Lesson 1: Comparing and Contrasting Attacks

Information Security

- **Information security:** The protection of available information or informationresources from unauthorized access, attack, theft, or data damage
- **Primary goals or functions**:
    - **Prevention**
    - **Detection**
    - **Recovery**
- **Classfications of assets**
    - **Tangible: Physical items**, such as buildings, furniture, computer equipment, software licenses, machinery, inventory (stock), etc.
    - **Intangible: Info resources**, such as IP, accounting info, plans and designs, etc..
    - **Employee:** Staff of an organization
- **Data assets** can be essential to many different business functions
- **CIA Traid:** Confidentiality, Integrity, Availability
- **Security policy**: A formalized statement that defines how security will beimplemented within an organization

Threat

- **Vulnerability:** A **weakness** that could be triggered accidentally or exploited
- **Threat:** The **potential for a threat agent or threat actor** that may trigger a vulnerability accidentally or exploit it.
- **Risk:** The **likelihood and impact** of a threat actor exercise a vulnerability
- **Control:** A system or procedure put in place to mitigate risk
- **Script kiddies**
- **Hackers**
- **Hacktivists:** Use cyber weapons to promote a **political** agenda
- **Newbie (n00b):** Someone with a bare minimum of experience and expertise
- **Nation state actors:** Goals are espionage and strategic adv,etc. Sponsored and protected by state
- **APT:** The ongoing ability of an adversary to compromise network security using a variety of tools and techniques
- **Killchain**

    - **Planning/scoping**
    - **Reconnaissance/discovery**
    - **Weaponization**
        - **Exploit**
        - **Callback:** Establish a covert channel to an external Command and Comtrol
        - **Tool download**
    - **Post-exploitation /lateral discovery/ spread**
    - **Retreat:** Remove any trace of their presence
- **STIX architecture**
    - **Observable**
    - **Indicator**
    - **Incident**
    - **TTP**
        - **Tatics**
        - **Techniques**
        - **Procedures**
    - **Campaign and Threat Actors**
    - **Exploit Target**
    - **CoA (Course of Action):** Mitigate actions or use of security controls to reduce risk
- **Deep web and Dark web**

Social Engineering

- **Impersonation**
    - **Familiarity/ Liking**
    - **Consensus/ Social proof**
    - **Authority and Intimidatoin**
    - **Scarcity and Urgency**
- **Trust and surveillance**
    - **Dumpster diving**
    - **Shoulder surfing**
    - **Tailgating**
- **Phishing, Whaling, and Vishing**
    - **Spear phishing**
    - **Whaling**

    - **Vishing**
- **Pharming and Hoaxing**
    - **Pharming**
    - **Hoaxing**
    - **Water hole attack**
- **Troubleshooting**
    - **Train employees**
    - **Establish a reporting system**

Malware

- **Virus**
    - **Boot sector virus:** Attack the disk boot sector information, the partition table,and sometimes the file system
    - **Program virus:** Sequences of code that insert themselves into anotherexecutable program
    - **Script virus:** Scripts are powerful languages used to automate OS functions andadd interactivity to web pages
    - **Macro virus:** Use the programming features available in Microsoft Officedocuments
    - **Multipartite virus:** Use both boot sector and executable file infection methodsof propagation.
- **Worms**
- **Trojans:** malware code concealed within an application package that the user thinks is benign. For **monitoring and controlling** a system
- **Bots**
- **RATs**
- **BackDoors**
- **Soyware**
- **Adware**
- **Keyloggers**
- **Rootkits:** Represents a class of backdoor malware that is harder to detect and remove. Work by changing core system files and programming interfaces…
- **Ransomware**
- **Crypto-Malware**
- **Logic bombs**

Lesson 2: Comparing and Contrasting Security Control

Security Control and Framework Types

- **Security control types**
  - **Administrative/ management:** Controls that determine the way people act,including policies, procedures, and guidance
  - **Technical**
  - **Physical**
  - **-OR-**
  - **Preventive:** Restricts unauthorized access
  - **Deterrent (震慑):** Psychologically discourages an attacker
  - **Detective:** Identify andrecord any attempted or successful intrusion
  - **Corrective:** The control responds to and fixes an incident and may also prevent its reoccurrence
  - **Conpensating:** Restore the function of the system through...
- **Frameworks and Fefference Architectures**
  - **NIST:** Focusing exclusively on IT security, rather than IT service provision more generally
  - **ISO:** In conjunction with the IEC
  - **COBIT:** An overall IT governance framework with security as a core component
  - **SABS:** A methodology for providing informationassurance aligned to business needs and driven by risk analysis
- **Regulatory compliance requirements**
  - **Due diligence:** A legal term meaning that responsible persons have not been negligent in discharging their duties
  - **SOX:** Mandate the implementation of risk assessments, internal controls,and audit procedures
  - **FISMA:** Govern the security of data processed by federal government agencies
  - **GLBA**
  - **HIPPA**
  - **PCI DSS**
- **Benchmarks and Secure configuration guides**
  - **Platform/ Vendor-specific guides**
  - **General purpose guides**

        - **OWASP:** A not-for-profit, online community that publishes several secure application developmentresources, such as the Top 10 list of the most critical application security risks
        - **STIGs:** Provide hardening guidelines for a variety of software and hardware solutions
        - **NCP (Nation checklist program):** Provide checklists and benchmarksfor a variety of operating systems and applications
        - **SANS Institute:** A company specializing in cybersecurityand secure web application development training and sponsors the GlobalInformation Assurance Certification (GIAC)
        - **Center for Internet Sercurity:** A not-for-profitorganization (founded partly by SANS). It publishes the well-known "Top 20 CriticalSecurity Controls" (or system design recommendations)

Incident Response Procedure

- **Incident management or Incident Response Policy:** The procedures and guidelinesfor dealing with security incidents
- **Incident:** Where security is breached or there isan attempted breach
- **Incident response lifecycle**
    - **Preparation**
    - **Identification**
    - **Containment, Eradication, and Recovery:** Limit the scope and impact of the incident. The typical response is to "pull the plug" on the affected system, but this is not always appropriate. Once the incident is contained, the cause can then beremoved and the system brought back to a secure state
    - **Lesson Learned:** Analyze the incident and responses to identify whetherprocedures or systems could be improved
- **IRP (Incident Response Plan):** List the procedures, contacts, and resources available to responders should be developed
- **CIRT (Cyber Incident Response Team)**
- **Incident types/ Category definitions**
    - **Date integrity**
    - **Downtime**
    - **Economic/ publicity**
    - **Scope**
    - **Detection time**
    - **Recovery time**

- **Quarantine and Device removal:** If further evidence needs to be gathered, the best approach may be to quarantine orsandbox the affected system or network
- **Escalation**
- **Data breach and reporting requirements**
- **Eradication and recovery**
    - **Investigation and escalation:** The causes or nature of the incident might not beclear, in which case further (careful) investigation is warranted
    - **Containment:** Allow the attack to proceed, but ensure that valuable systems ordata are not at risk
    - **Hot swap:** Backup system is brought into operation and the live system frozen topreserve evidence of the attack
    - **Prevention**

Lesson 3: Assessing Security Posture with Software Tools

Pentest

- **Security assessment framework**
    - **SP 800-115 (Technical Guide to Info Security Testing and Assessment)**
        - Testing the object under assessment to discover vulnerabilities or to prove the effectiveness of security controls.
        - Examining assessment objects to understand the security system and identify anylogical weaknesses. This might highlight a lack of security controls or a commonmisconfiguration.
        - Interviewing personnel to gather information and probe attitudes toward andunderstanding of security.
- **Vulnerability scanning**
- **Rules of engagement**
- **Pentest techniques**
    - **Reconnaissance**
        - **OSINT**
        - **Social engineering**
        - **Scanning**
    - **Initial exploitation**
    - **Persistence**
    - **Escalation of privilege and pivot**

Topology Discovery / Footprinting

- **Network scanner**
- **ipconfig**
- **ifconfig**
- **ip**
- **ping**
- **arp**
- **nmap host discovery**
- **tracert**
- **traceroute**
- **nmap topology discovery**

- **DNS harvesting (nslookup/ dig)**

Fingerprinting and Sniffing

- **Service discovery**
- **netstat:** Chech the state of ports on the local machine
- **nmap service discovery**
- **OS fingerprinting**
- **Banner/ OUI grabbing**
- **Sniffers**
    - **libpcap**
    - **winpcap**
- **Promicuous mode and sniffing switched ethernet**
    - **Port mirroring:** Forwardscopies of traffic on one or more standard ports to a designated mirror port. This allows legitimate sniffing applications and devices to monitor network traffic
- **Protocol Analyzer:** In conjunction with a sniffer toperform traffic analysis
- **tcpdump:** A command-line packet capture utility for Linux, though a version of theprogram is available for Windows
- **Wireshark**
- **Packet injection**
- **RAT**
    - **Netcat:** Available for both Windows and Linux
- **Steganography**

Vulnerability Scanning

- **Passive scan**
- **Active scan**
- **Non-credentialed scan**
- **Credentialed scan:** Allow much more in-depth analysis, especially in detecting when applications orsecurity settings may be misconfigured. It also demonstrates what an insider attack orone where the attacker has compromised a user account may be able to achieve.
- **Lack of controls and misconfigurations**
- **Exploitation frameworks**
- **Honeypot and Honeynets:** Honeynet is an entire decoynetwork. This may be set up as an actual network or simulated using an emulator

Lesson 4: Cryptography

Cryptographic Terminology

- **Plaintext/ Cleartext**
- **Ciphertext**
- **Cipher**
- **Cryptanalysis**
- **Cryptography supporting:**
    - **Confidentiality**
    - **Authentication and Access control**
    - **Non-repudiation:** Is linked to **identification** and **authentication**
    - **Integrity**
    - **Resiliency (弹性)**
    - **Obfuscation (混淆)**
- **Cryptographic ciphers and keys**
    - **Substitution cipher**
    - **Transposition cipher**
    - **Confusion:** The key should not be derivable from the ciphertext. If onebit in the key changes, many bits in the ciphertext should change
    - **Diffusion:** Predictable features of the plaintext should not be evident in the ciphertext. If one bit of the plaintext is changed, many bits in the ciphertextshould change as a result.
    - **Frequency analysis**
    - **OPT**
    - **XOR:** Have an advantage over OR or AND for equal chance of outputting one or zero
    - **IVs:** The principal characteristic of an IV is that it be random
    - **Nonces:** The principal characteristic of a nonce is that it is never reused within the same scope. It could be arandom or pseudo-random value,
    - **Salt:** Used specifically in conjunction with cryptographically hashing password values
- **Cryptanalysis techniques**
    - **Known ciphertext:** The analyst has obtained the ciphertext but has no additional information about it. The attacker may use statistical methods such as frequency analysis to try to break the encryption
    - **Known plaintext:** The attacker knows or can guess some of the plaintext present in a ciphertext, but not its exact location or context.

  - **Chosen plaintext:** The attacker can submit plaintexts to the same cryptographic process to derive corresponding ciphertexts, facilitating analysis of the algorithm and potentially recovery of the key
  - **Chosen ciphertext:** The attacker can submit ciphertexts to the same cryptographic process to derive corresponding plaintexts. The aim of this type of attack is to deduce the key used for decryption
- **Random Number Generation**
  - **TRNG:** sample some sort of physical phenomena, such as atmospheric noise, with a high rate of entropy
  - **PRNG:** Use software routines to simulate randomness.
- **Side channel attack:** Studying physical properties of the cryptographic system, information may be deduced about how itworks.

Hashing and Symmetric Cryptographic Algorithms

- **Resource vs Security constraints**
- **Low power devices**
- **Low latency uses**
- **Data states**
  - **Data at rest:** The data is in some sort of persistent storage media
  - **Data in transit**
  - **Data in use:** Data is present in volatile memory, such as system RAM or CPU registers and cache
- **Hashing**
  - **SHA1: 160 bit digest, have weakness**
  - **SHA2**
  - **MD5: 128 bit hash value. Weak algorithm**
  - **RIPEMD (Race Integrity Primitives Evaluation Message Digest):** Designed to replace MD5 and SHA. **RIPEMD-160** has similar performance and encryption strength to **SHA-1**
  - **HMAC:** Prove the integrity and authenticity of a message. The message is combined with a **secret key**.
- **Symmetric encryption**
  - **Stream Ciphers**
  - **Block Ciphers**
    - **DES/ 3DES: 56 bit key (*3)**
    - **AES/ AES256: Faster and more secure than 3DES**
    - **Blowfish/ Twofish**
- **Modes of operation**

- **ECB:** Apply the same key toeach plaintext block. This means that identical plaintext blocks can output identical ciphertexts, making the ciphertext vulnerable to cryptanalysis.
- **CBC:** Improve ciphertext integrity by applying an IV to the first plaintext block to ensure that the key produces a unique ciphertext from any given plaintext
- **CTR:** Each block is combined with a nonce counter value. This ensures unique ciphertexts from identical plaintexts and allows each block to be processed individually and consequently in parallel, improving performance

Asymmetric Algorithms

- **RSA Digital Signatures:** Used to prove the identity of the sender of a message and to show that a message has not been tampered with since the sender posted it. Provide **authentication**, **integrity**, and **non-repudiation**.
- **Digital Envelopes:** A secret key itself is encrypted using public key cryptography then attached to the encrypted message
- **Digital Certificates**
- **Diffie-Hellman:** A key agreement protocol.
- **DSA:** An adaptation of ElGamal's algorithms used by NIST
- **ElGamal encryption:** Adapt the Diffie-Hellman protocol to use for encryption and digital signing rather than simply as a mechanism for agreeing to a shared secret
- **ECC**
- **Key exchange**
- **Perfect forward secrecy:** Even if the encrypted session is recorded there will be no way of recovering a key to use to decrypt it at a later date.
- **MitM attack**
- **Downgrade:** Can be used to facilitate a Man-in-the-Middle attack by requesting that the server use a lower specification protocol with weaker ciphers and key lengths
- **Replay Attacks**
- **Birthday attack**
- **Collisions**

Lesson 5: PKI

Public and Private Key Usage

- **Digital certification:** A wrapper for a subject's public key
- **Fields**
  - **Version**
  - **Serial number**
  - **Signature algorithm**
  - **Issuer**
  - **Valid From/ To**
  - **Subject**
  - **Public Key**
  - **Extensions**
- **Extension:** Defined for version 3of the X.509 format, allow extra information to be included about the certificate
- **Components**
  - **Extension ID:** OID
  - **Critical:** A boolean value indicating whether the extensions is critical
  - **Value:** String value of the extension
- **Key usage:** Define the purpose for which a certificate was issued, such as for signing documents or keyexchange
- **Formats**
  - **DER (Distinguished Encoding Rules)**
  - **Base 64 PEM**
  - **.PFX**
  - **.P12**
  - **P7B**
- **CA:** The person or body responsible for issuing and guaranteeing certificates
- **Email/User certificates:** Used to sign and encrypt email messages, typically usingS/MIME or PGP
- **Code signing certificates:** Issued to a software publisher, following some sort of identity check and validation process by the CA
- **Root certificate:** The one that identifies the CA itself. The root certificate is self-signed.
- **Self-signed certificates**

PKI Management

- **Lifecycle**
    - **Key generation**
    - **Certificate generation**
    - **Storage**
    - **Revocation**
    - **Expiration and renewal**
- **Key escrow:** Archivie a key (or keys) with a third party
- **CRL (Certificate revocation lists)**
- **OSCP (Online Certificate Status Protocol)**
- **Singel CA**
- **Interneduate CA:** Certificate chaining or a chain of trust
- **Certificate pinning:** Several techniques to ensure that when a client inspectsthe certificate presented by a server or a code-signed application, it is inspecting theproper certificate
- **PGP:** A popular open standard for encrypting email communications and which can also be used for file and disk encryption
- **GPG:** GNU Privacy Guard

Lesson 6: Identity and Access Management Controls

Identity and Authentication

- **Identification**
- **Authentication**
- **Authorization**
- **Accounting**
- **IAM (Identity and Access Management)**
- **ACL (Access control list)**
- **AAA:** Authentication, Authorization, Accounting
- **Issuance/ Enrollment:** Processes by which a subject's credentials are recorded, issued, and linked to the correct account, and by which the account profile is created and maintained
- **Identity management**
- **Category of credentials**
  - **Something you know**
  - **Something you have**
  - **Something you are**
  - **Something you do**
  - **Somewhere you are**
- **Mutual authentication:** A security mechanism that requires that each party in a communication verifies each other's identity

Authentication Protocols

- **LM:** A challenge/response authentication protocol
  - Password are stored using **DES**
  - Alphabetic characters use the limited ASCII character set and are converted to **upper case**
  - Maximum password length is **14** characters. Long passwords are split into **two** and encrypted separately
  - Not salted
- **NTLM**
  - The password is Unicode and mixed case and can be up to **127** characters long.
  - The **128-bit MD4** hash function is used in place of DES

    - Vulnerable to MITM attack, pass-the-hash attack
    - Still the only choice for workgroups (non-domain networks)
- **Kerberos**
    - Provide SSO
    - Default logon provider for **Windows 2000 and later**
    - Provide authentication to **AD**, as well as other…
    - KDC: Key distribution center, using **TCP/UDP port 88**, the **single point-of-failure** for the network
    - TGS
    - AS: Authentication service
    - TGT: Contain info about the client plus a timestamp and validity period
    - Prevent **MITM** attack
    - Can be implemented with **DES**, **RC4**, or **AES** for encryption, as well as **MD5**, **SHA1** for hashing
- **PAP:** Password authentication protocol
- **CHAP:** Challenge handshake authenticatoin protocol
- **MS-CHAP:** Microsoft challenge handshake authentication protocol
- **Password cracker**
    - **Online attack**
    - **Offline attack**
    - **%SystemRoot%\System32\config\SAM:** Local users and passwords are stored as part of the Registry on windows machines
    - **%SystemRoot%\NTDS\NTDS.DIT:** Domain users and passwords are stored in the AD database on domain controller
    - **/etc/passwd:** Encrypted passwords are stored here for universally access
    - **/etc/shadow:** Readable by the root user in Linux
    - **Tools:**
        - **John and ripper:** Multi-platform password hash cracker
        - **THC Hydra:** Used against remote authentication such as Telnet, FTP, SMB, etc.
        - **Aircrack:** Sniff and decrypt WEP and WPA traffic
        - **L0phtcrack:** Best-known windows recovery tools
        - **Cain and Abel:** Password sniffing ultility
- **Attack**
    - **Brute force attack**
    - **Dictionary attack**
    - **Rainbow table attack**
    - **Hybrid attack**

    - **Pass-the-hash:** Authenticate it without cracking it.

MFA

- **Smart card**
- **IEEE 802.1X:** Some variant of the EAP
- **OPT**
- **OATH (Open authentication)**
- **HOTP: HMAC-based OPT algorithm**
- **TOTP: Time-based OPT algorithm**
- **Biometric authentication**
    - **Biometric factors**
        - **False negatives:** Rejection Rate (FRR), Type 1 error. A legitimate user is not recognized
        - **False positives:** FAR, Type 2 error. An interloper is accepted
        - **Crossover Error Rate (CER):** The point at which FRR and FAR meet. The lower the CER, the more efficient and reliable the technology.
    - **Fingerprint scanner**
    - **Restinal scan**
    - **Iris scan**
    - **Facial recognition scanners**
- **Behavioral technologies**
    - **Voice recognition**
    - **Signature recognition**
    - **Typing**
- **Common access card**
    - **Common access card (CAC)**
    - **Personal identification verification card (PIV)**

Lesson 7: Access Services and Accounts

Authorization and Directory Services

- **Implicit deny:** Unless there is a rule specifying that access should be granted, any request for access isdenied
- **Least privilege**
- **SSO**
- **Directory service:** Principal means of providing privilege management and authorization on an enterprise network
- **X.500:** The principal directory standrad
- **LDAP:** A protocol used to query and update an X.500 directory or any type of directory that can present itself as an X.500 directory.
- **X.500 Distinguished names:** A unique identifier for any given resource within an X.500-like directory. A distinguished name is made up of attribute=value pairs, separated bycommas.
- **LDAP weakness:** No security and all transmissions are in plaintext. Vulnerable to sniffing and MitM attack.
- **Authentication of LDAP**
    - **No authentication**
    - **Simple authentication**
    - **Simple authentication and Security Layer (SASL):** Typically use Kerberos ot TLS
    - **LDAP with SSL (LDAPS):** TCP Port 636
- **LDAP injection:** If the web application presents a search form to allow the user to query a directory, a malicious user may enter a search string that includes extra search filter
- **Enterprise authentication of LDAP**
    - **RADIUS**
    - **TACACS:** Similar to RADIUS but more flexible and reliable. Developed by Cisco. TCP Port 49. Often used for device administration than for authenticating end user devices
- **Federation:** If Google and Twitter establish a federated network for the purpose of authentication and authorization, then the user can log onto Twitter using his or her Google credentials or vice versa
- **Transitive trust**
    - **One-way trust**
    - **Two-way trust**

    - **Non-transitive trust**
    - **Transitive trust**
- **SAML (Security association markup language)**
    - **SAML authorization are written in XML.**
    - **Communications are established using HTTP/HTTPS and the SOAP**
    - **Secure tokens are signed using the XML signature specification**
- **SHIBBOLETH:** Open source implementation of SAML
- **Identity Provider:** Supports the authentication of users. Can be integrated with LDAP, Kerberos, X.509, and other directory and authentication systems
- **Embedded Discovery Service:** Allow users to select a preferred identity provider
- **Service Provider:** Process calls for user authentication by contacting the user's preferred identity provider and processing the authentication request and authorization response. Can be used with IIS and APACHE
- **OpenID:** The standard underpinning early "sign on with" features of websites. A solution such as SAML is typical of an enterprise-controlled federated identity management solution. OpenID is an example of a **"user-centric" version of federated identity management**.
- **OAuth**
    - With OpenID, the identity provider does not usually share any profile information or data with the relying party. This requires a different trust relationship to be established. To do so would require the user's consent.
    - OAuth is a protocol designed to facilitate this sort of transfer of information or resources between sites. With OAuth,the user grants an OAuth consumer site the right to access resources stored on an OAuth provider website.
    - Compared to SAML transactions, OAuth uses REST web services, rather than SOAP, and JSON message formatand JSON Web Tokens (JWT), rather than XML
    - In OAuth, the "auth" stands for "**authorization**," not "authentication."
- **OpenID Connect (OIDC):** Replace OpenID to provide an identity management layer over the OAuth 2 protocol so that a site can request an "authentication service" only

Access Management Controls

- **DAC: Discretionary Access Control.**
    - Stresses the importance of the owner. The owner is originally the creator of the resource, though ownership can be assigned to another user.
    - The owner is granted full control over the resource, meaning that he or she can modify its ACL to grant rights to others.

  - The most flexible model, it is also the weakest because it makes centralized administration of security policies the most difficult to enforce
  - Vulnerable to insider threats
- **RBAC: Role-based access control.**
  - Add an extra degree of administrative control to the DAC model. Under RBAC, a set of organizational roles are defined, and users allocated to those roles.
  - Under this system, the right to modify roles is reserved to administrative accounts.
  - The system is non-discretionary, as each user has no right to modify the ACL of a resource, even though they may be able to change there source in other ways. Users are said to gain rights implicitly (through being assignedto a role) rather than explicitly (being assigned the right directly)
  - Make it harder for anattacker to "escalate" permissions gained through a hacked user account
- **MAC: Mandatory access control.**
  - Based on the idea of security clearance levels. Rather than defining access control lists on resources, each object and each subject is granted a clearance level, referred to as a label
  - An instance of a Need to Know policy put into practice. The labeling of objects and subjects takes place using pre-established rules.
  - The critical point is that these rules cannot be changed (except by the system owner), and are, therefore, also non-discretionary. Also, a subject is not permitted to change an object's label or to change his or her own label
  - Associated with military and secret service organizations, where the inconveniences forced on users are secondary to the need for confidentiality and integrity
- **ABAC: Attribute-based access control.**
  - Is capable of making access decisions based on a combination of subject and object attributes plus any context-sensitive or system-wide attributes
  - Can be made sensitive to different levels of risk or threat awareness by making access conditional on the acceptance of a wide range of different attribute values
- **Rule based Access control**
  - Any sort of access control model where access control policies are determined by system-enforced rules rather than system users
  - RBAC, ABAC, and MAC are all examples of rule-based (or non-discretionary) access control
- **Service Accounts**
  - **System:** Have the most privileges of any windows account.

    - **Local Service:** Have the same privileges as the standard user account. Can only access network resources as an anonymous user.
    - **Network Service:** Have the same privileges as the standard user account but can present the computer’s account credentials when accessing network resources.

Account Management

- **Windows Active Directory**
    - **Domain controller:** The Active Directory is implemented as a database stored on one or more servers called a Domain Controller (DC).
    - **Domains:** Provide the primary grouping of users, groups,and computers. The simplest AD design is a single domain, representing the entire organization
    - **Organization Units:** Provide a way of dividing a domain up into different administrative realms.
- **User provisioning:** The processes involved in setting up user accounts
- **Onboarding**
- **Offboarding**
- **Privilege bracketing:** Privileges are granted only when needed,then revoked as soon as the task is finished or the need has passed.

Account Auditing and Recertification

- **Event view**
- **Recertification: Take account of changes to resources and users**

Lesson 8: Secure Network Architecture

Concept

- **Network Zones and Segments**
    - **Single points of failure:** A "pinch point" relying on a single hardware server orappliance or network channel.
    - **Complex dependencies**
    - **Availability over condidentiality and Integrity**
    - **Lack of documentation and change control**
    - **Overdependence on perimeter security:** If the network architecture is "flat" (that is,if any host can contact any other host), penetrating the network edge gives theattacker freedom of movemen
- **DMZ:** Perimeter network
- **Bastion host:** Hosts in a DMZ
- **Screened subnets:** One important use of subnets is to implement a DMZ. Two firewalls are placed ateither end of the DMZ. One restricts traffic on the external interface; the other restrictstraffic on the internal interface
- **Screened host**
- **Honeynet:** Network containing honeypot hosts, designed to attract and study malicious activity.

Secure Switching Infastructure

- **Ad hoc network:** Created when wireless stationsare configured to connect to one another in a peer-to-peer topology
- **STP: Prevent Layer2 loop**
- **MitM**
- **Spoofing**
- **ARP Poisoning**
- **MAC Flood**
- **Physical Port Security**
- **MAC Filter**
- **DHCP snooping**

Network Access Control

- **IEEE 802.11X:** Port-based network access control
- **Network Access Control**
- **Admission control:** Client devices are granted or denied access based on their compliance with the health policy
- **Posture assessment:** Host health checks are performed against a client device to verify compliance with the health policy
- **Remediation:** What happens if the device does not meet the security profile
- **Rouge system detection**

Secure Routing and NAT Infrastucture

- **Routing Attacks**
  - **Fingerprinting**
  - **Software exploits in the underlying OS**
  - **Spoofed routing info**
  - **DoS**
  - **ARP poisoning**
  - **Source routing**
- **IP Spoofing Attack**
- **NAT**
- **NAPT or NAT overloading:** Provide a means for multiple private IP to be mapped onto a single publice address
- **Port forwarding/ Destination NAT**
- **SDN**

Lesson 9: Security Appliances

Firewalls and Proxies

- **Packet filtering**
  - Inspect the headers of IP packets, rules can be based on **IP filtering, Protocol type filtering, Port filtering**.
  - A **stateless** technique because the firewall examines each packet in isolation and has no record of previous packets.
- **Stateful Inspection Firewalls**
  - A circuit-level stateful inspection firewall address these problems by maintaining stateful information about the session established between two hosts
  - Information about each session is stored in a dynamically updated state table
  - Examine the TCP three-way handshake and can detect attempts to open connections maliciously (**Flood guard**).
  - Monitor packet sequence numbers and can prevent **session hijacking** attacks.
- **Application Aware Firewalls**
  - Inspect the contents of packets at the application layer
- **Network-Based Firewalls**
  - Appliance firewall: A stand-alone hardware firewall
  - Router firewall
- **Application-Based Firewalls**
  - Host-based firewall (Personal firewall): A software application running on a single host designed to protect that host only
  - Application firewall: Software designed to run on a server to protect a particular application only.
  - Network OS firewall: A software-based firewall running under a network server OS.
- **Forward Proxy:** Deconstruct each packet, performs analysis, then rebuilds the packet and forwards it on, a legitimate man in the middle. More secure than a firewall
  - **Non-transparent server:** Client must be configured with the proxy server address and port.
  - **Transpartent Proxy:** Intercept client traffic without the client having to be reconfigured. Must be implemented on a switch or router or other inline network appliance.

- **Reverse Proxy Server:** Provide protocol-specific inbound traffic.

Load Balancers

- **DoS/ DDoS**
    - **DRDoS (Distuibuted Reflection DoS)/Amplification attack:** The adversary spoofs the victim's IP and attempts to open connections with multiple servers.
    - **Smurf**
    - **DNS/ NTP** can be abused effectively
    - **Black hole:** An area of the network that cannot reach any other part of the network
    - **Sinkhole Routing:** Traffic flooding a particular IP is routed to a different network where it can be analyzed.
- **Load Balancer:** Distribute client requests across available server nodes in a farm or pool.
    - **Types**
        - **Layer 4 load balancer:** Base forwarding decisions on IP address and TCP/UDP port values. This type of load balancer is stateless; it cannot retain any information about user sessions.
        - **Layer 7 load balancer**
    - **Configuration**
        - **Virtual IP:** CARP (Common Address Redundacy Protocol), Cisco's GLBP (Gateway Load Balancing Protocol)
        - **Scheduling Algorithm:** The code and metrics that determine which node is selected for processing each incoming request
        - **Round Robin DNS:** A client enters a web server name in a browser and the DNS server responsible for resolving that name to an IP address for client connectivity will return one of several configured addresses, in turn, from amongst a group configured for the purpose.
        - **Source IP/Session Affinity:** Layer 4 approach to handling user sessions. When a client establishes a session, it becomes stuck to the node that first accepeted the request.
        - **Persistence:** Keep a client connected to a session, by setting a cookie
- **Cluster service**
    - Fault tolerance of **stateful** data. The data residing on one node is made available to another node seamlessly and transparently in the event of a node failure.

    - Load balancing provides **front-end** distribution of client requests, clustering is used for **back-end** applications.
    - **A/A Clustering:** Consist of n nodes, all of which are processing concurrently
    - **A/P Clustering:** Use a redundant node to failover

IDS/IPS

- **Network-based IDS/IPS**
    - **TAPS and Port Mirrors**
        - **SPAN/Mirror port**
        - **Passive TAP (Test access point):** 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
        - **Active TAP:** A powered device that performs signal regeneration
- **Host-based IDS/IPS**
    - **Signature-based Detection (Pattern matching):** The engine is loaded with a database of attack patterns or signatures
    - **Behavior-based Detection:** Statistical- or profile-based detection, the engine is trained to recognize baseline normal traffic or event. Will be able to identify **0-day attacks.**
    - **Anomaly-based Detection:** Look for irregularities in the use of protocols.
- **Virus scanner**
- **UTM (Unified Threat Management):** A system that centralize various security controls, such as firewall, anti-malware, NIPS, etc.
- **Advanced Malware Tools:** Sysinternals, a suite of tools designed to assist with troubleshooting issues with windows

DLP System

- **Data exfiltration:** Unauthorized copying or retrieval of data from a system.
- **Data Loss Prevention:** Scan content in structured formats
- **DLP Remediation:** The action that the DLP takes when it detects a policy violation.
- **Right Management Services**

Logging and SIEM Systems

- **Security Information and Event Management:** Logs are most important.
- **Types of logs:**
  - Event log
  - Audit log
  - Security log
  - Access log
- **Baseline:** Establish the exptected pattern of operation for a server or network
- **Threshold:** Points of reduced or poor performance or change in configuration that generate an administrative alert.
- **WORM:** Write once, read many

Lesson 10: Wireless and Physical Access Security

Wireless Infrastructure

- **Wireless networks can be configured in one of two modes**
    - **Ad hoc:** The wireless adapter allows connections to and from other devices (a p2p WLAN). This is referred to as an IBSS (Indepentent basic service set)
    - **Infrastructure:** The adapter is configured to connect through an AP to other wireless and wired devices. This is referred to as a BSS. The mac address of the AP is BSSID. More than one BSS can be grouped in an ESS
- **Wireless Controller:** Allow for centralized management and monitoring of the access point on the network.
- **Fat AP:** An AP whose fireware contains enough processing logic to be able to function autonomously and handle clients without the use of wireless controller
- **Thin AP:** The one require a wireless controller in order to function
- **LWAPP:** Allow an AP configured to work in lightweight mode to download an appropriate SSID, standards mode, channel, and security configuration.
- **CAPWAP**
- **Band Selection**
    - **802.11a:** Legacy products working in the 5Ghz band only
    - **802.11bg:** Legacy products working in the 2.4Ghz band only
    - **802.11n:** Can be either dual band or 2.4 Ghz only
    - **802.11ac-5Ghz only**
- **Antenna**
    - **Yagi**
    - **Parabolic**
    - **Rubber Ducky Antennas**
- **MAC Filtering**

Wireless Security Settings

- **WEP:** 24Bit IV is the main problem, RC4 encryption
- **WPA:** TKIP+RC4
- **WPA2:** AES+CCMP
- **PSK Authentication:** Using a passphrase to generate the key that is used to encrypt communications. Also referred to as group authentication.

- **Enterprise/IEEE 802.1X:** Use EAP authentication. The AP passes authentication information to a RADIUS server on the wired network for validation.
- **Open Authentication**
- **Captive Portals**
- **WPS (WIFI Protected Setup):** Vulnerable to Brute-Force attack
- **EAP:** Designed to support different types of authentication within the same overall topology of devices
- **EAP-TLS:** Currently considered the strongest type of authentication and is very widely supported
- **PEAP:** As with EAP-TLS, an encrypted tunnel is established between the supplicant and authentication server, but PEAP only requires a server-side public key certificate
- **EAP-Tunneled TLS (EAP-TTLS):** Similar to PEAP. It uses a server-side certificate to establish a protected tunnel through which the user's authentication credentials can be transmitted to the authentication server.
- **LEAP:** Lightweight EAP
- **EAP-FAST:** Flexible Authentication via Secure Tunneling
- **EAP-MD5**
- **RADIUS Federation**
- **Evil Twin and Rouge AP**
- **Deauthentication/ Disassociation Attack**
- **Jamming (Interference)**
- **Bluetooth:** A short-range (up to about 10 m) radio link, working at a norminal rate of up to about 3Mbps.
- **RFID:** a means of encoding information into passive tags, which can be easily attached to devices, structures, clothing, or almost anything else
- **Skimming:** One type of RFID attack, which is where an attacker uses a fraudulent RFID reader to read the signals from a contactless bank card.
- **NFC (Near Field Communications):** A very shot range radio link based on RFID.

Importance of Physical Security Controls

- **Site Layout and Signs**
  - **Barricade:** Something that prevent access.
  - **Fencing**
  - **Security Lighting**
- **Gateway and Locks**
  - **Lock types**

        - **Conventional:** Prevent the door handle from being operated without the use of a key.
        - **Deadbolt:** A bolt on the frame of the door, separate to the handle mechanism
        - **Electronic:** Operated by entering a PIN
        - **Token-based**
        - **Biometric**
        - **Multifactor**
- **Alarm Systems**
    - **Circuit**
    - **Motion Detection**
    - **Duress**
- **Security Guard and Camera**
    - **Surveillance(监视)**
    - **CCTV (Closed circuit television)**
- **Access Lists and ID Badges**
- **Secure Cabinets, Cages, Cable Locks, and Safes**
- **Protected Distrubution, Faraday Cages, and Air Gaps**
    - **Air Gap:** One that is not physically connected to any network. Such a hostwould also normally have stringent physical access controls, such as housing it within a secure enclosure, validating any media devices connected to it, etc.
- **HVAC (Heating, Ventilation, Air Conditioning)**
- **Hot and Cold Aisles**
- **Fire Detection and Suppression**

Lession 11: Secure Host, Mobile, and Embedded Systems

Secure Hardware System Design

- **Common Criteria:** An ISO standard defining security framework.
- **Trusted OS:** An OS meets the criteria for a CC OS Protectoin Profile.
- **Trusted Computing Group:** A consortium of companies, including MS, Inter, AMD, etc. One of the major initiatives of it was the development of the TPM
- **Hardware/Firmware Security**
- **RoT/ Trust Anchor:** A secure subsystem that is able to provide attestation (Declare something to be true). In computer device, it is usually establiiished by a type of a type of cryptoprocessor called TPM
- **TPM:** A specification for hardware-based storage of digital certificates, keys, hashed passwords, and other user and platform indeitification information.
- **Supply Chain:** The end-to-end process of supplying, manufacturing, distributing, and finally releasing goods and services to a customer.
- **BIOS:** Provide industry standard program code that operates the essential components of the PC and ensures that the design of each manufacturer's motherboard is PC compatible.
- **UEFI:** Provide support for 64-bit CPU operation at boot, a full GUI and mouse operation at boot, and better boot security.
- **Secure Boot:** A security system offered by UEFI, it is designed to prevent a computer from being hijacked by a malicious OS.
- **EMI (电磁干扰) and EMP (电磁脉冲)**

Secure Host Systems Design

- **KIOSKS:** A computer terminal deployed to a public environment.
- **Baseline Deviation Reporting:** Testing the actual configuration of clients and servers to ensure that they are patched and that their configuration settings match the baseline template
- **Execution Control**
- **Removable Media Control**
- **Data Execution Prevention**
  - **DEP**
  - **ASLR (Address Space Layout Randominzation)**
- **Patch Management**

- **End of Life Systems:** The one that is no longer supported by its developer or vendor. End of life systems no longer receive security updates and so represent a critical vulnerability if any remain in active use
- **Lack of Vendor Support**

Secure Mobile Device System Design

- **Mobile Device Deployment Models**
  - **BYOD**
  - **COBO (Corporate Owned, Business Only)**
  - **COPE (Corporate Owned, Personally-Enabled)**
  - **CYOD (Choose Your Own Device)**
- **MDM**
- **PANs:** Personal Area Network, such as Bluetooth, ANT, WIFI Direct, Tethering
- **NFC (Near Field Communication):** Allow a mobile device to make payments via contactless point-of-sale (PoS) machines.
- **Mobile Payment Service**
- **USB and USB OTG**
- **SATCOM (Satellite Communication)**
- **Mobile Access Control System**
- **Remote Wipe**
- **Geolocation and Location Service**
- **App Management**
- **Rooting**
- **Jailbreaking:** Booting the device with a patched kernel.
- **Containment and Storage Segmentation**

Secure Embedded System Design

- **Embedded system:** A complete computer system that is designed to perform a specific, dedicated function.
- **System on A Chip (SOC)**
- **Real Time Operating Systems (RTOS)**
- **SCADA**
- **In-Vehicle Computing System and Drones**
- **IoT**

Lession 12: Secure Network Access Protocols

Secure Network Operations Protocols

- **DHCP**
- **DNS**
- **Host File**
  - **For windows:** /etc/hosts
  - **For linux:** %SystemRoot%\System32\Drivers\etc\hosts
- **Zone transfer**
- **DNSSEC**
- **Cybersquatting:** An attack where an adversary acquires a domain for a company'strading name or trademark, or perhaps some spelling variation thereof
- **Domain hijacking:** An adversary gains control over the registration of a domain name, allowing the host records to be configured to IP addresses of the attacker's choosing
- **Typosquatting:** Misspelled domains can be profitable depending on the frequency that users enter the misspelled name
- **Kiting:** A domain name can be registered for up to five days without paying for it. Kiting means that the name is continually registered, deleted, then re-registered
- **Tasting:** The registration of a domain to test how much traffic it generates within the five-day grace period; if the domain is not profitable, the registration is never completed.
- **SNMP**
  - **Monitor:** Provide a location from which network activitity can be overseen
  - **Agent:** Maintain a database called a MIB. Capable of initiating a trap operatoin.
  - SNMP v1, v2c community names are sent in plaintext
  - SNMP v3 support encryption and strong user-based authentication.
- **NTP**

Secure Remote Access Protocols

- **Tunneling:** A technology used when the source and destination computers are on the same logical network but connected via different physical networks
- **VPN**

    - **Remote Access VPN:** Clients connect to a VPN gateway on the local network. Allow home-workers working in the field to connect to the corporate network
    - **Site-to-Site VPN:** Connect two or more local networks, each of which runs a VPN gateway
- **TLS VPN:** A remote accessserver listening on port 443. The client makes aconnection to the server using TLS so that the server is authenticated to the client.
- **OpenVPN:** An open source example of TLS VPN
- **IPSec**
    - **AH (Authentication Header)**
    - **ESP (Enscapsulation Security Payload)**
    - **Transport mode:** Data encrypted
    - **Tunnel mode:** The whole packet is encrypted
    - **ISAKMP (IKE)**

Secure Remote Administration Protocols

- **Telnet**
- **SSH**
- **RDP**

Lession 13: Secure Network Applications

Secure Web Services

- **HTTP**
- **SSL/TLS and HTTPS**
    - **SSL/TLS Supported Cipher Suites**
        - **Asymmetric: RSA, DSA/DSS, DH**
        - **Symmetric: RC4, RC2, DES, 3DES, IDEA, AES**
        - **HMAC: MD5, SHA**
    - **Version**
        - **Only TLS versions are safe**
        - **Versions are not interoperable**
    - **TLS Accelerator:** Hardware device
- **FTP**
- **TFTP:** A connectionless protocol that also provides file transfer services
- **SFTP (SSH FTP)**
- **FTPS (FTP over SSL)**

Secure Communications Services

- **SMTPS (Secure SMTP)**
    - **STARTTLS:** A command that upgrade an existing unsecure connection to use TLS. Mode widely used than SMTPS
    - **SMTPS:** Establish the secoure connection before any SMTP command are changed
- **Secure POP (POP3S)**
- **IMAPS (Secure IMAP):** Addressed POP's limitation by Internet Message Access Protocol v4 (IMAP4). TCP Port 993
- **S/MIME**
- **VoIP**
- **SIP (Session Initiation Protocol)**.

Secure Virtualization Infrastructure

- **Hypervisor:** Manage the virtual machine environment and facilitates interaction with the computer hardware and network.

    - **Type 1: Such as VirtualBox, VMWare Workstation**
    - **Type 2: VMWare ESX Server, MS Hyper-V**
- **VM vs Container**
- **Hypervisor Security**
- **VM escaping:** Malware running on a guest OS jumping to another guest or to the host

Secure Cloud Service

- **Rapid-Elasticity:** The cloud can scale quickly to meet peak demand
- **Deployment Model**
    - **Public**
    - **Hosted Private:** Hosted by a third party for the exclusive use of the organization
    - **Private**
    - **Community**
- **Cloud Service Types**
    - **IaaS**
    - **SaaS**
    - **PaaS**
    - **SECaaS**

Lession 14: Risk Management and Disaster Recovery

Risk Management Processes

- **MEF (Mission Essential Function):** The one that cannot be deferred.
  - **MTD (Maximum Tolerable Downtime)**
  - **RTO (Recovery Time Objective)**
  - **WRT (Work Recovery Time)**
  - **RPO (Recovery Point Objective)**
- **Asset Management**
- **Threat Assessment**
- **Risk Assessment and Business Impact Analysis (BIA)**
  - **Likelihood:** The probability of the threat being realized
  - **Impact:** The severity of the risk if realized as a security incident.
  - **BIA:** The process of assessing what losses might occur for each threat scenario.
- **Quantitative Risk Assessment**
- **Qualitative(定性) Risk Assessment**
- **Risk Response**
- **Risk Register:** A document showing the results of risk assessments in a comprehensible format.
- **Change Management:** Implement changes in a planned and controlled way.

Resiliency and Automation Strategies

- **COOP (Continuity of Operations Planning):** Sometimes referred to as a business continuity plan (BCP), is a collection of processes that enable an organization to maintain normal business operations in the face of some adverse event.
- **Fault Tolerance:** Often archieved by provisioning redundacy for critical components and single points of failure.
- **Scalability:** The costs involved in supplying the service to more users are linear.
- **Elasticity:** The system’s ability to handle changes in demand in real time
- **Dirtributive Allocation:** The ability to switch between available processing and data resources to meet service requests.
- **RAID (Redundant Array of Independent Disks):** Many disks can act as backups for each other to increase reliability and fault tolerance.

    - **RAID 0:** Striping without parity (no fault tolerance)
    - **RAID 1:** Mirroring- Data is written to two disks simultaneously.
    - **RAID 5:** Striping with parity- Data is written across three or more disks, but additional information is calculated**.**
    - **RAID 6:** Double parity or level 5 with an additional parity stripe
    - Nested (0+1, 1+0, 5+0)
- **Non-Persistence:** Any given instance is completely static in terms of processing function.

Disaster Recovery and Continuity of Operation

- **Recovery Site:** Referred to as being hot, warm, or cold.
- **Location Selection:** Remote site has edges in detecting intruders, carrying risks.
- **Distance and Replication**
- **Legal Implications/Data Sovereignty**
- **Backup**
    - **Backup Types**
        - **Full**
        - **Incremental**
        - **Differential**
    - **Snapshots**
    - **Storage Issues:** Typically,backup media is physically secured against theft or snooping by keeping it in are stricted part of the building, with other server and network equipment. Many backup solutions also use encryption to ensure data confidentiality should the media be stolen
    - **Disaster Recovery**
    - **After-Action Reports (AAR):** Lessons learned is a process to determine how effective COOP and DR planning and resources were.

Forensics

- **ESI (Electronically Stored Information):** Like DNA or fingerprints, digital evidence.
- **Due Process:** A term used in US and UK common law to require that people only be convicted of crimes following the fair application of the laws of the land.
- **Legel Hold:** The fact that information thay may be relevant to a court case must be preserved.

- **eDiscovery:** A means of filtering the relevant evidence produced from all the data gathered by a forensics examination ahd storing it in a database in a format such that it can be used as evidence in a trial.
- **Image Acquistion**
- **Write Blocker**
- **Hashing Utilities**
- **Imaging Utilites**

Lession 15: Secure Application Development

Impact of Vulnerability Types

- **Software Exploitation**
- **Zero-day Exploitation**
- **Input Handling**
    - **Overflow**
    - **Injection**
- **Overflow Vulnerabilities**
    - **Buffer Overflow**
        - **Stack Overflow**
        - **Heap Overflow**
        - **Array Index Overflow**
    - **Integer Overflow**
- **Race Condition:** Occur when the outcome from execution processes is directly dependent on the order and timing of certain events, and those events fail to executein the order and timing intended by the developer. A race condition vulnerability is typically found where multiple threads are attempting to write a variable or object at the same memory location.
- **Pointer Dereference**
- **Memory Leak**
- **DLL Injection:** Not a vulnerability but of the way the OS allows one process to attach to another.
- **Refactoring:** The code performs the same function by using different methods (control blocks, variable types, etc.).
- **Shim:** The code library that intercepts and redirects calls to enable legacy mode functionality
- **Application Exploits**
- **Arbitraty Code Execution/Remote Code Execution**
- **Privilege Escalation**
    - **Vertical Privilege Escalation:** a user or application can access functionality or data that should not be available to them
    - **Horizontal Privilege Escalation:** A user accesses functionality or data that is intended for another user
- **SQL Injection**
- **Directory Traversal**
- **Command Injection:** Run OS shell commands from the browser

- **Transitive Access**
- **XSS**
    - **Reflected XSS/Non-persistent XSS**
    - **Stored XSS/Persistent XSS**
    - **DOM-based XSS:** Modify the content and layout of a web page
- **Session Hijacking**
- **CSRF**
- **Confused Deputy Attack:** If the target site assumes that the browser is authenticated because there is a valid session cookie and doesn't complete any additional authorization process on the attacker's input, it will accept the input as genuine
- **LSOs (Locally Shared Objects):** Or Flash cookies. A site may be able to track a user’s browsing behavior through LSOs, causing a breach of privacy.
- **HTTP Header Manipulation**
    - **HTTP Response Splitting**
    - **CRLF Injection**
- **Man-in-the Browser:** Where the web browser is compromised by installing malicious plug-ins or scripts or intercepting API calls between the browser process and DLLs.
- **Clickjacking:** Where what the user sees and trusts as a web applicationwith some sort of login page or form contains a malicious layer or invisible iFrame thatallows an attacker to intercept or redirect user input

Secure Application Development

- **Software Development Lifecycle**
    - **Waterfall Mode**
        - **Requirements**
        - **Design**
        - **Implementation**
        - **Verification**
        - **Testing**
        - **Maintenance**
        - **Retirement**
    - **Agile Development**
        - **Concept**

        - **Inception**
        - **Iteration**
        - **Transition**
        - **Production**
        - **Retirement**
- **OWASP Software Security Assurance Process**
    - **Planning**
    - **Requirements**
    - **Design**
    - **Implementation**
    - **Testing**
    - **Deployment**
    - **Maintenance**
- **Secure Staging Deployment**
    - **Development**
    - **Test/Integration**
    - **Staging:** A mirror of the production environment but may use test or sample data and will have additional access controls so that it is only accessible to test users
    - **Production**
    - **Sandboxing:** Each development environment should be segmented from the others.
    - **Secure Baseline:** Each development environment should be built to the same specification, possibly using automated provisioning
    - **Integrity Measurement**
- **Provisioning:** The process of deploying an application to the target environment, such as enterprise desktops, mobile devices, or cloud infrastructure.
- **Deprovisioning:** The process of removing an application from packages or instances.
- **Version Control**
- **Change Management**
- **Continuous Integration:** The principle that developers should commit updates often
- **Canonicalization (规范化) Attack:** The server converts between the different methods by which a resource such as a file path or URL may be represented and submitted to the simplest method used by the server to process the input.
- **Fuzzing**
    - **Application UI**
    - **Protocol**

    - **File format**
- **Stored Procedure:** A part of a database that executes a custom query
- **Code Signing:** The principal means of proving the authenticity and integrity of code. The developer creates a cryptographic hash of the file then signs the hash using his or her private key.
- **Unreachable Code:** Can nerver be executed.
- **Dead Code:** Executed code but has no effect on the program flow.
- **Data Exposure**
- **Obfuscation/Camouflage:** Randomize the names of variables, constants, functions, and procedures, removes comments and white space, and performs other operations to make the compiled code physically and mentally difficult to read and follow. Or encrypt the code.

Lession 16: Organizational Security

Importance of Security Policies

- **Standrad:** A measure by which to evaluate compliance with the policy
- **Procedure:** A standard operating procedure, is an inflexible, step-by-step listing of the actions that must be completed for any given task
- **Guidance:** Exist for areas of policy where there are no procedures, either because the situation has not been fully assessed or because the decision making process is too complex and subject to variables to be able to capture it in aprocedure.
- **Interoperability Agreements**
    - **Memoradum of Understanding (MOU):** A preliminary or exploratory agreement to express an intent to work togethe
    - **Memorandum of Agreement (MOA):** A formal agreement that contains specific obligations rather than a broad understanding.
    - **Service Level Agreeement (SLA):** A contractual agreement setting out the detailed terms under which a service is provided
    - **Business Partners Agreement**
    - **Interconnection Security Agreement (ISA)**
    - **NDA**

Data Security and Privacy Practices

- **Data handling**
- **Document Management**
- **Data Policy:** Describe the security controls that will be applied to protect data at each stage of its lifecycle
- **Data Goverance Policy**
    - **Data owner**
    - **Data Steward:** Responsible for data quality
    - **Data Custodian**
    - **Pricacy Officer**
- **Data Sensitivity**
    - **Unclassfied**
    - **Classified**
    - **Confidential**
    - **Secret**

    - **Top-Secret**
- **Persionally Identifiable Information (PII)**
- **Protected Health Information (PHI)**
- **Intellectual Property (IP)**
- **Data Retention (保留)**
- **Media Sanitization/Remnant Removel**
    - **Overwriting/Disk Wiping:** Suitable for all but the most confidential data, but is **time consuming** and **requires special software**
    - **Low-Level Format:** Reset a disk to its factory condition.
    - **Pulverizing/Degaussing:** A magnetic disk can be mechanically shredded or degaussed in specialist machinery. **Costly** and will usually render the disk unusable.
    - **Destroy the Dish with a Drill or Hammer:** Not appropriate for the most highly confidential data.
    - **Disk Encryption**
- Optical media cannot be reformatted. Discs shoud be **destroyed** before discarding them. **Shredders** are available for destroying **CD** and **DVD** media.

Importance of Personel Management

- **Separation of Duties**
- **Job Rotation**
- **Mandatory Vacations**
- **Acceptable Use Policy:** Set out what someone is allowed to use a particular service or resource for
- **Clean Desk Policy:** Each employee's work area should be free from any documents left there.
- **Security Awareness Training**

Lession XX: Addition

Exams

- **Threats, Attacks and Vulnerabilities 21% (19 questions)**
- **Technologies and Tools 22% (20 questions)**
- **Architecture and Design 15% (13 or 14 questions)**
- **Identity and Access Management 16% (14 questions)**
- **Risk Management 14% (13 questions)**
- **Cryptography and PKI 12% (11 questions)**