Planning:** attempts to mitigate adverse incidents to preserve business continuity
    - Backup sites
        - **Cold Site** - Takes weeks to bring online, basic office space, chairs, AC, no operational equipment. Cheap
        - **Warm Site** - Takes days to bring online, operational equipment but little or no data
        - **Hot Site** - Takes hours to bring online, real-time synchronization, almost all data ready to go, often just a quick update. Very expensive
        - Need to consider distance and location, internet requirements, housing and entertainment, legal issues
    - **Order of Restoration**
        - Power, outlets are functional
        - Wired LAN up and running
        - ISP link
        - Active directory/DNS/DHCP servers
        - Accounting Servers
        - Sales and accounting workstations
        - Video Production workstations
        - Wireless
        - Peripherals
    - Annual exercises
    - **Failover** - process of making it happen to see how well prepared
    - Alternative processing sites
    - Alternative business practices
    - After action reports
- **Archive Attribute** in windows on top of NTFS turns on when a file is changed (>Attrib g*.*)
    - Stat file in linux

- **Backup Methods**
    - **Full backup** - time consuming and a lot of overhead
    - **Differential Backup** - backup of all the changes since the last full backup
        - Only need 2 backups full backup and latest differential backup
        - backup sets get bigger and bigger
    - **Incremental Backup** - only back up changes made from the last backup
        - Need full backup plus all the incremental backups made
        - More backup sets but smaller
        - Usually method for cloud backups
    - **Snapshots** - used in VM. Copy of a previous state. Issue not stored in separate media
- **Local Backups** - nearby but can be lost if something happens in local location
- **Offsite Backups** - remote backup in case something happens at local location
- **Cloud Backups** - take up a lot of time for initial backup, but afterward quick as **does continuous incremental backup**