Security+ 601 note:

Chapter 1:

I. *Understanding core security goals*:

Ensure Confidentiality: Confidentiality prevents the unauthorized disclosure of data.
Encryption: Scramble data to make it unreadable by unauthorized personel.

1. Access Controls:
   a) Identification: Identity with a unique username.
   b) Authentication: Prove their identity with authentication such as password.
   c) Authorization: Grant or restrict access to resources using an authorization method such as permission.

Note: Confidentiality: ensure data only viewed by authorized users.
The best way to protect the confidentiality is Encrypting.

Provide Integrity: provide assurance that data has not been changed, on one has modified. *You can use hashing to protect data integrity, hash algorithms created a fixed-length irreversible output*

Ex. A variation in the hashes doesn't tell you what modified the message, only tells you the message has been modified.

Increase Availability: availability indicates that data and service are available when needed.

Note: Implement redundancy and fault-tolerant can ensure high levels of availability for key system. Ex. RAID, failover clusters, backups, and generator.

1. Redundancy and Fault Tolerance: redundancy adds duplication to the critical system and provide fault tolerance. Ex. if the component fails, redundancy allows services to operate without interruption. *Redundancy and fault tolerance techniques are to remove single point of failure (SPOF)*
   a) Disk redundancies: RAID 1 (Mirroring), RAID-5 (striping with parity), RAID-10 (striping with mirror).
   b) Server redundancies: Failover clusters includes redundant server. Virtualization can increase the availability of servers by reducing unplan downtime.
   c) Network redundancies: Load balancing uses multiple servers to support a single service, high-volume website. NIC teaming provide both redundancy support and increase bandwidth.
   d) Power redundancies: UPSs and power generator.
2. Scalability and Elasticity: contribute to high availability. Allow system to scale up by adding additional hardware resources such as memory, processing power, bandwidth capability, drive space.
   a) Scalability: manually adding or removing resources to a system to scale it up or out.
   b) Elasticity: dynamically adding or removing resources to a system to scale it.
   c) Cloud resources typically have elasticity allowing them to adapt on demand.
3. Patching: patches help improve availability.

Understanding Resiliency: A resiliency is how long a system can heal themselves or recover from a fault with a minimal downtime.

II. Introducing Basic Risk Concepts:

1. Risk: possibility or likelihood of a threat exploit vulnerabilities resuting in loss.
2. Threat: any events that has potential to compromise CIA.
3. Vulnerability: a weakness.

Reducing threat knowing as threat mitigation.

III. Understanding Security Control:

Control Categories:

1) Managerial Control: primarily administrative function, security policy and focus on managing risk.
   a) Risk Assessment: quantify risk based on monetary value.
   b) Vulnerable Assessment: attempt to discover current vulnerability.
2) Operational Control: Ensure day-to-day operations in org comply with security policy.
   a) Awareness and training
   b) Configuration Management: use baselines to make sure systems start in a secure, harden state.
   c) Media protection: USB flash drives, external, internal drives, backup tapes.
   d) Physical and environmental protection: cameras, door locks, heating and ventilation systems.
3) Technical Control: hardware, software, firmware reduces vulnerabilities.
   a) Encryption
   b) Antivirus
   c) IDSs and IPSs
   d) Firewall
   e) Least privilege

Control Types:

1) Preventive Control: prevent incident form occurring.
   a) Hardening: practice of making system more secure than default confi
   b) Training: security awareness
   c) Security guards: prevent unauthorize access, secure buildings
   d) Change management: changes don’t result in unintended changes.
   e) Account disablement: ensure account is disable when employee leaves
   f) IPs
2) Detective Control: detect incidents after they have occurred.
   a) Log monitoring: record detail of activities on the system
   b) SIEM
   c) Security Audit: examine security posture
   d) Video Surveillance
   e) Motion detection
   f) IDS

3) Corrective Control: attempt to reverse the impact of incident.
    a) Backups and system recovery
    b) Incident Response: Incident handling process
4) Deterrent Control: discourage Individual from causing an incident
    a) Cable locks
    b) Physical locks: locked doors, wiring closet
5) Compensating Control: used when primary control is not feasible.
    a) Give a temp access (TOTP)
6) Physical Control: controls you can physically touch

IV. Command Line Tools

1) Ping: test connectivity for remote system. Ping sends ICMP echo request to remote system answer with echo reply packets.

    Ping -t 192.168.1.1 (Window)
    Ping -c 192.168.1.1 (Linux)

2) Hping: send pings using TCP, UDP and ICMP. (Linux)
3) Ipconfig /all or Ipconfig -a: list TCP/IP for each NIC, MAC address, DNS server, DHCP address.
4) Ipconfig /displaydns: shows DNS cache
5) Ipconfig /flushdns: erase content cache
6) Ifconfig eth0: show config of first NIC. (Linux)
7) Ifconfig eth0 promisc: enable promiscuous mode. It allows NIC to process all traffic it receives. *Normally, NIC is on non-promiscuous mode, will ignore all traffic not address to it. * Disable premicuous mode: Ifconfig eth0 -promisc (Linux)
8) Ifconfig eth0 allmulti: allows multicast on the NIC. *Putting NIC on promiscuous mode allow traffic analyzer to see all the packets* (Linux)
9) Ip link show: show the interface along with some details on them (Linux)
10) Ip link set eth0 up: enable a network interface (Linux)
11) Ip -s link: show statistics on the network interfaces (Linux)

Netstat:

1) Netstat: display a list of TCP connection
2) Netstat -a: display a list of TCP and UDP
3) Netstat -r: display routing tables
4) Netstat -e: display detail on network statistic.
5) Netstat -s: display statistic of packet received and sent for specific protocols. Ex. TCP, ICMP, UDP
6) Netstat -n: Display addresses and port numbers in numeric orders.
7) Netstat -p protocol: display specific protocol. Ex. Netstat -p TCP.
8) Netstat -anp tcp: display the state of connection, as Establish, to indicate an active connection.

Tracert (window) and Traceroute (Linux): Listing all routes between 2 systems.
Ex. tracert -d google.com (-d switch forces tracert to not resolve IP to hostname, allow the connection to finish quicker)

Pathping: combine function of ping and tracert.

Arp: is the command line related to address resolution protocol, not the same as ARP protocol. (Arp: resolve IP address to MAC address and store result in ARP cache)
Arp***:*** show the help on window
*Arp -*a: show ARP cache on window
Arp: show ARP cache on Linux
*Arp -*a 192.168.1.1: displays the ARP cache entry for the specified IP address
Cat Command: display content of files, easier way to view file content.

Ex. sudo cat /var/log/auth.log

Grep Command: search for a specific string or pattern of text within a file.

Ex. sudo grep "authentication failure" /var/log/auth.log

Head Command: display the beginning of a log file.

Ex. sudo head /var/log/syslog

Tail Command: display the last 10 lines of a log file by default.

Ex. sudo tail -n 15 /var/log/message (n-15: specify how many lines)

Logger Command: add entries in the /var/log/syslog file from terminal.

Ex. logger Backup Started

Journalctl Command: queries the Linux system logging utility and display log entries from several sources.

Journalctl –since"1 hour ago": view entry from previous boot.
Journalctl –list-boots (show error while booting)
Journalctl –since"1 hour ago"> myjournal.txt (send the command to an output as a text file name: myjournal.txt)

Chmod Command: used to modify permission on Linux.

a) R: can open file, and view content
b) W: modify content, combine with read
c) X: launch file, used with executable file.

Permission applies to 3 identities:

a) First set: permission applied to owner of the file
b) Second set: permission applied to owner of the group
c) Third set: permission applied to everyone

Ex. chmod 760 filename
Note: u. indicates file owner
g. indicates owner of group
o. indicates all others
Ex. chmod g=r filename (add Read permission to Group)
Ex. chmod o-x filename (remove Execute permission from others)

V. Understanding Logs

1. Window logs:

a) Security log: function as security log, audit log, access log. Record events success or fail.
b) System log: function of operating system, start, shutdown, driver loading, services stop or start.
c) Application log: record event sent to it by application running, warning, errors, routine message.

2. Network logs: record traffic on the network, routers, firewall, web servers, IDS, IPS.

VI. Centralized logging methods:

1. SIEM: real-time monitoring, analysis, noti of security events, suspected security incidents. Provide long term storage of data, creating reports, verify compliance.
    a) Log collector: log data from devices thru network and store in a searchable database.
    b) Data input: log entries from various sources, firewall, router, IDS, IPS, monitor web servers, proxy server, database servers
    c) Log aggregation: combining several dissimilar items into a single format.
    d) Correlation engine: software engine used to collect, analyze event log data from various system
    e) Report, packet capture, user behavior analytic, sentiment analysis, security monitoring, automated triggers, time synchronization, event duplication logs/ WORM (write once read memory)
3. Syslog: specifies a general log entries format and the detail of how to transport log entries. * You can deploy centralized syslog server to collect syslog entries from a variety of devices in the network, similar to SIEM*

Syslog-ng and Rsyslog: open source utility on Linux.

Syslog-ng: allow system to collect log from any sources, correlation, routing ability to log entry.

Rsyslog: came out later as an improvement.

NXlog: another log management tool. This support log format on window as well. Event log.

Linux Logs:

1. Var/log/syslog: store all sys activities, start-up activities.
2. Var/log/message: general system message, logged during startup, mail, kernel, auth
3. Var/log/boot.log: entried created when system boots.
4. Var/log/faillog: fail login attempts
5. /var/log/kern.log: log by system kernel
6. /var/log/httpd/ Apache web server, view access and error log

Chapter 2:

I. Exploring authentication Management

You can't have any types of access control without authentication

1. Comparing Identification and AAA

Authentication: proves identity such as credential, username, password.

Authorization: access resources based on proven identity.

Accounting: track user activity and record the activity in logs. (Audit log, audit trail)

Note: Access control provides authorization by granting access resources based on permission granted to the proven identity. (Logging provides accounting)

II. Comparing authentication Factors

Something you know: password or PIN

Something you have: smart card, phone, token

Something you are: fingerprint, biometric

1. ***Something you know***

   Something you know is the least secure factor because password stays the same for a long time, called static passwords or static codes.

   a) Password Complexity: more than 8 characters with upper case, lower case, numbers, special characters.
   b) Password expiration: expire every 60-90 days.
   c) Password Keys: are used to reset passwords on systems, commonly bootable optical disc or bootable flash drive.

   Knowledge-based Authentication: static KB and dynamic KBA

   a) Static KB: typically used to verify your identity when you've forgotten your password. (Security questions)
   b) Dynamic KB: identifies individuals without an account. Ex. give you few questions that you might know, and you can guess.

Implementing Account Lockout Policies

a) Account lockout threshold: max of time, users can enter wrong passwords.
b) Account lockout duration: how long can acc remain locked.

Note: *Account lockout policy: thwart password attacks, brute force, dictionary attack*

2. ***Something you have***

   Something you have: authenticator factor refers sth you can physically hold.

   a) Smart card: Embedded microchip and a certificate used with digital signatures and encryption.

      ➔ smart card provides CIA

      Requirement for smart card:

      1) Embedded certificate: certificate holds a user's private key and is matched with a public key. Private key is used each time when users log on to a network.
      2) Public Key Infrastructure (PKI): supports issuing and managing cert

Note: *smart card are used with dual-factor authentication*

b) Token Key: Key fob, number changes periodically every 60 seconds.

c) HOTP and TOPT:

   1) Hash-base Message Authentication Code (HMAC): use a hash function and cryptographic key.

      HMAC-based One-time Password: creating one-time passwords. Algorithms combines a secret key and an incrementing counter and uses HMAC to create a hash of the result.

   ➔ Then, it converts the result into HOTP value of 6-8 digits.

Note: *HOTP remains valid until its used*

   2) Time-base One-Time Password (TOTP): use timestamp. Typically, expire after 30 seconds, but adjustable.

d)Authentication Application: Google or Microsoft software,

e)Two-step Verification: Short Message Service (SMS) to send pins.

3. Something you are:

Biometric methods:

a). Fingerprint: fingerprint readers

b). Vein (vein matching): near-infrared light to view their veins. Prevent misidentification.

c). Retina (Retina Scanner): scan the retina of both eyes. Need physical contact with scanner.

d). Iris (Irish scanner): capture patterns of iris around the pupil. 3-10 inches away, avoid physical contact.

e). Facial (Facial recognition): identify people, glancing at the machine or phone.

f). Voice (Voice Recognition): speech recognition.

g). Gait analysis: identified individuals based on the way they walk.

Note: *Iris and retina scanner are the strongest biometric*

Biometric Efficacy Rates: refer to the performance of the system under ideal condition.

a. False acceptance: incorrectly identifies unknown users as a registered. (FAR, false match rate, identify percentage of time false acceptance)
   (Crossover error rate, CER, where FAR cross over with FRR)
   ➔ Lower CER indicates biometric is more accurate.
b. False rejection: incorrectly reject registered users.
c. True acceptance: correctly identified register users.
d. Correctly rejection: correctly rejected unknown users.

Two-factor and Multifactor Authentication:

Sth you have and sth you know = two-factor authentication.

Mutifactor = uses two or more authentication factors.

III. Authentication attributes: identify users or a device based on characteristics or traits.
   1. Somewhere you are authentication: identify a user's location
   2. Something you do: refers to actions you can take. Ex. MS picture password
   3. Something you exhibit: sth you can show or display. Ex. badge
   4. Someone you know: someone vouching for you. Ex. referral

IV. Authentication Log: track successful or unsuccessful login attempts.

V. Managing Account: Creating, management, disablement, termination.

VI. Credential Policy Type: credential policies define login policies for different personnel.
   1. Personnel or end-user account: regular users that working in the org.
   2. Administrator and root account: have privilege and additional right beyond normal users.
   3. Service account: services need to run under the context of an account. Ex. Acronis
   4. Device account: MS active directory only allow users to log on to computer join to the domain.
   5. Third-party account: account from external entities that have access to a network.
   6. Guest account: Window OS include guest account.
   7. Shared and generic account/credential: account that users share

Privilege Access Management: sometimes called Privilege account management.

Allows an org to apply more stringent security controls over account with elevated privilege.

→ Administrator don't have admin privilege until they need them. Their acc send request for elevated privilege.

→ PAM grants request, typically adding account to a group with elevated privilege. After 15mn, the account will expire. (User won't know password at all).

PAM capabilities: Help with privilege escalation.

-Allow users access privilege without knowing password
-Automatically change privilege
-Limit time user can use the privilege account
-Allow user to check out credential
-Log all access of credential

Prohibiting Shared and Generic Account

Four key concepts: Identification, Authentication, Authorization, Accounting.

Disablement Policies: disable is better than delete. If delete account, also delete any encryption keys and security associate with account.

1. Terminated employee
2. Leave of absence
3. Delete account

Time-Based Login: restriction prevent users from logging on or accessing network during specific time.

Account Audit: right permission assign to users helps enforce the least privilege.

VII. Comparing Authentication Services:

1. Single Sign-On: log on once and access multiple systems.
   →SSO secure token used during the entire session.

Note: *Keberos includes SSO capabilities in network*

2. Keberos: network authentication used within Window AD domain and some Unix environment known as realms.

Keberos includes several requirements to work properly:

- Method of issuing ticket used for authentication. Key Distribution Center (KDC) issues ticket-granting tickets (TGTs) and other tickets. KDC packages user credential within a ticket. Tickets are sometimes referred as logical tokens.
- Time Synchronization: Keberos V.5 requires all system to be synchronized within 5mn of each other. Synchronization is used to timestamp tickets. *Help prevent relay attack*
- A database of subjects or users: in MS environment, this is AD.

SSO and a Federation:

Some SSO system can connect authentication from different environment.

A federated identity links a user's credential from different networks or operating systems, but the federation treats it as one identity.

SAML:

Security Assertion Markup Language (SAML): Extensible Markup Language (XML)-based data format used for SSO on web browser.

- Service Provider: an entity that provide services principals to users. It hosts one or more websites accessible through a web-based portal. Ex. When Mary accesses a school system, the service provider queries the IdP (identity provider: create, maintain, manage identity info) to verify that Mary has valid credential before granting access

SAML and Authorization: primary purpose of SSO if for the identification and authentication of users. *SSO doesn't provide authorization*

OAuth: open standard for authorization. Similar to an API, provide secure access to protected resources. Ex. paypal inside the amazon website. You don't have to create another account to use it.

OpenID and OpenID Connection:

OpenID: authentication standard, maintained OpenID Foundation. Use: Jason format.

→ You use your google account to sign into another app so that you won't have to create an account again.

VIII. Comparing Access Control Schemes

Access control: ensure only authenticated and authorized users can access resources.

Subjects: refer to users, groups that access an object.

Objects: items such as files, folders, shares, and printers.

1) Role-based access control (Role-BAC): uses roles based on jobs & functions. (perform job function)
   - Administrator, Executive, Project Managers, Team Members
   - Matrix: a planning doc, matches the role with require privilege
   - Group-based privilege: admin put users in a group that he gives permission and right to.
2) Rule-based access control: use rules, based on a set of instruction, such as ACL.
3) Discretionary access control: Most OS uses DAC. Ex. NTFS, FAT32
   - Filesystem permission: write, read, read & execute, modify, full control.
   - SIDs and DACLs: MS identify users with Security Identifier.

   → DAC scheme specifies that every object has owner.
4) Mandatory access control: use labels and data to determine access. SELinux used MAC.
5) Attribute-Based access control: use attributes defined policies to grant access based on the value of these attributes. *Mostly used in SDNs (software defined network)

Chapter 3:

Basic ***Network protocols***: provides the rules needed for computer to communicate with each other on the network.

1. TCP: connection-oriented, guarantee delivery. Use 3 way-handshakes.
   →Client send SYN packet, Server responds with SYN/ACK packet, Client completed with ACK packet to establish the connection.
2. UDP: connectionless-oriented. ICMP traffic such as ping, audio, video streaming use UDP
3. IPv4: uses 32 bits addresses and IPv6 has 128 bits addresses.
4. ICMP: used for testing basic connectivity, includes tool such as ping, pathping and tracert.
5. ARP: resolves IPv4 address to MAC address.

Voice and video Use Case:

1. Real-time Transport Protocol (RTP): delievers audio and videos over IP network.
   1) Secure Real-time Transport Protocols (SRTP): provides encryption, message authentication, and integrity for RTP. (Protect against reply attack)
2. Session Initiation Protocol (SIP): used to initiate, maintain, and terminate voice, video and messaging session.
   → After SIP establishes, RTP or STRP transports audio or video.

Note: *SIP don't contain data, but contain metadata about session*

1) VoIP log contains: timestamps, caller phone #, recipient phone #, ext, and miscall.
2) SIP log contains: timestamp, sender IP address, recipient IP address, and capture SIP message.

(FTP uses SSH to encrypt the traffic and FTPS use TLS to encrypt the traffic-TLS replaced SSL)

Protocols used to transfer data over the network

1. FTP: upload and download large files to and from FTP server. By default, FTP transfers data in clear text.

- FTP passive mode known as (PASV) use TCP 21 for control signal and Random port for data)
- Trivial File Transfer Protocol (TFTP)uses UDP:69 to transfer small amount of data.
- Secure shell (SSH): Encrypt traffic in transit and can be encrypted by another protocol such as FTP. *Secure Copy (SCP) based on SSH, used to copy encrypted files over a network*.
- SSL: can encrypt SMTP, LDAP.
- Transport Layer Security (TLS): should be used instead of SSL for browser using HTTPS. *Many protocols support TLS uses STARTTLS. STARTTLS is a command used to upgrade an unencrypted traffic connection to encrypted connection on the same port.
- Internet Protocol Security (IPSec): Is used to encrypt IP traffic. Native to IPv6 but also work with IPv4. *IPSec included 2 main components: Authentication Header (AH) identified by protocol ID number 51 and Encapsulating Security Payload (ESP) identified by protocol ID number 50.
  ➔ IPSec uses Internet Key Exchange (IKE) over UDP:500 & create a security association for VPN.
- Secure File Transfer Protocol (SFTP): a secure version of FTP. It's an extension of SSH, using SSH to transmit files in an encrypted format. SFTP transmit data using TCP:22.
- File Transfer Protocol Secure (FTPS): is an extension of FTP, uses TLS to encrypt FTP traffic.

→ *FTPS uses TLS and SFTP uses SSH*

Email and WEB Use Cases

- Simple Mail Transfer Protocol (SMTP): transfer email between clients and SMTP servers. SMTP uses port 25 for unencrypted email and port 587 for email encrypted with TLS.
- Post Office Protocol V3 (POP3): transfer emails from servers down to clients. POP3: port 110 for unencrypted connection and TCP port 995 for encrypted connection.

- Internet Message Access Protocol V4 (IMAP4): used to store email on email server. IMAP4: use TCP:143 unencrypted connection, and TCP: 993 encrypted connections.

Directory Services and LDAPS

- Active Directory Domain Services (AD DS): a database of objects that provides central access point to manage users, computer and other directory objects.
- Lightweight Directory Access Protocol (LDAP): is a protocol, format and method used to query directories. LDAP use TCp:389 and LDAPS encrypted data with TLS uses TCP:636.
- OpenSSH: a suite of tools that simplify SSH to connect to remote servers secure. It supports the use of SCP and SFTP to transfer file securely.

→ Command: ssh gcga (initiates SSH connection to remote server using default SSH port 22)

→ Command: ssh root@gcga (remote server will prompt her to enter a password). You can use openssh to create a public and private key pair. Lika keeps private key on her system and copies public key to remote server.

→ ssh-keygen -t rsa (this will create a match pair of a public key and a private key similar to private/public key pair used with certificate. When Lika connects to remote server and it prompts her to authenticate with the private key).

a) Id_rsa.pub: is the public key, copied to remote server.
b) Id_rs.: is the private key, store on client and must stay private

→ Command: ssh-copy-id gcga: copy the public key to remote server.

Time Synchronization Use Case:

- Keberos requires all system to be sync within 5 mn of each other.
- Network Time Protocol (NTP): commonly used protocol for time synchronization

Network Address Allocation Use Case:

- Network Address Allocation: allocating IP addresses to host within your network.
- IPv4 uses 32-bit IP

DHCP Snooping:

- DHCP snooping is a preventive measure, main purpose to prevent unauthorized DHCP servers (often called rogue DHCP) you enable it on Layer 2 switch ports.

→ DHCP client and server send four packets back and forth:

- DHCP Discover: DHCP client broadcast a message asking DHCP server for a lease
- DHCP Offer: DHCP server answer, offering a lease.
- DHCP Request: DHCP Client responded by requesting the offered lease
- DHCP Acknowledge: DHCP allocates the offered IP to DHCP client and send back the acknowledge packet.

Note: *Normally switch sends all broadcast traffic it received to all ports. When DHCP snooping is enable, switch only send DHCP broadcast traffic to trusted port*

→ Prevent someone plug in their router to one of the ports in the wall, and broadcast DHCP to other ports.

Domain Name Resolution Use Case:

- DNS resolve hostnames to IP addresses, uses TCP:53 for zone transfer and UDP:53 for DNS client queries. *DNSSEC adds a Resource Record Signature (RRSIG)-refer as digital signature, provides data integrity and authentication and help prevent DNS poisoning attack*

Basic DNS query

a. A.: calls host record, holds hostname and IPv4 address, most commonly used in DNS server.
b. AAAA.: holds the hostname for IPv6 address.
c. PTR: calls a pointer record. Instead of DNS client queries DNS with name, the DNS client queries DNS with the IP address.
d. MX: mail exchange or mail exchange server. MX records identifies mail server used for email server. (MX record linked to A record and AAAA record of a mail server) Note: *the lowest number in MX record is the primary mail server*
e. CNAME: An alias allows single system to have multiple names associated with a single IP address. Ex. a server named Server1 in domain *certified.com* might have an alias of FileServer1 in the same domain.
f. SOA: state of authority, record includes info abut DNS zones and some its settings, EX. includes TTL settings for DNS records. DNS client uses TTL setting to determine how long to cache DNS result. *Lower time causes clients to renew records more often*

DNSSEC: (Domain Name System Security Extensions)

- DNS poisoning, known as DNS cache poisoning: when attackers modify DNS cache with a bogus IP address.
- DNSSEC is an extension to DNS that provides validation for DNS response.

Nslookup and dig

- Nslookup: used to verify that a DNS server can resolve specific hostnames or fully qualified domain names (FQDN) to IP addresses.
- Dig: Linux command line used to query DNS servers to verify that DNS server is reachable and verify that a DNS server can resolve hostname to IP address.

Ex. nslookup -querytype=mx google.com

Subscription Services Use Case: Instead of selling software to users, the vendor allows users to subscribe to their service.

Quality of Service

- QOS: technology running on a network, measure and control different traffic types. QOS allows Admin to set the priorities of any traffic.

Understanding Basic Network Devices:

- Unicast: One host send traffic to another IP destination, other port on the switch won't process it because it is not for them.
- Broadcast: one host send traffic to other hosts, using a broadcast address. *Switch pass broadcast traffic between their ports, routers do not pass broadcast traffic*

Note: *If Lia and Tom are exchanging data on port 1 and 4, none of the traffic reaches port 3. The protocol analyzer can't capture traffic that doesn't reach the port*

- Port Security including disabling unused ports, limiting the number of MAC addresses per port.

Broadcast Storm and Loop Prevent

- Network can develop a switching loop or bridge loop problem. This floods a network with traffic and can effectively disable a switch.
- Spanning Tree Protocol (STP) or newer Rapid STP (RSTP) installed. They provide both ***broadcast storm prevention and loop prevention*** switches.

Bridge Protocol Data Unit Guard

  - STP sends bridge protocol data unit (BPDU) message in a network to detect loops. STP shuts down or block traffic from switch ports sending redundant traffic.
  - Switch exchanges BPDU messages with each other using their non-edge ports.
  - Many switches support a BPDU Guard feature that is enable on edge port. It monitors the ports for any BPDU messages. If receives any, it disables the port, effectively blocking the BPDU attack.
  - Edge port is a switch port that connect to a computer, printer. These devices shouldn't degenerate BPDU message.

Router: connect multiple network segment into a single network and routes traffic between the segment.

Router and ACLs: rules implement on routers or firewall, identifies what traffic allow or deny.

- Rules within ACLs provides rule-based management for the router and control inbound and outbound traffic.
- ACLs provides basic packet filtering, filter packet based on IP addresses, ports, some protocols such as ICMP, IPSec, protocol identifier.

Implicit Deny: indicates all traffic that isn't explicitly allowed, implicitly denied. (Default deny, block by default)

- Firewall and router use implicit deny as the last rule in the access control list.

Route Command and Route Security

- Route command used to display or modify system's routing table on Window and Linux.
- Route Add -add a path to a different network. (Default gateway is the IP address on a network, typically provide a path to internet `
- Rout Print: see all path known by computer to other network.

Hosted-Based Firewall=Software firewall: monitor traffic in and out of a single host, and traffic passing through NIC. (Firewall on the window computer)

Network-Based Firewall: dedicated servers, provide protection for network, is a physical device.

Stateless Firewall: Use ACL to block & allow traffic.

- ACL in stateless firewall following element:
  - Permission: permit or allow the traffic
  - Protocol: TCP or UDP
  - Source: traffic from a source IP
  - Destination: traffic is addressed to a destination IP address.
  - Port or protocol: HTTPS or HTTP

Stateful Firewall: Block traffic based on the state of a packet within a session.

  - Keep track of an establish session. Ex. TCP 3-way handshake

NGFW: deep packet inspection, application-level inspection, allow content filtering and URL filtering.

Screen Subnet: (known as demilitarized zone or DMZ) a zone between private network and internet. Allow access to services while segmenting access to the internal network.

Network Address Translating Gateway:

NAT is a protocol that translate public IP addresses to private IP address and private addresses back to public.

- Commonly used form of NAT is network address and port translation, commonly called port translation.

Some NAT benefits:

- Public IP addresses don't need to be purchased for all client: multiple computers that can access the internet through one router running NAT.
- NAT hides internal computer from the internet: computers with private IP are isolated from the internet.

Design IPSec going through NAT, need to closely examine:

- Static NAT: static NAT uses a single public IP address, map private IP address with a single public IP address.
- Dynamic NAT: use multiple public IP address.

Airgap: isolate one network from another by ensuring there is physical space between all system and cables.

- Vlan: separate or segment network traffic on a physical network
- Router: separate regard physical location.

East-West Traffic: traffic refers to traffic between servers. (Horizontal)

North-South Traffic: refer to traffic between clients and servers. (Vertical)

Zero Trust: a security model, network that doesn't trust any devices by default even previously verified. (Reduce attack form compromised internal clients)

Network Appliance: dedicated system designed to fulfil a specific need.

Proxy Server (Forward proxy servers): forward requests for services (HTTPS or HTTP) from clients. Some proxy servers can restrict users access to inappropriate website by filtering content.

- Caching content: proxy server increase performance, requests by caching result received from the internet. *Cache can be a dedicate area of RAM, could have high-performance disk of system.

Transparent Proxy Vs Non-Transparent Proxy:

- Transparent proxy: accept and forward request without modifying them.
- Non-transparent proxy: server can modify or filter requests.
  - Employees uses bypass proxy, but detected and blocked, and log attempts.
- Reserve proxy: caches the webpages just as a forward proxy server.
  - Used for a single web server or web farm (multiple servers). When used as web farm, can acted as load balancer.

Unified Threat Management: single solution, combines multiple security controls.

- URL Filtering, Malware inspection, content inspection, DDoS mitigator.
  Many UTM includes DDoS mitigator to block DDoS attack

Common to place UTM between internet and intranet

Jump Server: (known as jump box): harden server, used access and manage devices in another network with a different security zone. *Access servers in the screen subnet thru jump server*

- Command used with elevated privilege on jump server and on a CA server DMZ (named ca1): `ssh -J lika@jump lika@ca1`

How this works: -J tells ssh connect to jump server, then use TCP forwarding to connect to CA server. *Possible to use jump server, connect internal network, SCADA network isolated with VLAN.

Chapter 4:

Advanced Security Devices:

- Intrusion Detection Systems (IDSs): monitor network and send alerts when they detect suspicious events. *Primary goal of IDS is to monitor traffic)
- Intrusion Prevention System (IPSs): react to attacks in progress, preventing from reaching systems and network.
- Host-Based Intrusion Detection System (HIDS): additional software, install on PC or servers. (This traffic passes through NIC) similar to anti-virus.
    - Can monitor application and protect local resources such as OS.
- Network-Based Intrusion Detection System (NIDS): monitor activities on network.
    - Has sensors or collectors on devices such as switches, routers, firewall.
    - Sensors gathers info and report to central monitoring network appliance hosting NIDS console.
    - NIDS unable to decrypt traffic, only monitor and assess threats on network from traffic sent in plaintext or non-encrypted traffic.
- Most switches support port mirroring: configure switch to send all traffic the switch receives to a single port. After configure port mirror, use it as a tap to send all switch data to a sensor and forward it to NIDS console.

Note: *possible to configure port tap on router to capture all traffic sent through router and send to IDS*

Detection Methods

2 primary detection methods: signature-based and heuristic- or behavioral-based (known as anomaly-based).

HIDS monitors the network traffic reaching NIC, whereas NIDS monitor network's traffic.

- Signature-based IDSs (known as definition-based): use a database of known vulnerabilities or known attack patterns. Detect known anomalies.
- Heuristic/Behavioral-based Detection (known as anomaly-based detection): identify the network's regular operation or normal behavior, does by creating a performance baseline. Detect unknown anomalies. (Thwart zero-day attack)

Note: *Heuristic-based detection is similar to heuristic-based anti-virus software works*

Note: *The SYN flood attack is a common denial-of-service (DoS) attack*

Data Sources and Trends

- IDS includes an aggregator to store log entries from dissimilar systems.

Reporting based on Rules

- IDS reports events of interest based on rule configured within IDS.
- Other systems use an alarm for a potential serious issue and an alert as a relatively minor issue
- False positive: IDS or IPS alarm when there is no actual attack.
- False negative: IDS or IPS fail to alarm when there is an attack.
- True negative: IDS or IPS does not alarm when there is no attack.
- True positive: IDS or IPS send alarms when there is an attack.

IPS Vs IDS-Inline Vs Passive

- IPS: detect, react, and prevent attack. It is inline with traffic; all traffic passes through IPS. IPS can block malicious traffic. (Inline refer as ACTIVE)
  - IPS can inspect packets within data streams and block malicious packets.
  - Can used to protect private network, it is a preventive control.
- IDS: monitor, will respond after detecting an attack, does not prevent attack. IDS is out-of-band. It monitors network traffic; traffic does not go through IDS. (IDS is PASSIVE).

Note: IDS might be able to modify access control lists (ACLs) on firewalls to block offending traffic, close process on a system, divert attack to a safe environment.

Note: IDS and IPS have protocol analyzer capabilities.

Honeypot: some goals of honeypots are:

- Deceive the attacker and divert them from the live network.
- Allow observation of an attacker

Honeynets:

Honeynet is a group of honeypots within a separate network or zone. Professional often create honeynets using multiple virtual servers contained within a single physical server.

Honeyfile: a file designed to attract the attention of an attacker.

Fake Telemetry:

- Telemetry: refer to collecting info such as statistical data and measurement and forwarding it into a centralize system for processing.
- Fake telemetry can corrupt the data sent to monitoring systems and can disrupt the system.

Band Selection and Channel Overlaps:

Wireless network uses 2 primary radios band: 2.4Ghz and 5GHz.

Wireless network is identified by Service Set Identifier (SSID)

- 802.11b and 802.11g -2.4GHz
- 802.11n -2.4GHz and 5GHz
- 802.11ac -5GHz

Note: *Channel 6 is very noisy, whereas channel 1 is less noisy.

Enabling MAC Filtering: in the context of port security for switches.

MAC has is 48-bit hexadecimal address used to identify NICs.

- Every NICs includes wireless NICs, has a MAC address.
- MAC Cloning: refer to process of changing MAC address on a PC, with the same MAC address as the wide area network (WAN) port on an internet-facing router. Help fix

connectivity issue. Cloning gets around by copying the MAC address of an approved piece of hardware to the problematic device.

<u>Site Surveys and Foot printing:</u>

- Site survey: examine the wireless environment to identify potential problem areas.
- Heat map: shows wireless coverage and dead spot if they exist.
- Wireless footprint: give you a detail diagram of wireless access point, hotspots, and dead spots within organization.

<u>Wireless Access Point Placement:</u>

- Omidirectional antennas: transmit and receive signals in all direction at the same time.
- Directional antennas: transmit in a single direction and receives signal back from the same direction.
  - Directional antennas has greater gain than omni antennas, and it can transmit and receive signals over greater distance.

<u>Wireless Cryptography Protocols</u>

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) were weak.

- Wi-Fi Protected Access 2 (WPA2): known as IEEE 802.11i use strong cryptographic protocols such as AES and Counter-mode/CBC-MAC Protocol (CCMP)
  - WPA2 can operate either with pre-shared Key (PSK) or Enterprise modes.
  - PSK access wireless network anomalously with a PSK passphrase: doesn't provide authentication (no username, only provide authorization)
  - Enterprise Mode: forces users to authenticate with unique credential. Enterprise mode use 802.11x server often implement with RADIUS servers.
    802.11x server can provide certificated-based authentication to increase security of authentication process
    Enterprise Mode needs 3 info:
    - RADIUS server: IP address assigned to 802.11x server
    - RADIUS Port: port used by RADIUS server
    - Shared Secret: shared secret is similar to a password.

<u>WPA3 and Simultaneous Authentication of Equals</u>

- WPA3 is the newest wireless cryptographic protocols, uses Simultaneous Authentication of Equals (SAE). SAE is a variant of Dragon Key Exchange.

<u>Authentication Protocols</u>

- Extensible Authentication Protocol (EAP): 2 systems create secure encryption keys, known as Pairwise Master Key (PKM). AES-based CCMP uses this key.
- Protected EAP (PEAP): extra protection layer for EAP. PEAP protects communication channel by encapsulating and encrypting the EAP in TLS. *PEAP requires certificate on the server, but not the client) → common implementation with MS Challenge Handshake Authentication Protocol V2 (MS-CHAPv2)
- EAP-TTLS: EAP-Tunneled TLS is an extension of PEAP. Allow to use with old authentication protocols like Password Authentication Protocols (PAP) within TLS tunnel. (Require certificate on server, but not on client)
- EAP-FAST: Cisco designed EAP-Flexible Authentication via Secure Tunneling as a secure replacement for LEAP. EAP-FAST supports certificate, but optional.

- EAP-TLS: one of the most secure EAP standard.
    - PEAP and EAP-TTLS: requires certificate on server, not client
    - EAP-TLS require on both servers and clients
- RADIUS Federation: possible to create a federation using 802.11x and RADIUS server.

802.11x Security

Another method of port security is using IEEE 802.11x, port-based authentication protocol. It requires users or devices to authenticate when they connect to a specific wireless access point or a specific physical port.

- WAP2-Enterprise Mode requires 802.11x server
- EAP-FAST supports certificate
- PEAP and EAP-TTLS require certificate on 802.11x server
- EAP-TLS also sues TLS, requires certificate on both servers and clients.
- 802.11x server provides port-based authentication, prevent rogue devices

Captive Portal : a technical solution, forces clients using web browser to complete a specific process before allowing them access to the network.

- Free internet access: require users to acknowledge and agree by accept use of policy (AUP)
- Paid Internet Access: must successfully log on with a pre-created account or enter credit card info to pay for access
- Alternative to IEEE 802.11X: requires users to authenticate before granting access

Understanding Wireless Attack

- Disassociation attack: removes wireless client from a wireless network, forcing it to reauthenticate.

→Wireless client authenticates with AP, the 2 exchange frames, a wireless device can send a disassociation frame to the AP to terminate the connection. (Frame includes client's MAC address)

Note: disassociation attack, attacker sends a disassociate frame to AP, with a spoof MAC address of the victim. Now the victim gets disconnect from the AP, must go thru authentication process again.

- Wi-Fi Protected Setup: allow user to configure wireless device by entering an 8 digits PIN. (WPS attack guesses all possible PINs until it finds the correct one)

Rogue Access Point: AP placed within a network without official authorization. An example of Shadow IT.

Evil Twin: Rogue AP with the same SSID as a legitimate AP.

Jamming Attack: attacker transmit noise or another radio signal on the same frequency used by a wireless network, to degrade service, type of DoS.

→ Prevent user from connecting to wireless network. Intermittent connectivity, reauthenticate.

IV Attack: Initialization vector is a number used by encryption system and a relies IV attack attempt to discover the pre-shared key after first discovering the IV.

Near Field Communication Attack:

- During the attack, an attacker uses an NFC reader to capture data from another NFC device.

One method is Ear Dropping attack. *NFC use antenna to boost its range and intercepts the data transfer between other devices*

- Sniffing or eavesdropping: known RFID system's frequency used by RFID syste, to interpret data.
- Replay: configure bogus tag to mimic the tag attached to a valuable object.
- DoS: attempt to disrupt service, launch jamming, flooding frequency, prevent RFID from operating normally.

Bluetooth Attack: short range wireless system used in personal area network (PANs).

- Bluejacking: sending unsolicited message to nearby Bluetooth device.
- Bluesnarfing: unauthorized access to Bluetooth device.
- Bluebugging: like bluesnarfing, but a step further. On top of gaining full access, attaker install backdoor.

Wireless Replay Attack: capture data sent between 2 entities, modifies it and attempt to impersonate of the parties by replaying the data. *WPA2 and WPA3 are resistant to this attack*

War Driving: practice of looking for a wireless network. Can detect rogue access points and identify unauthorized users.

War Flying: people fly around in private plane, intercept wireless transmission.

Note: A wireless audit checks a wireless signal footprint, power level, antenna placement, and encryption of wireless traffic.

Using VPN for Remote Access:

VPN is used for remote access. Direct access VPN allows users to access private network via a public network,

VPNs and VPN Appliance:

In window server, you can enable Direct Access VPN and configure Routing and Remote Access console. → but you need to have 2 NICs. One NIC is accessible from the internet and second NIC provides access to the private network.

- VPN appliance typically places in the screen subnet

Remote Access VPN

- VPN server needs to authenticate clients (common method is by using internal Remote Authentication Dial-in User Service-RADIUS server. When users log on, VPN servers sends the users' credential to RADIUS.

Note: RADIUS server can pass the credential to Lightweight Directory Access Protocol (LDAP) server during authentication process. In MS domain, the LDAP server is a domain controller.

IPsec as a Tunneling Protocol: encrypt traffic on IPv4. Encrypt data in transit. Support both Tunnel Mode and Transport Mode.

- Tunnel Mode: encrypt the entire IP packet, include payload and packet header (has IP address and MAC address) *VPN often use Tunnel Mode*
  - IP address uses within internal network is encrypted and not visible to anyone who intercept traffic. Attackers can only see source IP address from client, and destination address to the VPN server, internal IP remains hidden.
- Transport Mode: only encrypt payload and used in private network, but not with VPN.

IPsec provides security in 2 ways

- **Authentication**: IPsec includes an Authentication Header (AH), allowing each of IPsec conversation host to authenticate with each other before exchanging data. (AH) provides authentication and integrity, use protocol # 51.
- **Encryption**: IPsec includes Encapsulating Security Payload (ESP) to encrypt data.
  → IPsec, a secure encryption protocol used with VPNs, Encapsulating Security Payload (ESP), provides confidentiality, integrity and authentication for VPN traffic.
  → IPsec uses Tunneling Mode for VPN traffic, can be identifies with protocol ID 50 for (ESP).
  → Split tunnel only encrypts traffic destined for the VPN's private network

IPsec uses Internet Key Exchange (IKE) over port 500 to authenticate client. (IKE) creates Security Association (SAs) for VPN and uses these to setup a secure channel between client and VPN server.

SSL/TLS as a Tunneling Protocol:

Secure Socket Tunneling Protocol (SSTP) encrypts VPN traffic using TLS port 443.
OpenVPN and OpenConnect use TLS to create a secure channel.

Split Tunnel Vs Full Tunnel

- **Split Tunnel**: VPN admin determine what traffic use encrypted tunnel. Possible to configure tunnel to encrypt only the traffic going to private IP address.
- **Full Tunnel**: all traffic goes through encrypted channel while users is connected to VPN.

Site-to-Sit VPN

- *Site-to-Site* VPN includes 2 VPN servers that act as a gateway or 2 networks separated geographically.
- *Traditional remote access VPN (*known as host-to-gateway)

Always-On VPN

Always-on VPN can be used with both site-to-site VPN and direct access VPNs.

- Some site-to-site VPN uses an on-demand connection.
- Vendors have always-on VPN for direct access VPNs, they attempt to create a VPN connection as soon as the user's device connects to the internet.

L2TP as a Tunneling Protocol

- L2TP, tunneling protocol used for VPNs. Recent version is L2TP3.
- L2TP doesn't provide any encryption. *Data encryption such as IPsec, then passed to L2TP for transport over the VPN.

HTML5 VPN Portal

HTML5 allow users to connect to VPN using their web browser, making it rather simple for users. HTML5 uses TLS to encrypt session, very resources-intensive.

- Org uses to give one or two users access to limited resources.

Network Access Control: (NAC) used to inspect health of VPN client.
User log on to a VPN with malware-infected computer, this computer can then infect other computers on the internal network. (NAC) continuous security monitoring by inspecting computers and preventing them from accessing the network if they don't pass inspection.

Host Health Checks

(NAC) conditions checked by a NAC are:

- Client's firewall is enabled
- Client's operating system is up to date and has all current patches and fixes
- Client's anti-virus is up to date and has all updated signature defienition

When client connects to NAN-controlled network, the agent report NAC client's health status.

- NAC will detect unpatch system and quarantine it.
- Agent client can be either permanent or dissolvable.
- Agentless NAC scans a client remotely without installing code on the client.

Authentication and Authorization Methods

Authentication method that VPN use:

- Password Authentication Protocol (PAP): used with Point-to-point (PPP) to authenticate clients. Send passwords over a network in cleartext.
    - (PPP) primarily used with dial-up connection.
- Challenge Handshake Authentication Protocol (CHAP): uses PPP and authenticate remote users.
    - Goal of CHAP to allow client to pass credential over public network

RADIUS

Remote Authentication Dial-in User Service (RADIUS): a centralized authentication service.

- RADIUS can be used as an 802.11X server with WPA2 Enterprise Mode.
- Each VPN server has a separate database

TACACS+

- Terminal Access Controller Access-Control System Plus (TACACS+): alternative to RADIUS and provides 2 essential benefits over RAIDUS. First, it encrypts the entire authentication process where RADIUS only encrypts only the password by default. Second, TACACS+ uses multiple challenging.
- Cisco created TACACS+, can be interreacted with Keberos. Microsoft Active Directory uses Keberos authentication

Chapter 5:

Virtualization Concept: allow you to host one or more virtual systems or virtual machines on a single physical system.

- Hypervisor: software that creates, runs, and manage VMs.
- Host: Physical system hosting the VMs
- Guest: Operating systems running on the host system.
- Host Scalability: ability to resize the computing capacity of the VM. Admin manually change the resources assigned to the VM.
- Host Elasticity: ability to dynamically change resources assigned to the VM based on the load. Monitoring software sense the traffic and automatically changes.

Virtualization provides the best return on the investment (ROI)

- Thin Client: computer with enough resources to boot and connect to a server to run specific applications.
- Virtual Desktop Infrastructure (VDI): host a user's desktop operating system on a server. Ex. You remote into a server to use any OS. (Horizon Client)
- Container Virtualization: run services or application within isolated containers or applications cell. *Containers don't host entire OS*

Note: Because they are running in separate containers, none of the services or apps can interfere with services and apps.

=➔ Container must use the operating system of the host.

I. VM Escape Protection: is an attack that allow attackers to access the host system from within the virtual system.
   - Some situations, the attackers can run code on the code the virtual system and interact with hypervisor.

II. VM Sprawl Avoidance: organizations have many VMs that aren't properly managed. (Make sure all OS in all containers is up to date)

III. Replication: Virtual machine is simply files. Replicating VM by copying the files from one physical server to another.
   - Replication is easier to restore a failed virtual server, and cloud is slower.

IV. Snapshots: provides you with a copy of a VM at a moment in time, which can be used as backup. After taking a snapshot, the hypervisor keeps a record of all changes to the VMs. (If VM has a problem, you can revert the VM to the state it was in when you took the snapshot)

V. Virtual Desktop
   - Non-Persistence: Users have access to remote server, provide desktop OS from a preconfig snapshot for users. User makes changes to the desktop, will reverts to a known state (Original snapshot)
   - Persistent: User has a custom desktop image, can customize them and save their data within the desktop.

VI. Endpoint Security: End point detection and response (EDR) sometimes called endpoint threat detection and response (ETDR), provide continuous monitoring of endpoints.
   - EDR is a part of defense-in-depth strategy.

VII. Hardening Systems: practicing of making an OS or application more secure from its default installation.

1. *Secure Baseline and Integrity Measurement (Known as starting point)*
   - Initial baseline Config: Admin uses various tools to deploy systems consistently in a secure state
   - Integrity Measurement for baseline deviation: automated tools monitor the system for any baselines changes.
   - Remediation: NAC method can detect some changes to baseline settings and automatically isolate or quarantine systems in a remediation network.
2. Using Master Images for Baseline Config
   1. Admin starts with blank source, configure, put desire application, and modify security settings.

2. Admin captures the image, then becomes master image
3. Admin deploy the image to multiples

→ Imaging provides 2 important benefits:

- Secure Starting Point: image includes mandated security config for the system (Deployed image retains all the settings of the original image)
- Reduce Cost: Deployed imaged systems reduce overall maintenance costs & improves reliability.

Patch management: ensure that systems and applications stay up to date with current patches. It includes a group of methodologies and consists of identifying, downloading, testing, deploying, and verify patches

- Change Management: defines the process for any types of system modification or upgrades, including changes to application. Two key goals:
  - Ensure changes to IT systems do not result in unintended outages
  - Provide an accounting structure or method to document all changes

VIII. Application Programming Interfaces (API): software component that gives developers access to features or within another application, a service, or OS.

  - Developers uses APIs with web application, IOT, cloud-based services.

- APIs includes:
  - Authentication: prevent unauthorized entity from using APIs.
  - Authorization: secure access to the API. API could use cloud-based authorization services such as OAuth.
  - Transport Level Security: API should use strong security such as TLS when transferring any traffic.

XI. Microservices and APIs

- Microservices: code module designed to do one thing well (small code modules receives a value and respond with a value)
    - Amazon: where value is the tracking ID, output is the tracking data. Ex. Customer enters a tracking ID and microservices API would determine the shipper.
- Full Disk Encryption (FDE): encrypt entire disk.
- Self-encryption drives (SEDs): known as hardware-based FDE drives. SEDs includes encryption circuitry built into the drive.

Note: Opal-compliant SED: requires authentication by a user entering a username and password to unlock the drive upon bootup. SED automatically encrypted and decrypt data on a drive without user intervention.

- A measure boot: goes through enough of boot process to perform this check without allowing a user to interact with the system. If detect system lost integrity, system won't boot.
- Unified Extensible Firmware Interface (UEFI): can boot from larger disks, designed to be CPU-independent.
- Trusted Platform Module (TPM): hardware chip on the computer's motherboard that stores cryptographic keys used for encryption.

        - TPM provides full disk encryption capabilities, keep hard drives locked or sealed until the system complete a system verification and authentication process.
        - TPM ships with RSA with private key burned into it, uses asymmetric encryption and can be used to support authentication. (Private key matches with public key provides Hardware Root of Trust)
- Boot Attestation process: TPM configured, it captures signatures of key files used to boot, and store a report of the signatures securely within the TPM.
- Remote Attestation: process works like the secure boot. Instead of checking the boot files against the report stored in the TPM, and send this report to a remote system.

Example: when TPM is configured, it captures signature key files, send this report to remote systems. (Remote system verifies the files are the same and attest, or confirms, that the system is safe)

VII. **Hardware Security Module (HSM):** a removeable or external security device, can generate, store, manage RSA keys used in asymmetric encryption key.

- **MicroSD HSM:** can be installed into any devices that has microSD HSM slot.
- **HSMs:** supports the security methods of a TPM, provide a hardware root of trust, secure boot, and can be configured for remoted attestation.

○ **Data Loss Prevention (DLP):** techniques and technologies to prevent data loss, examine outgoing data and detect many types of unauthorized data transfers.

- Admin configures the DLP to look for specific words, phrases, or character strings. (DLP includes keywords, within an email, an attachment, outgoing data)

○ **Rights Management** (digital rights management) refer to technology used to provide copyright protection for copyrighted works.

- DLP solution prevent users from copying or printing files with specific content, (DLP logs these events)

○ **Data Exfiltration** (unauthorized transfer of data outside an organization)

- A networked-based DLP monitors outgoing data looking for sensitive data, specified by an administrator.
- Encryption: prevents loss of confidentiality.

VIII. **Summarizing Cloud Concepts**

- Cloud computing refers to accessing computer resources via a different location (accessing recourses through the internet or off-premises)

○ **Software as a Service** (SaaS): software or application provide provides to users over

- Web-based email: is a SaaS cloud computing service.
- Internet users access the SaaS application with a web browser

○ **Platform as a Service** (PaaS): provide customers with preconfigured computing platform, they can use as needed.

- Host provider provides several features, including an installed operating system, a core system package used for web server, Apache as a web server, antivirus software, spam protection.
- Host provider takes care of servers, patches, and keep up to date.

- **Infrastructure as a Service** (IaaS): allows an organization to outsources its equipment requirements, including the hardware and all support operation.
    - **IaaS:** provides owns the equipment, houses it in its data center and performs all the requirement hardware maintenance. Customers rents access to the equipment and often pays on a per-use basis.
    - Provide access to a server and may include default operating system installation, but customer configure and install additional software based on their need.
    - Customers takes care of patches, system updates.

- **Anything as a Service (XaaS)**: refers to cloud-based services other than SaaS, PaaS, or IaaS, XaaS includes service such as communications, database, desktops, storage, security.
    - XaaS includes a wide assortment of services that can be delivered via the cloud, such as communication, databases, desktop, storages, security, and more.
    - The cloud provider manages all the resources keeping everything operational and up to date
- **Cloud Deployment Models:**
    - Four categories of cloud deployment models:
        - **Public Clouds:** service is available from third-party companies, such as Amazon, Google, Microsoft. Provide similar services to anyone willing to pay for it.
        - **Private Clouds:** set up for specific organization. Choose to host your own servers, and make these servers available to internal employees through the internet.
        - **Communities:** share cloud resources within a **community cloud**. Ex. company shares resources, employee can use it.
        - **Hybrid Cloud:** a combination of 2 or more clouds. Can be private, public, community
- **Managed Security Service Provider (MSSP)**: 3rd party vendor provides security services for smaller companies. It includes:
    - Patch management
    - Vulnerability scanning
    - Spam and virus filtering
    - Data Loss Prevention (DLP)
    - Virtual private network connections
    - Proxy services for web content filtering
    - Intrusion detection and preventing system
    - Unifies threat management (UTM) appliances
    - Advanced firewalls such as next-generation firewalls (NGFWs)
- **Cloud Service Provider (CSP) Responsibilities:** CSP is an entity that offers one or more-cloud services via one or more cloud deployment models**.**
- **Cloud Security Controls:**

- High availability across the zone: system or service remains operational with almost zero downtime.
- Resources policies: CSP resource policies ensure customers don't create more resources than their plan allows.
- Secrets management: Secrets refer to Password and Encryption Keys
- Integration and auditing: CSP integrate security controls into the cloud-based resources, help customers identity the effectiveness of security controls.

Note: AWS stores data in buckets, whereas Google uses google drive. They both have the same characteristic below: Permission, Encryption, Replication.

→ CSP provides entire networks to organizations that need them. Common characteristics of cloud-based networks:

- Virtual networks: Instead of physical routers and switches. A single server can host an entire virtual network.
- Public and private subnets: Public subnets have public IP addresses and accessible via internet. Private subnets have IP address and aren't directly accessible via the internet.
    - Org typically use screened subnets for any public subnets that need to be accessible via the internet.
- Segmentation
- Security groups: admin assign permissions to a group and add users to the account.
- Dynamic resources allocation: cloud-based resources typically support elasticity.
- Instance Awareness: refers to the ability of CSP to know and report how many instances of cloud-based resources an organization is renting.
- Virtual private cloud (VPC) endpoint: VPC endpoint is a virtual device within a virtual network. Users or services can connect to the VPC endpoint and then access other resources via the virtual network instead of accessing the resources directly via the internet. This can significantly reduce the bandwidth required to access resources directly.
- Transit gateway: used to connect VPCs to an on-premises network.
- Container security: container virtualization runs services or applications within containers.

- **On-premises and off-premises**
    - On-premises: indicate that resources are owned, operated, maintained within organization's property.
        - Org retains complete control over all the cloud-based resources, includes any data stored in the on-premises cloud.
        - Org implement its own authentication, authorization controls. This makes it easier to use single sign-on (SSO) without requiring employee to have separate accounts for cloud-based resources.
    - Off-premises: CSP maintains hardware used to host the resources, CSP maintain more than just the hardware.
        - CSP perform the maintenance

    - Drawback: Org doesn't know where data is stored. (Legal implication, comply with different laws in different countries.

- **Cloud Access Security Broker (CASB):** a software tool or service deployed between organization's network and the cloud provider.
  ➔ provide security by monitoring traffic and enforcing security policies. CASB can be either on-premises or in the cloud. It redirects all traffic to the cloud-based CASB solution.
- **Cloud-Based DLP:** enforce security for data stored in the cloud, such as ensuring that personal identifiable information (PII) is encrypted.
- **Next-Generation Secure Web Gateway** (provide services for traffic from clients to internet site)**:** combination of proxy server and a stateless firewall. SWG typically is a cloud-based service, but can be on site-appliance. Clients are configured to access all internet resources via the SWG: Include:
  - URL filtering
  - Stateless packet filtering to detect and block malicious traffic
  - Malware detection and filtering to block malware
  - Network-based data loss protection (DLP)
  - Sandboxing

→ **Cloud-based Firewall:** operate on all seven layers (OSI model). This service charges based in bandwidth.

- **Infrastructure as code:** refers to managing and provisioning data centers with code to define VMs and virtual networks.
- **Software-Defined Networking**: SDN uses virtualization to route traffic instead of using hardware routers and switches.
  - Hardware router use ACL to identify whether a router will forward or block traffic on the data plane.
  - **SDN** implements the data plane with software and virtualization
  - Routing protocols: Open Shortest Path First **(OSPF)** and Border Gateway Protocols (**BGP**) helps routers determine the best path to route traffic on the control plane.

NOTE: OSPF and **BGP** can be used with SDN for best routing path.

→ Attribute-based access control **(ABAC)** commonly used in SDNs instead of rules within ACLs, ABAC allows admin to create data plan policies to route traffic.

- **Software-Defined Visibility (SDV):** refers to technology used to view all network traffic. Most Org used cloud resources; some network traffic may bypass security devices.
- **Edge and Fog Computing:** practice of storing and processing data close to the devices that generate and use the data, whereas non-edging solution store all data in the cloud, but it takes so much time to retrieve.
  - **Fog Computer:** uses a network close to device and may have multiple nodes sensing and processing data within the fog network, whereas **Edging Computer** stores and processes the data on single node appliance.

- **Cloud Security Alliance (CSA):** not-for-profit Org that promotes best practices related to the clouds. Certificate of Cloud Security Knowledge (CCSK) certification focus on cloud security.
- **Deployment Models:**
  - Cooperated-owned: Org buys devices and issue to employee
  - Corporate-owned, personally enabled **(COPE)**: Org buys devices, but employees can use it as their personal device.
  - Bring your own device (**BYOD**): Bring their own mobile devices to work, and access the network. However, must comply with BYOB policy.
  - Choose your own device **(CYOD)**: Org includes a list of devices that employees can purchase and connect to the network.
- **Connection Method and Receivers**
  - Cellular: ability to connect to a cellular network such as LTE, 3G, 4G.
  - WIFI: wireless network
  - Bluetooth: Bluetooth is a wireless protocol commonly used with personal area networks (PAN). Ex. smart phone
  - Near Field Communication (NFC): commonly used as a payment gateway.
  - Radio Frequency Identification (**RFID**): Systems transmit data over the air using **RF** signals and some RFC uses RFID technology.
  - Infrared: Most being used remote controls for TVs and other audiovisual equipment.
  - Point-to-point: point-to-point connection is between 2 wireless devices using technology such as NFC, RFID, Bluetooth.
  - Point-to-multipoint: a point-to-multipoint connection creates an ad hoc network.
- **Mobile Device Management** (**MDM**): tech that manage devices.
  - Some vendors sell Unified Endpoint Management (**UEM**) solution to manage mobile devices.
    - **UEM:** systems are kept up to date with patches, have antivirus software installed with up-to-date definitions, and are secured using standard security practices.
  - **MDM Concepts:**
    - Application management**:** MDM restrict what applications can run on mobile devices.
    - Full device encryption: Encryption protects against loss of confidentiality.
    - Storage Segmentation: Users would store corporate data within an encryption segment and personal data elsewhere on the device.
    - Content Management: can force the user to authenticate again when accessing data within encrypted segment.
    - Containerization: Org implement containerization in mobile devices and encryption the container to protect it without encrypting the entire device.
    - Password and PINs: password policy
    - Biometrics and Screen locks

        - Remote wipe: capabilities to remote wipe when phones are lost. This will send signal to a lost or stolen device to erase all data.
        - Geolocation: uses Global Positioning System (GPS) and can help location a lost or stolen device.
        - Geofencing: creates a virtual fence or geographic boundary and can be used to detect when a device is within an org's property's property.
        - GPS tagging: add geographical data to file such as pictures.
        - Context-aware authenticate: use multiple elements to authenticate a user and a mobile device, includes: user's identity, geolocation, verification that the device's within a geofence.

          → These elements help prevent unauthorized users from accessing apps or data.
- **Unauthorization Software:**
    - **Jailbreaking:** removing all software restriction from an Apple device. Users can install software from third-party source.
    - **Root:** process of modifying an Andriod device to give the user root-level.
    - **Updates** to the operation system overwrite the firmware using **Over-the-air** (**OTA**) updates techniques.
        - **Firmware OTA** updates keep the device up to date.
        - **Custom OTA:** is another way root an Andriod device.
- **Sideloading:** process of installing software on an Andriod device from a source other than authorized store. (**Sideloading** is useful for developers testing apps)
- **Rich Communication Services (RCS):** a newer communication protocols designed to replace SMS. RCS is similar to MMS, and can transmit multimedia. Will send RCS message, but if network won't support RCS, will default to MMS and SMS.
- **Tethering:** allow you to share one devices' internet connection with other devices.
    - **MDM** tools can block access to devices using tethering, mobile hotspot, or Wi-Fi Direct to access to the internet.
- **A subscriber identification module** (SIM) card identifies what countries and/or networks the phone will use.
- **SEAndriod** (Enforce Security Andriod)
    - Security-enhance Andriod (**SEAndriod**): security model uses Security-Enhance Linux (SELinux) to enforce access security.

    → When enable, SELinux supports 2 modes:
        - Enforcing mode: activities that is denied by policy is blocked and logged
        - Permission mode: this mode does not enforce the SELinux, but log all activities.
- **Exploring Embedded Systems:** device has a dedicated function and use a computer system to perform that function.
- **Field Programmable gate array** (**FPGA**): is a programmable integrated circuit (**IC**) installed on a circuit board. When turned on, transfers a configuration program from a configuration memory chip or an external process.

- **Arduino:** microcontroller board. Arduino does not need an operating system to run but instead uses firmware.
- **Raspberry Pi:** microprocessor-based mini-computer

→ Industrial Control System (ICS): a broad term encompassing supervisory control and data acquisition (SCADA) system, programmable logic control (PLC) systems.

- **ICS and SCADA Systems:**
  - **ICS**: typically refer to systems within large facilities such as power plants or waster treatment facilities.
  - Supervisory Control and Data Acquisition (**SCADA**): controls an ICS by monitoring it and sending it command.

  Common uses of ICS and SCADA systems include:
  - **Manufacturing and Industrial**: Include any plants used to manufacturing. The systems can monitor every processing stage and report anomalies. It also can send some signals to adjust processes based on changes in the environment.
  - **Facilities:** monitoring the temperature and humidity and keeping the environment relatively stable.
  - **Energy:** include oil and gas processing, power generation, and more.
  - **Logistics:** monitoring process within shipping facilities.

Note: SCADA system has embedded systems that control an industrial control system (**ICS**).

  - **Wearables:** any devices you can wear or have implanted.
  - **System on a chip (SoC):** integrated circuit that includes all the functionality of a computing system within the hardware. Typically includes an application contained within onboard memory, such as read-on memory (**ROM**).
  - **Real-time Operating System:** OS that reacts to input within a specific time.
- **Embedded System Constraints:** has several constraints that can limit their use: Below:
  - **Compute:** ability of embedded systems, typically limit compared to full computing system.
  - **Crypto:** Limited processing power, embedded systems can't use all cryptographic protocols.
  - **Power**: embedded devices don't have power supplies.
  - **Range**: with limited power, these devices can have limited range.
  - **Authentication**. Skip authentication due to extra equipment.
  - **Network**: without an interface, the device must accept the default.
  - **Cost**: cost of device can minimize the security.
  - **Inability to patch**: not include method to patch.
  - **Implied Trust and Weak default.**
- **Communication Considerations:** when choosing communication method for embedded systems and IoT devices, there are lot of choices:
  - **5G:** higher than 4G, data transfer much quickrt.
  - **Narrow-band:** narrow-band signals have a very narrow frequency range. Commonly used in two-way radio systems, such as walkie talkies.
  - **Baseband radio:** Baseband radio signals include frequency very near zero. Typically used when transferring data over a cable rather than over the air.

- **Subscribe Identity Module (SIM): has unique serial number.**
- **Zigbee:** a suite of communication protocols used for smaller networks, such as within a home for home automation. Ex. light bulb, switch

Take a way:

1. **VM Escape:** allow attacker to access the host system from the VM**.**
2. **VM Crawl:** occur if personnel within the organization don't manage the VMs.
3. Self-encryption drive (**SED**): has the encryption circuitry built into drive.
4. **TPM:** full disk encryption
5. Hardware Security Module **(HSM):** removeable or external device used for encryption**.** HSM generates and stores RSA encryption keys, and can be integrated with servers to provide hardware-based encryption.
    - MicroSD HSM is a microSD chip with HSM device installed on it.
6. **Data Exfiltration**: unauthorize transfer of data outside an organization.
7. **SaaS**: web-based application such as web-based mail
8. **PaaS**: provide easy-to-configure OS. Vendor keeps system up to date.
9. **IaaS**: provide hardware resources via the cloud.
10. **XaaS**: any other services delivered via cloud.
11. **Cloud Access Security Broker (CASB)**: monitor all traffic and can enforce security policies.
12. **Private Clouds:** only available to personnel within the org.
13. **Third-party venders** sell access to public clouds service to anyone who want them.
14. Two or more Org that share concerns can share community cloud.
15. Cloud-based DLP: can enforce security policies for any data in clouds.
16. Next-generation Secure Gateway: provide proxy services for traffic from clients to internet sites. Filter URL and scan for malware.
17. Edge and Fog computing technologies: move the storing and processing of data closer to the devices.
18. Virtual Desktop Infrastructure (VDI): a virtual desktop, can be created to that user can access them from a mobile device.
19. A remote wipe: removes all the data from a lost phone.
20. Geolocation and Global Position System (GPS): identify a device's location.
21. Geotagging: use GPS to add geographical information to files.
22. Jailbreak: remove all software restriction on Apple devices, and rooting provide users with root-level access to and Andriod device.
23. Custom Firmware: also root an Andriod device. MDM block network access for jailbreaking or rooted devices.

Chapter 6:

What to know about the attack: their attribute, type of attacks.

I. **Understanding threat actors**
    - Advance Persistent Threat (APT): a group of Org threat actors that engage in targeted attacks against Org. APT normally sponsors by nation-states. Typically,

these state actors have specific targets. Primary goal is Money. APT from countries:

    - China: PLA Unit 61398, Buckeye, and Double Dragon
    - Iran: Elfin Team, Helix Kitten, and Charming Kitten
    - North Korea: Ricochet Chollima and Lazarus Group
    - Russia: Fancy Bear, Cozy Bear, Voodoo Bear, and Venomous Bear

- **Criminal Syndicates:** composed of a group of individuals working together in criminal activities. Typically, organized within a hierarchy composed of a leader and workers.
- **Ryuk:** well-known ransomware that targeted enterprise environment.
- **Script Kiddie:** very little expertise, very little funding.
- **Hacktivist:** launches attacks, part of activist movement.
- **Black hat:** unauthorized hackers.
- **White hat:** authorized hackers, identified as professional working with firms to protect Orgs.
- **Gray hat** (known- semi-authorized hacker) identifies individuals who may have good intentions, but their activities may cross ethical lines.
- **Insider Threat:** can be admin has so many accesses and if someone hacks his acc, this will be bad or can be some uneducated users open malicious emails.
- **Attack Vectors:** can be through emails, or though social media.
- **Shadow IT:** refers to unauthorized systems within an Org. *Can use white list application to prevent this from happening*

II. Determine Malware Type

- **Malware:** wide range of software that has malicious intent**.**
- **Virus**: attaches itself to a host application. The host application must be executed. Typically, the payload of a virus is damaging. It may delete files, cause random reboots, join the computer to a botnet or enable backdoor.
- **Worm:** self-replicating malware that travels throughout a network without the assistance of a host application or user interaction.
- **Logic Bomb**: strings of code embedded into an application of script that will execute in response to an event (a specific arrives)
- **Backdoor**: provides another way of accessing the system.
- **Trojan**: can come as pirated software. Attackers often used drive-by download to deliver trojans.
    - Attacker installs a trojan embedded in the website's code
    - Attackers have used is rogue, also known as **Scareware.**

- **Remote Access Trojan (RAT)**: type of malware, allows attackers to control system remotely. Typically, delivered via drive-by download or malicious attachments in email.
    - Attackers deliver trojans as Portable Execution (**PE**) files in or 32- or 64-bits formats. Sometimes as compressed file such as tar. Ex. tar.gz file extension
    - Some RATs auto collects and log keystrokes, username and passwords, incoming and outgoing email, chat sessions and browser history as well as take screenshot.

      →Then, auto send back the data to attackers.

- **Keyloggers**: attempt to capture a user's keystrokes, can be thwarted by using 2FA.
- **Spyware**: monitor user's computer and activities.
- **Privacy-invasive** software tried to separate users from their money using data-harvesting techniques.
- **Rootkit:** have system-level or kernel access, modify the internal OS process, often modify system files such as registry, modify system access, such as removing user's admin access.
  - Use hooked processes or hooking techniques. Hooking refers to intercepting system-level function calls.
  - Tools that inspect RAM can discover these hidden hooked processes
- **Bots and Botnets**: **Bots** are software robots. Ex. Google uses as search engine spiders to crawl through the internet looking for webpage. **Botnets** combines the words robots and network. (The infected computers check in the **command-and-control systems, receive commands**)
- **Command and Control**: resources to control infected computers.
- **Internet Relay Chat** (**IRC**): network was often used in early botnets. Infected computers were given internet location (such as servers, website), using an IRC channel.
- **Bot herder:** often use cryptography to access the botnet and insert command.

III. **Ransomware and Cryptomalware**

- Specific type of trojans is ransomware and cryptomalware.
  - Ransomware is a type of malware that takes controls of use's system or data.
  - Cryptomalware attackers encrypt the data on computers within network to prevent access.
  - Most all ransomware use cryptomalware technique Criminals often deliver ransomware via drive-by downloads or embedded in others software deliver via email.
- **Potentially Unwanted Programs** (**PUP**): Spyware, adware, junkware, crapware can be PUP. Many PUP can be a browser hijackers, they change user's browser setting without consent.
- **Fileless Virus:** runs in memory instead of from a file on disk. They are often scripts that are injected into legitimate programs. Some techniques used by fileless malware are:
  - Memory code injection: malware injects code into legitimate applications
  - Script-based techniques: used encrypted code that is only decrypted when run
  - Windows Registry manipulation: uses a Windows process to write and execute code into Registry
  - Vcard: a file format used for electronic business cards

IV. **Potential Indicators of a Malware Attack:** Some generic indicators are of malware:

- Extra traffic: extra traffic to a network. Abnormal traffic can be compared to a baseline known traffic
- Data Exfiltration: refers to unauthorized transfer of data out of a network. DLP would help in this case.
- Encrypted traffic: Some malware will encrypt the data before data exfiltration attempt. Can bypass DLP technique because DLP can't read the encrypted data.

- Traffic to specific IPs: Monitoring firewall logs for all traffic attempting to access these blacklisted IPs are a strong indicator infection.
- Outgoing Spam: desktop computers don't normally send image amounts of emails. Often been added to a botnet and are sending phishing emails.

V. Attacks

- Shoulder Surfing: looking over the shoulder of someone to gain information.
- Tailgating: one person following closely begin another. Mantraps can mitigate this attack.
- Dumpster Diving: searching through trash.
- Zero-day vulnerability: vulnerability or bug that is unknown to trusted sources.
- Watering Hole attacks: infected trusted website, waiting for people to visit with malware.
    - Often infected websites with zero-day. APT uses this method of infiltrating high-profile targets.
- **Typo Squatting** (misspell URL): buys a domain name that is close to a legitimate domain name. Reasons why attacker might buy similar domains:
    - Hosting a malicious website: install drive-by malware
    - Earning ad venture: pay-per-click ads (click bait)
    - Reselling the domain: buy domain names relatively cheap but resell them
- Elicitation Information: the act of getting information without asking for it directly. They start by gaining trust and will use social engineering as below:
    - Active listening: an attacker gives his full attention to a target; the target is encouraged to keep talking.
    - Reflective questioning:
    - False statement
    - Bracketing
- Identity Theft and Identity Fraud: Identity theft, when someone steals personal information.
- Gaslighting: manipulation to get individuals to question their sanity.
- Credential Harvesting: use techniques to collect username and password
- Reconnaissance: refer to gathering as much information as possible.
- Influence campaigns: variety of sources to influence public perception.
- Hybrid warfare military strategy that blends conventional warfare with unconventional methods.
- Spam: unwanted or unsolicited email, whereas Phishing is malicious spam.
- Spam over instant messaging (SPIM): unwanted messages sent over instant messaging (IM). SPIM can bypass typical antivirus and spam.
- Phishing: sending emails to users, tricking, revealing personal information or clicking on a link.

VI. Phishing to Validate Email Addresses

- Method used to validate email address is the use of beacons.

        - Beacon is a link includes in the email that links to an image stored on an internet server. The link includes a unique code that identifies the receiver's email address.

- **Spear Fishing:** a targeted form of phishing, specific group of users. One solution that deters the success of these types of spear fishing attack is to use "digital signatures" **(**provide assurances to receipts about who sent an email**)**
- **Whaling:** A form of spear phishing that attempts to target high-level executives.
- Windows Management Instrumentation **(WMI) and Power shell** are frequently used to scan the network.

VII. **Blocking Malware and other Attacks**

    - Security controls against malware**:**
        - Spam filter on mail gateway
        - Anti-malware software on mail gateway
        - All system: have anti-malware software installed
        - Boundaries on firewall: UTM, inspect network traffic

- **Spam Filter**: UTM detect or block spam. Then, the output of the UTM goes to an email server. Email servers have a method of detecting and blocking spam. After that, email server sends all email to users. Users' system also has anti-spam filters, junk mail, as a final check.
- **Antivirus software:** detect viruses using either signature-based detection or heuristic-based detection.
    - **Signature files** (also called data definition files)**:** define the patterns, and antivirus software scans files for the matching patterns.
    - **Heuristic-based detection:** attempts to detect viruses that were previously unknown and do not have signatures.
        - **Heuristic-based analysis:** run questionable code in sandbox or virtualized environment.
- **Polymorphic malware:** adds variations to files when it creates copies.
- **Cuckoo Sandbox:** open-source automated software analysis system. Primary purpose is to analyze suspicious files, such as suspected malware. Unlike malware that analyze files in real time, you need to submit files to Cuckoo Sandbox. Cuckoo then runs it in virtual machine (VM) and creates a report on its activity.

VIII. **Why Social Engineering Works**

    - **Authority:**
        - Impersonation: impersonate others to get people to do sth
        - Whaling: Executive respect authorities. Ex. legal entity
        - Vishing: use the phone to impersonate authority figure
    - **Intimidation**: intimidate victims into acting
    - **Consensus**: people, often more willing to like something that people like.
    - **Scarcity**: scare someone by stating about limited quantity of an item.
    - **Urgency**: sense of urgency
    - **Trust**: pretend to help you first

IX. Threat Intelligence Source (OSINT): use OSINT method to gather information on target.

Common types of OSINT are:

- **Vulnerability database**: document known Vulnerability and many public databases help automate vulnerability management. Ex. NVD (National Vulnerability Database) and CVE (common vulnerability and Exposure)
- **Trusted Automate eXchange of Indicator Information** (TAXII): open standard, provide a standard way for organizations to exchange cyber threat information.
- **Automated Indication Sharing (AIS):** AIS uses both TAXII and STIX.
- **Dark Web:** can't find dark web on web browser
- **Public/private information sharing center:** public and private Org are also involved in sharing information on cyber threat.
- **Indicators of compromise (IoC):** evidence that a cyberattack is happening or has happened. Obvious IoC are confirmed alerts from antivirus software or other devices that have detect malware or other potential attack.
- **Predictive analysis**: technique attempt to predict what attack will do next and how to thwart their attack.
- **Threat Map**: provide a visual representation of active threats.
- **File/Code repositories**: Many repositories include prewritten code that developers can use for a variety of purposes.

Chapter 7: Protecting Against Advanced Attacks

I. **Understanding Attack Frameworks:** Cybersecurity uses several attack frameworks to identify tactics, techniques, and procedure (TTPs). Goals: understand how attackers operate to decrease the impact of future attacks.

○ Cyber kill chain: Military use this concept. Start with the identification of a target, dispatching resources to the target, deciding to attack and giving the order and ends with the destruction of the target.

1) Reconnaissance: researching, identifying, and selecting target
2) Weaponization: Malware such as remote access trojan (RAT), embedded within deliverable payload.
3) Delivery: The payload is transmitted to the target.
4) Exploitation: activates and triggers the exploits.
5) Installation: exploit, often install a remote access trojan or a backdoor on the attacked system. This allows attackers to maintain persistence in the environment.
6) Command and Control (C2): infected systems often send out a beacon to an internet-based server, giving attackers full access to the infected system.
7) Action on Objectives: attackers can begin taking action to achieve their ultimate goals. Install ransomware to collecting, encrypting and extracting data.

II. **Diamond Model of Intrusion Analysis:** 4 keys components of every intrusion event**:**

- Adversary: can be identified by email addresses, handled used in online forums memberships in APT groups and other identifiers.

    - Capabilities: refer to malware exploits, and hacker tools used in intrusion.
    - Infrastructure: refers to the internet domain names, email addresses, and IP address used by the advisory.
    - Victim: can be identified by their names, email addresses, or network identified.
- **MITRE ATT&CK** (Adversarial Tactics, Techniques, and Common Knowledge): is complementary to Lockheed's cyber kill chain. It is a matrix of tactics and techniques used by attackers at different stages of an attack. Tactics in matrix are: initial access, execution, persistence, privilege escalation, defense invasion, credential access, discovery, lateral movement, collection and exfiltration, and command and control.
    - MITRE ATT&CK also maintain the common vulnerability and exposure (CVE) and common weakness Enumeration (CWE) project.
    - The CVE has become the standard for naming vulnerabilities and exposure and it used by Security Content Automation Protocol (SCAP). CWE project identifies software weaknesses and vulnerabilities.
- **Identify Network Attack**
    - Denial of Service (DoS): an attack from one attacker against one target.
    - Distributed Denial of Service (DDoS): an attack from 2 or more computers against a single target.

  → Goal of both attacks is to resource exhaustion which overload the system's resources, prevents legitimate users from accessing services on the target computer.
    - Indicator of a network-based DDoS:
        - sustained, abnormally high amount of network traffic on NIC of the attacked computer.
        - Abnormally high usage of system resources such as the processor or memory. Ex. overload server with login attempts as it tries to verify the credential of each login attempt.
    - **SYN Flood Attack**: common DDoS attack, used against servers. This attack disrupts TCP handshake process and prevent legit clients from connecting.

Note: Linux systems support an iptables command that can set a threshold for SYN packet.

- **On-Path Attack** (sometimes referred as MITM): form of active interception or active ear dropping.
- **Man-in-the-browser attack:** type of proxy trojan horse that infects vulnerable web browser. Success attack can capture browser session data.
- **Secure Sockets Layer Stripping (SSL Stripping) attack:** changes HTTPS connection to HTTP connection. HTTPS uses TLS instead of SSL.

Note: HTTPS sessions are encrypted, but the session is not encrypted until TLS set up the session. If an attacker can intercept the beginning of the TLS negotiation, the attacker can redirect the user to an HTTP page instead of an HTTPS page.

III. **Layer 2 Attacks:**

- **ARP Spoofing**: attack that mislead computers or switches about the actual MAC address.
    - **ARP**: resolves IP addresses of a system to their hardware address and stores the result in ARP cache. ARP uses 2 primary messages:

    - **ARP Request:** broadcasts the IP addresses in the ARP request responds with its MAC address.
    - **ARP Reply:** computer with IP address in the ARP request responds with its MAC address.
  - **ARP DoS Attack:** Where attackers send an ARP reply with a bogus MAC Address for the default gateway. If all the computers cache a bogus MAC address for the default gateway, none of them can reach it, and stops all traffics out of network.
  - **MAC Flooding:** attack against a switch that attempt to overload it with different MAC addresses.
    - Once the switch runs out of memory to store all the AMC addresses and enters a "fail-open state".
    - Instead of working a switch as a switch, it begins operating as a simple hub. Traffic sent to any ports of the switch is now sent to all other switch ports.
    - Flood Guard to protect against MAC flood attacks. You can limit memory on switch used to store MAC address. Ex. You can limit the entry to the ports. If switch detects an attempt to store more than 132 entries, it raise alerts.
    - "Flood Guard" sends SNMP trap or message in response to the alert. It can either disable the port or restrict updates. By disable it, the port will block all traffic whereas restricting update means switch will use currently logged entries for the ports but ignore attempts to update it all. All other ports will continue to operate normally.
- MAC Cloning: Changing a system's MAC address to another MAC address. If you use MAC cloning and set the new router's MAC address to be the same as the old router, the ISP will recognize it and give it an IP address.

IV. **DNS Attacks**: DNS resolves hostnames to IP addresses. Reverse lookups (Client sends IP address to a DNS server with a request to resolve it to a name).

- **DNS Poisoning Attack**: attempt to modify or corrupt DNS data.
- **Pharming:** attack on DNS, and it manipulate the DNS name resolution process.
    - **Ex. Pharming** attack on client computer have modified the hosts file used on Windows systems. This file is in C:\Windows\System\drivers\etc\host. You can map a different IP to Google.

Note: Primary indicator of both attacks is that a user tries to go to one website but is taken to a different website.

→ Domain Name System Security Extensions (DNSSEC) to protect the DNS records and prevent DNS poisoning attack.

- **URL Redirection:** redirect traffic to a different page within a site.
- **Domain Hijacking**: attackers change domain name registration without permission form the owner.
- **Domain Reputation**: Domain reputation helps ISPs determine the likelihood that an email is being sent by a legitimate Org**.**
- **DNS Sinkhole:** DNS server that gives incorrect results for one or more domain names.

        - If the DNS server has a sinkhole for the domain name, you won’t be able to reach the site.
        - Ex. Investigator authorities have used sinkhole to disrupt botnets and malware.
- **DNS Log Files**: DNS log files records DNS query such as each request to resolve a hostname to an IP address. These log entries would include the system that sent the request and the IP address returned for the hostname.
- **Replay Attacks and Session Replays**: A replay attack once attacker replays data that was already part of a communication session. The attacker first capture data sent over a network between 2 systems. Then, modified the data and then tries to impersonate one of the clients in the original session and send the modifies data in session replays.
    - Replay Attack capture data in session to impersonate one of the parties.
    - Timestamps and sequence numbers are effective countermeasures against replay attack.

V. Secure Coding Concept:

- **OWASP** (Open Web Application Security Project): non-project foundation that is focused on improving the security software.
- **Code Reuse and Dead Code**: Developers, encourages to reuse codes whenever possible instead of re-creating code that already exists. Code reuse saves time and helps prevent the introduction of new bugs.

Ex. Developers created a module that has 3 purposes: create users, modify users, and authenticate users. If he simply copies the entire module, it creates dead code. “**Dead Code”** is code that is never executed or used. It is more like if all modules are not being use, it creates dead.

Note: Logic error can create dead code. Ex. If Donuts has a value (such as 21), it squares it. If Donuts is null (a value of nothing), it returns an error and exits the function.

- Third-party Libraries and SDKs (Software development kits): are like third-parties library, but typically tied to a single vendor.
- **Input Validation:** practice of checking data for validity before using it. (Sanitizing the input to remove malicious code or rejecting the input.

→ Improper input handling (lack of input validation): common security issues with web-based application. Many types of attacks such as buffer overflow, Structured Query Language (SQL) injection, dynamic link library (DLL) injection, cross-site scripting (XXS).

<u>Some common input validation attack include</u>:

- <u>Verifying proper characters</u>: some fields, zip code uses only numbers.
- <u>Blocking HTML code</u>: some malicious attacks embed HTML code within the input as part of an attack. **Input Validation** code can detect HTML code, such as <and> characters and not use it.
- <u>Preventing the use of certain characters</u>: some SQL injection uses specific character, so avoid using (-, ‘, =) helps prevent these attacks.
- <u>Implement Boundary or range checking</u>: If maximum purchase for a product is 3, a range check verifies the quantity is 3 or less. The **Validation** check identifies data outside the range as invalid and the application does not use it.

- **Client-Side and Server-Side Input Validation**: **Client-side execution** indicates that the code runs on the client's system such as a user's web browser.

Note: Many web browsers allow users to disable JavaScript in the web browser, which bypasses client-side validation.

- **Server-side validation:** checks the inputted values when it reaches the server. This ensures that the user has not bypassed the client-side checks.

→ *Server-side validation is more secure than client-side validation*. **Input Validation** protects against many attacks, such as buffer overflow, SQL Injection, dynamic link library, and cross-site scripting attacks.

Note: Another method attempts to sanitize HTML code before sending it to a web browser. This method refers as "Escape the HTML code or encoding the HMTL code".

- **Avoiding *Race Condition***: 2 or more modules of an application, or 2 or more application attempt to access a resource at the same time, it can cause a conflict known as a **race condition**.

→ Most database application have internal "*Concurrency Control Processes*", preventing 2 entities from modifying a value at the same time.

Remember: Attackers can exploit a *time of check to time of use* (TOCTOU) race condition, sometimes called "State Attack".

Example: Imagine application first checked to see what seats are available and only offered available seats (time of check). Then, 2 people selected the same seats. A secure application would check again before reserving the seat (time of use).

- **Proper Error Handling** (improper error handling = Protect OS integrity): When application doesn't catch an error, it can cause the application to fail.
  - Improper error-handling techniques within an application can cause the operation system to crash.
  - Using effective error- and exception-handling routines protects the integrity of the underlying operating system.
  - Improper error handling often gives attackers information about an application. When application doesn't catch an error, it often gives debugging information that attackers can use against the application.
  - When application catches error, it can control what information it shows to the user. There are 2 important points about error reporting:
    - Error to Users should be General: Detail info, provides info that attackers can use against the system.
    - Detailed should be Logged:

Note: Error and exception handing helps protect the operating system's integrity and controls the error.

- **Obfuscation**: attempt to make sth unclear or difficult to understand, and code obfuscation is to make codes unreadable. Ex. rename variables, replace numbers with expressions, replace strings of characters with hexadecimal codes, remove comments.

VI. Outsourced Code Development

The following list identifies some vulnerabilities to consider:

1) Make sure the code work as expected

        2) Vulnerable Code: if developers don’t follow best practices for secure codes, easily create code that’s vulnerable to attack.
        3) Malicious Code: Developers could insert malicious code such as backdoors or logic bombs.
        4) Lack of Update: update the codes to fix any vulnerabilities

- **Data Exposure**: Secure coding technique to protect data at rest, data in transit, and data in processing.
    - To protect data at rest is using Encryption. If application processes encrypted data, it typically decrypts data first.
    - After processing it in memory, it encrypts it again and store it. The application should also flush the memory buffer to ensure unauthorized entities can’t access unencrypted ramnants.
- HTTP Headers: HTTP headers are formatted as pairs separated by a colon (:). A general header group applies to the entire message. The request header group typically includes info about the browser, and any encoding that the client’s browsers may accept. The entity header group gives info about the body of the message. Some headers that are commonly recommend as best practices:
    1) HTTP Strict-Transport-Security: tells browsers to display the page only if it’s sent as HTTP Secure (HTTPS). Includes the max-age=SECONDS and the includesSubDomains values.
    2) Content-Security-Policy: defines multiple sources of acceptable content, includes sources allowed for scripts, style (CSS), images, plug-ins, and more.
    3) X-Frame-Options: tells browsers if X-frames are allowed. X-Frame are rarely used anymore because they open up the page to vulnerabilities.
- **Secure Cookie**: A user visits a website; the website often creates a cookie and writes it to the user’s system. This cookie is a small text file and include anything that web developers choose to write.
    - Secure Cookie is one that has a Secure Attribute Set. Cookies only transmit over secure channel such as HTTPS. This protects confidentiality of cookie’s content.
- **Code Signing:** provides 2 benefits. 1. Certificate identifies the author. 2. Hash verifies the code hasn’t been modified.

VII. **Analyzing and Reviewing Code:** Common methods of testing code include:

1. Static Code Analysis: Examine the code without executing it. Developers performs a manual code review goes through the code line by line to discover vulnerabilities.
2. Manual Code Review: is static code analysis where someone goes though the code line by line.
3. Dynamic Code Analysis: checks the code as it is running. A common method is to use fuzzing. **Fuzzing** uses a computer program to send random data to an application.
    - The goal is to discover problems during a dynamic analysis so that they can be fixed.
4. Sandboxing: Test application within an isolated area. (Vms are often used for sandingboxing)

Note: Software Version control tracks the versions of software as it is updated.

VIII. **Secure Development Environment**: include multiple, typically include different systems used for each stage. Different stages used in this process are:

1) Development: developers used an isolated development environment to create the application.
2) Test: testers put application through its pace and attempt to discover any bugs or errors in the testing stage.
3) Staging: simulates production environment, used for late-stage testing. Provides a complete but independent copy of the production environment.
4) Production: Application goes live as the final product.
5) Quality Assurance (QA): ongoing process used throughout the lifetime of the project from the development stage and after it is deployed. Org for Standardization. (ISO) and the international Electrotechnical Commission.

Note: Individual elements within a database are called “fields”.

- Normalization: refers to organizing the tables and columns to reduce “redundant data”.
- First Normal Form (1NF): If meets following 3 criteria:
  - Each row within a table is unique and identified with a primary key
  - Related data is contained in a separate table
  - None of the columns include repeating group
- Second Normal Form (2FM): applies to table that have a composite primary key.
  - It is 1NF.
  - Non-primary key attributes are completely dependent on the composite primary key.
- Third Normal Form: help eliminate unnecessary redundancies.
  - It is in 2NF. This implies it is also 1NF.
  - All columns that aren’t primary keys are only dependent on the primary.
- SQL Injection: SQL query languages use a semicolon (;) to indicate the SQL line’s end and use 2 dashes (-) as an ignored comment.

  Ex: SELECT “FROM Books WHERE Author-“John”;
  SELECT “FROM Customers;

  The 1st line retrieves data from the database. The semicolon signals the end of the line, the database will accept another command. Next line reads all the data in the Customers table, giving attackers access to names, credit card data, and more. Last line comments out the second single quote to prevent SQL error.

  Many SQL injection attacks use a phrase of or’1’=’1’ to create a true condition. If attackers, type **or’1’=’1’**, it will create a query like this.

  Ex. SELECT *FROM Customers WHERE name=”or’1’=’1’;--'

  SQL injection attacks starts by sending improper formatted SQL statement to the system to generate errors.

Note: Proper handling prevents the attackers from gaining info from these errors.

- Protecting Against SQL injection Attacks (Store procedure help SQL attack)

    - Developer often users **Store procedures** with dynamic webpages. **Store procedure** is a group of SQL statements that execute as a whole, similar to mini-program.
    - Instead of copying the user's input directly into a SELECT statement, the input is passed to the store procedure as a parameter. The store procedure performs data validation. The store procedure uses the entire search string in a SELECT statement like this:
      Ex. SELECT *From Books Where Author =”John’;SELECT*From Customers;--”
- Provisioning and deprovisioning typically refer to user accounts.
    - Deprovisioning: account refers to removing access to these resources and can be as simple as disabling or deleting the account.
    - Provisioning an app: refers to preparing and configurating the app to launch different devices and to use different app services.
- **Integrity Measurement**: refers to the quality of the code. Code integrity measures the quality of code throughout the development life cycle.
- **Web Server Logs**: log activities on the server.
- **Using Script for Automation**: SIEM includes variety of scripts to collect and analyze log entries. Continuous integration includes continuous validation:
    - Automated courses of action: is a core principle of the DevOps model. It triggers an automated response
    - Continuous monitoring: process automatically monitors code changes to detect compliance issue and security threat. Allow developers to address them in real time.
    - Continuous Validation: revalidates code after every change. Code changes shouldn’t break this module, but sometimes it does.
    - Continuous Integration: occurs after continuous validation. Refer to the practice of merging code changes into a version control repository regularly.
    - Continuous Delivery: refers to a process where code changes are released automatically to a testing or staging environment.
    - Continuous Deployment: code changes are deployed automatically to the production environment. Code still being tested but without requiring manual approval.

Note: **Continuous deployment** deploys changes to a production, whereas **continuous delivery** only sends changes to a testing or staging environment.

IX. Identifying Malicious Code and Script

Common Indicators of malware infections:

- You can’t update the system
- Antivirus software is disabled
- A system runs slower than normal
- Internet traffic increases on its own
- A system randomly crashes or freezes
- Pop-ups or security warnings begin to appear
- Your browser home page or default search engine changes

- **Power Shell:** a task-based command-line shell and scripting language that uses cmdlets.

- **Powershell**: has full access to the Microsoft Component Model (COM) and Windows Management Instrument (WMI).
- The best way to detect a PowerShell cmdlet is by viewing logs and looking for PowerShell cmdlet.
- Common verbs in PowerShell are: Get, Add, Test, Remove, New, Find, and Move. PowerShell common nouns are: Command, Service, Location, Process, Childterm, WmiObject, PSDrive.
- "**Get-Command**" lists all Powershell commands.

- Bash (Bourne-Again Shell): command language interpreter for unix and unix-like operating system.
  - If you have a script in the current directory named mytest.sh, you would run it with: Ex. bash mytest.sh or sh mytest.sh
  - Users sometimes required to enter full path for bash or sh as follows. Ex. bin/bash mytest.sh or /bin/sh mytest.sh

Note: If logs show verb-noun cmdlets or calls to bash or sh, it maybe a potential attack indicator.

- Macro (repetitive automation function): Macro a short instruction that will run a longer set of instructions. Ex. CTRL + C=copy, and it will do sth. If attackers can edit these macros, they can replace them with malicious step.
- Visual Basic for Application (VBA): Microsoft created VBA, which runs as an internal programming language within Microsoft application such as Microsoft Words.

→ Macros (include VBA macros) are disable by default in Microsoft Office causes it is easy for attackers to create malicious macros and VBA code.

- **OpenSSL** (a tool used to implement **TLS & SSL**= a protocol uses to secure communication between server & client): a software library used to implement SSL and TLS.
  - OpenSSL is primarily used with TLS, not SSL.
  - Administration use OpenSSL top create key pairs before requesting a certificate
  - You can also use OpenSSL to create certificate signing requests (CSRs)
- **SSH (**protocol use to connect with remote system**):** SSH protocol to connect with remote systems. OpenSSH is a suite of tools that simplify the use of SSH.

X. Identifying Application Attacks:

- Zero-Day Attack: a weakness or bug that is unknown to untrusted source. Heuristic AV helps find Zero day.
- Memory Vulnerability: many app attacks take advantages of vulnerabilities in a system's memory. Poor memory management technique can result in a memory leak or allow various overflow issues.
  - **Memory Leak**: application can consume so much memory that OS can crash. Typically, caused by an app that reserves memory for short-term use but never releases.
- **Buffer Overflow**: occurs when an app receives more input or different input, that it expects. The result is an error that expose system memory that would otherwise be protected and inaccessible. Ex. app may expect to receive a string of 15 characters for a

username. If it receives more than 15 characters and tries to store the data in the buffer, it can cause a buffer overflow and expose system memory.

  - An EX of HTTP GET command shows an example of sending a long string to a system to create a buffer overflow:
    GET /index.php?username=ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
  - They exploit it and overwrite memory location by their own code. The goal is to insert malicious code in a memory location that system will execute.
  - Popular method that makes guessing easier is with no operation (NOP, pronounced as "no-op") commands, when a computer is executing code from memory and comes to a NOP (such as x90), it just goes to the next memory location.
  - Although error-handling routines and input validation go a long way to prevent buffer overflow, they don't prevent them all.
  - **Solution**: Keep system up to date with current patch.
- **Integer Overflow**: occur if app receives a numeric value that is too big for the app to handle. (Good practice to double check the size of the memory buffer to ensure they can handle ant data generated by app. Possible to use input validation technique to prevent integer overflow issues.
- Point/Object Dereference: use pointers, store a reference to a variable or object. Ex. Java refers to dereferencing a pointer or object as setting it to null.
  Note: NullPointerException error is an indicator of a pointer or object dereference error in Java.
- Dynamic Link Library (DLL): App uses DLL or multiple DLLs. DLL is a compiled set of code that an app can use without recreating the code.
  - Ex. most programming language includes math-based DLLs. Instead of writing the code to discover a number's square root, a dev can include the appropriate DLL and access the square root function within it.
  - **DLL Injection**: attack that injects DLL into a system's memory and causes it to run. Ex. attackers attaches this this malicious DLL to a running process, allocate memory within the running process, connects the DLL within the allocated memory, and then executes functions within the DLL.
- Lightweight Directory Access Protocol Injection: LDAP (method used to query database). MS AD uses LDAP to access objects within a domain.
- Extensible Markup Language (XML) Injection: a markup language used to transfer data. Ex. imagine online web application is used to create and transfer user information.
  - Directory Traversal: a specific of injection attack that attempt to access a file by including the full directory path or traversing the directory structure on a computer.
- Cross-Site Scripting: a web application vulnerability that allows attackers to inject scripts into webpage.
  - **Reflected XSS** or non-persistent: attacker crafting a malicious email, encouraging a user to click it. Malicious URL often placed within a phishing email. When user

    clicks on URL, it sends HTTP request to a server. This request includes malicious code, and the server sends it back to the user in the HTTP response.
    - Stored XSS or persistent: instead of the user sending the malicious code to the server, stored in a database or other location trusted by the web app.

Note: Input validation protects against XSS attacks.

- Cross-Site Request Forgery (XSRF or CSRF): attacker tricks user into performing an action on a website. Attacker creates a specially crafted HTML link, and the user performs the action without realizing it. Ex. Make users perform action without their knowledge. In some cases, allow attacks to steal cookies and harvest passwords.
    - Website won't typically allow these actions without users first logging. However, if users have logged on before, authentication information is stored on their system either in a cookie or in the web browser's cache.
    - One method is to use "Completely Automated Public Turing Test to Tell Computer and Humans Apart (CAPTCHA): Dual authentication
    - XSRF and CSRF token: The token includes along with other form of data. Generally, raise 403 Forbidden error if the token doesn't not match.

Remember: a giveaway of potential XSRF attack is the inclusion of a question mark **(?)** in the URL

- Server-side Request Forgeries (SSRF): exploit how a server processes external info. If attacker can modify the external URL, can potentially inject malicious code into the webpage. External data sources include API data, databases, and files.
- **Client-Side Request Forgeries**: occur if attacker can inject code into the client-side webpage after the server has crafted it and sent it to the user. (Most common way is using **cookies**).
    - Attacker can modify existing cookies that web application expects to read on the client. Possible to inject malicious code in these cookies, will then be placed in the webpage on the client-side.
- Driver Manipulation: OS use drivers to interact with hardware devices or software component.
- **Shimming:** provides the solution that makes it appear that the older drivers are compatible.
    - A driver shim is additional code that can be run instead of the original driver. When app attempts to call am older driver, OS intercepts the call and redirects it to run the shim code instead.
- **Refactoring code**: process of rewriting the code's internal processing without changing its external behavior. It's usually done to correct problems related to software design.

Note: attackers with strong programming skills can use this knowledge to manipulate drivers by creating shims or rewriting the internal code.
→ attackers can fool the OS into using a manipulated driver, cause it to run malicious code contained within the manipulated driver.

Artificial Intelligence and Machine Learning: refer to technologies that help computer systems improve with experience. Machine learning is a part of AI, AI is much broader. AI system often start with algorithms that represent a set of knowledge and rules:

  - Learn what works and keep doing it
  - Learn what doesn't work and stop
  - Try new things

Remember: Potential indicator of tainted data being use to confuse an AL and ML system is sudden unexpected activities. If a behavior-based NIPS previously gave at least on false positive everyday but hasn't raised any alerts for a few days. It could indicate an attack on the NIPS.

Chapter 8: Using Risk Management Tools

Risk: likelihood of threat will exploit a vulnerability.

Vulnerability: a weakness, and threat is a potential danger.

I. **Threat**

- Malicious human threat: include script kiddie, hacktivist, APTs,…etc.
- Accidental human threat: users can accidentally delete or corrupt data. Admin can unintentionally cause system outage.
- Environmental Threats: long-term power failure, pollution, natural threat.

→ **Threat Assessment:** helps Org identify and categorized threats.

II. **Risk Types:** Several risk types or risk categories include:

- Internal: refer to employees, all hardware, software used within Org.
- External: Any natural threat such as hurricane, earthquakes, tonardo.
- IP Thief: Intellectual property (IP) like copy right, patents, trademarks and trade secrets.
- Software compliance/licensing: Org uses the software without buying a license.
- Legacy systems and legacy platform: legacy system, vendors don't support them.
- Multiparty: If third-party suffers an attack, may expose the Org data to threats.

III. **Vulnerabilities:** a flaw or weakness.

- Default Config: changing default usernames and passwords.
- Lack of malware protection or updated definition: anti-malware, if there aren't kept up to date, system is vulnerable.
- Improper or weak patch management: patches, hotfixes
- Lack of firewalls: hosted-base and network-based firewall
- Lack of organizational policies: job rotation, mandatory vocation, least privilege policy. Can be susceptible to fraud and collusion from employees.

IV. **Risk Management Strategies**

Risk Management: practice of identifying, monitoring, and limiting risks to a manageable level.

- Risk awareness: acknowledgement that risks exist and must be addressed to mitigate them.
- Inherent risk: refers to the risk that exists before controls.
- Residual risk: the amount of risk that remains after managing or mitigating risk to an acceptable level.
- Control Risk: the amount of risk that exits if in-place controls do not adequately manage risks. Imagine systems have antivirus software installed, but they don't have a reliable method of keeping it up to date.

- Risk appetite: refers to the amount of risk an Org is willing to accept.

V. Risk management strategies includes:

- Avoidance: Org avoid a risk by providing a service or not participating in risky. Evaluate an App that requires multiple open ports the firewall.
- Mitigation: Org implements controls to reduce risks. Reduce the impact of the threat. Up-to-date antivirus software mitigates.
- Acceptance: when the cost of a control outweighs a risk, Org will often accept the risk.
- Transference: transfer the risk to another entity, purchasing insurance, outsourcing contracting a third party.
- Cybersecurity insurance

VI. **Risk Assessment Types**:

- *A risk assessment or risk analysis:* an important task in risk management. A risk assessment starts by first identifying assets and asset values.
- After identifying asset value, risk assessment then identifies threats and vulnerabilities and determines like the likelihood a threat will attempt to exploit a vulnerability.
- A risk assessment attempts to identify the impact of potential threats, identify the potential harm, and prioritize risks based on the likelihood of occurrence and impact. (it also includes recommendations on what controls to implement to mitigate risks)

*Risk control assessment: examines an Org knowns risk and evaluate the effectiveness of in-place controls.

*Risk Control self-assessment: risk control assessment, but employees perform. Risk control assessment is performed by a third-party.

VII. **Quantitative Risk Assessment** (Managerial Controls): use specific monetary amounts to identify the cost and asset value.

- **Asset value**: is important in a quantitative risk assessment.

Quantitative model used to determine risk:

- Single Loss Expectancy (SLE): identifies each loss's amount.
- Annual Rate of Occurrence (ARO): indicate the number of failure in a year.
- Annual Loss Expectancy (ALE): identifies to expected annual loss: The ALE= SLE x ARO

You can now calculate the SLE, ARO, and ALE as follow: Example as below:

- SLE: The value of each laptop is $2,000, so the SLE is $2,000
- ARO: Employees lose about one laptop a month, so the ARO is 12
- ALE: You calculate the ALE as SLE x ARO, so $2,000 x 12 = $24,000

Security experts estimate that these locks will reduce the number of lost or stolen laptops from 12 a year to only 2 a year. This changes the ALE from $24,000 to only $4,000 (saving $20,000 a year). In the other words, Org can spend $1,000 to save $20,000. It doesn't a rocket scientist to see that is a good fiscal decision, saving a net of $19,000.

VII. **Qualitative Risk Assessment:** use judge to categorize risks based on the likelihood of occurrence and impact.

- Risk analysis: identifies potential issues that could negatively impact an Org's goals and objectives.

- Risk register: listing known info about risks such as the risk owner, typically includes risk scores along with recommended security controls to reduce the risk scores.
- Risk matrix: plots risk onto a graph onto a graph or chart.
- Heat map: similar to a risk matrix. Instead of using words such as acceptable risk and unacceptable risk, they use colors such as green and red.
- Supply Chain Risks: includes all the elements required to produce and sell a produce.
- Org can eliminate the supply chain as a third-party risk simply by ensuring that it has multiple sources for everything that it needs.

VIII. **Threat Hunter:** process of actively looking for threats within a network.

- Internal sources include device logs, IDS, and data from past incident. Historical data on incidents can help you understand what happened, what worked to mitigate the incident, and what didn't work.
- Threat Feed: use both structure data reports and unstructured reports.
  - Structure report: use structure language such Structured Threat Information eXpression (STIX)
  - Unstructured reports: use white paper released as Word documents or PDF files.
- United States Computer Emergency Readiness Team (US-CERT): maintains the National Cyber Awareness System.
- Threat Intelligence Fusion: combine all this data to create a picture of likely threats and risks for an Org.
- A vulnerable assessment includes following high-level steps:
  - Identify assets and capabilities
  - Prioritize assets based on value
  - Identify vulnerabilities and prioritize them
  - Recommend controls to mitigate serious vulnerabilities

IX. Password Crackers: Passwords are typically hashed. Message Digest 5 (MD5) is a weark hashing algorithms.

- There are 2 types of passwords crackers-offline and online
  - Offline password cracker attempts to discovers passwords by analyzing a database or file containing passwords. (attackers have unlimited time ti analyze the passwords).
  - Online password attempts to discover passwords by guessing them in a brute force attack. Some online password crackers attempt to discover the passwords for specific account by trying to log on the amount remotely. Online passwords crackers collect network traffic and attempt to crack any passwords send over the network.

Network Scanners (Reconnaissance): use various techniques to gather info about hosts within a network. Network scanners typically use the following methods:

- Arp ping scan: ARP resolves IP address to MAC address. Any hosts that receive an ARP packet with its IP address responds to MAC address. If host responds, the network scanner knows that a host is operational with that IP address.
- Syn Stealth scan: can sends a single SYN packet to each IP address in the scan range. If a host responds, the scanner knows that a host is operational with that IP address. However, instead of responding with an ACK packet, a scanner typically sends an RST (reset) response to close the connection.
- Port Scan: checks for open ports on a system.
- Service scan: is like a port scan, but a step further. Port scan identifies open ports and give hints about what protocols or service might be running. Service scan verifies the protocols or service. (A service scan send a HTTPS command, such as "Get /:if HTTPS is running on port 443, it will respond to the GET command to verifies that it is a web service.)
- OS detection: analyze packets from an IP address to identify the OS.

X. **Vulnerability Scanning:** to identify which system are susceptible to attacks. Vulnerability scanning often includes the following actions:

- Identify vulnerabilities
- Identify misconfiguration
- Passively test security controls
- Identify lack of security controls

Identifying Vulnerabilities and Misconfiguration**:** Vulnerability scanners utilize a database or dictionary of known vulnerabilities and test systems against this database.

- Common Vulnerability Scoring System (CVSS): assess vulnerabilities and assigns severity scores in a range of 0-10.
- Vulnerability scanners includes Security Content Automation Protocols (SCAP) utilize the National Vulnerability Database (NVD), which includes a list of common misconfigurations, security-related software flaws, and impact ratings or risk scores.
- The SCAP uses both CVE and CSVV data: (vulnerabilities related to weak configuration includes:)
  - Open ports and services: Open ports can signal a vulnerability. Ex. port FTP is open, or TCP port 20, 21 are open. If these ports open, attackers can exploit.
  - Unsecure root account: admin account on the system
  - Default accounts and passwords: Some SQL database systems allow the sa (System Admin) account to be enable with a blank password. Scanner such as Nessus will detect this.
  - Default settings: default accounts and passwords
  - Unpatched systems: Vul Scanning can identify unpatched system, lack of antivirus software.
  - Error: Vul scanner check system against a config or security control baselines
  - Open permissions:
  - Unsecure protocols: no longer recommended for using. Ex. SSL
  - Weak Encryption: SSL has been deprecated, and no longer used
  - Sensitive data: some scanner includes DLP system

***Analyze Vulnerabilities Scan Output*:** output of the scan typically shows the following:

- A list of hosts that it discovered and scanned
- A detailed list of applications running on each host
- A detail list of open ports and services found on each port
- A list of vulnerabilities discovered on any of the scanned hosts

False Positive and False Negative

- **False Positive:** scanner incorrectly reports. Vulnerability is existed, but vulnerability does not exist on the scanned system
- **False Negative:** vulnerability exists, but scanner doesn't detect and does not report
- **True positive:** vulnerability scanner correctly identifies a vulnerability
- **True Negative:** system doesn't have a vulnerability, the vul scanner didn't report.

Note: Credential scan run under the context of a valid account and can get more detailed info on target, such as software versions of install applications. They are typically more accurate than non-credential scans and result in fewer false positives.

Credential Versus non-Credentialed

Vulnerable scanners can run as a credentialed scan using an account's credentials or as a non-credentialed without any user credentials.

- Attackers typically do not have an internal account's credentials, so when they run scans against systems, they run non-credentialed scans.
- Admin run credentialed scans with the privileges of an admin acc. This allows the scan to check security issues at a much deeper level than a non-credentialed scan.
- Credentialed scan can access a system's internal workings, it results in a lower impact on the tested systems, along with more accurate test results and fewer false positive.
- Attackers typically start without any credentials but use privilege escalation technique to gain admin access.

Configuration Review:

- Config compliance scanner performs a config review of systems to verify that they are config correctly.
- When running the scan, scanner will verify that systems have the same config defined in the config file. (also known as config validation)
- Security admin config these tolls to use automation or scripting methods so that they automatically run on schedule.

Penetration Testing: actively assesses deployed security controls within a system or network.

- Start with reconnaissance to learn about the target but takes it a step further and tried to exploit vulnerabilities by simulating or performing an attack.

Rule of Engagement: or boundary of the test. Should be all in writing consent.

- ○ Reconnaissance: Collects info about a targeted system, system, network, or Org.
- ○ Passive Reconnaissance: gain info about targeted computers and networks without actively engaging with the systems
- ○ Active Reconnaissance: attacker engages with the target system, typically conducting a port scan to determine find any open ports.

Network Reconnaissance and Discovery: use tools to send data to systems and analyze the response. Some tools using this phase includes:

- IP Scanner: search network for active IP addresses. Typically, send ICMP ping to a range of IP addresses in a network. (Firewall often blocks ICMP, often give inconsistent result)
- Nmap: network scanner, includes identifying all the active hosts, IP addresses, service running on each of these hosts, host's OS.
- Netcat: admin often use for remotely accessing Linux system. Banner grabbing will identify the target's operating system along with info about some App, can also be used to transfer files and check for port open.
- Scanless: Python-based command-line utility to perform port scanning.
- Dnsnum: will enumerate DNS records for domains. List DNS servers holding the records and identifies the mail servers by listing MX record.
    - Next attempting to do an AXFR transfer to download all DNS records from the DNS servers holding the records. However, unauthenticated AXFR transfer are usually block on DNS servers so the AXFR (replication of DNS data across multiple DNS including subdomain name) request will normally fail.
- Nessus: Vulnerability scanner, scan both window and Unix system.
- Hping: Using TCP, UDP, and ICMP to ping. Scan system for open ports in remote system
- Sn1per: automated scanner used for vulnerability assessments and to gather info on targets during pen testing.
- Curl: Client URL (command curl) used to transfer and retrieve data to and from servers such as web server.

Footprinting Versus Fingerpriting

- Fingerprinting attack sends protocols queries or port scans to a server and analyzes the responses.
- IDSs & IPSs: can detect them and reduce port scanning and fingerprinting.

Initial Exploitation: After scanning the target, tests discover vulnerabilities.

- A vulnerabilities scan may discover that a system doesn't have a patch installed for a known vulnerability.
- The vulnerability allows attackers (and testers) to remotely access the system and install malware on it.

Persistence: attacker's ability to maintain a presence in a network for weeks, months, or even years without being detected.

- Common technique used to maintain persistence is to create a backdoor into the network.

Lateral Movement: refers to the way attackers maneuver throughout a network.

- Window Management Instrumentation (WMI) and PowerShell as frequently used to scan a Window network.

Privilege Escalation: APTs often use remote access trojan (RATs) to gain access to a single system.

Pivoting: process of using various tools to gain additional information.

Note: After exploiting a system, pen testing use privilege escalation technique to gain more access to target systems. **Pivoting** is the process of using an exploited system to target other systems.

XI. **Known, Unknown, and partially Known Testing Environment**

- Unknown Environment testing (Black box testing): testers have zero knowledge of the environment prior to starting an unknown environment test.
- Known Environment testing (White box testing): full of knowledge of the Environ* b4 starting. (Have access to product doc, source code, and possible even log in detail)
- Partially Known Environmental Testing (Gray box testing): have some knowledge of the Environ*. (Have access to some Doc, but not full network layout)

Clean Up: one of the last steps of a pen test. Removing all traces of the penetration test's activities. Clean-up activities includes:

- Remove any user accounts created
- Removing any scripts or application added or installed on systems
- Removing any files, such as logs or temporary files, created on systems
- Reconfig all settings modified by testers during the pen test

Bug Bounty Programs: provide a monetary incentive for security researchers to discover bugs or vulnerabilities.

XII. **Intrusive Vs Non-Intrusive Testing:**

- Tools using intrusive methods can potentially disrupt the operations of a system.
- Tools using non-intrusive methods will not compromise a system
- These terms apply to penetration testing (intrusive) and vulnerability scanning (non-intrusive)

Note: Important to remember that pen tests are intrusive and more invasive than vulnerability scans.

Exercise Types: Cybersecurity awareness

- Red team: The read team attack. Personnel on a red team are experts in attack systems, breaking into defense, and exploiting vulnerabilities.
- Blue Team: The blue team defense. Employee of the Org and they know about security controls used to protect network resources
- Purple team: can do either red team or blue team activities
- White team: personnel establish the rules of engagement for a test and oversee the testing

Packet Capture and Replay: Protocol analyzer, which is sometimes called sniffing or using a sniffer.

Remember: Red team use TTPs, and blue teams defend against these attacks. Members of the purple team can perform as either red ream members or blue teams. White team personnel set the rules and oversee testing.

- Port Address Translating (PAT) translate public and private IP addresses.
  - If the traffic goes through a device using PAT, the protocol analyzer only captures the translated IP address, not the original IP address.
- Normally, NIC uses non-promiscuous mode, only processes packets addressed directly to its IP address.
  - However, when you put it in promiscuous mode it processes all packets regardless of the IP address, allow protocol analyzer to capture all packets that reach NIC.

TCPreplay and TCPdump

- TCPreplay: a suite of utilities used, edit packets and send the edited packets over the network. It includes tcpreplay, tcpprep, tcprewrite, more. Often used testing network devices.
    - Ex. Network admin modify packets to mimic known attacks, send them to all IDS. Using tcpreplay, admin can prove that IDS can detect specific attack.
- tcpdump command: command-line protocol analyzer, allow to capture packets like you can with Wireshark. **Wireshark** is window-based tool and **tcpdump** is executed from the command line.

  Note: Capture packets use tcpdump, analyzing packets use Wireshark.
    - Kali Linux includes tcpdump, tcpdump is case sensitive. Need enter tcpdump in all lower case, and the switch might need to enter with proper case.
    - Ex. -c (represent counts and indicates capture should stop after receiving specific number of packets). Howerver, -C (represent file size)

Note: Tcpdump closes it and starts storing packets in a new file. (Not available on Windows by default, but there are versions for Windows available for download.)

NetFlow, sFlow, and IPFIX

- NetFlows: feature available on many routers and switches that can collect IP traffic statistics and send them to a NetFlow collector.
    - Wireshark allows you to capture headers, view all data and payloads of individual, but **NetFlow** doesn't include payload data, individual packet headers. NetFlow records only show counts, statistics, related to data a device receives.
- SFlow: a sampling protocol, provides traffic info. It may capture 1 packet out of every 10 packets it receives and send this sampled data count to the sFlow collector.
- IP Flow Information Export (IPIX): very similar to NetFlow v9.

XIII. **Understand Framework and Standards:** Framework: a structure used to provide a foundation, provide guidance to professional on how to implement security in various systems.

- International Org for Standardization (ISO):
    - **ISO 27001:** "Information Security Management"
    - **ISO 27002:** "Information Technology Security Techniques"
    - **ISO 27701:** "Privacy Info Management System" (Framework for managing and protecting PII)
    - **ISO 31000:** a family of standards related of risk management.
- Auditing Standards Board of the American Institute pf Certified Public Accountants (AICPA)
- Standard for Attestation Engagement (SSAE): provides Org and auditors with guidance on creating various reports.
- System and Org controls (SOC) 2 report covers Org cybersecurity controls:
    - SOC 2 Type I: describe Org's system and covers designs effectiveness of security controls on specific dates.

- SOC 2 Type II: describe Org's system and covers security controls operational effectiveness over a range of dates. (SOC 2 Type 2 compliance gives a higher level of assurance than SOC 2 Type 1)

- Center for Information (CIS): stated mission to "Identify, develop, validate, promote, and sustain best practice solution for cyber defense and build and lead communities to enable an environment of trust in cybersecurity.

XIV. **Risk Management Framework**: NIST SP 800-37, "Risk Management for Information Systems and Org" covers Risk Management Framework (RMF). These seven steps are:

1) Prepare: identifies key roles for implementing the framework. Risk tolerant strategies: update (or create) risk assessments, and identifies in-place controls. Create a continuous monitoring strategy.
2) Categorize Information systems: determine the adverse impact to operation and assets if there is loss of CIA, allow them to prioritize the systems.
3) Select Security Controls: personnel select, tailor controls necessary to protect their operations. Typically, start with baseline, tailor baseline as needed.
4) Implement Security Controls: personnel implement the selected controls. If change is required, personnel document them.
5) Assess Security Controls: Personnel assess controls to see if they are producing desired outcome. Verifying if implementation is correctly done and operating as expected.
6) Authorize Information Systems: senior official determines if system is authorized to operate. Official makes this decision based on the output of the previous steps.
7) Monitor Security Controls: Ongoing step where personnel constantly assess change in system and environment. Includes performing periodic risk assessments and analyzing risk response.

The NIST Cybersecurity Framework (CSF) aligns with the RMF. CSF includes 3 components:

1. Framework Core: a set of activities that Org can select to achieve desired outcomes. It includes 5 functions: identify, protect, detect, respond, and recover.
2. Framework Implementation Tiers: tiers help Org identify how it views risk. Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4)-the highest.
3. Framework profile: provide a list of outcomes for Org based on its need and risk assessments. Current profiles describe the current state of cybersecurity activities, target large profiles describe the desired outcome.

Reference Architecture: doc or set of doc that provides a set of standards. Some software reference architecture doc list procedure, functions, and methods that a software project should use.

Exploitation Framework: is a tool used to store info about security vulnerabilities. Typically, it includes tools used for check for vulnerabilities and execute exploits on any discovered vulnerabilities. Some commonly used exploitation frameworks are:

1. Metasploit Framework: Metasploit is an open-source project that runs on Linux systems, includes methods to develop, test, and use exploit code.

2. BeFF (Browser Exploitation Framework): Focus on identifying we browser vulnerabilities.
3. w3af (Web App Attack and Audit Framework): focus on web app vulnerabilities.

Note: Remaining Risk is known as residual risk.

Chapter 9: Implementing Controls to Protect Assets

I. **Comparing Physical Security Controls:** Sth you can touch such as hardware, locks, a fence, ID badge, camera.

- Perimeter: Military base & many other Org erect a fence around that entire perimeter. Security guard at gates to control access. Install barricades to block vehicles.
- Buildings: Locked doors restrict entry so only authorized personnel enter. Lighting and video cameras to monitor the entrance and exits.
- Secure Work Areas: some companies restrict access to specific work areas.
- Server rooms: locking a wiring closet prevents
- Hardware: additional physical security controls protect individual system.

II. Securing Door Access with Cards:

- Proximity cards: small credit card-sized cards that activate when they are close to a proximity card reader.
- Card includes a **capacitor and a coil** (radio frequency) that can accept a charge from the proximity card reader.
  1. Physical Cipher Locks: Many manual cipher locks includes a code that requires 2 numbers entered at the same time. Instead, of just 1, 3, 2, 4 the code could be 1/3 (pressed simultaneously), then 2,4,5. This adds complexity to the lock and reduces brute force attacks.
  2. Biometric Locks: Biometric methods provide both identification and authentication.

Note: Door access systems includes physical locks, cipher locks, and biometrics. Cable locks are effective threat deterrents for small equipment such laptops and some workstation.

III. Increasing Security with Personnel:

- Two-person integrity: a security control that requires the presence of at least 2 authorized individuals.
- COMSEC: is communications security and keying material refers to the materials used to encrypted and decrypted classified communications.
- CCTV systems can be used as a compensating control in some situation.

Sensor: Many physical security controls use sensors to detect changes in an environment. It's common to use sensor with cameras, alarms, fire detection. Common sensor below:

- Motion detection: light dimmer. It can also trigger alarms. Only enable when are empty
- Noise detection: detection sensors, detect any noises or when noise exceeds a certain level.
- Temperature: HVAC system have temperature and humidity controls to maintain proper temperature and humidity values.
- Moisture detection: Some Org are located within flood zones and use moisture detection methods to detect flood events.

- Proximity reader: small card that activate when they are close to a card reader. Many Org use these for access point.
- Cards: smart cards and badges include sensors that can be used for access. User inserts the badge or card into a reader instead of waving them in front of proximity reader.
- Infrared detectors sense infrared radiation, sometimes called infrared light which effectively sees a different between objects of different temperature.
    - Infrared detector detect movement by objects of different temperature

Securing Access with Barricades:

- Bollards ae short vertical posts composed of reinforced concrete and/or steel, are effective barricades that can block vehicles.
- Signage is a simple physical security control. Ex. “Authorized Only” or “Restricted”
- Barricade: provide stronger barriers than fence and attempt to deter attackers.

Asset Management: process of tracking valuable assets throughout their life cycles.

- Architecture and design weakness: evaluate the purchase to ensure it fits in the overall network architecture. Unapproved assets often weaken security by adding in additional resources that aren’t changed.
- System sprawl and undocumented assets: system sprawl occurs when an Org has more systems than it needs, and the systems it owns are underutilized.

Implementing Diversity: defense in depth (known as layer of security) refer to the security practice of implementing several layers of protection

IV. **Creating Secure Areas**:

- Air gap: physical security controls that ensure that a computer or network is physically isolated from another computer or network.
- Vaults: a room or a large compartment used to store valuables.
    - Many vaults are used store and access classified info. Ex. US Department of Defense (DoD) uses sensitive Compartment Information Facilities (SCIFs), are within a building used to process classified information.
- Faraday Cage: typically, a room that prevent radio frequency (RF) signals from entering into or emanating beyond a room.
    - Includes electrical features that cause RE signal that reach the boundary of the room to be reflected back. (can also be a small enclosure)
- Hot and Cold Aisle: helps regulated the cooling in data center with multiple rows of cabinet.

Malicious Universal Serial Bus (USB) cable: has an embedded Wi-Fi controller capable of receiving commands from nearby wireless devices, such as a smartphone.

Card Skimming and Card Cloning: skimming is the practice capturing credits data at the point of sale. Skimmer captures the data on the magnetic strip but also allows the transaction to go through.

- Card cloning: refers to making a copy of a credit card using data captured from a magnetic strip.

Adding Redundancy and Fault Tolerance: Org often add redundancies to eliminate a single point of failure.

- Disk redundancies *using RAID*

- NIC redundancy with *NIC teaming*
- Server redundancies by *adding load balancers*
- Power redundancies by *adding generators or an UPS*

Single Point of Failure: system that can cause the entire system to fail if the component fails. Some examples of single points of failure include:

- Disk: If a server uses a single disk, system will crash if the single drive fails. **(RAID** provides fault tolerance for hard drives)
- Server: If a server provides a critical service. (Load balancer provides fault tolerance for critical servers.)
- Personnel: that only one person can perform that person becomes a single point of failure.

IV. **Disk Redundancies**: Four primary resources: processor, memory, disk, and the network interface.

- RAID-0 (Striping): doesn't provide any redundancy or fault tolerance. File stored on a RAID-0 array are spread across each of the disks. RAID-0 increased read and write performance.
- RAID-1 (Mirroring): uses 2 disks. Data written to 1 disk is also written to the other disk. If one of the disks fails, the other disk still has all the data.
- RAID-5: 3 or more disks that are striped together. One drive includes parity info. (Parity info is striped across each of the drives in a RAID-5 and provides fault tolerance. 2 of the drives fall in a RAID-5, the data is lost.)
- RAID-10: config combines the feature of mirroring (RAID-1) and striping (RAID-0). Sometimes called RAID 1+0. The minimum # of drives in a RAID-10 is 4.

V. **Server Redundancy and High Availability**

High availability: refer to system or service that needs to remain operational with almost 0 downtime. The equate to less than 6 minutes of downtime a year: 60 minutes x 24 hours x 365 days x .00001 = 5.256 minutes.

- *Active/Passive Load Balancers:* Load balancers can also be configured in an active/passive configuration, one server is active, and the other server is inactive. If the active server fails, the inactive server takes over.
  - The 2 nodes have a monitoring connection to each other used to check each other's health or heartbeat.
- NIC Teaming: allow you to group 2 or more physical network adapters into a single software-based virtual network adapter.
  - This provides increase performance because the NIC team handles all the individual NICs' bandwidth.
  - The NIC team uses load-balancing algorithms to distribute outgoing traffics equally among the NICs.
  - If one NIC in the NIC team fails, the software detects the failure and logically removes the team's failed NIC
- Power Redundancies: For critical systems, you can use uninterruptible power supplies, generator, and managed power distribution units (PDUs) to provide both fault tolerance and high availability:

- Uninterruptible power supplies: UPS provides short-term power and protect against power fluctuations.
- Dual supply Dual power supply is a second power supply that can power a device if the primary power supply fails. A dual power supply provides both positive voltage and negative voltage of devices.
- Generators: provide long-term power during extended outages.
- Managed power distribution units: Power distribution units (PDUs). Monitor the quality of power such as voltage, current, and power consumption and report this measurement to a central monitoring console.
    - Allows admin to use a single application to monitor power in all the racks within a data center.

VI. Protecting Data with Backups

- Backup Media: Most common media used for backups is tape. Tapes store more data are cheaper than other media.
    - Disk: disk access is much quicker than tape. Disks are more expensive.
    - Network-attached Storage (NAS): dedicated computer used for file storage and is accessible network. (NAS provides file-based data storage allowing users access file on NAS devices and copy backup files to NAS devices.)
    - Storage Area Network (SAN): provides block-level data storage via a full network, SANs to provide high-speed access to disk arrays or tape libraries. SANs can also be used for real-time replication of data.

        + NAS requires dedicated hardware and uses different protocols such as Fibre Channel.

        + NAS uses network protocols such as TCP and IP.
    - Cloud: store in cloud.
- Online Versus Offline Backups:
    - Offline backups use traditional backup media within a network such as tapes, local disks, drives in a NAS, and even backup targets within a SAN. Easy access, better control, relatively fast and restore capabilities.
        - ➢ Offline backup is a cold backup or a backup performed while the database is offline. (Offline backup of a database as a local backup)
    - Online Backups stores within cloud. An online database backup is a hot backup meaning that it backs up the database while it is operational.

VII. Comparing Backup Types: There are 4 types of backups

- Full backup: normal backup, backs up all selected data
- Differential backup: Backup all the data that has changed, different since the last full backup
- Incremental backup: Backs up all the data has changed since the last full or incremental backup
- Snapshot and Image backup: a snapshot backup captures the data at a point in time

Full Backups: backs up all data specified in the backups. 2 limiting factors:

- Time: take several hours to complete and can interfere with operations
- Money: Backup need to be store. Backups every day requires more media.

Differential Backups: starts with a full backup.

- Full/differential backup strategy could start with a full backup on Sunday night. On Monday night, a differential backup would back up all files that changed since the last full backup on Sunday.

Order of Restoration for a Full/Differential Backup Set: Ex. system crashed on Wed morning. They stored each backup on different tapes.

- 2 tapes need to be recovered. First, recover the full backup from Sunday because the differential backup on Tuesday night includes all the files that changed after the last full backup. They would then restore that tape to restore all the changes up to Tuesday.

Incremental Backups: start with a full backup. Includes the last full backup or last incremental backup.

- A full/Incremental strategy could start with full backup on Sunday night.

Order of Restoration for a full/Incremental Backup Set: Ex. System crashed on Thur morning. They stored each backup on different tapes.

- 4 tapes. First, need to recover the full backup from Sunday. Because the incremental backups would be backing up different data each day of the week, each of the incremental backups, must be restored and restore in chronological order.

Snapshot and Image Backups: (also known as Image backup) captures data at the moment in time. Commonly used with virtual machine.

Note: Test restores are the best way to test integrity of a company's backup data.

Backups and Geographic Considerations:

- Off-site storages: at least one copy of backups should be store off-site.
- Distance: distance between the main site and the off-site location.
- Location selection: environmental issues.
- Legal implications: Backups need to be protected according to governing laws.
- Data sovereignty: when data is stored off-site, stores in different countries, subject to that country's laws.

Comparing business Continuity Elements: helps and predict, plan for potential outage of critical services. Org often create a business continuity plan (BCP).

- Environmental: natural disaster, hurricane, flood.
- Person-made: refer to those caused by human activity, includes fire caused by human.
- Internal versus external: internal (fire within data center), external (wild fire).

Business Impact Analysis Concepts (BIA): an important part of a BCP. Helps an Org identifying critical systems and components that are essential to the Org success. Critical systems support **mission-essential** functions. Mission-essential function, activities that must continue or be restore quickly after a disaster.

- What critical system and functions?
- Are there any dependencies to these critical systems and functions?
- Maximum downtime limit of these critical systems and functions?
- What scenarios are most likely to impact these critical systems and function?
- What potential loss from these scenarios?

Note: ***BIA*** identifies mission-essential functions and critical systems that are essential to the Org success. Identifies maximum downtime limits for these systems and components, various scenarios that can impact these systems and components, potential losses from an incident.

Impact: BIA evaluates various scenarios, natural disasters, fires, attacks, power outages, data loss and hardware & software failures. BIA looks at multiple items:

- Will a disaster result in loss of life?
- Will a disaster result in loss of property?
- Is there a way to minimize the risk to personnel?
- Will a disaster reduce safety for personnel or property?
- What are the potential financial losses to the organization's reputation?

Recovery Time Objective (RTO): identifies the maximum amount of time, take to restore a system after an outage. (How long system takes to restore)

***Recovery Point Objective* (RPO)**: Identify a point in time where data loss is acceptable. Management might decide that some data loss is acceptable. Want to recover data from at least the previous week.

- With an RPO of one week, admin would ensure that they have at least weekly backups. In the event of failure, they will be able to restore recent backups and meet the RPO.

Note: RTO identified the max time to restore the system whereas RPO refers to the amount of data you can afford to lose.

Comparing MTBF and MTTR: Likelihood that a hard disk within a RAID config will fail?

- Mean time before failures (MTBF): provides a measure of a system's reliability and is usually represented in hours. It identifies the average (the arithmetic mean) time between failure.
  - Higher MTBF, indicate higher reliability
- Mean time to repair (MTTR): identifies the average time it takes to restore a failed system.

Note: MTBF *provides a measure of a system's reliability and would provide an estimate of how often the systems will experience outage.* *MTTR refers to the time it takes to restore a system*.

Continuity of Operations Planning (COOP): focuses on restoring mission-essential functions at a recovery site after a critical outage.

- Failover, process of moving mission-essential functions to the alternate site.

Site Resiliency: recovery site, alternate processing site that Org uses for site resiliency. 3 primary types of recovery sites are hot site, cold site and warm site. Other types of recovery sites are mobile sites and mirrored sites.

- Hot site: be up and operational 24 hours a day, 7 days a week and be able to take over primary site quickly after a primary site failure.
  - Hot site is another active business location that has the capability to assume operations during a disaster.
- Cold site: requires power and connectivity but not much else. Org brings all the equipment, software, and data to the site when it activates it.
- Warm site: provides a compromise that an Org can tailor to meet its needs. Org place all the necessary hardware at the warm site, but not include.

- Mobile site: self-contained transportable until with all the equipment needed for a specific requirement. Can outfit a semitrailer with everything needed for operations, including a satellite dish.
- Mirrored sites: identical to the primary location and provide 100 percent availability. Although a hot site can be up and operational within an hour, the mirrored site always up and operational.

+Cold site will have power and connectivity needed for a recovery site, but little else. Cold sites are the least expensive and the hardest to test.
+Warm site is a compromise between a hot site and a cold site.
+Mobile sites do not have dedicated locations but can provide temporary support during a disaster.

Disaster Recovery:

- Disaster recovery plan (DRP) identifies how to recover critical systems and data after a disaster. A part of an overall business continuity plan.
- A DRP or a BCP will includes a hierarchical list of critical system. List identifies what systems to restore after a disaster and in what order.
- Hierarchical list: valuable when using alternate sites. DRP prioritizes the services to retore after an outage.
    - Activate the disaster recovery plan
    - Implement contingencies: recovery plan requires the implementation of an alternate site; critical functions are moved to these sites.
    - Recover critical system: Org begins recovering critical systems using the prioritization listed in the DRP. Also includes reviewing change management documentation to ensure that recovered systems includes approved changes.
    - Test recovered systems: Bringing systems online, admin test and verify them. Include comparing the restored system with a performance baseline to verify functionality.
    - After-action report: Final phase of disaster recovery includes a review of the disaster, sometimes called an after-action review. Includes a lesson learned review to identify what went right and what went wrong. Org often updates the plan to incorporate any lessons learned.

Note: DRP identifies how to recover critical systems after a disaster, prioritizes services to restore after an outage. Testing validates the plan. Final phase includes a review to identify any lessons learned and may include an update of the plan.

IX. **Testing Plans with Exercises**

- Business continuity plan (BCP) and DRP includes testing (Testing validates that the plan works as desire).
- BCPs and DRPs includes tabletop exercises, walk-through, and simulations.
- NIST SP 800-34 (Contingency Planning Guide for Federal Information Systems"
- ***Tabletop exercise*** (known desktop exercise) discussed-based. Gathers participants in a classroom or conference room and leads them through one or more hypothetical scenarios such as a cyberattack or a natural disaster.

- ***Walk-throughs*** are workshops or orientation seminars, that train team members about their roles and responsibilities.

As a summary, these 3 exercises are:

- *Walk-throughs*: a training, provided to personnel in a classroom setting before a tabletop exercise.
- *A tabletop exercise*: discussion-based exercise where participants sit around a table and talk through one or more scenarios.
- *Simulation*: go through all exercise but in a simulated environment

Some common elements of testing plans include:

- Backups: are tested by restoring the backup data.
- Server restoration: Disaster recovery exercise rebuilds a server.
- Server redundancy: active/passive load balancing, test it by taking a primary node offline.
- Site resiliency: moving some of the functionality to the alternate site and ensuring the alternate site works as desired.

Remember: Validate business continuity plans through testing.

Chapter 10: Understanding Cryptography and PKI

- Integrity: provides assurances that data has not been modified.
  - Hashing: fixed-length string of bits or hexadecimal characters. (Common hashing algorithms in use today "secure Hash Algorithm 3" SHA-3.
- Confidentiality: ensures that data is only viewable by authorized users.
  - Encryption protects confidentiality of data, and includes an algorithm and key.
  - Symmetric encryption: use the same key to encrypt and decrypt data. Most symmetric algorithms use either a block cipher or a stream cipher.
  - Stream Cipher: encrypt data 1 bit at a time Block ciphers encrypt data in blocks.
  - Asymmetric encryption: use 2 keys (public and private) created as a matched pair.
    - Asymmetric encryption: requires PKI to issue certificates.
    - Anything encrypted with the public key: can only be decrypted with the matching private key.
- Stenography: provides a level of confidentiality by hiding data within other files.
- A digital signature: provides authentication non-repudiation and integrity.
  - Authentication: validate identify
  - Non-repudiation: prevents a party from denying an action
  - Users sign emails with a digital signature, is a hash of an email message encrypted with the sender's private key
  - Only the sender's public key can decrypt the hash, providing verification it was encrypted with the sender's private key

I. **Providing Integrity with Hashing:** verify integrity with hashing. Hashing is an algorithm performed on data such as a file or message to produce a number called a "hash".

   - Hashes are created at least twice so that they can be compared
   - SHA-3 hash is the calculated number displayed in hexadecimal

- Hashing verifies integrity for data such as email, downloaded files, and file stored on a disk. (A hash is a number created with a hashing algorithm)

II. **Hash Versus Checksum:** Hashes much longer numbers, used in strong cryptographic implementations. A checksum, a small piece of data only 1 or 2 bits, and quickly verify the integrity of data.

- Checksum, RAID-5 disk: use a single party bit per byte and can identify corrupt data.
- Initial check for credit cards often uses a checksum. 16-digits credit card, first 6 digits identify the institution that issued the card, the next nine represent the account number, 16th digit is a check digits or checksum.
- Checksum, gives a quick indication when data integrity has been lost.
- Popular hashing algorithms MD5 and SHA-256.
- Hash-based message auth code (HMAC): verifies both the integrity and authenticity of a message with the use of a shared secret.
- IPsec and TLS use HMAC-MD5 and HMAC-SHA256.
- **MD5** produces a 128-bit hash.
  - Hashes are commonly shown in hexadecimal format instead of a stream of 1s and 0s.

III. Secure Hash Algorithms (SHA): group of hashing algorithms with variations in groups four families—SHA-0, SHA-1, SHA-2, SHA-3:

- SHA-0 is not used
- SHA-1 is an updated version that creates 160-bit hashes. Similar to the MD5.
- SHA-2 improved SHA-1, includes four versions. SHA-256 creates 256 bit hashes and SHA-512 creates 512-bit hashes.
- SHA-3 (previously known as Keccak): alternative to SHA-2. U.S National Security Agency (NSA)

→ MD5 used to verify the integrity of files SHA also verifies file integrity.
Some malware modifies executable file by adding malicious code into the file.
NOTE: Some Host-based intrusion detection system (HIDs) and antivirus software capture hashes of files on a system when they first scan it and include valid hashes of system files in signature definition files. When they scan a system again, they can capture hashes of executable and system files and compare them with known good hashes. If the hashes are different for an executable or system file, it indicates the file has been modified, and may have been modified by malware.

- HMAC: fixed-length string of bits similar to other hashing such as MD5 and SHA-256.
  - HMAC: uses a shared secret key to add some randomness to the result and only the sender and receiver know the secret key.
  - IPsec and TLS use a version of HMAC such as HMAC-MD5 and HMAC-SHA256.

Remember: hashing is one-way function that creates a string of characters. Cannot reverse the hash to re-create the original file. Passwords are often store as hashes instead of storing the actual password. Application often salt passwords with extra characters before hashing them.

IV. Hashing Files

- Digital signature use hashes within email and email app automatically create and compare the hashes.
- By running the **sha256sum** command against the file, I calculated the hash. I first used the dir command. Then, ran sha256sum against the Kali Linux file three times.
- Each time, sha256sum calculated the same hash.
- Hash doesn't give you a clue about the size of the file, the type of the file, or anything else.

Hashing Password: Most system don't store the actual password for an account.

Understanding Hash Collisions: hash collision occurs when hashing algorithm creates the same hash from different input.

Understanding Password Attacks:

- Online password attack: attempts to discover a password from an online system.
  - Attacker tries to log on to an acc by repeatedly guessing the username and password.
- Offline password attacks attempt to discover passwords from a captured database or captured packet scan.
  - Attacker hack into a system or network causing a data breach, they can download entire database.

→ Unsuccessful logons: comes from a security log.

- Spraying attacks (Use same password try log on many system) attempt to avoid acc lockout policies, but log will show a large volume of failed logon attempts.
- Dictionary Attacks: one of the original password attacks, uses a dictionary of words and attempts every word in the dictionary to see if it works.
- Brute Force Attacks: attempts to guess all possible character combination.
- Spraying Attack: special type of brute force or dictionary attack designed to avoid being locked out.
  - Automated program starts with a large list of targeted user accounts. The, pick a password and tries it against everyone account in the list.
  - It picks another passwords and loops through the list again.
  - Spray attack loops through a long list of acc, it takes a while before it hits the same acc twice.
- Pass the Hash Attack: attacker discovers the hash of the user's password. Then, use it to log on to the system as the user.
  - Any authentication protocol that passes the hash over the network in an unencrypted format is susceptible to this attack.
  - Microsoft LAN Manager (LM) and NT LAN Manager (NTLM), 2 older security protocols used to authenticate Microsoft clients.
  - Attackers first try to gain admin access to a system, either gaining access as a member of the local admin group or gaining certain equivalent privilege.

→ One attacker has these privileges, steal password hashes stored in multiple locations on the compute, such as Security Account Manager (SAM) database, Local Security Authority Subsystem (LSASS) process, Credential Manager (CredMan), LSA Secrets stored in the registry.

➔ Normal users wouldn’t use admin privilege when connecting to other computers. However, an active pass the hash attack would use admin privilege when moving laterally to similar computers around the network.

- Passwords are typically stored as hashes. Pass the hash attack attempts to use an intercepted hash to access an acc.

Birthday Attacks: attacker attempts to create a password that produces the same hash as the user’s actually (also known as a hash collision).

- **Birthday attacks** exploit collisions in hashing algorithm.
- **Hash collision** occurs when the hashing algorithm creates the same hash from different passwords.
- Salting adds random text to passwords before hashing them and thwarts many passwords attack, including rainbow table attacks.

Rainbow Table Attacks: type of attack that attempts to discover that password from the hash. Rainbow table is a huge database of possible passwords with precomputed hashes for each.

1) App guesses a password (or uses a password from a dictionary)
2) App hashes the guessed password
3) App compares the original password hash with the guessed password hash. If they are the same, the app now knows the password.

- Rainbow tables are huge database of passwords and their calculated hashes.
- Rainbow table attacks are often performed offline on stolen or compromised database.

Salting Passwords: a common method of preventing rainbow table attacks. Along brute force and dictionary attacks.

- A salt is a set of random data such as 2 additional characters.
- Cause passwords attacks that compare hashes with a rainbow table to fail

Key Stretching: advanced technique used to increase the strength of stored password.

- Instead of just adding a salt to the password before hashing it, key stretching applies a cryptographic stretching algorithm to the salted password.
- Benefit of key stretching, consumes more time and computing resources frustrating attackers who are trying to guess passwords.

→ Key stretching techniques are bcrypt, Password-Based Key Derivation Function 2 (PBKDF2) and Argon2.

Bcrypt: based on the blowfish block cipher and is used on many Unix and Linux distributions to protect the passwords stored in the shadow password file. ***Bcrypt salts*** the passwords by adding additional random bits before encrypting it with blowfish.

→ Bcrpt, PBKDF2, and Argon2 are key stretching techniques that help prevent brute force and rainbow table attacks.

- They salt the password with additional bits and then send the result through a cryptographic algorithm.

PBKDF2: use salts of at least 64 bits and uses a pseudo-random function such as HMAC to protect passwords.

V. **Providing Confidentiality with Encryption:** **Data at rest**: refers to any data stored on media and it's common to encrypted sensitive data, individual files, folders, or a full disk.

- *Data at rest or data in motion:* refers to any data stored on media. E-commerce websites use HTTPS sessions to encrypt transactions that includes credit card data.
- *Data in processing (data in use) refers to data being used by a computer.* Computer needs to process the data, encrypted while in use. Data is encrypted, an app will decrypt it and store it in memory while in use.
- Two primary encryption method are symmetric and asymmetric.
  - Symmetric encryption encrypts and decrypt data with the same key.
  - Asymmetric encryption encrypts and decrypts data using a matched key pair of a public key and a private key.

These encryption methods include 2 elements:

- Algorithm: performs mathematical calculations on data. Algorithm is always the same.
- Key: is a number, provides availability for the encryption. Kept private and/or changed frequently.

Symmetric Encryption: use the same key to encrypt and decrypt data. Secret-key encryption or session-key encryption.

- Encryption algorithm: Move X spaces forward to encrypt
- Decryption algorithm: Move X spaces backward to decrypt

Example: Imagine the word "PASS" need to be sent and we are moving 3 spaces:
Answer: Start at P (Q,R,S), A (B,C,D), S (T,U,V), S (T,U,V) = SDVV is the encryption (ciphertext). If you want to decrypt, just moved 3 letters backward.

A substitution cipher: replaces plaintext with ciphertext using a fixed system.

The Rot13 (short for rotate 13 place): always uses a key of 13. To encrypt a message, you would rotate each letter 13 spaces. To decrypt a message, you would rotate each letter 13 spaces. Because ROT13 uses both the same algorithm and the same key, it doesn't provide true encrypted but instead just obfuscate the data.

- Obfuscation: method attempt to make something unclear or difficult to understand. (Security through obscurity)
- Advance Encryption Standard (AES): symmetric algorithm typically uses 128-bits key but can use keys with 192 or 256 bits.
- *Radius uses symmetric encryption*

→*Symmetric encryption algorithm:* changes keys much more often than once a day. Algorithm uses a key of 123 to encrypt a project file. It could then use a key of 456 to encrypt a spreadsheet file. The key of 123 can only decrypt the project file and the key of 456 can only decrypt the spreadsheet file.

→**Radius** uses shared keys for symmetric encryption. Radius servers and clients use the shared key to encrypt and decrypt data exchanged in a challenge/response session.

VI. **Block Versus Stream Cipher:** Most symmetric key algorithm cipher suite use either a block cipher or a steam cipher.

- **Block Cipher:** encrypt data in specific-sized blocks, such as 64-bits blocks or 128-bit blocks.

    - Block Cipher divides large file or messages into these blocks and then encrypts each individual block separately.
    - Block Cipher is more efficient when the size of the data is knowns such as when encrypting a file or a specific-sized database field.
- **Steam Cipher:** encrypts data as a stream of bits or bytes rather than dividing it into blocks.
    - Stream cipher are more efficient than block ciphers when the size of the data is unknown or sent in a continuous steam, such as when streaming audio and video over a network.

Note: ***stream cipher*** encrypts data a single bit, or a single byte, at a time in a stream. ***Block ciphers*** encrypt data in specific-sized blocks such as 64-bit or 128-bit blocks. Stream ciphers are more efficient than block ciphers when encrypting data in a continuous stream.

Remember: A stream cipher is that encryption keys should never be reused. If a key is reused, it is easier to crack the encryption.

VII. Common Symmetric Algorithm

- AES: a strong symmetric block cipher that encrypts data in 128-bits blocks. Can use key sizes of 128-bits, 192 bits, or 256 bits. (Refers to how many bits can use in the key). Some of AES's strengths are:
    - Fast: requires one pass to encrypts and decrypt data
    - Efficient: AES is less resources intensive than other encryption algorithms such as 3DES. AES encrypts and decrypts quickly even when ciphering data on small devices, such as USB flash drives.
- 3DES: data encryption standard. Encrypts data in 64-bit blocks.

→If hardware doesn't support AES, 3DES is a suitable alternative. 3DES uses key sizes of 56 bits, 112 bits, or 168 bits.

Blowfish and Twofish: Blowfish, strong symmetric block cipher. Encrypt data in 64-bit blocks and support key sizes between 32 and 448 bits. (A general purpose to replace DES).

- Blowfish is faster than AES is some instances. It encrypts data in smaller 64-bit blocks, whereas AES encrypts data in 128 -bit blocks.

Twofish: related Blowfish, encrypts data in 128-bit blocks, supports 128-, 192-, or 256-bit keys. (one of finalist algorithm evaluated by NIST).

Remember: AES, a strong encryption block cipher that encrypts data in 128-bit blocks. 3DES is a block cipher that encrypt data in 64-bit blocks. 3DES was originally designed as a replacement for DES, but NIST selected AES as the current standard.

VIII. Asymmetric Encryption: 2 keys in a matched pair to encrypt and decrypt data—a public key and a private key.

- Public key: matching private key can decrypt the same information
- Private key: matching public key can decrypt the same information

→ Private Key: always kept private and never shared

→Public key: freely shared by embedding them in a shared certificate

Asymmetric encryption is strong, also very resource intensive. Take a significant amount of processing power to encrypt and decrypt data, especially when compared with symmetric encryption. Most cryptographic protocols that use asymmetric encryption only use it for key exchange.

Key Exchange: share cryptographic keys between 2 entities. Asymmetric encryption uses key exchange to share a symmetric key. Cryptographic protocols then use the symmetric encryption to encrypt and decrypt data because symmetric encryption is much more efficient.

The Rayburn Box: a lock box allows people to securely transfer items over distances. One key can lock the box but can't unlock it. Other keys can unlock the box but can't lock it.

Both keys are matched to one box and won't work with other boxes:

- Only one copy of one key exists
- Multiple copies of the other key exist, and copies are freely made and distributed –think of these as public keys.

Remember: Only a private key can decrypt info encrypted with a matching public key. Only a public key can decrypt info encrypted with a matching private key. Several asymmetric encryption methods is that they require a cert and a PKI.

"Box comes in 2 different versions. One version, used to send secrets in a confidential manner to prevent unauthorized disclosure. Other version, send messages with authentication, the sender sent the message and that message wasn't modified in transit.

Certificate: Key element of asymmetric encryption is a certificate.

1. Certificate is a digital document, includes the public key and info on the owner of the certificate.
2. Certificate authorities (CA) issue and manage certificate. It is used beyond just asymmetric encryption, including authentication and digital signatures.

→ Certificate, important part of asymmetric encryption. Certificates include public key along with details on the owner of the certificate and on the CA that issued the certificate. Certificate owners share their public key by sharing a copy of their certificate.

+ Common elements within a certificate include:

- Serial number: uniquely identifies the certificate. CA uses third serial number to validate a certificate. If the CA revokes the certificate, it publishes this serial number in a certificate revocation (CR).
- Issuer: This identifies the CA that issued the certificate.
- Validity dates: expiration dates
- Subject: identifies the owner of the certificates.
- Public key: Asymmetric encryption uses the public key in combination with matching private key.
- Usage: Some certificates are only for encryption or authentication, whereas other certificates support multiple usage.

+ Certificate attribute identify the issues using Distinguished Name attributes:

- CN: CommonName (also known as Fully Qualified Domain Name such as letsencrypt.org)
- O: Organization (such as internet Security Research Group)
- L: Locality
- S: StateOrProvinceName (such as CA)
- C: CountryName

Ephemeral Key: sth that lasts a short time. Context of cryptograph, an ephemeral key has a short lifetime and is re-created for each session. A static key is semipermanent and stays the same over a long period of time.

- An ephemeral key pair includes a private ephemeral key and a public ephemeral key.
- Systems use these key pairs for a single session and then discard them. Some versions of Diffie-Hellman use ephemeral keys.
- Certificate are based on static keys. Certificate includes an embedded public key matched to a private key and this key pair is valid for the lifetime of a certificate.
- A benefit of static keys is that a CA and validate them.

Perfect forward secrecy: important characteristic that ephemeral keys comply with in asymmetric encryption.

- Cryptography system generates rando, public keys for each session.

Elliptic Curve Cryptography (ECC): doesn't take as much as processing power. Use mathematical equations. Then, graphs points on the curve to create keys.

- Key benefit is that ECC keys can be much smaller.
- Digital signature: are commonly used to sign emails. Digital Signature Algorithm (DSA) use key pairs managed by a PKI with the public key distributed in a certificate.
- Elliptic Curve Digital Signature Algorithm (ECDSA) can also be used for digital signatures.

Quantum Computing: used quantum mechanical properties to perform cryptographic tasks.

- Qubit can be entangled with other qubits.

Quantum Cryptography: Quantum key distribution (QKD): similar to how asymmetric encryption is used to allow 2 parties to establish a shared key used with symmetric encryption.

Post-Quantrum Cryptography: refers to cryptographic algorithms that are likely to be resistant to attacks using a quantum computer.

Lightweight Cryptography: refers cryptography deployed to smaller devices such as radio-frequency identification (RFID) tags, sensor nodes, small cards, health care devices, IoT.

Homomorphic Encryption: allow data to remains encrypted while it is being processed.

- Homomorphic encryption methods work best when data is stored and manipulated as integers.
- A centralized system using homomorphic encryption can allow multiple health care Org to submit their data in an encrypted form and the centralized database can be updated in real time.

Key Length: Any individual algorithm is strengthened is by increasing the length pf a key. Ex. RSA supports key size of 1024, 2048, and 4096.

- NIST predicts that 2048-bit keys should be safe until 2030. 4096-bit keys will be needed if RSA is still in widespread users.

IX. **Mode of Operation:** Authenticated encryption modes ensure the confidentiality of data and the authenticity of the data.

- Confidentiality is provided with encryption. Authenticity allows you to verify that data came from a trusted entity and that the data hasn't lost integrity,
- Authentication Encryptions implementation are in used with symmetric block cipher. They commonly combine a symmetric encryption with a message authentication code (MAC).

- The key is that the authentication is performed on each block when used with block ciphers.

Example: Imagine Homer is visiting a website using TLS. His computer and the website establish a session and share symmetric keys. One key, used to encrypt the webpage before sending them. The second key, used with hashed function on the ciphertext to create a MAC. At this point, only the website and Homer's computer know these keys. Then, the website then sends the ciphertext and the MAC to Homer.

→ Homer's computer uses the second key with the hash function to recalculate the MAC.

- A counter mode cipher (CTR) effectively converts a block cipher into a stream cipher. It combines an initialized vector (IV) with a counter and uses the result to encrypt each plaintext block. The IV is a fixed-sized random or pseudo-random number that helps create random encryption keys, provides a starting value for a cryptographic algorithm.

Note: CTR mode is a form of authentication encryption and CTR modes allow block ciphers to function stream cipher.

Each block uses the same IV, but CTR combines it with the counter value, resulting in a different encryption key for each block. Multiprocessor system can encrypt or decrypt multi blocks at the same time, allowing algorithm to be quicker on multiprocessor or multicore system. CTR is widely used and respected as a secure mode of operation.