Sec+ 501 Objectives

## Remember this:

* Pass the Hash: An authentication attack that that captures and uses the hash of a password. The attacker then attempts to log on as the user with the stolen hash. This type of attack is commonly associated with the Microsoft NTLM (New Technology LAN Manager) protocol
* TCP/IP Hijacking
  + Occurs when an attacker takes over a TCP session between two computers without the need of a cookie or other host access
* Blind Hijacking
  + Occurs when an attacker blindly injects data into the communication stream without being able to see if it is successful or not
* Known ciphertext: Attacker has only access only to encrypted messages
* Downgrade: TSL 🡪 SSL, MITM POODLE – TLS v1.0 -CBC or SSLv3 CBC
* Weak implementations: The main cause of failures in modern cryptography systems are because of poor or weak implementations instead of a failure caused by the algorithm itself.
* Race condition: The behaviour of a software, electronic, or another system's output is dependent on the timing, sequence of events, or a factor out of the user's control.
* Embedded Systems: Programs added for automation and/or monitoring. Can allow for malicious programs to gain access through the added programs.
* Resource Exhaustion: DoS attack. Makes it unable for action to be performed
* Untrained Users: Users are not properly informed on how to use system
* Improperly Configured Accounts: Users should only be allowed to access parts they need to complete their work
* System sprawl/undocumented assets: Lack of internal inventory and allowing unsecure devices and systems to connect to the network.
* Application-based(Firewall): Protects the user from applications and services by monitoring and potentially blocking the input, output, or system service calls that do not meet the configured policy of the firewall.
* Tunnel: Entire packet encrypted -ESP
* Transport: Private network, encrypts packet payload – AH
  + End to end communication in IPSEC. Encrypted Telnet or RDP from workstation 🡪 server
* Switch: Networking device connects devices together on computer network
* Scheduling: Sends requests to servers using set rules
* Controlled based: Require a controller for **centralized management and aren’t manually configured**
* Standalone: Used in smaller environments
* NAC – uses 802.1x
* Agentless: Is not installed on the device itself but instead is embedded within a Microsoft Windows Active Directory domain controller.
* Network Map: Identifies devices on network w/ ports & devices
* Netstat – b (binary) Netstat -n (Don’t resolve names)
* Access Violations: Segmentation fault, OS locks you out, prevents access to restricted memory
* Certificate issues: Must be signed by someone trusted, up to date, and checked properly.
* Misconfiguration:
  + AP: No encryption, open
  + Content Filter: URL not specific, protocols not filtered
* Policy Violation: Transferring private data or visiting unsafe websites
* Host based firewall – restricts incoming and outgoing network activity for a host
* Whitelisting: Only allowed approved programs. Unapproved programs are blocked.
* Advanced malware tools: Block malware from running by blocking file signature, heuristics/Anomalous behavior, sandboxing, virtualizing. Need to be routinely updated with the latest definitions to be secure and protect against current threats.
* Cellular: Susceptible to traffic monitoring, location tracking and gain access to device from anywhere in the world
* WiFi - If the Wi-Fi connection is not encrypted it is vulnerable to eavesdropping. Frequency jamming or interferences can cause a denial of service.
* SATCOM - Satellite Communications that is used for communications in remote areas and during natural disasters.
  + Potential Risks: SATCOM devices are at risk of leaking geopositioning data and remote code execution, and are not easily updated remotely.
* Bluetooth: Allows electronic devices like cell phones and computers to exchange data over short distances using radio waves.
* NFC: Susceptible to relay/replay attacks and jamming/interference cause DoS
* ANT: 2.4 GHz ISM. Heart monitors, sport and fitness sensors
  + Risk of jamming band, and eavesdropping as encryption is vulnerable.
* IR: Control Entertainment devices and other IR devices.
* Content management: Limiting access to content hosted on company systems, and controlling access to company data stored on mobile devices.
* Push notification services: Using SMS texts to send messages to selected users or groups.
* Directory Service SASL:
  + SASL (Simple Authentication and Security Layer): Provides a source of additional authentication using many different methods, such as Kerberos or client certificates.
* DNS resolution: DNSsec
* Network address allocation: DHCP, there is no secure version it.
* DHCP starvation attack: Using spoofed MAC addresses to exhaust the amount of DHCP's pool. Can configure a switch to limit the number of MAC addresses on an interface.
* Subscription services: Anti-viruses and anti-malware are subscription based. Must check regularly for updates. Set up integrity checks to verify the updates are coming from the correct source.
* Application server: Securing an application server means using industry standard guides, vendor specific, locking down the server to only the ports it needs for its specific role.
* Network infrastructure devices: Use national vs international guides, regulatory/non-regulatory and general purpose guides for securing.
* General purpose guides: Security configuration guides that are generic in scope.
* Guest: Network with access to the internet but no access to the internal network. Is useful in congested areas and is generally unsecured.
* Air gaps: Be careful with removal media
* Sensors: Can give transactions, logs, or other raw data. Can be integrated or built-into switches, servers, firewalls, routers, or other network devices.
* Collectors: Could be a console or SIEM. Gathers all the data from sensors into one place and attempts to make sense of it.
* Proxy: Intermediary point between the client and the service. Ensures that the response arrives safely and that the traffic flow is correct.
* SSL Accelerator: Offloads the SSL process to a hardware accelerator. SSL handshake is complicated and time consuming.
* SDN: separated into the control (configuration) and data plane (forwarding and firewalling). Directly programmable from a central location, often automatically.
* FDE (Full Disk Encryption)/SED (Self Encryption Drives): Programs and technologies that encrypt everything on the storage drive.
* Kiosk: A system or computer with a touch screen designed to provide information or directions.
* TOS – Trusted Operating System
* Version control and change management: The ability to track change and ability to revert to previous versions.
* Obfuscation is camouflage
* Memory management: Checking and ensuring that the program does not use too much memory.
* Use of third-party libraries and SDKs: Commonly used so is better understood by attackers.
* Cloud: Has no investment cost, and a low operational cost. Can be accessed anywhere anytime and has high mobility.
* CASB: See applications, encryption, DLP, identify malware/rogue devices, monitor user activity
* Automated courses of action: Automated scrips that give a basis for secured configuration with a secured template. Can be configured to accommodate for constant changes or can be launched on a specific schedule.
* Templates: Give a basis for secured configuration with a standard secured configuration.
* Fault Tolerance: Stops SPoF
* Redundancy: Secondary or alternate solution. Boosts fault tolerance
* Distributive allocation: Provide resources across services/servers instead of reallocation or concentrated resources based on physical system location.
* PDS: Cable troughs, conduits, STP/UTP
* SAML: Authenticate through 3rd party source to gain access, resource is not responsible for authentication.
* OPENID Connect: Authentication, OAUTH: Authorization – token authorization
* NTLM – Authenticate Windows domain, replaced by Kerberos
* PIV: Civilians CAC: Government/Department of Defense
  + Both provide identification + Auth with digital sig+ enc
* 802.1x used with RADIUS and WLANS. NAC uses 802.1x
* Recertification: Action of regaining a certification due to expiry
* Separation of duties: A security principle that prevents any single person or entity from controlling all the functions of a critical or sensitive process.
* System owner: Executive level manager, has overall responsibility for the system. Makes decisions about the overall operation of the app and data. Defines security policies and backup policies. Manages changes and updates
* MEF – mission essential functions. A set of functions that must be continued throughout, or resumed rapidly after a disruption of normal operations
* Impact: Life 🡪 Property (Risk to buildings and assets) 🡪 Safety (Environments are sometimes too dangerous to work) 🡪 Finance 🡪 Reputation
* Quantitative: Metric
* Documented incident types/category definitions: Helps employees identify the difference between an event and an actual incident.
* Roles and responsibilities: Many incident response plans identify specific roles for an incident response team along with their responsibilities.
* Reporting requirements/escalation: Depending on the severity of the incident, sec personnel might need to escalate it or notify executives within the company of the incident.
* Differential: Backup data that has been last changed or different from last backup
* Incremental: Last change since full/incremental backup
* Order of restoration: After the disaster has passed, the least critical functions go to the primary site first
* Off-site: Seperation Location
* Salt: Add random data at end of password when creating a hash
* IV: Random value used with an encryption key
* Nonce: One-time use random value for authentication
* Key Exchange:
  + Out of band: Key sent offline, on phone or in person
  + In-Band: Encrypted over internet
* Session Key: Symmetric keys used to provide a secure and fast online connection. The server's public key is paired with a random key to produce a symmetric key, that the server uses to encrypt and the user to decrypt.
* Ephemeral key: Session keys that only last temporarily and change frequently.
* Crypto service provider: A library of cryptographic standards and algorithms.
* Crypto modules: Hardware, firmware or software that provides the hash, HMAC, cipher, decipher, sign, and verify methods.
* Low latency: Low amount of time occurs between input and output
  + Use less resources, encrypt and decrypt quickly with smaller key sizes + symmetric encryption. Fast computation. Hashing provides data integrity
* Higher resiliency: The longer/larger key size, the better the encryption algorithm quality
* Resource vs. security constraints: Limitations in providing strong cryptography due to the amount of available resources (time and energy) vs the security provided by cryptography.
* Blowfish/Twofish not limited by patents
* PGP: Used with IDEA
* HMAC: Combines with symmetric key, implemented with DH.
  + Faster than asymmetric. Provides Data integrity and authentication. Used with IPSEC/TLS
* Obfuscation:
  + XOR (Exclusive OR): Mathematical operation that's a part of all symmetric operations, done by comparing bits of plaintext and a key (same=0, different=1). Can be reversed to get plaintext back.
  + ROT13 (Rotate by 13): Common substitution cipher, rotates each letter 13 places.
  + Substitution ciphers: Cipher that changes one symbol for another, like the Caesar Cipher. Easy to decrypt.
* WPA2-E /WPA-2 uses CCMP for enc
* RADIUS Federation: RADIUS Federation: Members of one organization can authenticate to the network of another network using their normal credentials.
* TKIP (Temporal Key Integrity Protocol): Protocol that mixes a root key with an initialization vector, a new key for each packet.
* Captive portal: Alt to 802.1x, authenticate clients via web form to complete task, before accessing network
* Intermediate CA (Intermediate Certificate Authority): An entity that processes the CSR and verifies the authenticity of the user on behalf of a CA.
* OID: Serial no. that authenticates a certificate
* Offline CA: CA that is offline preventing exploitation of ROOT CA. often used for root certificates.
* Pinning: The application has hard-coded the server's certificate into the application itself.
* Trust model: A complex structure of: systems, personnel, applications, protocols, technologies, and policies working together to provide protection.
* Root cert: Self signed. Self-signed create own certificates to save cost and time.
* DV: Uses TLS. Most common form of certificate. Extension of X.509
* X.690 – BER, CER, DER
* EV: More secure because they require more validation from the certification holder.
* Apache use PEM. PEM is base 64 ASCII