**1.0 Threats, Attacks, and Vulnerabilities**

**1.1 Compare and contrast different types of social engineering techniques**

Social engineering: eliciting information from someone or getting them to perform some action for the threat actor; can be used to gather intel. 74

• **Phishing**: social engineering + spoofing; email-based attack where attacker sends email from a seemingly trusted source to try to elicit private info from victim or to infect with malware. 77

• **Smishing**: SMS (text) phishing to trick a person into revealing info. 78

• **Vishing**: voice over IP phishing to trick a person into revealing info. 78

• **Spam**: unsolicited email that gets sent in masse. 78

• **Spam over instant messaging (SPIM)**: spam attack through text messaging. 79

• **Spear phishing**: email-based phishing that targets specific individuals. 78

• **Dumpster diving**: discovering things about an organization based on what it throws away. 76

• **Shoulder surfing**: peeking over someone’s shoulder to obtain password or PIN as they type it. 77

• **Pharming**: impersonation attack where a request for a website is redirected to a fake website. 79

• **Tailgating**: following closely behind someone to gain access to a building that has a key card entry. 76

• **Eliciting information**: extracting information during a seemingly normal & innocent conversation

• **Whaling**: spear fishing attack aimed at upper-level management/senior execs or wealthy people. 78

• **Prepending**: adding text that appears to have been generated by the email system. 79

• **Identity fraud**: impersonation. attacker uses specific details of someone’s identity. Name, address. 77

• **Invoice scams**: type of identity fraud, spoof invoice details of genuine supplier but change bank acct #

• **Credential harvesting**: steal account credentials through pharming, malvertising or injected scripts. 80

• **Reconnaissance**: gathering information about the target computer systems, supply chains to prepare for an attack. 76

• **Hoax**: examples are security alerts or chain emails intended to deceive the victim. 79

• **Impersonation**: pretending to be someone else. 75

• **Watering hole attack**: attacker targets specific groups or organizations through injecting malicious code into the websites the people tend to frequent such as an insecure third part website. 79

• **Typosquatting**: attacker registers a domain name with a common misspelling of an existing domain so that a user who misspells the URL in a browser is taken to the attacker’s website... URL hijacking. 79

• **Pretexting**: attacker comes up with a fabricated story to gain victim’s trust and manipulate them into sharing sensitive info, downloading malware, sending money etc. 75

• **Influence campaigns**: major program launched by an adversary with a high level of capability such as a nation-state actor, terrorist group or hacktivist group. Goal is to shift public opinion on a topic. 80

- **Hybrid warfare**: conventional and unconventional actions such as espionage, disinformation campaigns/fake news, hacking, cyber-attacks, election meddling. 80

- **Social media**: hoaxes can be widely spread through social media. 80

• **Social Engineering Principles** (reasons for effectiveness) 75

- **Authority/intimidation**: people find it difficult to refuse a request by someone they perceive as superior… use intimidation or technical arguments and jargon… people don’t want to admit ignorance

- **Consensus/social proof**: people will act as they think others would act… be persuaded into thinking that to refuse a request would be odd/something people don’t normally say no to

- **Scarcity/urgency**: target is pressured to make a quick response or is made to believe it is a limited time offer

- **Familiarity/liking**: social engineer is affable and likeable and presents requests as reasonable

- **Trust**: impersonator establishes trust with target with use of privileged info

**1.2 Given a scenario, analyze potential indicators to determine the type of attack.**

• **Malware**: software that is intentionally designed to cause disruption/perform malicious actions

- **Ransomware**: malware that is used to try to extort money from the victims. 88

- **Trojans**: malware concealed within an installer package for software that appears to be legitimate. Tries to compromise the security of the computer. 82

- **Worms**: malware that replicates in system memory and can spread over network connections rather than infecting files… don’t need user intervention to run. 84

- **Potentially unwanted programs (PUPs)**: software installed alongside a package selected by the user or perhaps bundled with a new computer system. Grayware. 82

- **Fileless virus**: does not write code to disk, uses memory resident techniques to run its processes; uses lightweight shellcode to achieve a backdoor mechanism on the host to evade detection; uses legitimate system scripting tools to execute payload actions. Resides in RAM… within a Powershell script. 85

- **Command and control (C2)**: use of a covert channel or backdoor between server and compromised network or machine to communicate with and control the machine or network. 87

- **Bots**: automated script or tool that performs some malicious activity. Group of bots that are under the same control is called a botnet. Botnet is used for DDoS attacks. 86

- **Cryptomalware**: malware that attempts to encrypt data files on any drives. Used as a form of ransomware where user is unable to access files without encryption key they have to pay for. 89

- **Logic bombs**: malicious code that is set to run at a pre-configured date or time. 89

- **Spyware**: malware that performs tracking and monitoring, takes screenshots, activates recording devices. 65

- **Keyloggers**: spyware that attempts to steal confidential info by recording keystrokes. 85

- **Remote access Trojan (RAT)**: backdoor malware that is capable of operating covertly. Allows the actor to access the host, upload files, install software and change settings. 86

- **Rootkit**: malware that modifies system files at kernel level to conceal its presence. 87

- **Backdoor**: access method to a host that circumvents the usual authentication method and gives the remote user administrative control. 86

• **Password attacks** 159

- **Spraying**: horizontal brute force online attack where attacker chooses one or more common passwords and tries them in conjunction with multiple usernames. Bypasses account lockout policies. 159

- **Dictionary attack**: software generates hash values from a dictionary of plaintexts to try to match one to a captured hash. Predefined list of words. 160

- **Brute force**: attempts every possible combination in the output space in order to match a captured hash and guess at the plaintext that generated it. 160

- **Offline attack**: attacker obtained a database of password hashes and the cracker does not interact with the authentication system… will only be seen in an audit log or presence of attack tools on host. 159

- **Online**: attacker interacts with the authentication service directly and submits passwords using a database of known passwords or a list of passwords that have been cracked offline. 159

- **Rainbow table**: attacker uses a precomputed lookup table of all possible passwords and their matching hashes… slow down this attack by adding a salt. 160

- **Plaintext/unencrypted attack**: exploits password storage or a network authentication protocol that does not use encryption…protocols such as PAP, HTTP/FTP, and Telnet. 159

• **Physical attacks**

- **Malicious Universal Serial Bus (USB) cable**: modified USB device that can be used as a keylogger. 321

- **Malicious flash drive**: modified flash drive that can be used as a keylogger or a network device and corrupt name resolution. 321

- **Card cloning**: making one or more copies of a card. Can be indicated through use in a suspicious location of time of day. 543

- **Skimming**: using a counterfeit card reader to capture card details which is then used to program a duplicate… threat actor can have a portable RFID reader on them to capture credentials. 543

• **Adversarial artificial intelligence (AI)**: manipulated sample data injected into AI that affects the training/learning of the AI in a way to prevent it from achieving its intended security objectives. 480

- Tainted training data for machine learning (ML)

- Security of machine learning algorithms: they are sensitive to noise

• **Supply-chain attacks**: attacker can infiltrate multiple companies linked through supply chain. 23

• **Cloud-based vs. on-premises attacks**: software and configuration vulnerabilities and third-party vendor management can exist on a private network or on the cloud. 55

• **Cryptographic attacks**

- **Birthday attack**: a type of brute force attack aimed at exploiting collisions in hash functions. Can be used for forging a digital signature. Benign document and malicious one, take signature from benign and throw it on the malicious one. Probability theory. 117

- **Collision**: when a function produces the same hash value for two different plaintexts. 117

- **Downgrade attack**: can facilitate a man-in-the-middle attack by requesting that the server use a lower specification protocol with weaker ciphers and key lengths. 116

**1.3 Given a scenario, analyze potential indicators associated with application attacks.**

• **Privilege escalation**: attacker can access functionality or data that should not be available to them (vertical privilege escalation) or attacker can access functionality or data that is intended for another user (horizontal privilege escalation). 366

• **Cross-site scripting**: inserting a malicious script that appears to be part of a trusted site. 376

• **Injections**: exploits an unsecure way in which an application processes requests & query. 378

- **Structured query language (SQL) injection**: attacker modifies the select, insert, delete or update functions by adding code to some input accepted by the app, causing it to execute the attacker’s own set of SQL queries…they can extract or insert info into the database or execute arbitrary code using the same privileges as the database application. Countermeasure: stored procedures & input validation. 378

- **Dynamic-link library (DLL) injection**: vulnerability in the way the operating system allows one process to attach to another making it so that a legitimate process is forced to load a malicious link library. DLL must be operating with sufficient privileges already and evade detection by antivirus software. 369

- **Lightweight Directory Access Protocol (LDAP) injection**: LDAP is a query language used to read and write network directory databases… threat actor can exploit unauthenticated access or a vulnerability in a client app to submit arbitrary LDAP queries… this would allow accounts to be created or deleted or for the attacker to change privileges and authorizations. Adding filter parameters as unsanitized input can bypass access controls.

- **Extensible Markup Language (XML) injection**: XML is used by apps for authentications and authorizations and data exchange and uploading. Data needs encryption and input validation so it does not become susceptible to spoofing, request forgery and code injection. 378

• **Pointer/object dereference**: pointer is a variable that stores a memory location; pointer dereferencing is attempting to read or write a memory address via the pointer that produces the memory location as invalid or null… this might allow a threat actor to run arbitrary code.

• **Race conditions**: when the outcome from an execution process is directly dependent on the order and timing of certain events, and those events fail to execute in the order and timing intended by the developer. 368

- **Time of check/time of use**: when there is a change between when an app checked a resource and when the app used the resource. Attacker will attempt to manipulate data after it has been checked but before it has been used by the application. 368

• **Directory traversal**: injection attack performed against a web server. Threat actor submits a request for a file outside the web server’s root directory by submitting a path to navigate to the parent directory… if input is not filtered. (../)

• **Buffer overflows**: attacker passes data that deliberately overfills the buffer, which is an area of memory that is reserved to store expected data. Get unpredictable results. 367

• **Error handling**: process of responding to and recovering from error conditions in a program. Application should not reveal configuration or platform details when there is an error. 367

• **Improper input handling/validation**: input should be tested to ensure that it is valid. Attacks pass invalid or maliciously constructed data to the vulnerable process. Exp Overflow or injection attacks. 367

• **Replay attack**: sniffing or guessing the token value and then submitting it to re-establish the session illegitimately. 374

- **Session replays**: replaying a cookie… attackers sniff network traffic to obtain session cookies sent over an unsecured network. Identify possible weakness in the generation of session tokens so attacker can’t predict future valid tokens and take over a session that has yet to be established. 375

• **Integer overflow**: causes target software to calculate a value that excess the upper and lower bounds of integers causing a positive number to become negative etc. 368

• **Request forgeries**

- **Server-side**: 380. Causes server application to process an arbitrary request that targets another service. Exploits the lack of authentication between internal servers and services and weak input validation. 380

- **Cross-site**: 375. exploit applications that use cookies to authenticate users & track sessions

• **Application programming interface (API) attacks**: APIs allow consumers to automate services. API must be used over an encrypted channel (HTTPS). Vulnerabilities include ineffective secrets management, lack of input validation, error messages revealing clues, or DoS attacks. 374

• **Resource exhaustion**: overuse of CPU time, system memory allocation, fixed disk capacity and network utilization. Exp. DoS attack. 368

• **Memory leak**: continue to consume memory even after a program no longer requires the block of memory because it doesn’t release it… this could be due to a corrupted process. 368

• **Secure Sockets Layer (SSL) stripping**: on path + downgrade attack. performed on clients on a local network as they try to make connections to websites. First is man-in-the-middle attack via ARP poisoning to masquerade default gateway. Then client requests an HTTP site that redirects to an HTTPS site unsafely and the sslstrip utility serves the client the HTTP site in unencrypted manner. SSL is a deprecated encryption protocol. 376

* **Driver manipulation**

- **Shimming**: attacker inserts malicious code into a legitimate process or application. Alters the external behavior of an application but no changes to application code. 369

- **Refactoring**: code performs the same function by using different methods. Modifies the application’s code without changing its external behavior. 369

• **Pass the hash**: process of harvesting an account’s cached credentials when the user is logged into a single- sign-on system so the attacker can use the credentials on other systems. Provide the hash, don’t need plaintext in order to authenticate. 369

**1.4 Given a scenario, analyze potential indicators associated with network attacks.**

• **Wireless**

- **Evil twin**: a rogue wireless access point masquerading as a legitimate one… does this by having a similar name SSID to the real one or by using a DoS technique to overcome the real WAP… authentication security must be enabled on the WAP. Used for eavesdropping. 243

- **Rogue access point**: access point that has been installed on the network without authorization. 243

- **Bluesnarfing**: using an exploit to circumvent the authentication mechanism in Bluetooth to steal info from someone’s phone. Unauthorized access. 359

- **Bluejacking**: spam where someone sends you unsolicited text/pic/vid or contact info. 359

- **Disassociation/ deauthentication**: send a stream of spoofed frames to cause a client to deauthenticate from a WAP… MAC address of the target station is spoofed, opening up vulnerability to replay attack. Temporary DoS. 244

- **Wifi Jamming**: setting up a WAP w/ a stronger signal to interfere w/ the wireless network. Type of DoS. 245

- **Radio frequency identification (RFID)**: way to encode info into passive tags that can be attached to devices. Type of RFID attack is skimming. Vulnerable to spoofing, eavesdropping, data interception, replay attacks and DoS attacks. 359

- **Near-field communication (NFC)**: standard for peer-to-peer radio communications over very short distances, facilitating contactless payment… based off RFID. No encryption. Vulnerable to data interception, replay attacks, DoS attacks. 359

- **Initialization vector (IV) attack**: a wireless attack where the attacker is able to predict or control the IV of an encryption process, thus giving the attacker access to view the encrypted data that is supposed to be hidden from everyone else except the user or network. Attempt to discover the passphrase. 245

• **On-path attack (man-in-the-middle attack)**: threat actor gains a position between two hosts, and transparently captures, monitors, and relays all communication between the hosts. 228

• **Layer 2 attacks** 🡪 data link layer…focused on information gathering

- **Address Resolution Protocol (ARP) poisoning**: use of a packet crafter to broadcast unsolicited ARP reply packets; the receiving devices trust the communication and update their MAC: IP address cache table with the spoofed address. 228

- **Media access control (MAC) flooding**: exhaust the memory used to store the switch’s MAC address table, switch stops trying to apply MAC-based forwarding & flood unicast traffic out of all ports… makes sniffing network traffic easier. 228

- **MAC cloning/spoofing**: attacker falsifies the factory-assigned MAC address of a device’s network interface card (NIC). 227

• Domain name system (DNS) (layer 7) resolves fully qualified domain names to IP addresses. Port 53.

- **Domain hijacking**: an adversary gains control over the registration of a domain name and acquires the domain for a company’s trading name or trademark or a spelling variation. 285

- **DNS poisoning**: an attack that compromises the process by which clients query name servers to locate the IP address for a FQDN... can be done through man-in-the-middle, DNS client cache poisoning, DNS server cache poisoning. Direct client to any dest. 286

- **Uniform Resource Locator (URL) redirection**: pharming; the use of HTTP redirects to open a page other than the one the user requested. Hosts enables client-side URL redirection. 286

- **Domain reputation**: domains that have been hijacked will lead to complaints and may even be blacklisted. 286

• **Distributed denial-of-service (DDoS)**: attack is done by multiple hosts simultaneously… point is to consume network bandwidth or do resource exhaustion. 247

- **Network**: SYN or SYN/ACK flooding. 247

- **Application**: targets vulnerabilities in the headers and payloads of specific application protocols. 247

- **Operational technology (OT)**: between embedded systems devices and their controls… overwhelm available memory or CPU time.

• **Malicious code or script execution**

- **PowerShell**: .ps1 file extension. command shell and scripting language built on the .NET Framework. 392

- **Python**: .py file extension. popular scripting language. 390

- **Bash (Bourne Again Shell)**: command line in Linux. 396

- **Macros**: sequence of actions performed in the context of a word processor, spreadsheet, or presentation file. 396

- **Visual Basic for Applications (VBA)**: macros. scripting language used by Microsoft Office… .vbs file extension.

**1.5 Explain different threat actors, vectors, and intelligence sources**

• Actors and threats

- **Advanced persistent threat (APT)**: the ongoing ability of an adversary to compromise network security (obtain and maintain access) using a variety of tools and techniques. 20

- **Insider threats**: an individual within an organization who has been assigned privileges on the system that cause an intentional or unintentional incident.

- **State actors**: threat actor that is supported by the resources of its host country’s military and security services… goals are espionage and strategic advantage. 20

- **Hacktivists**: use cyber weapons to promote a political agenda. 20

- **Script kiddies**: someone who uses hacker tools without understanding how they work. 20

- **Criminal syndicates**: financial fraud and extortion or cyber espionage. 21

- **Hackers**: an individual who has the skills to gain access to computer systems through unauthorized means. 20

- Authorized 🡪 white hat

- Unauthorized 🡪 black hat

- Semi-authorized 🡪 gray hat

- **Shadow IT**: users purchase or introduce computer hardware or software to the workplace without the sanction of the IT dept and without going through a procurement and security analysis process. 22

- **Competitors**:

• **Attributes** of actors

- **Internal/external**: with account and authorized access vs not. 19

- **Level of sophistication/capability**: ability to craft novel exploit techniques & tools. 19

- **Resources/funding**:

- **Intent/motivation**: what an attacker hopes to achieve from the attack and the attacker’s reason for perpetrating the attack. 19

• **Vectors**: path that a threat actor uses to gain access to a secure system. 22

- **Direct access**: physical or local attack. 22

- **Wireless**: attacker obtains credentials for a remote access or wireless connection to the network. 23

- **Email**: attacker sends a malicious file attachment via email and uses social engineering techniques to persuade or trick victim into opening attachment. 23

- **Supply chain**: infiltrate companies in the supply chain of the target company. 23

- **Social media**: malware concealed in files attached to posts. 23

- **Removable media**: malware on a USB drive. 22

- **Cloud**: attacker gains access to an account with weak credentials. 23

• **Threat intelligence sources**

- **Open-source intelligence (OSINT)**: publicly available info. 27

- **Closed/proprietary**: data available as a paid subscription. 26

- **Vulnerability databases**: Common Vulnerabilities and Exposures (CVE) and NVD. 30

- **Public/private information**- sharing centers: sector-specific resources for companies and agencies working in critical industries

- **Dark web**: not indexed by a search engine…anonymity… no activity tracking. 25

- **Indicators of compromise (IOC)**: forensic evidence or residual sign that an asset or network has been successfully attacked or is continuing to be attacked. 28-29

- **Automated Indicator Sharing (AIS):** offered by Dept of Homeland Sec… threat intel sharing. 30

- **Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Intelligence Information (TAXII)**: syntax and means for transmitting CTI data. 30

- **Predictive analysis**: threat forecasting; system can anticipate a particular type of attack and possibly identify the threat actor before the attack is fully realized. 31

- **Threat maps**: graphic showing the source, target, and type of attacks that have been detected by a CTI platform. 30

- **File/code repositories**: holds signatures of known malware code. 30

• **Research sources**. 28

- **Vendor websites**

- **Vulnerability feeds**

- **Conferences**

- **Academic journals**

- **Request for comments (RFC)**

- **Local industry groups**

- **Social media**

- **Threat feeds**

- **Adversary tactics, techniques, and procedures (TTP)**

**1.6 Explain the security concerns associated with various types of vulnerabilities.**

• **Cloud-based vs. on-premises vulnerabilities**: on private network vs on cloud. Shared responsibility model (CSP secures the cloud, consumer responsible for security in cloud). 55

• **Zero-day**: a vulnerability that is exploited before the developer knows about it or can release a patch. 51

• **Weak configurations**

- **Manufacturer default settings**: may leave unsecure interfaces enabled. 51

- **Unsecure root accounts/default admin account**: has no restrictions over system access… need effective user management and authorization policies… least privilege. 51

- **Open permissions**: provisioning data files or applications without differentiating access rights for user groups. Read and write access permissions. 52

- **Open ports and services**: increases attack surface. Restrict access, disable unused services, block port with firewall, segment the network. 52

- **Unsecure protocols**: transfers data as cleartext and does not have encryption for data protection. No secure way to authenticate endpoints. Man-in-the-middle susceptible. 52

- **Weak encryption**: allow unauthorized access to data. Password length and complexity to avoid brute force. 52

- **Errors**: errors should not reveal info that could assist the development of an exploit. 53

• **Third-party risks**

- **Vendor management**: assess risks when determining whether to outsource all or part of a workflow and have contingency plans if a vendor does not perform as expected. 54

- **System integration**: using components or services from multiple vendors to implement a business workflow. 54

- **Lack of vendor support**: retooling the workflow to use a different vendor can be complex. 54

- **Supply chain**:

- **Outsourced code development**: use different vendors for code development and for vulnerability and penetration testing to make sure you are using secure code. 55

- **Data storage**: vendor access to your data and vendor hosting your data and data backups… ensure authorization, access management, encryption, compliance. 55

• **Improper or weak patch management**

- **Firmware**: vulnerabilities in BIOS/UEFI that controls the boot process, also in network cards and disk controllers… can run with the highest level of privilege. 50

- **Operating system (OS)**: vulnerability in the OS kernel file likely leads to privilege escalation. 50

- **Applications**:

• **Legacy platforms**: one that is no longer supported with security patches by its developer or vendor and this highly vulnerable to exploits. 51

• **Impacts**

- **Data loss**: info becomes unavailable temporarily or permanently. 53

- **Data breaches**: confidential data is read or transferred without authorization. 53

- **Data exfiltration**: transfer of data without authorization from the victim’s system to an external network or media. 53

- **Identity theft**: use of personal details and financial info to make fraudulent actions. 53

- **Financial impacts**: damages, fines, loss of business. 54

- **Reputation**: drops. 54

- **Availability loss**: availability of data has a severe impact on business workflows. 53

**1.7 Summarize the techniques used in security assessments.**

• **Threat hunting**: assessment technique that utilizes insights gained from threat intelligence to proactively discover whether there is evidence of TTPs already present within the network or system. 64

- **Intelligence fusion**: using sources of threat intelligence data to automate detection of adversary indicators of compromise and TTPs. SIEM. 64

- **Threat feeds**:

- **Advisories and bulletins**: from vendors and security researchers about new TTPs and vulnerabilities. 64

- **Maneuver**: passive discovery techniques to avoid detection to obtain positional advantage. 65

• **Vulnerability scans**

- **False positives**: something identified by a scanner as being a vulnerability when in fact it is not. 62

- **False negatives**: potential vulnerabilities that are not identified in a scan and thus go undetected. 62

- **Log reviews**: see what processes have failed. 62

- **Credentialed vs. non-credentialed**: user account within log-on rights plus permissions for testing vs directing test packets at a host without being able to log on to the OS or app. 61

- **Intrusive vs. non-intrusive**: run code to gain access to system vs probing the device’s config using a network connection w/ the target vs analyzing indirect evidence (traffic). 60

- **Application scanners** are configured with detailed scripts to test for known attacks as well as scanning for missing patches and weak configurations. 59

- **Web application**: type of application scanner…detects web exploits such as SQP injection and XSS. 59

- **Network vulnerability scanner**: test network hosts, including client PCs, mobile devices, routers, switches…. Compares results to configuration templates. 58

- **Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS)**: dictionary of vulnerabilities in published operating systems and applications software. 59

- **Configuration review**: assessment of the configuration of security controls and application settings and permissions compared to established benchmarks. 63

• **Syslog/Security information and event management (SIEM)**: aggregate traffic data & logs. 276

- **Review reports**:

- **Packet capture**: data captured from network sensors provides summary stats about bandwidth and protocol usage and detailed frame analysis. 275

- **Data inputs**:

- **User behavior analysis**: identification of malicious behaviors from comparison to a baseline. Heavily dependent on AI and machine learning. 277

- **Sentiment analysis**: identify intent, context, interpretation, emotion. Gather threat intel. 278

- **Security monitoring**:

- **Log aggregation**: normalizing data from different sources so that it is consistent and searchable… interpret and parse data. 277

- **Log collectors**: appliance that gathers or receives log data from other network systems. 276

**Syslog server** collects diagnostic and monitoring data from networked devices.

• **Security orchestration, automation, and response (SOAR)**: integrated with a SIEM… scan the organization’s store of security and threat intelligence, analyze it using machine/deep learning, use the data to automate and provide data enrichment for workflows that drive incident response and threat hunting. 278

**1.8 Explain the techniques used in penetration testing**

• **Penetration testing/ethical hacking**: authorized hacking to discover exploitable weaknesses in the security system. 67

- **Known environment (white box)**: consultant is given complete access to information about the network… simulates a privileged insider threat. 68

- **Unknown environment (black box)**: consultant is given no privileged information about the network and its security systems… simulates an external threat. 68

- **Partially known environment (grey box)**: consultant is given some information about the network… simulates an unprivileged insider threat. 68

- **Rules of engagement**: specify what activity is permitted or not… made explicit in a contractual agreement… objective + scope. 67

- **Persistence**: tester’s ability to reconnect to the compromised host and use it as a RAT or backdoor… must establish command and control. 70

- **Privilege escalation**: gain greater level of access. 70

- **Lateral movement**: gaining control over other hosts… usually done PowerShell. 70

- **Pivoting**: pivot allows tester to bypass a network boundary and compromise servers on an inside network… accomplished using remote access and tunneling protocols (SSH, VPN). 70

- **Cleanup**: removing evidence of the attack… evidence of backdoors. 70

- **Bug bounty**: program where rewards are given for reporting vulnerabilities…crowd sourcing 68

• **Passive and active reconnaissance**: undetectable vs risk of detection

- **Drones**: unmanned aerial vehicles. 69

- **War flying**: war driving from the air

- **War driving**: mapping the location and type of wireless networks operated by the target. 69

- **Footprinting**: using software tools such as Nmap to obtain info about a host or network topology. 69

- **OSINT:** using webs search tools, social media, and sites that scan for vulnerabilities to obtain info about the target. 69

• **Exercise types**

- **Red-team**: offense. 68

- **Blue-team**: defense. 68

- **White-team**: sets rules of engagement and monitors the exercise (referee). 68

- **Purple-team**: red & blue teams meet for regular debriefs while exercise is ongoing. 69

**2.0 Architecture and Design**

**2.1 Explain the importance of security concepts in an enterprise environment.**

• **Configuration management**: ensures that each component of information and communications technology (ICT) is in a trusted state that has not diverged from its documented properties. 530

- **Diagrams**: best way to capture the complex relationships between network elements… show how configuration items (CIs) are involved in business workflows, etc. 531

- **Baseline configuration**: template of settings that a device was configured to and that it should continue to match. 530

- **Standard naming conventions**: consistent way of naming hardware assets and digital assets so that errors are easier to spot and easier to automate scripting. Rules for host & DNS names. 531

- **Internet protocol (IP) schema**: address that is used to uniquely identify a device on an IP network. Easier to apply firewall access control lists (ACLs), perform security monitoring, makes configuration errors less likely & easier to detect, identify manual or static vs DHCP address. 531

• **Data sovereignty**: a jurisdiction preventing or restricting processing and storage from taking place on systems that do not physically reside within that jurisdiction. 443

• **Data protection**:

- **Data loss prevention (DLP)**: automate the discovery and classification of data types and enforce rules so that data is not viewed or transferred without proper authorization. 449

- **Masking**: all of parts of the contents of a field are redacted xxx. 452

- **Encryption**: used to mitigate the risk that an authorization mechanism can be revoked. 447

- **At rest**: data is in some sort of persistent storage media… data should be encrypted. 447

- **In transit/motion**: data is transmitted over a network… exp website traffic, data being synced between cloud repos… protected by a transport encryption protocol (TLS or IPSec). 447

- **In processing/in use**: data is present in volatile memory such as system RAM or CPU registers and cache… 447

- **Tokenization**: all or part of the data field is replaced with a randomly generated token which is stored along with the original value in a token server. 452

- **Rights management**: file permissions, restrict printing and forwarding

• **Geographical considerations**: mitigate data sovereignty issues and employees needing access from multiple geographic locations. 443

• **Response and recovery controls**

• **Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection**: to secure application protocols… digital certificate signed by a trusted certificate authority… encrypted comms. 292

• **Hashing**: produces a fixed length string from an arbitrary length plaintext… prove integrity. 452

• **API considerations**: secrets management requirements and ensure only authorized endpoints are making transactions. 295

• **Site resiliency**

- **Hot site**: can failover almost immediately. 532

- **Cold site**: takes longer to set up… empty building. 533

- **Warm site**: latest dataset will need to be loaded. 533

• **Deception and disruption**

- **Honeypots**: computer system set up to attract threat actors, with the intention of analyzing attack strategies and tools, to provide early warming of attack attempts, or possibly as a decoy to divert attention from actual computer systems… used to detect fraud, snooping, malpractice. 534

- **Honeyfiles**: convincingly useful but actually fake data that is usually trackable so that when a threat actor successfully exfiltrates it, the attempts to reuse or exploit it can be traced. 535

- **Honeynets**: an entire decoy network. 534

- **Fake telemetry**: deception strategy that returns spoofed data in response to network. 535

- **DNS sinkhole**: sinkhole server that routes suspect traffic so that it can be analyzed. 535

**2.2 Summarize virtualization and cloud computing concepts**

• **Cloud models**

- **Infrastructure as a service (IaaS)**: provisioning IT resources such as servers, load balancers, and storage area network components by renting them on an as-needed basis from the cloud service provider. 409

- **Platform as a service (PaaS)**: provisioning servers and storage network infrastructure and a multi-tier web application/database platform… your own developers would have to create the software that runs on the platform. 409

- **Software as a service (SaaS)**: provisioning software that is hosted on a supplier’s servers on a pay-as-you-go or lease arrangement… apps can be developed and tested in the cloud. 409

- **Anything as a service (XaaS)**:

- **Public/multi-tenant**: shared resource where businesses can offer subscriptions or pay-as-you-go financing while providing lower-tier services free of charge. 408

- **Community**: several organizations share the costs of either a hosted private or fully private cloud… pool resources for a common concern. 408

- **Private**: cloud infrastructure that is completely private. 408

- **Hybrid:**

• **Cloud service providers**:

• **Managed service provider (MSP)/ managed security service provider (MSSP)**: fully outsourcing responsibility for information assurance to a third party. 411

• **On-premises vs. off-premises**: onsite delivers better performance and is less subject to outages whereas offsite may provide better shared access for users in diff locations. 408

• **Fog computing**: placing fog node processing resources close to the physical location for the IoT sensors… the fog node prioritizes traffic, analyzes and remediates alertable conditions, and backhauls remaining data to the data center for storage and low-priority analysis. 433

• **Edge computing**: close to the network edge… collect and depend on data for operation. 433

• **Thin client**: simple, low-performance computer that has been optimized for establishing a remote connection with a server-based computing environment. 412

• **Containers**: light-weight, agile virtualization…don’t use a hypervisor… fast resource provisioning and speedy availability… OS virtualization. 413

• **Microservices**: a software architecture where components of the solution are conceived as highly decoupled services not dependent on a single platform type or technology. 429

• **Application programing interfaces (API)**: a library of programming utilities used to enable developers to access functions of the network stack under a particular operating system. The means by which external entities interact with the service, calling it with expected parameters and receiving expected output. 430

• **Infrastructure as code**: automation and orchestration fully replace manual configuration.

- **Software-defined networking (SDN)**: an approach to networking that uses software-based controllers or APIs to communicate with underlying hardware infrastructure and direct traffic on a network… more flexible and easier to manage. 432

- **Software-defined visibility (SDV)**: supports assessment and incident response functions… can help security data collection process… collection, aggregation, and reporting of data about network traffic flows and config of all hosts, apps and accts in it. 432

• **Serverless architecture**: all architecture is hosted within a cloud… applications are developed as functions and microservices interacting with other functions to facilitate client requests. 430

• **Services integration**: way of making decoupled service or microservice components work together to perform a workflow. 430

• **Resource policies**: like an access control list in the cloud… permission statements are written in JSON. 421

• **Transit gateway**: a virtual router that handles routing between the subnets in each attached Virtual Private Cloud (VPC) and any attached VPN gateway. 424

• **Virtualization**

- **Virtual machine (VM) sprawl:** configuration vulnerability where provisioning and deprovisioning of virtual assets is not properly authorized and monitored. Virtual machine life cycle management (VMLM) enforces VM sprawl avoidance. Security policies, secure configurations, and controls for avoidance. Prevent with usage audit and asset documentation. 416

- **VM escape protection**: an attack where malware running in a VM is able to interact directly with the hypervisor or host kernel… malware running on a guest OS jumping to another guest or to the host… identify vulnerabilities in the hypervisor and patch… isolate VMs in different zones on separate hardware. Sandboxing. 414

**2.3 Summarize secure application development, deployment, and automation concepts.**

**Environment**. 400

- **Development**: code hosted on a server, each developer edits their portion of code, sandbox for local testing.

- **Test:** code from multiple developers is merged to a single master copy and subjected to basic unit and functional tests to ensure the code builds correctly and fulfills functions required the design.

- **Staging**: mirror of the production environment but may use test or sample data and will have additional access controls so it’s only accessible to test users.

- **Production**: application is released to end users.

- **Quality assurance (QA**): tests to see whether it complies with the requirements and expectations… compliance factors.

• **Provisioning and deprovisioning**: process of deploying and application to the target environment; process of removing an application from packages or instances. 401

• **Integrity measurement**: determines whether the development environment varies from the configuration baseline.

• **Secure coding techniques**

- **Normalization**: a string is stripped of illegal characters or substrings and converted to the accepted character set to ensure the format can be processed correctly by the input validation routines. 383

- **Stored procedures**: using a prebuilt function to perform a database query. Effective at preventing SQL injection. 386

- **Obfuscation/camouflage**: software that randomizes code to make it difficult to read… way of making reverse engineering an application more difficult. 386

- **Code reuse/dead code**: executed but has no effect on the program flow. Should be removed. 386

- **Server-side vs. client-side execution and validation**: locally vs remotely. Client is more vulnerable to malware but server can be more time consuming. 384

- **Memory management**: 385

- **Use of third-party libraries and software development kits (SDKs):** must monitor for vulnerabilities and patched promptly. Specialized suite of software tools used for developing applications for a specific platform. 386

- **Data exposure**: a fault that allows privileged info to be read without being subject to the appropriate access controls. 385

• **Open Web Application Security Project (OWASP):** nonprofit. used in static code analysis. 387

• **Software diversity**. 403

- Compiler

- Binary

**• Automation/scripting**

**- Automated courses of action**

**- Continuous monitoring**: to detect service failures and security incidents. 402

**- Continuous validation**: determining whether the design goals of the application meet the user requirements. 403

**- Continuous integration**: principle that developers should commit and test updates often to reduce the chances of two developers spending time on code changes that are later found to conflict one another. 402

**- Continuous delivery**: testing all of the infrastructure that supports the app. 402

**- Continuous deployment**: making changes to the production environment to support the new app version. 402

• **Elasticity**: the system’s ability to handle changes on demand in real time… like loss of service or performance when demand goes up. 399

• **Scalability**: the costs involved in supplying the service to more users are linear. 399

**• Version control**: an ID system for each iteration of a software product… supports the change management process for software development projects. 401

**2.4 Summarize authentication and authorization design concepts**

• Authentication methods

**- Directory services**: the principal means of providing privilege management and authorization on an enterprise network, storing info about users, comps, roles, services. 202

**- Federation:** the notion that a network needs to be accessible to more than just a well-defined group of employees… needs to be open to partners, suppliers, customers… means a company trusts accounts created and managed by a different network. 203

**- Attestation:** proof of identity. 203

**- Technologies**

**- Time-based one- time password (TOTP):** forces one-time passwords to expire after a short time. 169

**- HMAC-based one-time password (HOTP)**: algorithm that generates a one-time password using a hash-based authentication code to verify the authenticity of the message. Token. 168

**- Short message service (SMS)**: code that is send as a text to the registered phone number. 170

**- Token key**: a physical or virtual item that contains authentication and/or authorization data, commonly used in multifactor authentication.

**- Static codes**: highly vulnerable to cloning and replay attacks. Programmed into device. 168

**- Authentication applications**:

**- Push notifications**: code is sent to a registered authenticator app. 170

**- Phone call**: code is delivered as an automated voice call to the registered phone. 170

**- Smart card authentication**: programming cryptographic info onto a card equipped with a secure processing chip that stores the user’s digital certificate, the private key, and a PIN. 164

**• Biometrics**

**- Fingerprint, Retina, Iris, Facial, Voice, Vein, Gait analysis**

**- Efficacy rates**

**- False acceptance rate (FAR)**: most important metric. an illegitimate user is recognized/accepted 172

**- False rejection rate (FRR)**: when a legitimate user is not recognized.

**- Crossover error rate (CER):** the point at which FRR and FAR meet… the lower the CER, the more efficient and reliable the technology. 172

**• Multifactor authentication (MFA) factors and attributes 152**

**- Factors**

**- Something you know 🡪** PIN

**- Something you have 🡪** smart card, fob, token

**- Something you are 🡪** fingerprint, gait

**- Attributes**: non unique property or factor that cannot be used independently

**- Somewhere you are 🡪**  location-based authentication… GPS reading

**- Something you can do 🡪**  way you walk or hold your phone, gait analysis

**- Something you exhibit 🡪**  behavioral, pattern recognition, handwritten signature

**- Someone you know 🡪** vouched for by existing users = web of trust

**• Authentication, authorization, and accounting (AAA)**: identity and access management. 149

**• Cloud vs. on-premises requirements**: authentication and authorization come with more constraints and addtl requirements… cloud networks require use of standards for federation and attestation between web apps. 204

**2.5 Given a scenario, implement cybersecurity resilience**

**• Redundancy**

**- Geographic dispersal:** data replicating hot and warm sites that are physically distant from one another so data is protected against natural disaster wiping out storage. 520

**- Disk 519**

**- Redundant array of inexpensive disks (RAID) levels**

**Drives, Striping, Mirroring, Parity**

**Level 0:** 2, Y, N, N

**Level 1:** 2, N, Y, N

**Level 5:** 3, Y, N, Y, 1 drive can fail and system will still work

**Level 6:** 4, 2 drives can fail and system will still work

**Level 10:** 4,stripe of mirrors

**- Multipath:** ensure that there is a controller redundancy and/or multiple network paths to the storage devices. Overprovisioning controllers and cabling so that a host has failover connections to storage media. 519

**- Network 518**

**- Load balancers:** distributes workloads between available servers. Managing the optimal distribution of workloads across multiple computing resources.

**- Network interface card (NIC) teaming:** the server is installed with multiple NICs or NICs with multiple ports and each port is connected to separate network cabling. Multiple network adaptors on a single interface for increased throughput/ redundancy.

**- Power 517**

**- Uninterruptible power supply (UPS)**: provides a short-term/temporary power source in the event of a blackout.

**- Generator**: can provide power to a whole building for several days/longer term... takes time to be brought online.

**- Dual supply:** two or more PSUs for redundancy.

**- Managed power distribution units (PDUs):** have circuitry that helps clean the power signal, provide protection against spikes, surges, and brownouts and integrate with USPs.

**• Data Replication 520**

**- Storage area network (SAN):** high-speed fiber optic network of storage devices.

**- VM:** replicating the VM’s disk image and configuration settings.

**• On-premises vs. cloud:** local and geographic redundancy are built into cloud systems

**Backup types 524**

**- Full:** all data regardless of when previously backed up

**- Incremental:** new files as well as files modified since last backup

**- Snapshot:** point-in-time copy of data maintained by the file system. Common with VMs

**- Differential:** all new and modified files since the last full backup

**- Digital tape:** provides robust, high-speed, high-capacity backup storage. Tape drives and autoloader libraries can be connected to SATA and SAS buses or accessed via a SAN.

- **Magnetic tape** is a type of sequential access backup media 527

**- Disk:** individual removable hard drives… con is capacity and flexibility of use. 527

**- Copy:**

**- Network-attached storage (NAS):** a specially configured server that makes RAID storage available over common network protocols. dedicated storage appliance that can be added to a local network. 527

**- Storage area network:** based on block-level addressing, good for scalability, can incorporate RAID arrays and tape systems within the same network and can achieve offsite storage through replication. 527

**- Cloud:**

**- Image:** duplicate the OS installation. exact copy of the entire state of a computer system. 526

**- Online vs. offline:** instantly available to perform a backup or restoration vs having to manually connect a backup media.

**- Offsite storage:** offsite media must be brought onsite, perform latest backup, then brought back to offsite storage… difficulty and expense… cloud storage solves this. 526

**- Distance considerations:**

**• Non-persistence:** any given instance is completely static in terms of processing function. 528

**- Revert to known state:** a saved state that can be reapplied to the instance. 528

**- Last known-good configuration:** restoring the baseline system configuration. 528

**- Live boot media:** an instance that boots from read-only storage to memory rather than being installed and configured. Non-persistent OS. 528

**• High availability:** the percentage of time that a system is online. 516

**- Scalability:** capacity to increase resources to meet demand within similar cost ratios.

**• Restoration order:** order at which systems are brought back online so as not to cause additional power problems because of dependencies between different appliances. 527

**• Diversity = defense in depth. 533-534**

**- Technology diversity:** different OSs, applications, coding languages, virtualization solutions.

**- Vendor diversity:** security controls are sourced from multiple vendors.

**- Cryptography diversity:** different cryptographic algorithms force threat actors to develop new attack approaches.

**- Control diversity:** the layers of controls should combine different classes of technical and administrative controls.

**2.6 Explain the security implications of embedded and specialized systems**

**• Embedded systems:** complete computer systems designed to perform a specific function

**- Raspberry Pi:** system on a chip

**- Field-programmable gate array (FPGA):** a processor that can be programmed to perform a specific function by a customer rather than at the time of manufacture.

**- Arduino:** system on a chip

**Supervisory control and data acquisition (SCADA)/industrial control system (ICS) 334**

**- Facilities:** HVAC, lighting, security

**- Industrial:** mining and refining raw materials

**- Manufacturing:** creating components and assembling them into products…high precision

**- Energy:** power generation and distribution… water and sewage

**- Logistics:** automated transport and lift systems plus sensors for component tracking

**Internet of Things (IoT):** global network of appliances and personal devices that have been equipped with sensors, software and network connectivity. 335

**- Sensors:** temp, light level, humidity, pressure, motion, gas, heart monitor, gyroscope

**- Smart devices:** smart lightbulb

**- Wearables:** watches, fitness monitors, eyeglasses

**- Facility automation:** process and memory vulnerabilities such as buffer overflow, use of plaintext credentials, code injection for attacks like XSS. 336

**- Weak defaults:** minimum configuration without security in mind

**• Specialized systems for**

**- Medical devices:** portable devices such as cardiac monitors/defibrillators, insulin pumps etc. can have unsecured communication protocols or unsupported versions of OS. 338

**- Vehicles:** with electronic systems to control engine and power systems, braking and landing, suspension/stability, features like driver-assist or driverless… electronic control unit (ECU) connected via controller area network (CAN) serial communication buses which have no source addressing pr message authentication… Dos attacks, remote wifi. 338

**- Aircraft**

**- Smart meters:** continuous updating of electrical, gas or water usage to supplier… use cellular data for communication. 336

**• Voice over IP (VoIP):** devices that connect to the internet… unpatched vulnerabilities. 337

**• Heating, ventilation, air conditioning (HVAC):** environmental control system. 335, 550

**• Drones**

**• Multifunction device (MFD) printer (MFP):** patch and update firmware, delete images and documents. 337

**• Real-time operating system (RTOS):** time-sensitive tasks… drip meters, flow valves etc.… must be more stable and reliable and cannot tolerate reboots or crashes… designed with small attack surface. 332

**• Surveillance systems:** vulnerabilities in CCTV cameras that allow hijackers to perform surveillance. 336

**• System on chip (SoC):** raspberry pi and Arduino. Processors, controllers and devices are provided on a single processor die or chip. Integrated circuit. 332

**Communication considerations**

**- 5G**

**- Narrow-band:** low-power version of LTE… signal occupies less bandwidth

**- Baseband radio:** baseband processor performs the function of a cellular modem

**- Subscriber identity module (SIM) cards:** identifier issued by a cellular provider… encryption

**- Zigbee:** wireless protocol for home automation

**Constraints 331**

**- Power**: battery powered… to extend life, keep processing to minimum.

**- Compute:** processor capability, system memory, persistent storage

**- Network:** power-efficient transfer of small amounts of data with high degree of reliability and low latency. 332

**- Crypto:** use of cryptoprocessors to ensure CIA

**- Inability to patch:** vendor doesn’t produce security updates/support or for short time, patching without service interruption can be tricky. 339

**- Authentication:**

**- Range**

**- Cost 331**

**- Implied trust:** on PC there is root of trust but in embedded systems must use implied trust… every device added to the system is trusted… rely on perimeter security model 331

**2.7 Explain the importance of physical security controls 21A, 21B**

**Restrict and monitor access to specific physical areas or assets**

**• Bollards/barricades**: prevent access, prevent vehicles from getting close to building. 541

**• Access control vestibules/mantrap**

**• ID Badges:** challenge policy… grant access depending on ID. 546

**• Alarms**: good perimeter alerts to entry and exit instances. 544

**• Signage**: good deterrent… warnings. 541

**• Cameras 545**

**- Motion recognition:** gait identification. 545

**- Object detection**: changes to the environment… missing object. 545

**• Closed-circuit television (CCTV):** effective deterrent, movement & access can be recorded.544

**• Industrial camouflage:** make buildings and gateways protecting high-value assets unobtrusive or create high visibility decoy areas to draw out potential threat actors. 541

**• Personnel**

**- Guards:** monitor critical checkpoints, verify ID, visual deterrent. 544

**- Robot sentries:** surveillance system mounted on a robot. 545

**- Reception:** access list. 546

**- Two-person integrity/control**: reduce the risk of insider threat. 546

**• Locks 542**

**- Biometrics**

**- Electronic**

**- Physical**

**- Cable locks**

**• USB data blocker:** DLP. prevents data transfer when connected to a USB charge point. 543

**• Lighting**: perception of safety, makes intrusion more difficult, surveillance easier. 541

**• Fencing**: transparent, robust, secure against climbing. 541

**• Fire suppression**: fire requires heat, oxygen, and fuel to ignite and burn and removing any one of these elements provides fire suppression and prevention. 552

**• Sensors**

**- Motion detection**

**- Noise detection**

**- Proximity reader:** contactless smart card read at close range

**- Moisture detection**

**- Cards**

**- Temperature**

**• Drones**

**• Visitor logs 546**

**• Faraday cages**: install communications equipment within a shielded, charged conductive mesh that blocks signals from entering or leaving the area. Protection against RFI and EMI. **550**

**• Air gap**: empty area surrounding a high-value asset that is closely monitored for intrusions **549**

**• Screened subnet (demilitarized zone):** servers placed outside of the firewall

**• Protected cable distribution**

**• Secure areas**

**- Air gap:** isolation from external computer networks.

**- Vault**: room hardened against unauthorized entry by physical means. 549

**- Safe:** for storage of portable devices and media. 549

**- Hot aisle/cold aisle arrangement:** to maximize air flow in a server room, server racks are placed back-to-back so hot air exhaust does not go to fresh air intake. 551

**• Secure data destruction**

**- Burning 552**

**- Shredding 553**

**- Pulping 553**

**- Pulverizing 553**

**- Degaussing:** exposing a hard disk to a powerful electromagnet that disrupts the magnetic pattern that stores the data on the hard disk. **553**

**- Third-party solutions**: provider must keep detailed inventory of how each media item was sanitized and certificates of destruction. 553

**2.8 Summarize the basics of cryptographic concepts**

**• Digital signatures**: a message digest encrypted using the sender’s private key that is appended to a message to authenticate the sender and prove message integrity, non-repudiation. 104

**• Key length:** using a longer key makes the encryption scheme stronger. 100

**• Key stretching:** takes a key that is generated from a user password and repeatedly converts it to a longer and more random key. Slow the attack. Bcrypt and PBKDF2. 117

**• Salting:** mitigates the impact of a rainbow table attack by adding a random value to each plaintext input. Initialization vector also provides randomization. 117

**• Hashing:** converts an arbitrary length string input to a fixed length string output… output is a checksum, message digest or hash. Reduces chances of collision. Used for integrity. 87

**• Key exchange:** digital envelope… sender and recipient exchange a symmetric encryption key by using public key cryptography. 105

**• Elliptic-curve cryptography:** trapdoor function… an asymmetric encryption algorithm that leverages the algebraic structures of elliptic curves over finite fields to derive public/private key pairs. Suited for low power devices. 102

**• Perfect forward secrecy:** uses Diffie-Hellman key agreement to create ephemeral session keys without using the server’s private key… ensures that if a key is compromised it will only affect a single session and not facilitate recovery of plaintext data from other sessions. 107

**• Quantum**

**- Communications:** entanglement, superposition, and collapse help to design temper-evident comms system that would allow secure key agreement. 120

**- Computing:** processing on qubits...120

**• Post-quantum:** when quantum computers that can perform useful tasks are a reality. 120

**• Ephemeral:** asymmetric encryption key designed to be used only for a single session

**• Modes of operation**

**- Authenticated:** provides an authentication and integrity mechanism by hashing a combination of the message output and a shared secret key. 109

**- Unauthenticated:**

**- Counter:** applies an initialization vector plus an incrementing counter value to the key to generate a keystream. 108

**• Blockchain:** each record or block is run through a hash function. The hash value of the previous block in the chain is added to the hash of the next block which ensures that each successive block is cryptographically linked. 121

**- Public ledgers:** blockchain is recorded on a public ledger. Decentralized in that it is distributed across a peer-to-peer network. 121

**• Cipher suites**

**- Stream:** each byte or bit of data in the plaintext is encrypted one at a time. 100

**- Block:** plaintext is divided into equal-sized blocks. Simplest/weakest is Electronic Code Book (ECB). 100

**• Symmetric vs. asymmetric:** one in which encryption and decryption are both performed by the same secret key (secret key/session key) vs a public and private key in a pair. 100

Symmetric ciphers: RC4, DES, AES, Blowfish, 3DES, Twofish

Asymmetric ciphers: RSA, GPG, DSA, DHE, ECDHE, PGP

**• Lightweight cryptography:** cryptographic algorithms with reduced compute requirements that are suitable for use in resource-constrained environments, such as battery powered. 121

**• Steganography:** obscuring the presence of a message. 121

**- Audio:**

**- Video**

**- Image**

**SSID broadcast suppression** is security through obscurity

**• Homomorphic encryption:** method that allows computation of certain fields in a dataset without decrypting it. Processing data in encrypted form.

**• Common use cases 111**

**- Low power devices 114**

**- Low latency**

**- High resiliency**

**- Supporting confidentiality**

**- Supporting integrity**

**- Supporting obfuscation**

**- Supporting authentication**

**- Supporting non-repudiation**

**• Limitations 113**

**- Speed**

**- Size**

**- Weak keys**

**- Time**

**- Longevity**

**- Predictability**

**- Reuse**

**- Entropy:** ciphertext must have high level of entropy or disorder

**- Computational overheads:** CPU and memory resources **113**

**- Resource vs. security constraints**

**3.0 Implementation**

**3.1 Given a scenario, implement secure protocols**

**• Protocols**

**- Domain Name System Security Extensions (DNSSEC):** provides a validation process for DNS responses. Authentication of DNS and DNS data integrity. 287

**- Secure Shell (SSH)🡪 TCP port 22:** obtain secure remote access to a command-line terminal. Remote administration and secure file transfer. Cryptographic network protocol. 311

**- Secure/Multipurpose Internet Mail Extensions (S/MIME):** email encryption standard that adds digital signatures and public key cryptography to traditional MIME communications. 297

**- Secure Real-time Transport Protocol (SRTP):** provides confidentiality for call data. 299

**- Lightweight Directory Access Protocol Over SSL (LDAPS)🡪 port 636:** LDAP with secure tunnel. Secure directory access protocol. 288

**- File Transfer Protocol, Secure (FTPS):** FTP using TLS for confidentiality. 296

**- SSH File Transfer Protocol (SFTP):** addresses privacy and integrity issues by encrypting the authentication and data transfer between client and server. Over SSH. 296

**- Simple Network Management Protocol, version 3 (SNMPv3):** management and monitoring that supports encryption and strong user-based authentication… usernames and hash of passphrase. 290

**- Hypertext transfer protocol over SSL/TLS (HTTPS)🡪 port 443:** encrypted connection using TLS which uses asymmetric public key pairs. It is the primary protocol used to send data between a web browser and a website. 293

**- IPSec:** operates at the network layer (layer 3) and provides confidentiality and integrity. Used to secure data through authentication and encryption as the data travels across the network or the internet. 304

**- Authentication header (AH)/ Encapsulating Security Payloads (ESP):** two protocols used… prior performs a cryptographic hash on the whole packet…. Payload is not encrypted so no confidentiality. Latter provides confidentiality and/or authentication and integrity b encapsulating the header and payload in the ESP and encrypting it. 305

**- Tunnel/transport:** transport mode is used to secure communications between hosts on private network whereas tunnel mode is used for communications between VPN gateways across and unsecured network. 306

**- Post Office Protocol (POP3)🡪 TCP port 110**: mailbox protocol designed to store messages delivered by SMTP on a server. POP3S 🡪 port 995. 297

**- Internet Message Access Protocol (IMAP)🡪 TCP port 143:** supports permanent connections to a server and connecting multiple clients to the same mailbox simultaneously. IMAPS🡪 TCP port 993. 297

**• Use cases**

**- Voice and video**: VOIP, web conferencing, video teleconferencing. SIP 🡪 TCP port 5060

**- Time synchronization:** Network time protocol (NTP)🡪 UDP port 123

**- Email and web:** SMTP🡪 port 25

**- File transfer**

**- Directory services**

**- Remote access**

**- Domain name resolution**

**- Routing and switching**

**- Network address allocation**

**- Subscription services**

**3.2 Given a scenario, implement host or application security solutions**

**• Endpoint protection**

**- Antivirus:** signature-based detection and prevention of known viruses. 327

**- Anti-malware:** generalized malware detection…viruses, worms, trojans, spyware, PUPs, cryptojackers. 327

**- Endpoint detection and response (EDR):** provide real-time and historical visibility into the compromise, contain malware within single host, and facilitate remediation. 328

**- Data Loss Prevention (DLP):** configured with policies to identify privileged files and strings that should be kept private/confidential so data cannot be copied or attached to message. A software or hardware-based security solution designed to detect and prevent unauthorized use and transmission of confidential information outside of the corporate network (data exfiltration). Content inspection. 328

**- Next-generation firewall (NGFW):** advances in firewall technology, from app awareness user-based filtering and intrusion prevention to cloud inspection… layer 7 firewall. 271, 329

**- Host-based intrusion prevention system (HIPS):**

**- Host-based intrusion detection system (HIDS):** threat detection via log and file system monitoring. 327

**- Host-based firewall**

**• Boot integrity**

**- Boot security/Unified Extensible Firmware Interface (UEFI):** provides code that allows the host to boot to an OS and can enforce boot integrity checks. 319

**- Measured boot:** uses platform config registers in the TPM at each stage of the boot process to check whether hashes of key system state data have changed. It will record the presence of unsigned kernel-level code. 319

**- Boot attestation:** transmit boot log report signed by the TPMvia a trusted process to a remote server such as a NAC server… boot log analyzed for signs of compromise. 320

**• Database**

**- Tokenization:** all of part of data in a field is replaced with a randomly generated token which is stored with the original value on a token server separate to production database. 452

**- Salting:** additional value stored with the hashed data field so you can’t use a rainbow table to figure out the hash to the plaintext. 452

**- Hashing:** prove integrity… produces a fixed-length string from arbitrary-length plaintext data.

**• Application security**

**- Input validations:** make sure data entered into input field matches what it should to avoid overflow attacks or SQL injection. 383

**- Secure cookies:** avoid using persistent cookies for session authentication. type of HTTP cookie that has Secure attribute set. The Secure attribute prevents the transmission of a cookie over an unencrypted channel. 384

**- Hypertext Transfer Protocol (HTTP) headers:** 385

**- Code signing:** means of providing authentication and integrity of code. Create a cryptographic hash of the file, sign hash with private key, receiving comp uses public key to read. 393

**- Allow list:** highly restrictive, only running authorized processes and scripts. 393

**- Block list/deny list:** permissive policy, only prevents execution of listed processes and scripts.

**- Secure coding practices:** remove unreachable or dead code, use obfuscation to make reverse engineering more difficult. 386

**- Static code analysis:** performed against the application code (to check for logic and syntax errors) before it is packaged as an executable process and scan it for known issues… will not reveal vulnerabilities that might exist in the runtime environment. 387

**- Manual code review:** human analysis of software source code. 387

**- Dynamic code analysis:** application is tested under “real world” conditions. 387

**- Fuzzing:** form of stress testing in which a test or vulnerability scanner generates large amounts of deliberately invalid or random input and records the responses made by the application to test if input validation routines work properly. 387

**• Hardening:** putting an OS or application in a secure configuration 325

**- Open ports and services:** disable services that are installed but not needed, restrict endpoints that are allowed to access the service by IP address, block access to ports at border firewalls or segment the network. 52

**- Registry:** configuration settings are stored in the registry… rights to modify the registry should only be issued to user and service accounts on a least privilege basis. 326

**- Disk encryption**

**- OS**

**- Patch management:** automated vulnerability scanners. 326

**- Third-party updates**

**- Auto-update:** check for and install updates automatically. 327

**• Self-encrypting drive (SED)/ full-disk encryption (FDE):** drive controller encrypts data written to it vs entire contents of the drive are encrypted. 321

**- Opal storage specification**: standard for implementing device encryption on storage devices.

**• Hardware root of trust:** secure subsystem that is able to provide attestation. 318

**• Trusted Platform Module (TPM):** specification for hardware-based storage of digital certificates, keys, hashed passwords, and other user and platform identification

**• Sandboxing:** isolates an untrusted host or app in a segregated environment to conduct tests. 329

**3.3 Given a scenario, implement secure network designs**

**• Load balancing:** distribute client requests across available server nodes in a farm or pool. Used to provision services to mitigate against DDoS attacks and provides fault tolerance. 249

**- Active/active clustering:** both nodes are processing connections concurrently… use max capacity from the available hardware. 251

**- Active/passive clustering:** one node is active and one is passive… performance is not adversely affected during failover. 251

**- Scheduling algorithm:** the code and metrics that determine which node is selected for processing each incoming request. Round robin…picking the next node. Picking the node with fewest connections and best response time are other methods. 250

**- Virtual IP:** an IP address that does not correspond to a physical network interface… used for network address translation, fault-tolerance… allows failover. 250

**- Persistence:** setting a cookie on a node or injected by the load balancer to keep the client connected to a session. 250

**• Network segmentation:** where all hosts attached to the segment can use local forwarding to communicate freely with one another.

**- Virtual local area network (VLAN):** a logistically separate network, created by using switching technology. Even though hosts on two VLANs may be physically connected to the same cabling, local traffic is isolated to each VLAN so they must use a router to communicate. 220

**- Screened subnet (previously known as demilitarized zone):** uses two firewalls placed on either side of the DMZ… edge firewall/screening firewall and the internal firewall/choke firewall. 222

**- East-west traffic:** traffic between servers and the data center. 222

**- Extranet:** network of semi-trusted hosts (business partners, suppliers, customers) who must authenticate to join the extranet. 220

**- Intranet:** zone permitting anonymous access by untrusted hosts over the internet. 220

**- Zero Trust:** based on the idea that perimeter security is unlikely to be completely robust. Uses continuous authentication and conditional access to mitigate privilege escalation and account compromise… microsegmentation also used. 224-225

**• Virtual private network (VPN) config**

**- Always-on:** the computer establishes the VPN whenever an internet connection over a trusted network is detected, using the user’s cached credentials to authenticate. 308

**- Split tunnel vs. full tunnel:** client access the internet directly using its “native” IP configuration and DNS servers vs internet access is mediated by the corporate network, which will alter the client’s IP address and DNS servers may use a proxy. Full tunnel offers better security. 309

**- Remote access vs. site-to-site:** clients connect to a VPN gateway on the edge of the private network vs connecting two or more private networks…configured to operate automatically. 302

**- IPSec:** network layer. Confidentiality (encrypt data packets). Integrity/anti-replay (signing each packet). Used to secure communications on local networks and as remote access protocol. 304

**- SSL/TLS VPN:**

**- HTML5 VPN:** clientless remote desktop gateway…uses protocol called WebSockets which enables bidirectional messages between server and client without requiring the overhead of separate HTTP requests. 310

**- Layer 2 tunneling protocol (L2TP):** client and VPN gateway set up a secure IPSec channel, VPN gateway uses L2TP to set up tunnel to exchange local network data encapsulated as PPP frames, user authenticates over the PPP session using EAP or CHAP. 308

**• DNS servers:** layer 7… host name records and perform name resolution to allow applications and user to address hosts and services using FQDNs rather than IP addresses. 217

**• Network access control (NAC):** the collected protocols, policies, and hardware that authenticate and authorize access to a network at the device level. Inspect for health status **231**

**- Agent and agentless:** NAC client software (agent) to gather info about the device such as antivirus and patch status, presence of prohibited applications, or as defined by the health policy. Client can be persistent or non-persistent. Agentless is no installation req. BYOD. 232

**• Out-of-band management:** accessing the administrative interface of a network appliance using a separate network from the usual data network. This could use a separate VLAN or a different kind of link, such as a dial-up modem. 310

**• Port security**

**- Broadcast storm prevention** by spanning tree protocol (STP) which prevents loops. 229

**- Bridge Protocol Data Unit (BPDU) guard**: used to communicate info about the topology and are not expected on access ports…protects against misconfiguration or malicious attack. 230

**- Loop prevention:** bridges organized in hierarchy to prevent loops from forming. 229

**- Dynamic Host Configuration Protocol (DHCP) snooping:** DHCP allows a server to assign IP address info to a client when it connects to a network… inspects the traffic arriving on access ports to ensure that a host is not trying to spoof its MAC address. 230

**- Media access control (MAC) filtering:** defining which MAC addresses are allows to connect to a particular port by creating a list of valid MAC addresses... guard against MAC flooding. 230

**• Network appliances**

**- Jump servers:** single admin server added to the secure zone that only runs the necessary admin port and protocol. Admins connect to the jump server then use it to connect to the admin interface on the application server, denying connection attempts from other hosts. 311

**- Proxy servers:** server that mediates the communications between a client and another server. It can filter and modify communications, provide caching services to improve performance. 260

**- Forward proxy server:** provides protocol specific outbound traffic. 261

**- Reverse proxy server:** provides protocol specific inbound traffic. 262

**- Network-based intrusion detection system (NIDS):** tools that provide a real-time analysis of either network traffic or system and application logs via a packet sniffer. Used to identify and log hosts and apps and detect attack signatures, password guessing attempts, port scans, worms, backdoor applications, malformed packets or sessions, and policy violations. 268

**- Network-based intrusion prevention system (NIPS):** provide an active response to any network threats that it matches. Inline meaning all traffic passes through them. End a TCP session, apply a temp filter on a firewall to block the attacker’s IP address, throttle bandwidth to attacking hosts. 270

**- Signature-based detection:** the engine is loaded with a database of attack patterns or signatures, and if traffic matches a pattern, the engine generates an incident. 270

**- Heuristic:** to learn from experience… NBAD generates statistical models of what baseline normal traffic looks like. 271

**- Behavioral based detection:** trained to recognize baseline “normal” traffic or events… anything that deviates creates an incident. 271

**- Anomaly:** looking for irregularities in the use of protocols. 271

**- Inline vs. passive:** all traffic passes through vs packet sniffer captures traffic and creates an alert when a detection signature is matched… does not block source host. 268-270

**- Hardware security modules (HSM):** a network appliance designed to perform centralized PKI management for a network of devices… it can act as an archive or escrow for keys in case of loss or damage. 165

**- Sensors:** packet sniffer. Network tap or port mirror that performs packet capture and intrusion detection. 467

**- Collectors:** collect data input from multiple sources… hosts can be configured to push updates to the SIEM server using syslog of SNMP. 276

**- Aggregators:** normalizing data from different sources so that it is consistent & searchable. 277

**- Firewalls:**

**- Web application firewall (WAF):** designed to protect software running on web servers and their backend databases from code injection and DoS attacks. 273

**- NGFW:** combination of application-aware filtering and user account-based filtering and the act as an IPS. 271

**- Stateful:** tracks info about the session established between two hosts or blocks malicious attempts to start a bogus session. 257

**- Stateless:** does not preserve info about network sessions. Each packet is analyzed independently. 256

**- Unified threat management (UTM):** centralizes many types of security controls into a single appliance. Firewall + anti + malware + NIPS + spam filtering + DLP + VPN etc. 271

**- Network address translation (NAT) gateway:** a service that translates between the private addressing scheme used by hosts on the LAN and the public addressing scheme used by router, firewall or proxy server on the network edge. No filtering functions. 264

**- Content/URL filter:** designed to apply filtering rules that appear on content blacklists or apply time-based restrictions to browsing. 272

**- Open-source vs. proprietary:** can be used independently of the vendor vs vendor specific that requires a commercial contract with the vendor. 266

**- Hardware vs. software:** hardware = appliance firewall deployed to monitor traffic passing into and out of a network zone vs software = application firewall designed to run on a server to protect a particular application. 259-260

**- Appliance:** monitor traffic passing into and out of the network zone. 259

**vs. host-based:** software application running on a single host designed to protect only that host. 260

**vs. virtual:** deployed within data centers and cloud services... role is to support east-west security and zero-trust microsegmentation design paradigms. 265

**• Access control list (ACL):** ingress and egress traffic filtering on separate ACLs… rules for a specific type of data packet and the appropriate action to taken for it. 256

**• Route security:** configure how a router identifies the peers from which it will accept route updates, block source routed packets, embedded OSs with reduced attack surface. 233

**• Quality of service (QoS):** framework for prioritizing traffic based on its characteristics… used to support voice and video applications that require a min level of bandwidth and are sensitive to latency and jitter. 252

**• Implications of IPv6:** impacts for premises networks, for access to cloud services, and clients’ access to web servers. 224

**• Port spanning/port mirroring:** a sensor is attached to a specially configured port on the switch that receives copies of frames addressed to nominated access ports. 269

**- Port taps:** box with ports for incoming and outgoing network cabling and an inductor or optical splitter that physically copies the signal from the cabling to a monitor port. 269

**• Monitoring services:**  SIEM, SOAR, logs, network monitors. 275

**• File integrity monitors:** core feature of HIDS. Audits the key system files to make sure they match the authorized versions. 272

**3.4 Given a scenario, install and configure wireless security settings**

**• Cryptographic protocols**

**- WiFi Protected Access 2 (WPA2):** uses AES cipher with 128-bit keys deployed within the counter mode within CCMP (authenticated encryption). Pre-shared key (PSK) authentication uses a passphrase to generate the key that is used to encrypt comms… access point is set to WPA2-PSK mode, admin configs passphrase between 8-63 ASCII characters which is converted to a 256-bit HMAC referred to as the pairwise master key (PMK). 4-way handshake. 238

**- WiFi Protected Access 3 (WPA3):** uses AES Galois Counter Mode Protocol (GCMP), SAE using dragonfly handshake (Diffie Hellman over elliptic curves key agreement which implements ephemeral session keys providing forward secrecy), enhanced open and management protection frames. Used password authentication key exchange (PAKE). 238

**- Counter-mode/CBC-MAC Protocol (CCMP):** provides authentication encryption. 237

**- Simultaneous Authentication of Equals (SAE):** uses dragonfly handshake which is Diffie Hellman over elliptic curves key agreement, combined with a hash value derived from the password and device MAC address to authenticate the nodes… dragonfly implements ephemeral session keys providing forward secrecy. 238

**• Authentication protocols**

**- Extensible Authentication Protocol (EAP):** framework for negotiating authentication methods that enables systems to use hardware-based identifiers such as fingerprint scanners or smart card readers for authentication. 241

**- Protected Extensible Authentication Protocol (PEAP):** EAP implementation that uses a server-side public key certificate to create a secure (encrypted) tunnel for user authentication, referred to as the inner method. Must use authentication protocols EAP-MSCHAP or EAP-GTC. 242

**- EAP-FAST:** uses a protected Access Credential (PAC) which is generated for each user from the authentication server’s master key. Problem is secure PAC distribution. 243

**- EAP-TLS:** EAP method that requires server-side and client-side certificates for authentication using SSL/TLS. Strong authentication. Encrypted TLS tunnel established. Mutual authen. 241

**- EAP-TTLS:** EAP method that enables a client and server to establish a secure connection without mandating a client-side certificate. It can use any inner authentication protocol (PAP or CHAP). 242

**- IEEE 802.1X:** a standard for encapsulating EAP communications over a LAN to implement port-based authentication. 240

**- Remote Authentication Dial-in User Service (RADIUS) Federation:** a standard protocol used to manage remote and wireless authentication infrastructures. Multiple organizations allow access to one another’s users by joining their RADIUS servers into a RADIUS mesh. 243

**• Methods**

**- Pre-shared key (PSK) vs. Enterprise vs. Open:** passphrase-based mechanism to allow group authentication to a wireless network. The passphrase is used to derive an encryption key. vs IEEE 802.1X to use an EAP over wireless… vs client is not required to authenticate (public WAP).

**- WiFi Protected Setup (WPS):** a feature of WPA and WPA2 that allows enrollment in wireless network based on an 8-digit PIN. 239

**- Captive portals (splash page):** allows the client to authenticate to the hotspot provider’s network.

**• Installation considerations**

**- Site surveys:** used to measure signal strength and channel usage throughout the area to cover. Map of site with site features. 236

**- Heat maps:** showing where the signal is strong or weak, which channel is being used and how they overlap. 236

**- WiFi analyzers:** software that records info about the signal obtained at regularly spaced points as the surveyor moves around the area. 236

**- Channel overlaps:** make sure they overlap as little as possible so as to cover more area. 236

**- Wireless access point (WAP) placement:** avoid co-channel interference and adjacent channel interference. 235

**- Controller and access point security** using secure management interfaces and strong admin controls. 237

**3.5 Given a scenario, implement secure mobile solutions**

**• Connection methods and receivers**

**- Cellular:** disable cellular data connection when device has access to an enterprise network to prevent data exfiltration. 356

**- WiFi:** disable peer-to-peer functions. 357

**- Bluetooth:** take off device discovery, choose a secure phrase for pairing with a passkey, keep devices updated with the latest firmware. 358

**- Near Field Communications (NFC):** does not provide encryption. Turn off NFC capability. Check surrounding, don’t let people too close to your phone. Use PIN. use secure chip. 360

**- Infrared:** uses such as allowing a device to operate as a remote-control handset and use as a proximity sensor and to measure health information. 359

**- USB:** don’t use/plug in media that you don’t know where it came from. 360

**- Point-to-point****:** over-the-air encryption. 362

**- Point-to-multipoint:** over-the-air encryption. 362

**- Global Positioning System (GPS):** triangulates device position using signals from orbital GPS satellites. Disable to avoid tracking. Geofencing. 357

**- RFID:** cryptography. Keeping distance. 359

**• Mobile device management (MDM)**

**- Application management:** service provider manages apps, authenticates and authorizes valid developers, issuing them a certificate to use to sign their apps and warrant them as trusted. Analyze code and apply policies to allow/not allow certain apps/features. Private app dist. 352

**- Content management:** using containerization so employer manages and maintains the portion of the device that interfaces with the corporate network. Storage segmentation. 353

**- Remote wipe:** if a device is stolen, it can be set to the factory defaults or cleared of any personal data. 349

**- Geofencing:** creating a virtual boundary based on real-world geography… restricting camera and screen capture based on location. 351

**- Geolocation:** the use of network attributes to identify the physical position of a device. 350

**- Screen locks:** if incorrect password entered, device locks for set period of time. 349

**- Push notifications:** an app or website can use to display an alert on a mobile device. 361

**- Passwords and PINs:** authentication. 348

**- Biometrics:** authentication. 348

**- Context-aware authentication:** an access control scheme that verifies an object’s identity based on various environmental factors, like time, locations and behavior. 349

**- Containerization:** employer manages and maintains the portion of the device that interfaces with the corporate network… keeps corporate apps separate from the rest of the device. 353

**- Storage segmentation:** the container is associated with a directory on the persistent storage device that is not readable or writable by apps that are not in the container. 353

**- Full device encryption:** all user data on the device is encrypted but the key is stored on the device. 350

**• Mobile devices**

**- MicroSD hardware security module (HSM):** a small form factor hardware security module designed to store cryptographic keys securely. 350

**- MDM/Unified Endpoint Management (UEM):** sets device policies for authentication. Feature use, and connectivity. Enterprise software for controlling device settings, apps, and corporate data storage on all types of fixed, mobile and IoT computing devices. 345

**- Mobile application management (MAM):** sets policies for apps that can process corporate data, and prevents data transfer to personal apps. 345

**- SEAndroid** uses mandatory access control (MAC) policies to run apps in sandboxes.

**• Enforcement and monitoring of:**

**- Third-party application stores** can allow users to install untrusted apps. Use management suite to prevent the use of third-party stores or sideloading. 353

**- Rooting/jailbreaking:** being able to access the root account on a device/ obtain root privilege. 353

**- Sideloading:** untrusted apps are downloaded to a device from a website. 353

**- Custom firmware image:** remove the protections that enforce segmentation. 354

**- Carrier unlocking:** remove the restrictions that lock a device to a single carrier. 353

**- Firmware over-the-air (OTA) updates:** a firmware update delivered on a cellular data connection. 361

**- Camera use** restricted using geofencing.

**- SMS/Multimedia Messaging Service (MMS)/Rich Communication Services (RCS):** allow transmission of text messages and binary files. 360

**- External media:**

**- USB On-The-Go (USB OTG):** allows a port to function either as a host or as a device. 360

**- Recording microphone** prevented with geofencing. 351

**- GPS tagging:** process of adding geographical ID metadata such as longitude and latitude where device was located at the time when a photo or video was taken. 352

**- WiFi direct/ad hoc**: allows one-to-one connections between stations or peer-to-peer connections between wireless stations rather than an access point. 357

**- Tethering:** connecting a smartphone to a PC over a USB cable or via Bluetooth. 358

**- Hotspot:** when a smartphone shares its internet connection with other devices. 357

**- Payment methods:** using NFC with wallet apps. 360

**• Deployment models**

**- Bring your own device (BYOD):** mobile device is owned by the employee. 344

**- Corporate-owned personally enabled (COPE):** device is chosen and supplied by the company and remains its property. 344

**- Choose your own device (CYOD):** employee is given a choice of devices from a list. 344

**- Corporate-owned:** device is property of the company and may only be used for work.

**- Virtual desktop infrastructure (VDI):** provisioning an OS desktop to interchangeable hardware capable of running a VDI client viewer. Remote access. Segmentation. 344

**3.6 Given a scenario, apply cybersecurity solutions to the cloud**

**• Cloud security controls**

**- High availability across zones:** regions are divided into availability zones with independent data centers that have their own power, cooling, and network connectivity. Redundancy. Tiers of replication. Local, regional and geo-redundant storage replication. 422

**- Resource policies:** act as the ACL for an object. Permissions statements written in JSON. 421

**- Secrets management:** don’t use root user acct, require MFA, only use secret key for programmatic access. 420

**- Integration and auditing:** cloud-based SIEM solutions. SLA with the cloud service provider. Reporting mechanism and review of disaster recovery plans. Separation of duties and M of N control. 418

**- Storage:** hard disk, object-based storage, block storage. 421

**- Permissions:** resource policies are like ACLs and written in JSON. 421

**- Encryption:** cloud storage encryption using an AES key… minimize data loss. 421

**- Replication:** requires low latency network connections, security and data integrity. Cloud is central storage area. Hot and cold storage. 422

**- High availability:** regions are divided into availability zones with independent data centers… choose region with lower latency. Provision resources in multiple zones to increase redundancy. 422

**- Network:**

**- Virtual networks:** are isolated from other CSP accounts and from other VPCs operating in the same account. 423

**- Public and private subnets:** to configure a public subnet, an internet gateway (virtual router) must be attached to the VPC and configured as the default route, otherwise the subnet remains private. 423

**- Segmentation:** necessary for separating workloads for performance and load balancing, keeping data processing within an isolated segment for compliance with laws and regulations, and compartmentalizing data access and processing for different departments. 425

**- API inspection and integration:** monitor API usage such as number of requests, latency, error rates, and unauthorized and suspicious endpoints. 420

**- Compute**

**- Security groups:** provide stateful inbound and outbound filtering at layer 4… allows established and related traffic if a new connection has been accepted. 425

**- Dynamic resource allocation:** ensures the resources required are made available on-demand. 420

**- Instance awareness:** where undocumented instances (VMs and containers) are launched and left unmanaged… to avoid sprawl. 421

**- Virtual private cloud (VPC) endpoint:** gateways and interfaces. A means of publishing a service so that it is accessible by instances in other VPCs using only AWS internal network and private IP addresses. 424

**- Container security:** containers are isolated through namespaces & control groups. 420

**• Solutions**

**- CASB:** an enterprise management software designed to mediate access to cloud services by users across all types of devices. 426

**- Application security:** both the software dev process and identity and access management 419

**- Next-generation secure web gateway (SWG):** a proxy-based firewall, content filter, IDS/IPS + DLP + CASB. 427

**- Firewall considerations in a cloud environment:**

**- Cost:** time deployed and traffic volume.

**- Need for segmentation:** separate workloads, data processing, and data access 425

**- Open Systems Interconnection (OSI) layers:** network layer 3 firewall accepts or denies connections on basis of IP addresses and TCP/UDP; transport layer 4 firewall stores connections states and uses rules to allow traffic; application layer 7 firewall parses app protocol headers and payloads and makes filtering decisions. 425

**• Cloud native controls vs. third-party solutions:** cloud native controls might not exist for certain use cases, might not meet functionality requirements, might be too difficult to transition to vs third party solutions are installed as a virtual instance within the cloud. 419

**3.7 Given a scenario, implement identity and account management controls.**

**• Identity**

**- Identity provider (IdP):** provisions the user account and processes authentication requests.

**- Attributes:** full name, email address, contact number, department, etc. 191

**- Certificates:** a certificate authority issues certificates to validated subjects and thus their identities can be trusted by any third party that also trusts the CA. certificate contains the public key which is part of a pair with a linked private key. 180

**- Tokens:** with a single sign-on system, users authenticate to an IdP and receive a cryptographic token that allows them to present it to compatible apps as proof of authentication. 180

**- SSH keys:** host key pair identifies an SSH server & is used to encrypt the network connections & start a session; a user key pair is a means for a client to login to an SSH server. 187

**- Smart cards:** a user’s certificate and private key can be stored on a smart card and used to authenticate to different PCs and mobile devices. 180

**• Account types**

**- User account:** limited privileges. 183

**- Shared and generic accounts/credentials:** passwords are known to more than one person (breaking non-repudiation) … higher likelihood of password compromise due to sharing. 186

**- Guest accounts:** shared account with no password. Allows anonymous and unauthenticated access to a resource. 183

**- Service accounts:** used by scheduled processes and application server software (databases) 185

**• Account policies**

**- Password complexity:** at least 8 upper/lower alpha and non alpha numeric characters. 192

**- Password history:** prevents selecting a password that has been used already. 192

**- Password reuse:** prevents selecting a password that has been used already. 192

**- Network location:** user or device has a logical network location identified by IP address, subnet, VLAN, or OU and this can be used for account restriction. 193

**- Geofencing:** accepting or rejecting access requests based on location. 193

**- Geotagging:** addition of location metadata to files or devices. 193

**- Geolocation:** IP address associated with a map location or location services to calculate a device’s geographical position using GPS. 193

**- Time-based logins:** time of day policy establishes authorized logon hours for an account and time-based login is the max time an account may be logged in for. 193

**- Access policies:** determine the right to log on to a computer locally or via remote desktop, install software, change the network configuration, etc. 191

**- Account permissions:** escalation, authorization creep… revoke privileges at the end of the agreed period, review privileges regularly during auditing, review access control lists. 195

**- Account audits:** whether an account has been compromised or is being misused. Security or audit log. Changes to resources and users. 194

**- Impossible travel time/risky login:** tracks the location of login events over time… can’t login from Miami and 10 minutes later login from California. 194

**- Lockout:** login is prevented for a period of time. 197

**- Disablement:** login is permanently prevented until an admin manually re-enables the account. 196

**3.8 Given a scenario, implement authentication and authorization solutions**

**• Authentication management**

**- Password keys:** USB tokens for connecting to PCs and smartphones. 161

**- Password vaults:** software-based password manager, typically using a cloud service to allow access from any device. 161

**- TPM:** a specification for hardware-based storage of digital certificates, keys, hashed passwords, and other user and platform identification information. Prevents brute force. 164

**- HSM:** a network appliance designed to perform centralized PKI management for a network of devices. Manages certificates and digital keys. 165

**- Knowledge-based authentication (KBA):** authentication which seeks to prove the identity of someone accessing a service. They must answer a secret question.

**• Authentication/authorization**

**- EAP:** framework for deploying multiple authentication protocols and technologies. Use of a digital certificate on the server that allows the machines to establish a trust relationship and create a secure tunnel to transmit user credential or smart card authentication. 165

**- Challenge-Handshake Authentication Protocol (CHAP):** remote access authentication protocol that relies on a three-way handshake (challenge, response, verification) … guards against replay attacks. 158

**- Password Authentication Protocol (PAP)**

**- IEEE 802.1X:** means of using an EAP method when a device connects to an ethernet switch port, WAP, or VPN gateway. Uses AAA architecture. Centralized authentication. 166

**- RADIUS:** a standard protocol used to manage remote and wireless authentication infrastructures. 166

**- Single sign-on (SSO):** an authentication technology that enables a user to authenticate once and receive authorizations for multiple services. 155

**- Security Assertion Markup Language (SAML):** an XML based data format used to exchange authentication information between a client and a service. 204

**- Terminal Access Controller Access Control System Plus (TACACS+):** an AAA protocol developed by Cisco that is often used to authenticate to administrator accounts for network appliance management. 167

**- OAuth:** standard for federated identity management, allowing resource servers or consumer sites to work with user accounts created and managed on a separate identity provider. 205

**- OpenID:** an authentication protocol that can be implemented as special types of OAuth flows with precisely defined token fields. Uses XML messaging and only supports web apps. 206

**- Kerberos:** a single sign-on network authentication and authorization protocol used on many networks and is based on a time-sensitive ticket-granting system.

**• Access control schemes**

**- Attribute-based access control (ABAC):** access control technique that evaluates a set of attributes that each subject possesses to determine if access should be granted. 201

**- Role-based access control:** access control model where resources are protected by ACLs that are managed by administrators and that provide user permissions based on job functions. 199

**- Rule-based access control:** access control model where access control policies are determined by system-enforced rules rather than system users. 201

**- Mandatory Access Control (MAC):** control mode where resources are protected by inflexible, system-defined rules. Resources and users are all allocated a clearance level. 201

**- Discretionary access control (DAC):** access control model where each resource I s protected by an ACL managed by the resource’s owner. 199

**- Conditional access:** monitors account or device behavior throughout a session and if certain conditions are met, the account may be suspended or the user may be required to re-authenticate. 201

**- Privileged access management (PAM):** policies, procedures and technical controls to prevent malicious abuse of privileged accounts and to mitigate risks from week configurations controls over privileges. 202

**- File system permissions:** each object in the file system has an ACL associated with it. Read, write, and execute permissions. 200

**3.9 Given a scenario, implement public key infrastructure**

**• Public key infrastructure (PKI)**

**- Key management:** operational considerations for the various stages in a key’s life cycle. 137

**- Certificate authority (CA):** a server that guarantees subject identities by issuing signed digital certificate wrappers for their public keys. Issues and guarantees certificates. 126

**- Intermediate CA:** is issued certificates by the root CA; issues certificates to subjects (leaf entities) … different intermediate CAs can have different certificate policies. 127

**- Registration authority (RA):** entity that completes identity checking and submits CSRs on behalf of end users but not actually sign or issue certificates. 129

**- Certificate revocation list (CRL):** list of all revoked and suspended certificates. 139

**- Certificate attributes:** serial number, signature algorithm, issuer, validity dates, subject, public key, extensions, subject alternative name. 130

**- Online Certificate Status Protocol (OCSP):** server that communicates the status of the requested certificate. 139

**- Certificate signing request (CSR):** used to configure a certificate on a host. 142

**- Common Name (CN) attribute:** used to identify the FQDN by which the server is accessed. 130

**- Subject alternative name (SAN):** extension field used to identify the DNS name or names by which a host is identified. Multiple domains that have different names. 130

**- Expiration:** keys that are not revoked expire after a certain period for security reasons... must be renewed. 137

**• Types of certificates**

**- Wildcard:** the certificate issued to the parent domain will be accepted as valid for all subdomains. 131

**- Code signing certificate:** certificate issued to a software publisher who then signs the executables or DLLS that make up the program to guarantee the validity of a software application or browser plug-in. 135

**- Self-signed certificate:** marked as untrusted by the OS or browser. 135

**- Machine/computer certificate:** certificates issued to domain controllers, member servers, or client workstations, routers, switches, and firewalls. 134

**- Email certificate:** used to sign and encrypt email messages using S/MIME or PGP. 134

**- User**

**- Root**

**- Domain validation:** proving the ownership of a particular domain. 132

**- Extended validation:** process that requires a more rigorous check on the subject’s legal identity and control over the domain or software being signed. 133

**• Certificate formats**

**- Distinguished encoding rules (DER):** the binary format used to structure the information in a digital certificate.

**- Privacy enhanced mail (PEM):** base64 encoding scheme used to store certificate and key data as ASCII text.

**- Personal information exchange (PFX):** windows file format for storing a private key and certificate data. The file can be password protected.

**- .cer:** file extension used in Windows

**- P12:** format that allows a private key to be exported along with its digital certificate.

**- P7B:** file format for transmitting a chain of digital certificates using PKCS #7.

**• Concepts**

**- Online vs. offline CA:** online is one that is available to accept and process certificate signing requests, publish certificate revocation lists and perform other certificate management tasks. Offline is disconnected from any network and kept in powered-down state. Root = offline. 128

**- Stapling:**

**- Pinning:** ensures that when a client inspects the certificate presented by a server or a code-signed application, it is inspecting the proper certificate. 140

**- Trust model:** critical PKI concept that shows how users and different CAs are able to trust one another. 127

**- Key escrow:** keep a copy of the private key in escrow… must password-protect the key. 142

**- Certificate chaining:** hierarchical model has a root CA and leaf CAs that can be traced back to the root CA along the certification path. 127

**4.0 Operations and Incident Response**

**4.1 Given a scenario, use the appropriate tool to assess organizational security.**

**• Network reconnaissance and discovery**

**- tracert/traceroute:** reports the round-trip time for hops between the local host and a host on a remote network. 37

**- nslookup/dig:** query name records for a given domain using a particular DNS resolver to see if DNS is misconfigured. 41

**- ipconfig/ifconfig:** show the configuration assigned to network interfaces including the hardware or MAC address, IPv4 and IPv6 addresses, default gateway and whether the address is static or assigned by DHCP. 36

**- nmap:** open-source port scanner. 38

**- ping/pathping:** probe a host on a particular IP address or host name using ICMP; provides statistics for latency and packet loss along a route over a longer measuring period. 36-37

**- hping:** open-source spoofing tool that provides the ability to craft network packets to exploit vulnerable firewalls and IDSs. It can do host/port detection and firewall testing, traceroute, and DOS. 44

**- netstat:** shows the state of TCP/UDP ports on the local machine. 40

**- netcat:** tool for testing connectivity, port scanning and fingerprinting. 46

**- IP scanners:** performs host discovery and identifies how the hosts are connected together in an internetwork. 38

**- arp:** display the local machine’s ARP cache which shows the MAC address of the interface associated with each IP address the local host has communicated with recently. 37

**- route:** view and configure the host’s local routing table. 37

**- curl:** command-line client for performing data transfers over many types of protocol. 42

**- theHarvester:** tool for gathering open-source intelligence for a particular domain or company name. 41

**- sn1per:** framework designed for penetration test reporting and evidence gathering. 46

**- scanless:** tool that uses third-party sites to scan ports. 41

**- dnsenum:** packages a number of tests into a single query… hosts information and name records and tries to work out the IP address ranges that are in use. 41

**- Nessus:** vulnerability scanner produced by Tenable. 42

**- Cuckoo:** packaged software that aims to provide a turnkey sandbox solution. 90

**• File manipulation**

**- head:**  first 10 lines of a file. 278

**- tail:** last 10 lines of a file. 278

**- cat:** view the contents of one or more files. 278

**- grep:** string matching or regex syntax to search text files for specific strings. 279

**- chmod:** used to modify permissions. 200

**- logger:** writes input to the local system log or to a remote syslog server. 278

**• Shell and script environments**

**- SSH:** means of obtaining secure remote access to a command-line terminal. Used for remote administration and secure file transfer (SFTP). 311

**- PowerShell:** a command shell and scripting language built on the .NET framework. 392

**- Python:** scripting language used for automation tools and security tools. 390

**- OpenSSL:** provides secure communications over computer networks. Certificate management. 141

**• Packet capture and replay**

**- Tcpreplay:** takes previously captured traffic that has been saved to a .pcap file and replays it through a network interface. 45

**- Tcpdump:** command-line packet capture utility for Linux. 42

**- Wireshark:** open-source graphical packet capture and analysis utility. 43

**• Forensics**

**- dd:** linux command that makes a bit-by-bit copy of an input file, typically used for disk imaging.

**- Memdump:** linux utility developed as part of the Coroner’s toolkit to dump system memory data to a file.

**- WinHex:** commercial tool for forensic recovery and analysis of binary data, with support for a range of file systems and memory dump types. 491

**- FTK imager:** forensic investigation suite designed to run on windows server. 491

**- Autopsy:** graphical front-end that acts as a case management/workflow tool. 491

**• Exploitation frameworks:** uses the vulnerabilities identified by an automated scanner and launches scripts of software to attempt to deliver matching exploits. 45

**• Password crackers:** hashcat. 161

**• Data sanitization:** erasing data. 552

**4.2 Summarize the importance of policies, processes, and procedures for incident response.**

**• Incident response plans:** procedures, contacts, resources available to responders for various incident categories. Playbook. 458

**• Incident response process 456**

**- Preparation:** make the system resilient to attack in the first place. Hardening systems, writing policies and procedures, setting up confidential lines of communication, and creating incident response resources and procedures.

**- Identification:** from the info in an alert or report, determine whether an incident has taken place, assess how severe it might be, and notify stakeholders.

**- Containment:** limit the scope and magnitude of the incident.

**- Eradication:** remove the cause and restore the affected system(s) to a secure state.

**- Recovery:** reintegrate the system(s) into the business process, restoration of data from backup, security testing.

**- Lessons learned:** analyze the incident and responses to identify whether procedures or systems could be improved. Documentation.

**• Exercises**

**- Tabletop:** least expensive. facilitator presents a scenario and responders explain what action they would take to identify, contain, and eradicate the threat. 461

**- Walkthroughs:** facilitator presents a scenario and responders demonstrate what actions they would take in response such as running scans and analyzing sample files. 462

**- Simulations:** team-based exercise where red team attempts an intrusion and blue team does response and recovery while white team moderates and evaluates. 462

**• Attack frameworks**

**- MITRE ATT&CK:** matrix of known TTPs. 460

**- The Diamond Model of Intrusion Analysis:** framework to analyze an intrusion event by exploring adversary, capability, infrastructure, and victim. Attack reporting. 461

**- Cyber Kill Chain:** framework used to describe the stages of an attack. Includes: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. 460

**• Stakeholder management:** internal and external stakeholders; ensure parties with privileged info do not release it to untrusted parties; obligation to report the attack; marketing and PR impact. 458

**• Communication plan:** secure communications between trusted parties. Need an out-of-band or offline communication strategy that cannot be intercepted. Messaging with end-to-end encryption. 458

**• Disaster recovery plan:** when the organization’s primary business function is disrupted. Resources to shift processing to a secondary site and involvement of more stakeholders. 462

**• Business continuity plan:** how business processes should deal with disruption and includes ensuring processing redundancy. 463

**• Continuity of operations planning (COOP):** used for govt facilities… backup methods of performing mission functions without IT support. 463

**• Incident response team:** CIRT, CSIRT, or CERT are dedicated teams that act as a single point of contact for the notification of security incidents. They usually work in SOC 24/7. Sometimes may need involvement of legal, HR, and marketing departments. 457

**• Retention policies:** policies for historic logs and data captures sets the period for which these are to be retained. Helpful for future investigations. 463

**4.3 Given an incident, utilize appropriate data sources to support an investigation.**

**• Vulnerability scan output:** report can be analyzed to identify which vulnerabilities have not been patched or config weaknesses that have not been remediated.

**• SIEM dashboards 466**

**- Sensor:** a network tap pr port mirror that performs packet capture and intrusion detection.

**- Sensitivity:** reduce false positive indicators being reported as an event. Log only, alert, alarm.

**- Trends:** patterns or indicators within a data set over a time series. Incident type and frequency over time. 468

**- Alerts:**

**- Correlation:** interpreting the relationship between individual data points to diagnose incidents of significance to the security team. 466

**• Log files**

**- Network:** logs generated by routers, firewalls, switches, and access points. They record the operation and status of the appliance as well as network behavior. 469

**- System:** events generated by the OS and its services. 469

**- Application:** application may use Event Viewer or syslog to write event data. 470

**- Security:** audit events… failed logon or denied access to a file. 469

**- Web:** log HTTP traffic that encounters an error or that matches a predefined rule set. 470

**- DNS:** log an event each time it handles a request to convert between a domain name and an IP address. 470

**- Authentication:** authentication attempts for each host. 470

**- Dump files:** an image file that can be analyzed to identify the processes that are running, the contents of temporary file systems, registry data, network connections, cryptographic keys. 471

**- VoIP and call managers:** VoIP uses SIP and RTP and should use TLS for security. Call managers are gateways that connect endpoints within the local network and over the internet. 471

**- Session Initiation Protocol (SIP) traffic:** SIP log identifies the endpoints involved in a call request and the type of connection and status messaging. 472

**• syslog/rsyslog/syslog-ng:** open format protocol and server software for logging event messages. 468

**• journalctl:** command that prints the entire journal log to view the events of journald. 469

**• NXLog:** open-source log normalization tool. 469

**• Bandwidth monitors:** key indicator of suspicious behavior because unexpected bandwidth consumption could be evidence of data exfiltration attack. 473

**• Metadata:** the properties of data

**- Email:** internet header contains address info for the recipient and sender and details of the servers handling transmission. 471

**- Mobile:** call detail records of incoming, outgoing and attempted calls and SMS text time, duration, and recipient’s number as well as data transfer volumes. 472

**- Web:** resource plus headers and authorization info in the form of cookies. 471

**- File:** stored as attributes. When a file was created, accessed and modified. 471

**• Netflow/sFlow**

**- Netflow:** a Cisco developed means of reporting network flow information to a structured database. 473

**- sFlow:** developed by HP… uses sampling to measure traffic statistics at any layer of the OSI model for a wider range of protocol types than the IP-based Netflow. 473

**- IPFIX:** the new Netflow.

**• Protocol analyzer output:** info captured from network packets can be aggregated and summarized to show overall protocol usage and endpoint activity. 472

**4.4 Given an incident, apply mitigation techniques or controls to secure an environment**

**• Reconfigure endpoint security solutions**

**- Application approved list:** denies execution unless the process is explicitly authorized. 478

**- Application blocklist/deny list:** allows execution, but explicitly prohibits listed processes. 478

**- Quarantine:** sandbox the endpoint or suspect process/file. 479

**• Configuration changes**

**- Firewall rules:** ingress and egress filtering rules. 477

**- Mobile device management (MDM):** provides execution control over apps and features of smartphones. 478

**- DLP:** mediates the copying of tagged data to restrict it to authorized media and services. 477

**- Content filter/URL filter:** secure web gateways (SWG) mediate user access to internet services with the ability to block content from regularly updated URL/domain/IP blacklists and perform ID/IP on traffic. 477

**- Update or revoke certificates:** remove compromised root certificates and revoke certificates on compromised hosts. 478

**• Isolation:** removing an affected component from the larger environment it is a part of. 475

**• Containment:**

**• Segmentation:** achieving the isolation of a host or group of hosts using network technologies and architecture such as VLANs, routing/subnets, and firewall ACLs. 476

**• SOAR 479**

**- Runbooks:** automate as many stages of the playbook as possible leaving clearly defined interaction points for human analysis. 479

**- Playbook:** checklist of actions to perform to detect and respond to a specific type of incident.

**4.5 Explain the key aspects of digital forensics**

**• Documentation/evidence**

**- Legal hold:** information that may be relevant to a court case must be preserved. 485

**- Video:** crime scene is recorded using video and must capture identifying, collecting and handling of evidence. 486

**- Admissibility:** quality of being acceptable or valid as evidence in a court of law. 484

**- Chain of custody:** documentation that reinforces the integrity and proper handing of evidence from collection, to analysis, to storage, and to presentation. 485

**- Timelines of sequence of events:** tying events to specific times to establish a consistent and verifiable narrative. 486

**- Time stamps:** many OS and file systems record time stamps but you must note the offset between local system time and UTC. 486

**- Time offset:** offset between local time and UTC. 486

**- Tags:** apply standardized keywords or labels to files and metadata to help organize the evidence. 485

**- Reports:**

**- Event logs:** event logs for one or more appliance or hosts.

**- Interviews:** witness interviews to establish what they were doing at the scene, whether they observed suspicious behavior, etc. 486

**• Acquisition**

**- Order of volatility:** more volatile to least volatile. 1) CPU registers and cache, 2) RAM, 3) HDD, SDD, 4) remote logging and monitoring data, 5) physical configuration and network topology, 6) archival data and printed documents.

**- Disk:** disk image acquisition from nonvolatile storage (HDD, SDD, firmware, flash memory). 493

**- Random-access memory (RAM):** non-persistent system memory. 490

**- Swap/pagefile:** partition that stores pages of memory in use that exceed the capacity of the host’s RAM modules. 493

**- OS:**

**- Device**

**- Firmware:** implemented as flash memory… extracted using a imaging utility. 496

**- Snapshot:** live acquisition image of a persistent disk. 495

**- Cache:** stored in the file system and can be acquired as part of a disk image. 495

**- Network:** packet captures and traffic flows come from a SIEM. 495

**- Artifacts:** any type of data that is not part of the mainstream data structures of an OS. 495

**• On-premises vs. cloud**

**- Right-to-audit clauses:** in public cloud in SLA. 496

**- Regulatory/jurisdiction:** may restrict what evidence the CSP is willing to release to you. 496

**- Data breach notification laws:** cloud processors have to coordinate the timing of notification and contact with the regulator between the organization and the CSP. 496

**• Integrity**

**- Hashing:** produces a fixed length string from an input plaintext that can be of any length. 97

**- Checksums:** message digest or hash is the output.

**- Provenance:** recording the whole process proves origin. 494

**• Preservation:** ensure that nothing you do alters data or metadata on the source disk or file system. Label, bag and seal all host devices and media taken from the crime scene. 494

**• E-discovery:** filtering the relevant evidence produced from all the data gathered and store it in a database in a format such that is can be used as evidence in a trial. 485

**• Data recovery:** analyzing a disk for file fragments stored in slack space. 495

**• Non-repudiation:** data acquisition with integrity ensures this. 494

**• Strategic intelligence/counterintelligence:** data and research that has been analyzed to produce actionable insights; identification and analysis of specific adversary TTPs provides info about how to configure and audit active logging systems so that they are most likely to capture evidence of attempted and successful intrusions. 488

**5.0 Governance, Risk, and Compliance**

**5.1 Compare and contrast various types of controls 8-9**

**• Category**

**- Managerial:** gives oversight of the information system.

**- Operational:** implemented by people rather than systems. Security guards.

**- Technical:** implemented by a system (hardware, software) such as firewalls, AV software

**• Control type**

**- Preventive:** eliminate or reduce the likelihood that an attack can succeed. 9

**- Detective:** identify and record any attempted or successful intrusion… logs. 9

**- Corrective:** eliminate or reduce the impact of an intrusion event… used after the attack. Backup system and patch management system. 9

**- Deterrent:** psychologically discourages an attacker from attempting an intrusion

**- Compensating:** substitute for main controls and affords the same or better level of security.

**- Physical:** alarms, gateways, locks, lighting, security cameras, guards.

**5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture**

**• Regulations, standards, and legislation**

**- General Data Protection Regulation (GDPR):** EU’s regulation that states that personal data cannot be collected, processed or retained without the individual’s informed consent. 14

**- National, territory, or state laws**

**- Payment Card Industry Data Security Standard (PCI DSS):** defines safe handling and storage of financial information. 14

**• Key frameworks**

**- Center for Internet Security (CIS):** 20 CIS controls… produces benchmarks for different aspects of cybersecurity. 12

**- National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)/**

**Cybersecurity Framework (CSF):** focuses on IT security. CSF for business vs RMF for fed agencies

**- International Organization for Standardization (ISO) 27001/27002/27701/31000:** information security standards, security controls, cloud security, personal data and privacy, ERM

**- SSAE SOC 2 Type I/II:** audit specifications… Type 1 assesses system design; Type 2 assesses ongoing effectiveness of the security architecture over 6-12 months. 12

**- Cloud security alliance:** assists CSPs in setting up and delivering secure cloud platforms. 11

**- Cloud control matrix:** lists specific controls and assessment guidelines that should be implemented by CSPs. 11

**- Reference architecture:** best practice methodology and tools for CSPs to use in architecting cloud solutions. 11

**• Benchmarks /secure configuration guides**

**- OS/Network Platform/vendor-specific guides:** lists the settings and controls that should be applied for a computing platform to work in defined roles. guides for configuring the deployment of network appliances, OSs, web servers, app/database servers.

**- Application server:** client/server model so part of the application is a client software program that is installed and runs on separate hardware to the server application. 13

**5.3 Explain the importance of policies to organizational security.**

**• Personnel**

**- Acceptable use policy (AUP):** protects against misuse of equipment. Forbids the misuse of equipment to defraud, defame, or to obtain illegal material. 208

**- Job rotation:** rotate individuals in and out of roles. 182

**- Mandatory vacation:** employees are forced to take their vacation time during which someone else fulfills their duties. 183

**- Separation of duties:** prevent ethical conflicts and abuse of powers.

**- Least privilege:** user is granted sufficient rights to perform their job and no more. Mitigates authorization creep.

**- Clean desk space:** employee’s work area should be free of any documents to prevent sensitive info from being obtained by unauthorized staff. 209

**- Background checks:** determines a person is who they say they are and are not concealing any criminal activity. 181

**- Non-disclosure agreement (NDA):** assertion that they will not share confidential info with a third party. 182

**- Social media analysis:** check for policy infringements. 208

**- Onboarding:** welcoming a new employee, create accounts and user access. 181

**- Offboarding:** exit interview. Disable user account and privileges, retrieve company assets, wipe employee-owned devices of corporate data. 183

**- User training:** mitigates against social engineering and malware attacks. 209

**- Gamification/Capture the flag:** gamified competition… complete a series of challenges. 210

**- Phishing campaigns:** sending simulated phishing messages to users. 210

**- Phishing simulations:** interfaces or emulators 211

**- Computer-based training (CBT):** allows a student to acquire skills and experience by completing simulations and scenarios on the computer. 211

**- Role-based training:** training for security -sensitive roles. 210

**• Diversity of training techniques** improves engagement and retention. Exp. Facilitated workshops, 1 on 1 instruction, mentoring, comp-based online training, videos, books, blogs. 210

**• Third-party risk management 322**

**- Vendors:** supplier of commodity goods and services… must be trustworthy

**- Supply chain:** establishing a trusted supply chain for computer equipment means denying malicious actors the time or resources to modify the assets being supplied.

**- Business partners:** close relationship where two companies share closely aligned goals and marketing opportunities.

**- Service level agreement (SLA):** contractual agreement setting out the detailed terms under which a service if provided.

**- Memorandum of understanding (MOU):** preliminary agreement to express intent to work together…informal…respect confidentiality.

**- Measurement systems analysis (MSA):** means of evaluating the data collection and statistical methods used by a quality management process to ensure they are robust.

**- Business partnership agreement (BPA):** partner agreement of IT companies with resellers and solution providers.

**- End of life (EOL):** support and availability of spares and updates become more limited.

**- End of service life (EOSL):** no longer supported by developer or vendor… no longer receive security upgrades and represent a critical vulnerability.

**- NDA:** legal basis for protecting information assets. Deterrence.

**• Data**

**- Classification:** tag assets so that they can be managed through the information life cycle… public, confidential, critical, proprietary, sensitive etc. 440

**- Governance:** the security controls that will be applied to protect data at each stage of its life cycle. Data owner, steward, custodian, controller, processor. 439

**- Retention:** backing up and archiving information assets in order to comply with business policies and applicable laws and regulations. 442

**• Credential policies**

**- Personnel:** credential management must have strong policies and training. 183

**- Third-party:** used by vendors… admin logons + password or cryptographic keys… no plaintext

**- Devices:** use TACACS+ and ensure separation of duties to ensure proper configuration. 187

**- Service accounts:** used by scheduled processes and applications server software (databases)… system vs local service vs network service accounts. 185

**- Administrator/root accounts:** able to install and remove apps and device drivers, change system-level settings and access any object in the file system. Default account = admin = superuser…should be restricted to logging on only during disaster recovery… group policy. 184

**• Organizational policies 530**

**- Change management:** every change needs a rollback plan and should be carefully scheduled…authorized downtime

**- Change control:** to request and approve changes in a planned and controlled way… request for change document… stakeholder notification and approval.

**- Asset management:** tracks all the orgs critical systems, components, devices, and other objects of value in an inventory… collecting and analyzing data about these assets. 531

**5.4 Summarize risk management processes and concepts**

**• Risk types**

**- External:** external threat actors, natural disasters, accidents. 501

**- Internal:** assets and workflows that are owned and managed by the org… malicious and accidental or non-malicious. 501

**- Legacy systems:** no longer receive security updates and expertise is scarce. 502

**- Multiparty:** adverse event affects multiple orgs. Usually arises from supplier. Supply chain.

**- IP theft:** copyrighted material that is stolen can lose commercial value. 502

**- Software compliance/licensing:** shadow IT… EULA… license issues and fines.

**• Risk management strategies**

**- Acceptance:** no countermeasures are put in place because the level of risk does not justify the cost or because there will be unavoidable delay before the countermeasures are deployed. 505

**- Avoidance:** stop doing the activity that is risk-bearing.

**- Transference:** assigning risk to a third party.

**- Cybersecurity insurance:**

**- Mitigation:** reducing exposure to or the effects of risk factors… deploy countermeasures

**• Risk analysis**

**- Risk register:** document showing the results of risk assessments in a comprehensible format. Graphs of impact vs likelihood of risk factor. Shared between stakeholders. 506

**- Risk matrix/heat map:** columns for impact vs likelihood, date of ID, description, countermeasures. Owner/route for escalation, and status. 506

**- Risk and control assessment (RCA):** assessment done by a third party. 501

**- Risk and control self-assessment:** internal process undertaken by stakeholders to identify risks and the effectiveness with which controls mitigate those risks. QA. Workshops. 501

**- Risk awareness:** the cause & effect of risks can be clearly understood by the asset owner. 505

**- Inherent risk:** risk before mitigation

**- Residual risk:** likelihood and impact after specific mitigation, transference or acceptance measures have been applied. “leftover”

**- Control risk:** measure of how much less effective a security control has become over time.

**- Risk appetite:** strategic assessment of what level of residual risk is tolerable. 505

**- Regulations that affect risk posture:** SOX, HIPAA, Gramm-Leach-Bliley, Homeland Security Act, and PCI DSS

**- Risk assessment types:**

**- Qualitative:** risk factors placed in categories of high, medium and low value

**- Quantitative:** assigns concrete values to each risk factor

**- Likelihood of occurrence:** rate of occurrence…

**- Impact:** effect it will have on business

**- Asset value:** material value as well as the direct costs associated with the asset being compromised (downtime) and consequent costs to intangible assets (reputation)

**- Single-loss expectancy (SLE):** amount that would be lost in a single occurrence of the risk

**- Annualized loss expectancy (ALE):** amount that would be lost over the course of a year

**- Annualized rate of occurrence (ARO):** how many times it is estimated to occur over a year

**• Disasters 509**

**- Environmental:** one that cannot be prevented through human agency… natural disaster

**- Person-made:** where human agency is the primary cause… terrorism, war, vandalism, arson

**- Internal vs. external:** by employee or contractor or by outside threat actors

**• Business impact analysis**

**- Recovery time objective (RTO):** amount of time it takes to identify that there is a problem and then perform recovery.

**- Recovery point objective (RPO):** amount of data loss a system can sustain, measured in time.

**- Mean time to repair/restore (MTTR):** time taken to repair or restore a product so that the system is restored to full operation.

**- Mean time between failures (MTBF):** expected lifetime of a product before needs repair. This is for a repairable product.

**- Functional recovery plans:** walkthroughs, workshops, tabletop exercises, action-based exercises, full scale exercises

**- Single point of failure:** causes the entire workflow to fail if it damaged or unavailable and can be mitigated by redundant components.

**- Disaster recovery plan (DRP):** the specific procedures to follow to recover a system to a working state following a disaster level event.

**- Mission essential functions:** functions that can not be deferred… continuous

**- Identification of critical systems:** compiling an inventory of business processes and the assets that support them… people, intangible and tangible assets, procedures.

**- Site risk assessment:** evaluation of risk from disaster events, risk from disruption to utilities, risk to health and safety on premises

**5.5 Explain privacy and sensitive data concepts in relation to security.**

**• Organizational consequences of privacy and data breaches**

**- Reputation damage:** negative publicity... loss of trust

**- Identity theft:** data subject can sue for damages

**- Fines:** regulator can levy fines

**- IP theft:** loss of revenue… commercial losses

**• Notifications of breaches**

**- Escalation:** breach is detected and passed up through the hierarchy to senior decision makers

**- Public notifications and disclosures:** notification to regulators, law enforcement, third-party companies, and affected individuals. Disclosure requirements

**• Data types**

**- Classifications:**

**- Public:** unclassified… no restrictions

**- Private:** individual identity

**- Sensitive:** personal data

**- Confidential:** secret… highly sensitive

**- Critical:** top secret… severely restricted

**- Proprietary:** info created and owned by a company

**- Personally identifiable information (PII):** data that can be used to identify, contact or locate an individual. SSN, DOB, address, etc.

**- Health information:** medical and insurance records, test results

**- Financial information:** data held about a bank and investment accounts, payroll, tax returns

**- Government data:** data about citizens and taxpayers

**- Customer data:** institutional info or personal info about the customer’s employees

**• Privacy enhancing technologies**

**- Data minimization:** principal that data should only be processed and stored if that is necessary to perform the purpose for which it is collected.

**- Data masking:** all or part of the contents of a field are redacted by substituting all character strings with xxx… an irreversible deidentification technique. 452

**- Tokenization:** all or part of data in a field is replaced with a randomly generated token. Token is stored with the original value on a token server. Reversible technique. Substitute for encryption. 452

**- Anonymization:** individual subjects can no longer be identified even if the data set is combined with other data sources. Identifying info is permanently removed. 451

**- Pseudo-anonymization:** modifies or replaces identifying information so that reidentification depends on an alternate data source which must be kept separate. 451

**• Roles and responsibilities 439**

**- Data owners:** senior exec role with ultimate responsibility for maintaining the CIA of information assets. proper classification of data.

**- Data controller:** entity responsible for determining why and how data is stored, collected, and used and for ensuring these purposes and means are lawful.

**- Data processor:** entity engaged by the data controller to assist with technical collection, storage, or analysis tasks.

**- Data custodian/steward:** handles managing the system on which the data assets are stored/ responsible for data quality. Data backup. Manages access rights and security controls.

**- Data protection officer (DPO):** responsible for oversight of any PII assets managed by a company. Law compliance.

**• Information life cycle:** creation/collection, distribution/use, retention, disposal.

**• Impact assessment:** identify the risks of collecting and processing personal data in the context of business workflow or project and identify mechanisms that mitigate those risks.

**• Terms of agreement:** legal contract stating the responsibilities and obligations of each party

**• Privacy notice:** consent statement that states that data collected cannot be used for any other purpose that intended.