CompTIA Security+

**1.1 Analyze IOC and Malware**  
Malware Attacks:  
-Delivery: How it gets to target  
-Propagation: How malware spreads  
-Payload: What malware does once it’s there  
-Indicators of Compromise(IOC): An artifact observed on a network or in a n operating system that with high confidence indicated an intrusion (Virus signatures / Unknown IP Addresses )  
  
Viruses:  
-Armored: Protected in a way that makes disassembling it difficult  
-Companion: Creates new program that runs in place of expected program of same name  
-Macro: Software exploit virus that works by using macro feature included in applications   
-Multipartite: Virus that attacks system in 1+ ways  
-Phage: Modifies/alters programs   
-Polymorphic: Changes form or mutates   
-Retrovirus: Attacks/bypasses antivirus software  
-Stealth: Avoid detection  
  
Crypto-Malware and Ransomware:  
-Uses crypto as part of attack  
-Cryptolocker, WannaCr, Locky, zCrypt, NotPetya  
  
Rootkit:  
-A computer program designed to provide continues access to pc while hiding its presence  
-Ability to obtain admin/root access  
-NTRootkit, Zeus, Stuxnet  
  
Trojan:  
-Any app that masquerades as one thing in order to get past scrutiny   
-BackOrifice, Stuxnet, Zeus  
  
Worms:  
-Replicate themselves to systems and exploit vulnerability or use social engineering to trick users into executing  
-Worms travels via info-transport features on system  
-ILoveYou, MyDoom, StormWorm, Slammer

Bots/Botnets:  
-Bot: automated program that collects info on web systems, maliciously is compromised pc being controlled remotely  
-Botnet: network of compromised pcs under control  
  
RATs(Remote Access Trojans):  
-Gives person full control of device, and provide capability to surveil computer  
-SubSeven, ProRat, Turkojan, Poison-Ivy  
  
Advanced Persisten Threat:  
-Set of stealthy continuous computer hacking processes  
-Require high degree of covertness over long period of time

**1.2 – Threats, Attacks and Vulnerabilities**  
-Whaling: Phishing attack aimed at wealthy, powerful people  
-Vishing: Making phone calls pretending to be reputable company  
-Pharming: Traffic redirect to spoofed website  
-Watering Hole Attack: Security exploit in which attacker seeks to compromise specific group of end users by infecting websites that members are known to visit  
  
Application Attacks:  
-Buffer overflow: When more data is written to buffer than it can hold  
-Injections: When untrusted data Is sent to interpreter as command/query (Defend against injections by filtering input)  
-Cross-site scripting: Whenever app includes untrusted data in new web page without proper validation or escaping, or updates an existing web page with user-supplied data using browser API that can create HTML or JS  
-Cross-site request forgery: attack that force end user to execute unwanted actions on web app  
-PrivEsc: Exploiting bug, design flaw or configuration oversight in OS or app, to gain elevated access to resources normally protected  
  
Attack Prevention:  
-OWASP coding practices  
-Filter and validate user input  
-Use Web Application Firewall  
-Build security into software development lifecycle  
-Have an incident response plan  
  
Zero-Day Exploits:  
-Attack that exploits previously unknown security vuln  
-Ex: Stuxnet  
  
Crypto Attacks:  
-Birthday: Attack on crypto hash that looks for hash collisions – exploiting 1-1 nature of hashing functions  
-Known plain text/cipher text: Attacker attempts to derive crypto key by using pairs of plain text with cipher text  
-Frequency analysis: Looking at blocks of encrypted message to determine patterns   
-Rainbow tables: All possible password hashes computed in advance and those hash values are compared with password database  
  
Hijacking attacks:  
-Clickjacking: tricks web user into clicking spoofed button/img  
-Session hijacking: exploiting valid computer session/session key, to gain unauthorized access to info  
-URL hijacking: Registering domains that are similar to those for known entity but based on misspelling  
-MAC spoofing: Media Access Control is hard-coded on network interface controller, many drivers allow MAC address to be changed   
-IP spoofing: Attacker impersonates another machine by manipulating IP packets, modifies packer header with forged ip, checksum or order value  
-ARP spoofing: when attacker sends fake Address Resolution Protocol message of LAN. Results in linking of attacker Mac address with legit IP   
  
Amplification Attack:  
-To get response to request greater than 1:1 ratio, so additional bandwidth traffic works to congest and slow server down  
  
Wireless Attacks:  
-Evil twin: Rogue wireless access point poses as legit service provider to intercept info   
-Rogue AP: Any wire access point added to your network that has not been authorized  
-Bluejacking: Sending unsolicited messaged over Bluetooth  
-Bluesnarfing: Gaining access through Bluetooth  
  
**1.5 Vulnerability Scanning Concepts**  
-Identify unpatched or non updated systems  
-Misconfigurations   
-False positive: when scan mistakenly identifies vuln when it is not

**1.6 Impact of Vulnerabilities**  
-Race condition: Behavior of electronics, software, where output is dependent on sequence or timing of uncontrollable events  
-Improper input handling: When system does not validate input attacker can craft input in a form that is not expected  
-Improper error handling: when sys generates error message that includes sensitive info about environments/users/etc  
  
Vuln Types:  
-Misconfig/weak config: Insecure config control settings  
-Using default configuration  
-Weak cipher suites (WEP)   
-Improper certificate and key management: allows sensitive data to be decrypted  
-Improperly configured accounts  
-Resource exhaustion: Denial of service that happens when resources req to execute an action are expended  
-Vulnerable business processes  
-System sprawl / undocumented asset  
-Architecture / design weakness

**2.0 Networking Basics**  
Protocol Concepts:  
-Set of rules  
-What do you want to do?  
-Where are you going?  
-How do you get there?  
-Did you get there?   
  
OSI 7-Layer Model:  
1. Physical  
2. Data: MAC Address/Ethernet/Physical Addresses.   
3.Network: IP Addresses, Address Resolution Protocol   
4.Transport: Host-host communication. Http: port 80 / Https: port 443. TCP (Connection oriented)/UDP (Connectionless used for streaming)  
5.Session: Establish and maintain connections  
6.Presentation: Ensures data is in useable format (Data encryption)   
7.Application

**2.1 Network Security Components**Networking Devices:  
-Router: Connects computer networks, operates at layer 3 (network layer) and stores info about network   
-Switch: Connects devices with computer network by using packet switching to receive, process and forward data to destination. Used in layer 2 / layer 3   
-Bridge: Connect 2 diff physical networks using layer 2.   
-Proxy: Device that acts on behalf of others, provides security, logging or caching.   
-Proxy Server: Blocks known malicious websites  
-Forward Proxy: Retrieves data on behalf of a client  
-Reverse Proxy: Protects access to a server on the internal network  
-Transparent Proxy: Caching server that redirects client requests without modifying them   
-Load Balancer: Shifts burden from one device to another (split traffic on website)  
-Access Points: Layer 2 of the OSI model, can operate as bridge to share wired network to wireless devices, or as router passing data from one AP to another.   
-SSID (Service Set Identifier)  
  
Router Security:  
-Access Control Lists: filter packets by source address, destination address, protocol or port  
-Zones: Segmenting networks based on functionality or security  
-Antispoofing: Creating a set of access lists that deny access to private IP  
  
 Switch Security:  
-Virtual LANS: Segment networks and limit broadcast traffic  
-Port security: Enable/disable switch ports based on MAC address. Vulnerable to MAC address spoofing  
-Flood guard: Detect and prevent malicious traffic (DOS)

Network Address Translation (NAT)  
-A method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in traffic  
  
Firewall:  
-Isolate one network from another  
-Monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on set of rules   
-Network or host-based  
  
  
Firewall Types:  
-Packet filter: Passes/blocks traffic to specific ports/IPs, little intelligence and faster than stateful inspection  
-Proxy Firewall: intermediary, application and web proxy  
-Stateful packet inspection  
  
Stateful Inspection Firewalls:  
-Analyzes data flows and traffic patterns  
-Dynamic access control decisions  
-Records are kept using state table that tracks every communications channel  
-Remembers where packets come from and where next ones should come from  
  
Firewall Rules:  
-Implicit deny: Access or resource availability is restricted to only those that are granted access  
  
Application Firewalls:  
-Controls input/output and access to or from an application   
-Deep packet inspection, functions at Layer 7 of OSI model  
-Web App Firewall protects from injection/buffer/overflows/etc  
  
Intrusion Detection / Intrusion Protection Systems:  
-Sensor: the IDS component collects data from the data source and passes it to analyzer  
-Deception active response: attacker believes attack is succeeding while system monitors the activity and redirects the attack to honeypot or logging system  
Types:  
-Signature based: detects known vulnerabilities, reactive  
-Behavior based: Outside normal bounds, anomaly based  
-Heuristic based: Uses algorithms to analyze activity  
-False positive: when typical or expected behavior is identified as irregular/malicious  
-False negative: when alert that should have been generated did not   
  
Network Intrusion Detection/Protection Systems:  
-Combined with firewalls  
-Passive nip where traffic is mirrored to sensor  
-Inline with traffic flows and prevent attacks in real time  
  
VPN Concentrators:  
-Single device to funnel all VPN access with encrypted tunnels and centralized authentication (RADIUS/Kerberos)  
-Network security through encryption (SSL/IPsec)  
  
Internet Protocol Security (IPsec):  
-Provides authentication services and encapsulation of data through support of Internet Key Exchange protocol  
-Function within IP network layer (layer 3)  
3 services:  
1. Data verification   
2. Data tampering protection  
3. Private transactions  
-Two separate protocols AH and ESP  
  
SSL / TLS VPN:  
-TLS now replaces SSL  
-Point to point encrypted communications  
  
VPN Tunneling:  
-Full tunnel: all requests are routes and encrypted through VPN (most secure)  
-Split tunnel: only some are routed and encrypted over VPN   
  
Network Access Control (NAC)  
-Uses a set of protocols to define and implement a policy that describes how to secure access to network nodes by devices upon initial access.  
Components:  
 -Access Requestor: Requests access where assessment of device can be performed to another system  
-Policy Decision Point: System that assigns a policy based on assessment  
-Policy Enforcement Point: Enforces policy, can be switch, firewall or router.  
  
Security information and event management   
-SIEM tools collect, correlate and display data feeds that support response activities  
-Log aggregation, manage security events, correlate and normalize events (whats normal network activity), report on data gathered from apps   
-Benefits: Aggregation, correlation, automated alerts, event deduplication, time sync, WORM  
  
Data Loss Prevention (DLP)  
-Prevents sensitive info from physically or logically leaving corporate system  
-Designed to detect and prevent unauthorized use and transmission of confidential info  
-Can be a proxy, USB blocking, application white-listing or cloud data  
  
  
  
  
SSL / TLS accelerators  
-SSL offloading: process of shifting burden of encrypting and decrypting traffic sent via SSL from the web server to another device  
  
Gateways  
-Centralization and routing (Router)  
  
Hardware Security Module (HSM)  
-Hardware based encryption that manages digital keys, accelerates crypto, and strong access authentication  
-Trusted Platform Module (TPM) used to assist with crypto key generation  
  
International standard used for Network Access Control?  
- IEEE 802.1X  
  
 **2.2 Security Assessment Tools**Protocol Analyzers  
-Packet Sniffers, gather packet-level info on a network (Wireshark, TCPDump)  
   
Network Scanners/mappers  
-Know what’s on your network via network enumeration (solarwinds/Nmap/ZenMap/Fing for mobile)  
  
Vulnerability Scanner  
-Software that scans a range of IP addresses and tests for presence of vulnerabilities   
-Relies upon a database of known vulns  
Examples:  
-Nessus, one of the most popular  
-OpenVAS  
-Nexpose Community: Scan web apps, databases, virtual environments  
-Qualys FreeScan: Checks for hidden malware and SSL issues  
  
OWASP ZAP  
-Discover security vulns in web apps   
  
Exploitation Frameworks  
-Contain set of exploits for known vulns (Metasploit, Canvas, Core Impact)  
-Browser Exploitation Framework: pen testing tool for web vulns  
  
Kali Linux  
-Debian-derived Linux distribution designed for digital forensics and pen testing  
-Supported platform of Metasploit framework  
  
Social Engineering Toolkit (SET)  
-Info resource of social engineering   
-Social engineering attacks  
  
Metasploit  
-Database of exploits

Wireless Scanners  
-Gather info about wifi networks, detect Access Points, break encryption keys (Aerodump, Kismet)  
  
Configuration Compliance  
-Microsoft Baseline Security Analyzer, is a software vuln scanner to analyze targeted Microsoft systems  
  
Banner Grabbing  
-Technique to identify operating system, applications and services on a system  
-Netcat nc [www.google.com](http://www.google.com) 80  
  
Password Crackers  
-Brutus, Cain and Able, John the Ripper, THC Hydra  
  
Honeypots   
-Systems or networks exposed to capture malicious activity, gather investigation evidence and study attack strategies  
  
Steganography  
-Hidden writing / message in media  
-Approaches: Least significant bit insertion, masking and filters, algorithms and transformations  
-Steghide, OpenPuff, rSteg, Camouflage  
  
Data Sanitization  
-Process of removing contents from device or media (DBAN, BCWipe, Cryptographic Erase)  
  
Command Line Tools  
-man: manual page  
-ping: checks if you can interact with address

-tracert: shows path from my computer to address  
-nslookup/dig: performs dns query  
-ipconfig/ifconfig: network addresses of local machine  
-netcat, arp, netstat, tcpdump   
  
**2.3 Given Scenarios Troubleshoot Security Issues**  
Asset Management   
-Step #1 for both NIST and CIS controls  
-You can’t secure something you cant see or know  
-Use automated tools to maintain asset list  
-Issue: assets that go lost   
-Includes software management, disables employees from downloading stupid shit  
  
Access Violations  
-People: occurs when someone accesses data they shouldn’t  
  
Permission Issues:  
-Least privilege violation  
-Write and execute allowed instead of read-only  
-Solution: Auditing, Reporting, Response  
  
Authentication Issue  
-Expired password, incorrect username/pass, poor password, user rights  
  
Unencrypted credentials / clear text  
-No password rules  
-System config stored with clear text  
  
Certificate Issues  
-Date/time not set correctly, expire certificates, certificate revoked  
-Use of SSL instead of TLS on web server  
  
Data exfiltration  
-Unauthorized transfer or storage of data  
-Solution: Data Loss Prevention (DLP)  
  
Security Configuration  
-Misconfigured devices / not enabling security features / firewall rules / default passwords  
-Baselines established by government / industries (PCI/HIPAA)  
  
Application Issues  
-Unauthorized software, license compliance violations  
  
Logs and events anomalies  
-Process of collecting data for monitoring and auditing purposes  
-Logging standards for platforms, apps, servers  
-SOC, Use of SIEM, Centralized Logging  
  
Personnel Issues  
-Insider threat, social media, policy violation  
-Solution: Policies and security awareness training  
  
  
**2.4 Analyze and Interpret output from security technologies**Host Technologies – Firewalls  
-Firewalls and Firewall configuration: Users shouldn’t be allowed to disable firewall, monitor both incoming and outgoing traffic  
-Windows Event Viewer and Linux Logging  
  
Host Technologies – HIDS/HIPS  
-Provide sensors on each host relay to a centralized management console  
-May be included with Host Firewall or AntiVirus solution   
-Issues: False positives / False Negatives   
  
Antivirus / Anti-malware  
-Windows defender on WIN 10  
Problems:  
-End user pop up warning  
-Centralized management console warning  
-Quarantine vs Removal  
  
File Integrity Checker  
-Computes a crypto hash for all selected files and creates a database of the hashes  
-Hashes are periodically recalculated and compared to hashes in database to check for modification  
-Output to centralized server   
-Tripwire app

Data Loss Prevention (DLP)  
-Prevent sensitive info from physically or logically leaving system  
-Designed to detect and prevent unauthorized use and transmission of info  
-Network: Content-filtering (proxy)  
-System: Application white-listing  
-Hardware: USB blocking  
  
Patching Process  
1. Vendor notification  
2. Testing  
3. Staged deployment  
4. Reporting

Patch Management Services  
-Microsoft System Center Configuration Manager (SCCM)  
-Linux RPM (Red Hat Package Manager)  
  
Unified Threat Management (UTM) Next Generation Firewall (NGFW)  
-An all in one firewall / single interface / single vendor  
-Management console with URL filtering, content inspection and malware inspection  
  
**2.5 Mobile Security**  
Cellular Communications  
-Components: Cellular towers, base station, mobile switching office, public switched telephone network  
-Voice technologies: Long-term evolution (LTE) Code division multiple access, global systems mobile  
  
Connection methods: WI-fi, Bluetooth, NFC, SATCOM, ANT, Infrared, USB  
  
Bluetooth  
-Personal-area network, short range connectivity  
-Uses spread spectrum, frequency hopping and full-duplex signal  
-Pairing devices form a piconet  
-Bluesnarfing / bluejacking  
-Set to non discoverable

Near-Field Communication (NFC)  
-Standards for contactless communication between devices  
-Chips generate electromagnetic fields  
-Peer to peer, Read/write, card emulation mode

Mobile Device Management (MDM)  
-Administration of mobile devices in an organization  
-Software used to inventory, monitor, manage and secure employees mobile devices  
  
Mobile Application Management(MAM)  
-Restricting apps, distribution from centralized controlled source, white and blacklisting   
  
Mobile Content Management(MCM)  
-Control access to data and file storage  
  
Mobile Device management concepts  
-Separate personal and business content  
-Storage segmentation, segregates business and personal storage  
-Containerization separates sensitive corporate info from users personal use of device  
-Remote wipe / sanitization sends a command to clear data  
-Full device encryption   
-Biometrics  
-Context-aware authentication (Authentication with location, time,etc)  
  
Geolocation: Uses devices GPS  
Geofencing: Defining a geographic perimeter

Deployment Models  
Bring your own device (BYOD):  
-Highest risk  
Choose your own device (CYOD):  
-Employees choose from list of approved devices  
Company owned provided equipment (COPE)  
-Company has complete control over device  
Virtual desktop Infrastructure (VDI)  
  
Enforcement and Monitoring  
-Third party app store restriction  
-Rooting Jailbreaking   
-Sideloading (transfer between 2 devices)  
-USB on the go  
-Custom firmware  
-Carrier unlocking  
  
Containerization: Controls access to file storage and sharing capabilities of services   
  
**2.5 Security Protocols**Web protocols  
Secure sockets layer (SSL):  
-Uses certificates for authentication and encryption for message integrity and confidentiality  
-Stateful connection  
Transport Layer Security (TLS):  
-Provides privacy, message integrity and authentication   
-Forward secrecy ensures that any future disclosure of encryption keys cannot be used to decrypt any TLS comms recorded in the past  
HTTPS:  
-Uses SSL/TLS to secure web-based comms  
  
DNSSEC  
-Domain name service security  
-Protects against DNS cache poisoning  
  
Secure Shell (SSH)  
-Replaces telnet for remote comms  
-Establishes session between client and host computers using authenticated and encrypted connection  
-Uses asymmetric RSA crypto for both connection and authentication  
  
Secure Email:  
S/MIME:   
-Standard for encryption and signing of email data  
-Requires PKI and uses Certificate Authorities  
POP3S and IMAPS:  
-Use SSL to secure emails in transit between POP or IMAP server  
  
FTPS – Securing FTP  
-File transfer protocol, passes credentials in clear text  
-FTPS adds SSL/TLS protocol to text (Authentication/Data confidentiality/ FTPS port 990/ FTPS port 21)  
-SFTP uses SSH to transfer files  
  
  
SRTP  
-Secure voice and video transmission  
-Voice and video calls are established with session initiation protocol and data transmitted with real-time transfer protocol  
  
LDAPS  
-LDAP is directory protocol  
-Attackers may sniff network to read unencrypted LDAP traffic  
-LDAPS uses SSL/TLS to protect over TCP port 636   
  
SNMPv3  
-Used to manage networks  
-Each managed device has software agent reporting config settings and alerts to a central SNMP management server  
-SNMPv3 encrypts data  
  
Use Cases – Network Address Allocation  
-Dynamic host control protocol (DHCP) assigns internal IP addresses   
-Use of network subnets to segregate multiple hosts and control network traffic   
  
IPv4 Address Classes  
0 to 127 = Very Large networks  
128 to 191 = Medium Networks  
192 to 223 = small networks   
224 to 239 = multicast   
240 to 247 = experimental  
  
Use case – Time synchronization  
-Network Time Protocol is a UDP protocol used to synch time based on atomic clock  
-NTP servers are redundant and secured   
  
Use case – Subscription Services   
-Software as a services (SaaS)  
-Cloud email example  
-Network defenses such as firewall / IDS / IPS / Web and app filtering / Anti-virus / Patching

**Domain 3 – Architecture and Design  
  
3.1 Cybersecurity Frameworks**Types of Frameworks  
-Regulatory (Mandated by law) vs Non-regulatory   
-National vs international   
-Industry specific frameworks  
  
Industry Standard Frameworks  
-International Organization Standardization (ISO)  
-National Institute of standards and tech (NIST)  
-Center for internet security (CIS)  
-Open Web App Security Project (OWASP)   
  
ISO 27001: 2013  
-Specifies requirements for establishing, implementing, maintain and improving an info security management system  
  
ISO 27002: 2013  
-Guidelines for organizational info security standards and info security managements practices including selection, implementation and management of controls in security risk environments   
  
ISO/IEC 27017:2015  
-Guidelines for info security controls applicable to provision and use of cloud services

NIST  
-US national standards  
-Group of related standards designed to provide guidance on cybersecurity  
SP 800-30 Guide for conducting risk assessment  
SP 800-35 Guide to info tech security services  
SP 800-53 Security and privacy controls for federal info systems and organizations  
SP 80054A Assess security and privacy controls in federal info systems and organizations

Payment Card Industry Data Security Standards (PCI-DSS)  
-Used by VISA, mastercard, Apex  
-Creates common security controls for protection for Card Holder Data  
  
Benchmarks / Secure Configuration Guides  
-Security Tech Implementation Guides, contain tech guidance to lock down info systems that may be vulnerable  
-Center for internet security benchmarks: best practices for secure config of target system  
  
Platform specific guides  
-Network: Cisco  
-Operating System: Microsoft Technet, MacIntosh, Linux  
-Web server: Microsoft IIS, Apache  
  
Defense in Depth / Layered Security   
-Defense in Depth is coordinated use of multiple security countermeasures to info assets  
-Segmentation is the act or practice of splitting a computer network into zones or subnetworks based on business function or security needs  
-Control diversity: Addressing security concern using multiple controls that don’t depend on eachother  
-Vendor diversity: Addressing security concern using multiple vendor products  
-User Training: reduce impact of threats and vulns  
  
ISO/IEC 27017:2015 gives guidelines for info security controls applicable to use of cloud services

**3.2 Network Architecture**

Security Zones / Topologies  
-Each zone on a network is separated based on organizational role or level of security  
-Secure Zone: Sensitive systems, with mission-critical data  
-General Work Zone: Standard work stations and servers, typical data and functionality  
-Low Security Zone: Computers, network segments and systems that have no high sensitivity info  
  
Demilitarized Zone (DMZ)  
-A network segment located between protected (internal) and unprotected (public) networks  
-Provides a buffer zone/defense-in-depth  
-Usually set up using firewalls  
-Contains hardened systems that need to reach each network segment  
  
Extranet / Intranet  
-Extranet: Private network that uses internet tech and public telecom system to securely share part of a business’s info or operations with suppliers, vendors, partners, etc  
-Intranet: Website or app that are only accessible within organizations network  
  
Wireless Segmentation  
-Separate wireless access on internal network, creating buffer between wireless and wires  
-Controlled by 801.1X port based access control  
-MAC filtering

Security Device Placement  
-Firewall/Unified Threat management system placed between internal network and internet  
-VPN remote access  
-Proxies in between internal users and external websites   
-Load balancers between 2 networks   
-DDoS mitigation placed in border router

Firewall Functions:  
-Packet filter  
-Proxy firewall  
-Stateful packet inspection  
  
Intrusion Detection (IDS) / Protection System (IPS)  
-Sensors collect data and react to detected events (Traffic outside normal, signatures, behavior, heuristics)  
-NIDS / NIPS are network based  
  
Segregation, Segmentation and Isolation  
-Dividing network into zones based on business security needs  
-Logical (VLAN): Network of pcs that behave as if they are connected to the same wire   
-Virtualization: virtual servers easy to separate  
-Air gaps: physical separation, diff networks  
  
Virtual Local Area Network  
-VLAN 1 Management 10.X1.0/24  
-VLAN 2 Computers 10.X.2.0/24  
-VLAN 3 VoIP 10.X.3.0/24  
-VLAN 4 Cameras 10.X.4.0/24  
  
Software Defined Network (SDN)  
-Entire network is virtualized, which allows for easier network segmentation  
-Allows admins to place virtualized security devices anywhere  
-SDN Architecture is: Agile, Centrally manages, Open standards-based, Directly programmable  
  
Honeypots / Honeynets  
-Systems or networks meant to be breached, to capture malicious activity

**3.3 Systems Design**Hardware/Firmware Security  
-Full disk encryption (FDE): Bitlocker, veracrypt  
-Self-encrypting Drive (SED): Automatically encrypts a drive  
-Trusted Platform Modules (TPM): A special chip on endpoint device that stores encryption keys specific to host system for hardware authentication. Usually on a motherboard  
-Hardware Security Modules (HSM): Physical computing device that safeguards and manages digital keys for strong auth and crypto processing  
-BIOS: boot-up config  
-Unified Extensible firmware Interface (UEFI): Modern boot-up config  
-Secure boot and attestation: crypto hash of BIOS/UEFI OS boot loader and drivers, compares that against stored hash. Prevents rootkits and boot sector viruses  
-Root of Trust (RoT): Reliable hardware, firmware and software components that perform specific functions  
-Supply Chain: Confirming the origin of hardware is secure

Operating System Types  
-Network, Server, Workstation, Appliance, Kiosk, Mobile OS   
  
OS Security  
-Patch management: Set of changes to program. Hotfix are small updates, service pack is collection of hotfixes, updates provide big improvements and upgrades are new versions  
  
**3.4 Staging**-Secure baseline: Process where you use a security standard for any system, app, or service that is considered secure to create your own security benchmark  
  
Environments  
-Separating environments for increased sec  
-Development environment, Test, Staging, Production and Sandboxing  
  
Sandboxing  
-Safe execution environment for untrusted programs  
-Allows programs and processes to be run in an isolated environment to limit access to files and host system

**3.5 Embedded Systems**Embedded Systems-Dedicated computer system dedicated on performing specific function   
-Smart devices, HVAC, Cameras, Printers, etc.   
-One that has software embedded within the hardware, usually with read only memory  
  
System on a Chip (SoC)  
-Integrated circuit that integrates all components of a computer or other electronic systems on a single computer chip  
  
Real-Time Operating Systems (RTOSs)  
-An OS intended to serve real-time application that process data as it comes in, without buffer delays  
-Designed to have 0 latency (Military, Space)  
  
Internet of Things (IoT)  
-System of interrelated computing devices, machines, objects, etc that are provided with unique identifiers and ability to transfer data over a network without human-to-human interaction  
  
Industrial Control Systems (ICS) / SCADA  
-ICS encompasses several types of control systems and instrumentation used for industrial process control  
-Supervisor Control and Data Acquisition are used by utilities and manufacturing that collect data and control system  
-Programmable Logic Controllers (PLC) are single use pcs used in manufacturing  
  
Securing Embedded Devices  
-Secure by design/default  
-Shield from electromagnetic interference  
-Encrypt networks using TLS  
-Automated patching  
-Anomaly alerts  
  
**3.6 AppSec**

Software Development Life-Cycle Models  
-Waterfall: Requirements gathering, design, implementation/coding, testing/verification, deployment, and maintenance. Each stage is self-contained and completed in order  
-Agile: Works in cycles with each cycle producing deliverables. Scrum, Adaptive Software Dev, Crystal, Feature-driven, Lean Software Dev

Secure DevOps  
-Security integrated into all of your dev operations, which includes database design, programming and infrastructure  
-Having security practices integrated into software delivery cycle  
-Continuous integration: security in every step  
-Security automation  
-Baselining: reference points that require completion and approval of project reqs  
-Immutable systems: no changing to systems  
-Infrastructure as code (IaC): programmable infrastructure  
  
Compiled vs Runtime code  
-Compiled: C or C++  
-Runtime: Java or .NET (Faster but less secure)

Change Management / Version Control  
-Control and manage software changes for quality and security  
-Version control prevents tampering of source code, tracks software file changes and uses distributed storage for code  
-Benefits: Historical data on changes to files, breaching and merging capabilities, traceability  
  
Provisioning and Deprovisioning-Provisioning: creation/update of resource  
-Deprovisioning: removal of resource  
-Generally automated where software packages are made available to users

Secure Coding Techniques  
-Authentication, use cookies or hard code credentials  
-Proper error handling, comments shouldn’t be visible, errors should be generic  
-Proper input validation  
-Normalization, converts data to simplest known form  
-Stored procedures, associated with database queries  
-Code reuse / dead code, no longer provide useful function  
-Third party libraries, check for CVE  
-Code signing, sign executable code using certificate based signature which provides code integrity  
-Data exposure, encrypts sensitive data   
-Encryption  
-Obfuscation/camouflage, hide back-end code  
-Memory management, optimizes performance by assigning blocks of memory to processes  
-Server side: back-end server housing app code, protect against malicious attacks  
-Client side: entered data is validated via script before being sent to server

**3.7 Could concepts**

Cloud computing: A model for enabling convenient, on-demand network access to shared pool of configurable resources

On-premise vs Hosted vs Cloud  
-Servers at organizations location (You control physical access)  
-Servers outsourced to external provider (They are responsible for security)  
-Using shared servers

Could computing service models  
Software as a service (SaaS):  
-Uses providers application running on cloud infrastructure. The apps are accessible from various client devices through web browser. Consumer does not manage or control anything.  
Platform as a Service (PaaS):  
-Deploy onto cloud consumer-created application . Consumer does not manage or control anything except the deployed applications  
Infrastructure as a Service (IaaS):  
-Processing, storage, network where consumer deploys software. Consumer does not manage anything but has control over operating systems, storage and apps.

Cloud Deployment Models  
-Private cloud: Intended for single tenant  
-Hybrid Cloud: Bridges one or more private, public or community cloud  
-Community Cloud: Bring together groups with common goal, resource portability  
-Public Cloud: Pay as you go, supports multiple tenants  
  
Hypervisors  
-Underlying tech that creates and runs VMs  
-Presents guest OS with virtual operating platform and manages execution of the guest OS’s  
-Two implementation methods: Native(Independent of OS) and Hosted(cannot boot till os is running)  
  
Containers  
-Replace or used with hypervisors  
-Lightweight, stand-alone, executable package that includes everything needed to run it

Virtual Desktop Environment / Infrastructure  
-VDE: Desktop virtualizations  
-VDI: User’s desktop runs inside a VM that resides on server in a datacenter  
  
Cloud Storage – Network Storage  
-DSA (direct attached storage)  
-NAS (network area storage)  
-SANs(storage area networks)  
  
Virtualization Security  
-VM Escape Protection: leaving an assigned VM  
-VM Sprawl Avoidance: Overusing shared resources   
-Cloud access security broker (CASB) are security policy enforcement points  
-Security as a service: subscription based model for managing security functions  
  
Elasticity: Cloud feature involving dynamically allocating resources  
  
**3.8 Resiliency**  
  
Automation/scripting  
-Reduces risk through repeatable processes and automated courses of action  
-Leveraging sophisticated monitors and sensors  
-Config validation  
-OS scripting languages (Linux: Bash / Windows: Powershell)

Frameworks and Templates  
-Baselines using standard templates, compare current state vs desired state  
  
Master Image  
-Creating a model OS verified as clean  
-Used for system restores  
  
Managing Cloud Risk  
-Nonpersistence: Temporary system images  
-Elasticity/scalability: Adjust resources as needed  
-High Availability: measures redundancy, failover and mirroring   
-Redundancy: Replicate systems at multiple sites  
-Distributive allocation / Load balancing: distribute burden across multiple systems

Fault Tolerance  
-Ability of a system to sustain operations in case of component failure  
-Two key components: Spare parts and electric power   
RAID Storage  
-Redundant array of inexpensive disks  
-Focuses on availability of data  
-Raid types:  
0 – Disk striping  
1 – Disk mirroring  
3 – Disk striping with parity disk  
5 – Disk striping with parity   
  
 **3.9 Physical Security**

Physical Security Concepts  
-Protection Detection Delay Deterrence  
  
Lighting   
-Used for deterrence, should be in protected, locked, central areas.  
-Response Area Illumination: Takes place when IDS detects sus activities and turns on light  
  
Perimeter Security  
-Fencing, gates  
-CPTED: Crime Prevention Through Environmental Design  
  
Locks  
-Combination locks, Cipher locks  
-Lock grades:   
Grade 1 – commercial   
Grade 2 – heavy duty residential  
Grade 3 – Residential trash locks  
-Cylinder categories:  
Low: no pick resistance  
Medium: little resistance  
High: high resistance  
  
Physical Access Control (Turnstiles)  
  
  
Faraday Cage / Shielding  
-Shielding prevents electronic emissions from your computer systems from being used to gather intel and preventing outside electronic emissions from disrupting info (Microwave)  
-Faraday cage is an enclosure to block electromagnetic fields  
  
Personnel access controls  
-User activated (swipe cards)  
-Proximity devices  
  
Site Access Controls  
-Key cards: Centralized access control, easy 2 use, provides audit record, each permissions  
  
Biometric Access Controls  
-Fingerprint, iris recognition  
-Based on biometric measurement

Fire Extinguisher Ratings  
-A: wood and paper   
-B: flammable liquids  
-C: Electrical  
-D: Flammable Metals

Sprinkler Systems  
-Wet pipe, filled with pressurized water  
-Dry pipe, fills with water when activated  
-Deluge, discharges water from all sprinklers  
-Pre action, dry pipe that turns to wet pipe when activated  
-Foam water uses water and fire-retard foam  
-Gaseous fire suppression, displaces oxygen

**4.1 Identity and Access Management Concepts**Identification & Authentication  
-Identification is the 1st step, subject provides ID info (username, account #)  
-Authentication verifies the ID info, proving identity (pass)  
  
Authorization & Auditing  
-Authorization is what the subject is allowed to see or do, permissions  
-Auditing/Accounting is the record of events, logs

Authentication Factors  
-Something you know (pass)  
-Something you have (token)  
-Something you are (biometrics)  
-Something you do (actions for authentication)  
-Somewhere you are (geolocation)  
  
Authentication   
-Single Factor (FSA): traditionally a password  
-Multi-Factor Authentication (MFA): 2 or more access methods  
-Mutual authentication: each party validates the others identity  
  
Biometric Errors  
-False Acceptance Rate (FAR): When system accepts intruder  
-False Rejection Rate (FRR): When system reject authorized user  
-Cross over Error Rate (CER): Metric for comparing biometric systems  
  
Federation / Federated Identity  
-Linking person’s electronic identity and attributes, stored across multiple ID management systems  
-Means of linking a users identity with their privs   
-Allows user to have single identity that they can use across businesses  
  
Single Sign-On(SSO)  
-Allows user to authenticate one time   
-Vuln: If attacker uncovers user’s credentials  
-Single point of failure  
  
Transitive Access / Trust  
-In a transitive trust, if Domain A trust Domain B and Domain B trust Domain C, then Domain A also trust Domain C

**4.2 Access Protocols**Directories / Directory Service Protocols  
-Repositories of an organizations network resources and users  
-Most follow hierarchical database format X.500 standard  
-A directory service manages the entries and data in the dir and enables access control and ID management (LDAP, Microsoft AD)

Lightweight Directory Access Protocol (LDAP)  
-A standardized dir access protocol  
-Main purpose it the query the LDAP user database  
-Supported by most major vendors  
-Hierarchical structure

LDAP Security  
-Vulnerable to snooping, buffer overflow, format string vulns  
-Encrypt comms using SSL/TLS   
-Certificates can validate authentication requests  
-LDAPv3 bind request should use Authentication and Security Layer  
  
Kerberos  
-A symmetric key authentication protocol   
-Kerberos v5 uses mutual authentication between requesting client and the supporting server through Key Distribution Center (KDC)  
-Once authenticated, user if given ticket granting ticket (TGT)   
  
Kerberos Authentication Process  
-Each time user wishes to access some resource ,users computer presents KDC with TGT  
-The TGT then sends that computer a service ticket, granting service  
-Users pc then sends service ticket to server   
-As final auth check the server comms with TGT to confirm and validate ticket  
  
Remote Auth Dial-In User Service (RADIUS)  
-An IETF standard  
-Uses UDP transport to a centralized server providing auth and access control for networks  
  
Terminal Access Controller Access Control System Plus (TACACS+)  
-Handles auth, authorization, and accounting (AAA) services  
-TCP rather than UDP as transport method  
-Takes a client/server model approach  
-Advantages over RADIUS: TCP rather than UDP, encrypts entire packet not just auth, controls authorization of router commands  
  
Password Authentication Protocol (PAP)  
-Legacy protocol that should no longer be used  
-User ID and pass sent in clear text

Challenge Handshake Authentication Protocol (CHAP)   
-Provides on-demand auth over encrypted channels   
-Client generates a one-way hashing function (MD5) and sends to service  
-Client hash is compares against services hash  
  
MSCHAP & PEAP  
-MSCHAPv2 uses new string each time for auth, client & server mutually authenticate and use 2 encryption keys  
-Use MS-CHAP with Protected Extensible Auth Protocol (PEAP) which provides TLS/SSL tunnel, which protects authentication traffic and uses certificate on auth server  
  
NTLM (NT Lan Manager)  
-Legacy auth from MS  
-Replaced by Kerberos  
-Weak crypto scheme  
  
Federated Services  
-Security Assertion Markup Language (SAML)  
-Simple Web tokens and JSON Web tokens  
  
Security Assertion Markup Language (SAML)  
-An extensible markup language framework for creating and exchanging security info between online systems  
3 main functions:  
1. User seeking to verify its identity is the principal  
2. The entity that can verify the ID of the user is the ID provider  
3. The entity that uses the ID provider to verify the ID of the user is service provider   
  
Open Authorization (OAuth)  
-Framework used for internet token-based auth  
-Purpose is API auth between apps  
-Allows access token to be issues to 3rd party clients with approval of resource owner  
-OAuth2.0 uses JSON and HTTP protocols  
  
OpenID and OpenID Connect  
-An identity layer based on OAuth 2.0 specs  
-OpenID Connect implements auth as an extension to OAuth2.0 process  
-Uses an ID token structure including the auth of an end user via a JSON web token (JWT)  
A JWT is used to prove that an authentic source created the originating data

**4.3 Implement Identity and Access Management Controls Models**  
Access Control Models  
Terms:  
-Subject is an active entity   
-Object is some resource that the subject is attempting to access  
  
Mandatory Access Control (MAC)  
-Assigning labels to resources and accounts  
-Used in government / military  
-Rigid and most secure  
  
Discretionary Access Control  
-Access rights at discretion of sys or info owner  
-Owner assigns access   
  
Attribute Based Access Control (ABAC)  
-Defined in NIST 800-1622  
-Attributes are characteristics that define specific aspects of the subject, object, etc that are predefined by an authority  
-Based on Extensible Access Control Markup Language  
  
RBACs  
-Role based access control: Access control based on roles or job function, group-based permissions  
-Rule based access control: Uses settings in preconfigured sec policies to make all access decisions. Implemented with Access Control Lists  
  
Tokens  
-Physical device used for access  
-One time password (OTP), time based or hashed  
-Contains digital certificate / static password token  
  
Physical Access Controls  
-Both use Embedded microchips  
-Proximity cards / Smart cards

Certificated-based auth  
-Personal ID verification (PIV) cards  
-Common Access Card (CAC)   
-IEEE 802.1X only auth devices to connect  
  
File System Security  
-Leverage access controls, encryption and RAID  
-MS NTFS allows file-level access control where FAT allows only share-level access  
  
Database Security  
-Leverage network sec & access controls within the DBMS  
-Transparent Data Encryption (TDE)  
-Crypto key mgmt.  
  
-Token provide credentials valid only during a single session (OTP one time pass)  
 -ABAC can be used when you are looking to implement a new access control mech that takes into account the entire environment and req actions for access  
  
  
**4.4 Account Management Practices**General Concepts  
-Onboarding/offboarding: when employee joins and leaves organization  
-Standard naming conventions  
-Least privilege: access control practice, where log on gives minimum resource for type of user  
-Time-of-day restrictions: only allow employees to log in at a set time  
-Location based policies: sign in from corporate office only   
-Group based access control: if you are member of group, you have access to a set of resources  
-Account maintenance / privilege audit: evaluate accounts in infrastructure   
-Recertification / permission creep: recertify or remove privs no longer needed   
-Permission auditing and review: watch what people are doing  
-Usage auditing and access review  
  
Account Types  
-User accounts  
-Guest accounts  
-Shared and generic accounts  
-Service accounts: used by systems / apps   
-Privileged accounts / admins   
  
  
Account Policy Enforcement  
-Credential management  
-Group policy  
-Password policies  
-Expiration  
-Recovery  
-Locking accounts   
  
Windows Password Policies  
-Enforce password history  
-Max/min password age  
-Min password length  
-Password complexity reqs  
-Store passwords using reversible encryption  
  
Windows Account Lockout Policies  
-Account lockout duration  
-Account lockout threshold  
-Reset account lockout counter after  
  
Windows Audit Policies  
-Logon events  
-Account mgmt.  
-Dir service access  
-Process tracking  
-System events  
  
Other Windows Access Policies  
-Admin/Guest status  
-Renaming accounts  
-Audit system objs / backup and restore points  
-DCOM machine access restriction  
-Restrict floppy/cd-rom/printers   
  
Linux Password Policies  
-Min/max lifetime  
-History size  
-Char classes  
-Min length  
  
-Setting up account for SQL server system, what is best account to use? Service account  
-Recertification is the annual auditing whereby you determine if accounts continue to req a set of privs

**5.1 Personnel Policies**