Important Notice:

These notes were specifically created for the **CompTIA Security+ SY0-601 exam**, which was introduced in November 2020 and officially retired on **July 31, 2024**. Please note that the exam has since been replaced by the **SY0-701 version**.

While these notes are tailored to the SY0-601 version, much of the foundational content may still be relevant for understanding key concepts. However, you should cross-reference this material with the latest exam objectives and study resources for the SY0-701 version to ensure you're fully prepared.

Use these notes with caution, as they may not cover all updated topics or changes introduced in the new exam.

These notes are intended to support and guide your preparation. May they serve as a helpful resource on your journey toward certification. Best wishes for success as you work toward achieving your goals!

Chapter 1: Mastering Security Basics

Confidentiality ensures that data is only viewable by authorized users.

- The best way to protect the confidentiality of data is by encrypting it
- This includes any type of data, such as PII, data in databases, and data on mobile devices
- Access controls help protect confidentiality by restricting access

Integrity verifies that data has not been modified

- Loss of integrity can occur through unauthorized or unintended changes
- Hashing algorithms (SHA-Secure Hash Algorithm), calculate hashes to verify integrity
- A hash is simply a number created by applying the algorithms to a file or message at different times
- By comparing hashes, you can verify integrity has been maintained

Availability ensures that systems are up and operational when needed and often addresses single points of failures

- You can increase availability by adding fault tolerance and redundancies, such as RAID, failover clusters, backups, and generators

Redundancy and fault tolerance methods increase availability of systems and data

- Scalability refers to manually adding or removing resources to a system to scale it up or out
- Elasticity refers to dynamically adding or removing resources to a system to scale it

Risk is the likelihood that a threat will exploit a vulnerability

- Risk mitigation reduces the chances that a threat will exploit a vulnerability or reduces the risk's impact by implementing security controls

- Managerial controls are administrative in function and documented in security policies
- Operational controls are implemented by people who perform the day-to-day operations to comply with an organization's overall security plans
- Technical Controls: use technology to reduce vulnerabilities
    - Encryption, antivirus, IDS, IPS, firewalls, least privilege principle
- Physical controls: locks, cameras
- Environmental controls: HVAC (heating, ventilation, air conditioning)

Preventative Controls: attempt to prevent security incidents

- Hardening systems modifies the basic configuration to increase security (defense in depth layered security, disabling ports, patches, strong password policy)
- Security guards can prevent unauthorized personnel from entering a secure area
- Change management processes help prevent outages from configuration changes
- Account disablement policy ensures that accounts are disabled when a user leaves an organization

Detective Controls: attempt to detect when vulnerabilities have been exploited, resulting in security incidents (discovers event **AFTER** it has occurred)

- Log monitoring, SIEM, video surveillance, motion detection, IDS

Corrective and Recovery Controls: attempt to reverse impact of an incident or problem after it had occurred

- Backup systems, incident response policies/procedures

Physical Controls: any controls that you can physically touch

Deterrent Controls: attempt to discourage potential attackers and malicious employees from attacking

- Deterrent controls overlap with preventative controls
- Cable locks(to keep computers locked to ground), physical locks

Compensating Controls: alternative controls used instead of primary controls

- New employees given TOTP (Time-based one-time password)
- Still strong authentication solution

Response Controls/Incident Response Controls: controls designed to prepare for security incidents and respond to them once they occur

- Starts with creating security policies, and then training personnel on how to respond

Fire Suppression System: is a physical control (can touch) and technical control (technology needed to detect

Terminal Commands To Know:

a) **Ping:** used to test connectivity for remote or local systems and verify valid hostname to Ip address
- You can ping a hostname to verify name resolution is working
- Sends a ICMP(internet control message protocol) echo request packet and remote system answers with an ICMP echo reply packet → indicating it is operational
- Windows sends out 4 ICMP packets
- Linux sends out unlimited ICMP packets until you manually stop
- **Ping <ipaddress>**
- c: count => -c 4

Firewalls can block ICMP traffic → preventing DoS (Denial of Service) attacks via ping echo packets
- Systems can be operational but give impression that they're not by **NOT** sending ICMP back

Administrators use ping to check the connectivity of remote systems and verify name resolution is working
- They can use ping to check systems and networks' security posture by verifying that routers, firewalls, and IPSs block ICMP traffic when configured to do so

b) **Hping**: similar to ping command, but it can send ping using TCP, UDP, ICMP
- Useful if you're trying to identify whether a firewall is blocking a ICMP
- Also used for scanning for open ports

c) **Ipconfig(Windows)/ifconfig(Linux)**: shows the TCP/IP configuration for Window system
- Includes information about computer's IP address, subnet mask, default gateway, MAC address, DNS Server address
- Shows config information about all NICs on a system, including wired and wireless
- First command used by technicians to troubleshooting network problems

Windows systems us ipconfig to view network interfaces
Linux Systems use ifconif to view network interfaces
- Also used to manipulate the settings on the network interface

You can enable promiscuous mode on a NIC with ifconfig
The IP command is recommended in place of ifconfig in many situations, such as viewing and manipulating NIC settings

Promiscuous Mode: allows network device to intercept and read each network packet that arrives in its entirety

d) **Netstat:** allows you to view statistics for TCP/IP protocols on a system
- Allows you to see active TCP/IP network connections
- Many attacks establish connections from an infected computer to a remote computer
    - Can be identified with netstat

TCP/IP: end-to-end communication

e) **Tracert/Tracerout:** lists all the routers between two systems
- Each router = hop
- Tracert identifies the ip address, round-trip times (RTT), and sometimes hostname of each hop as well as
- If ping fails, admins can use tracert to identify where the traffic stops or look at RTT increasing (when traffic routed around faulty router)

f) **Pathping:** combines ping and traceroute command ➔ USED FOR ROUTERS
- The tracert function identifies all hops (routers) on path and the ping function sends pings to each router and computes stats
- Used by admins to identify any intermittent problems on hops or between hops

g) **Arp:** related to Address Resolution Protocol (ARP) but not the same thing
- ARP resolves IP addresses to MAC addresses and stores result in ARP cache
- Arp command used to view and manipulate ARP cache

Many organizations host web servers using open-source LAMP stack

LAMP (Linux, Apache, MySQL, PHP or Pearl, or Python)
- Linux is OS
- Apache: Web Server Application
- MySQL: database management systems
- PHP: scripting language for dynamic webpages

Linux-Only File Manipulation/Log-Related Commands

a) Cat (concatenation): used to display the contents of a file, and make copies of a file

Sudo (Super User Do): allows you to run the command with root, or elevated privilges, assuming you have permission to do so

Pipe (|) : allows you to send the results from the first command to the second command

b) Grep (Globally search a regular expression and print): used to search for a specific string or pattern of text within a file

c) Head: allows you to see the beginning of a log file if you don't want to print everything
- By default, it shows the first 10 lines of a file

d) Tail: displays the last 10 lines of a log file byu default

e) Logger: adds entries to a file from the terminal or from scripts and applications

f) Journalctl: queries the linux system logging utility (journald) and displays log entires from several sources

g) Chmod (change mode): used to modify permissions on linux system files and folders
- U = file owner
- G = owner group
- O = all others
- R = read
- W = write
- X = execute
- (0-7) octal numbers can be used to indicate permission sequence

e.g) rwx—x-rw
- 1st Set: Owner
- 2nd Set: Owner Group
- 3rd Set: Others

**Expected to read log entries → appendix B

Windows Logs
- Security log: functions as security log, audit log, and access log that records auditable events such as successes or failures
- System log (OS): records events related to the functioning of the OS
- Application log: records events sent to it by applications or programs running on the system

SIEM (Security Information and Event Management)
- SIEM store network activity logs
- Aggregate log and categorize
- Packet sniff

- UBA (User Based Activity): analyze user behavior and identify abnormal behavior
- Admins choose sensor alert numbers from (0-100) in terms of seriousness

Syslog: protocol that specifies a general log entry format and the details on how to transport log entries
Rsyslog: upgrade to syslog
Nslog: another log management tool for windows and linux

Var/log/directory → common linux log commands in here

dig: command used to query about DNS server

Use Case: the goal that an organization wants to achieve

NXLog: another log management tool that is similar to ryslog and syslog, but also supports Windows log formats

Summary

- Ping can be used to check connectivity, check name resolution, verify that routers, firewalls, and IPS block ping traffic
- Tping can also identify open ports on remote systems
- Netstat can view all network connections
    - Useful if you suspect malware is causing a computer to connect with remote computer

- Journalctl displays log entries from different sources on Linux System

---

END OF CHAPTER 1

Chapter 2: Understanding IAM (Identity and Access Management)

Users claim an identity using their username
Users prove identity by authenticating (ex. Password)

Identification occurs when a user claims an identity, such as a username or email address

- Authentication occurs when the user proves the claimed identity (such as with a password) and the credentials are verified (such as with a password)
- Access control systems provide authorization by granting access to resources based on permissions granted to the proven identity
- Logging provides accounting

In authenticating management, at least two entities know credentials (user and server)

AAA (Authentication, Authorization, Accounting)→ provide comprehensive access management system

- Accounting: track user activity and record activity in logs
    - Audit trail: allows security professionals to re-create the events that preceded a security incident by auditing log activity
- Access controls = authorization restriction

Authentication Types:

a) Something you know (password, pin)
    - Static codes = passwords b/c they remain the same for quite a while
    - Complex passwords use a mix of character types. Strong passwords use a mix of character types and have a minimum password length of at **least eight characters**. A password expiration identifies when a password must be changed
    - Password reset keys: used to reset passwords on systems → commonly bootable optical disc or bootable USB flash drive → after rebooting system, they allow you to recover or reset all user and admin passwords

KBA (Knowledge-Based Authentication): prove the identity of individuals

a) Static KBA: used to verify you identity when you've forgotten your password (what's your first pet's name, maidan name etc.)
b) Dynamic KBA: identifies individuals without account

- Organizations use this for high-risk transactions, such as with a financial institution or a health care company
- Crafts multiple choice questions that only the user would know using public and private data sources such as credit reports and third-party organizations

Account Lockout Policies (Lockout Threshold and Duration): thwart brute force and dictionary password attacks

Account lockout policies thwart some password attacks, such as brute force and dictionary attackers
Many applications and devices have default passwords (wireless routers have default)
These should be changed before putting the application or device into service

- Admin Accounts **don't have lockout policies** and so attackers can conduct brute force and dictionary attacks on them
    - Admins may make dummy accounts "administrator" to trick

b) Something you have: refers to something you can physically hold (smart card, hardware tokens)
    - Certificates: digital files that support cryptography for increased security
        - The embedded certificate allows the use of a complex encryption key and provides much more secure authentication than is possible with a simple password

Smart cards are often used with dual-factor authentication where users have something (the smart card) and know something (such as a password or PIN)

- Smart cards include embedded certificates used with digital signatures and encryption
- They are used to gain access to secure locations and to log on to computer systems

Requirements for Smart Card:

a) Embedded Certificate: the embedded certificate holds a user's private key (which is only accessible to the user) and is matched with a public key (that is available to others). The private key is used each time the user logs onto a network
b) Public Key Infrastructure (PKI): PKI supports issuing and managing certificates

Token Key: electronic device size of remote key for car

- Displays a number that changes frequently (every 60s)
- Tokens are synced with a server that knows that the number is at any moment
- Users often use tokens to authenticate via a website (username, password, token)
- Ex) RSA Secure ID

HMAC (Hash-Based Message Authentication Code): uses hash function and cryptographic key
HOTP (HMAC-based One-Time Password
TOTP(Time-Based One-Time Password)

HOTP and TOTP are open source standards used to create one-time-use passwords

- HOTP creates a one-time-use password that does not expire until it is used
- TOTP creates a one-time password that expires after 30 seconds
- Both can be used as software tokens for authentication

VIP Access app by Symantec: once you configure it to work with a compatible authentication server, it creates a steady stream of one-time-use passwords

SMS (Short Message Service)

Two-step verification methods typically use a PIN retrieved from a user's smartphone

- They can be sent via SMS, a phone call, a push notification, or retrieved from an authentication application

c) Something You Are: uses biometrics for authentication

- The STRONGEST form of authentication b/c they are the most difficult for an attacker to falsify
- Passwords are the WEAKEST form of authentication

The third factor of authentication (something you are, defined with biometrics) is the strongest individual authentication factor

- Biometric methods include fingerprints, palm veins, retina scans, iris scans, voice recognition, facial recognition, gait analysis (way individual walks -> feat, hip, knee)

Iris and Retina Scans are the strongest biometric methods mentioned

- Though iris scans are used instead of retina scans b/c retina scans are intrusive and reveal private medical issues
- Facial recognition and gait analysis can bypass the enrollment process when done for identification instead of authorization

Biometric Efficacy Rate: refers to the performance of the system under ideal conditions (accuracy)

- False acceptance
- False rejection
- True acceptance
- True rejection

Using two or more methods in the same factor of authentication (pin and password) is a single-factor authentication

- Dual-Factor (two-factor) authentication uses two different authentication factors, such as using a hardware token and a pin
- Multifactor authentication uses two or more factors

<u>Somewhere You Are</u>

- Authentication identifies user's location (geolocation)
- IP Address commonly used for geolocation → helps identify country, region, state, city, zip code
- Can determine impossible travel time and risk login situations
- VPN can be used to pose as IP Address somewhere else in world

<u>Something You Can Do</u>

- Refers to actions you can take such as gestures on a touch screen

<u>Something You Exhibit</u>

- Something that you show or display (Badge Cards)

<u>Someone You Know</u>

- Indicates that someone is vouching for you
- Antivirus software place green check marks next to websites it deems to be safe

Authentication log files: displays or successful and unsuccessful login attempts

Credential policies: define login policies for different personnel, devices, and accounts

Privileged Access Management (PAM) systems implement stringent security controls over accounts with elevated privileges such as administrator or root-level accounts

- Some capabilities include allowing authorized users to access the administrator account without knowing the password, logging all elevated privileges usage, and automatically changing the administrator account password

Requiring Administrators to use two accounts, one with administrative privileges and another with regular user privileges, helps prevent privilege escalation attacks
Users should not use shared accounts

An Account Disablement Policy identifies what to do with accounts for employees who leave permanently or are on a leave of absence

- Most policies require administrators to disable the account as soon as possible so that ex-employees CANT use the account
- Disabling the account ensures that data associated with it remains available
- Security keys associated with an account remain available when the account is disabled, but the security keys (and data they encrypted) are no longer accessible if it is deleted
- Time-based login restrictions prevent users from logging on or accessing network resources during specific hours

Usage Auditing: records user activity in logs
Usage Auditing Review: looks at the logs to see what users are doing and it can be used to re-create an audit trail
Permission Auditing Reviews: help ensure the users have only the access they need and no more and can detect **privilege creep issues** (when user has more privilege as job roles change b/c prior privileges were not removed)

Some Authentication Services ensure unencrypted credentials are not sent across networks:

a) SSO
b) Kerberos

SSO (Single Sign-On)

- Refers to user's ability to log-on once and access multiple systems without logging on again
    - Limit number of passwords to remember
    - Uses secure token
    - Strong password policy

Kerberos

- A network authentication protocol within Microsoft Windows and Unix
- It uses a database of objects such as Active Directory and KDC (Key Distribution Center) to issue timestamped tickets that expire after a certain time period
- User credentials are packaged within tickets, providing authentication for users when they access resources such as files on file server
- Key Distributed Center (KDC) has an authentication and ticket granting server

Kerberos (Three-Headed Dog => Client, Key Distribution Center, File Server)

- Client sends request to authentication server in KDC and is given encrypted token
- Client sends encrypted token to ticket-granting server and is provided a ticket
- Client takes the ticket and provides file server the ticket for a request

SSO → Authentication Server gives ticket granting token for ticket-granting server → ticket granting server gives ticket for accessing file in file server for a limited time

Federation: provides central authentication in a non-homogenous environment

- Sign-in credentials in one network works for another network that offers different resources
- A way of telling external applications and services that a user is who they say they are → SAML a way to make a user authenticate via SSO once and then communicate that authentication to multiple applications
- Ex) SAML

SAML = Security Assertion Markup Language

SAML is an XML-based standard used to exchange authentication and authorization information between different parties

- SAML provides SSO for web-based applications

OAuth: open standard for authorization that many companies use to provide secure access to protected resources

- Allows one web service to access protected resources stored with another service
- Instead of creating a different account for each website you access, you can often use the same account you used for Google and use Facebook, Paypal, Microsoft, Twitter
- ****OAuth focuses on authorization, NOT authentication**

Access Control Themes:

A Role-Based Access Control (Role-BAC): scheme uses roles based on jobs and functions

- A matrix is a planning document that matches the roles with the required privileges

Group-Based Privileges: reduce the administrative workload of access management

- Administrators put user accounts inot security groups and assign privileges to the groups
- Users witin a group automatically inherit the privileges assigned to the group

Rule-Based Access Control (Rule-BAC): based on a set of approved instructions, such as an access control list (ACL)

- Some Rule-BAC systems use rules that trigger in reponse to an event, such as modifying ACLs after detecting an attack or granting additional permissions to a user in certain situations
- Most common example is routers or firewalls using ACLs

Discretionary Access Control (DAC): specifies every object has an owner, and the owner has full, explicit control of the object

- DACL (List): is a list of ACEs(Access Control Entries) that identifies who can access it in a system and what privileges they have

MAC (Mandatory Access Control): uses sensitive labels for users and data

- It is commonly used when access needs to be restricted based on a need to know
- Sensitive labels often reflect classification levels of data and clearances granted to individuals

Three Different MACS:

1) MAC (Media Access Control) Addresses: the physical address assigned to network interface cards (NICs)
2) MAC (Mandatory Access Control) Scheme: discussed later
3) MAC (Message Authenticating Code): provides integrity similar to how a hash is used

The ABAC (Attribute-Based Access Control) Scheme uses attributes defined in policies to grant access to resources

- Sets and enforces policies based on characteristics such as department, location, manager, time of day
- It's commonly used in software-defined networks (SDN)

Policies in ABAC system control the traffic instead of rules on physical routers

- Ex: "allow logged-on researchers to access research sites via the main network
- Policy Statements have 4 elements:
    - Subject (user)
    - Object (resource)
    - Action
    - Environment (everything outside of subject and object)

**Token Key that is connected to a server in organization that releases continuous one-time password for quick and secure authentication to resources distributed by particular server

VIP Access by Symantec is the mobile app version!

SMS
FRR (False Rejection Rate): identifies the percentage of times false rejection occurs
FAR (False Acceptance Rate): identifies the percentage of times false acceptance occurs
CER (Crossover Error Rate): indicates the biometric systems' ability or the system's efficacy rate

- Lower CERs are better

TPM (Trusted Platform Module): chip attached to motherboard for generating and keep safe cryptographic keys
HSM: similar to TPM but it is removable from hardware
Generic account
Shared account

Somewhere you are: geolocation, computer name, MAC address
Kerberos used for SSO authentication in Microsoft and Unix

Conditional Access: similar to ABAC:

- User or group membership: users in Nuclear Group may be allowed but no one else
- IP Location restriction
- Device: only allow desktop PCs but nothing else

HMAC (Hash-Based Message Authentication Code): uses hash function and cryptographic key
HOTP (HMAC-based One-Time Password
TOTP(Time-Based One-Time Password)

HOTP and TOTP are open source standards used to create one-time-use passwords

- HOTP creates a one-time-use password that does not expire until it is used
- TOTP creates a one-time password that expires after 30 seconds
- Both can be used as software tokens for authentication

END OF CHAPTER 2

Chapter 3: Exploring Network Technologies and Tools

Poisoning Attack: many protocols store data in cache for temporary access, poisoning attacks attempt to corrupt the cache with different data

Data Link Layer of OSI (Open Systems Interconnection): responsible for ensuring that data is transmitted to specific devices on the network

- It formats the data into frames and adds a header that includes MAC Address for the source and destination device
- Layer 2 also includes ARPs
- Layer 2 Attacks attempt to exploit vulnerabilities in MAC Address and ARP

Basic Networking Protocols

- TCP (Transmission Control Protocol): connection-oriented 3-way handshake
- UDP (User Datagram Protocol): connectionless (no-3-way handshake)
- IP (Internet Protocol): identifies hosts in network
- ICMP (Internet Control Message Protocol): tests basic connectivity (includes ping, pathping and tracert tool)
- ARP (resolves IPv4 addresses to MAC Address)

UDP most commonly used instead of TCP for void and video streaming

RTP (Real-Time Transport Protocol): delivers audio and video over IP Networks
SRTP (Secure Real-Time Transport Protocol): delivers secure, encrypted RTP
SIP (Session Initiation Protocol): used to initiate, maintain, and terminate voice, video and messaging sessions

- SIP (Session Initiation Protocol) used to initiate, maintain, terminate voice, video messaging sessions)

Secure Shell (SSH) encrypts traffic over TCP port 22 and is used to transfer encrypted files over a network (Communication)

- Transport Layer Security (TLS) is a replacement for SSL and is used to encrypt many different protocols, including browser-based connections using HTTPS
- Secure FTP(File Transfer Protocol) (SFTP) uses SSH to encrypt traffic
- SFTP uses TLS to encrypt traffic

**TLS replaced SSL

Protocols For Transferring Data over Network:

FTP (File Transfer Protocol): uploads and downloads large files to and from an FTP server

- By default, transmits data in cleartext
- Uses TCP port 21 for control signals
- Uses TCP port 20 for data

TFTP (Trivial File Transfer Protocol): uses UDP port 69 and is used to transfer smaller amount of data, such as when communicating with network devise

- Commonly disabled, not widely used

Encryption Protocols:

SSH (Secure Shell): encrypts traffic in transit and can be used to encrypt other protocols such as FTP

SSL (Secure Socket Layer): the primary method used to secure HTTP traffic as HTTPS

- Can encrypt SMTP and LDAP
- Can be compromised, so not endorsed

TLS (Transport Layer Security): the designated replacement for SSL and should be used instead of SSL for browser using HTTPS

- STARTTLS: command used to upgrade unencrypted connection to an encrypted connection on the same port

IPsec (Internet Protocol Security): used to encrypt IP traffic

- Encapsulates and encrypt IP packet payloads and uses **tunnel mode** to protect VPN traffic

SFTP (Secure File Transfer Protocol): secure implementation of FTP

- Extension of SSH, using SSH to transmit file in an encrypted format
- Uses TCP port 22

FTPS (File Transfer Protocol Secure): an extension of FTP and uses TLC to encrypt FTP traffic

- NOTICE:
  - SFTP uses SSH
  - FTPS uses TLS

STARTTLS: instead of using one port to transmit data in cleartext and a second port to transmit data in ciphertext, STARTTLS allows the protocol to use the same port for both

Email Protocols:

SMTP (Secure Message Transfer Protocol), POP3 (Post-Office Protocol), and IMAP4 (internet message access protocol) are primary email protocols

- Well known ports for encrypted and unencrypted traffic (respectively):
    - SMTP uses ports 25 and 587
    - POP3 uses ports 110 and 995
    - IMAP4 uses ports 143 and 993
    - HTTP and HTTPS uses ports 80 and 443

Directory Services, such as Microsoft Active Directory Domain Service (AD DS), provide authentication services for a network

- AD DS uses LDAP, encrypted with TLS (Transport Layer Security) when querying the directory
- LDAP (Lightweight Directory Access Protocol): specifies the formats and methods used to query directories such as AD DS

Domain Controller/Server: server that responds to authentication requests and verifies users on computer networks

Administrators connect to servers remotely using protocols such as SSH and the RDP (Remote Desktop Protocol)

- In some cases, admins use VPN to connect to remote systems

OpenSSH is a suite of tools that simplify the use of SSH to connect to remote servers securely

- The **ssh-keygen** command creates a public/private key pair
- **Ssh-copy-id** command copies the public key to a remote server
- The private key should always stay private

Time Synchronization

NTP (Network Time Protocol): used for time synchronization for a network
SNTP (Simple NTP): not as precise as NTP

DHCP

DHCP (Dynamically Host Configuration Protocol): used to dynamically assign IP Addresses to Hosts

DHCP Snooping: prevent unauthorized DHCP servers (rogue DHCP servers) from operating on a network

- Sounds malicious, but actually preventative measure

Four Steps:

1) DHCP Discovery: DHCP client broadcasts message asking DHCP for lease
2) DHCP Offer: DHCP server answers, offering lease
3) DHCP Request: DHCP client responds by requesting the offered lease
4) DHCP Acknowledge: DHCP allocates the offered IP Address to DHCP client

Private Networks:

- 10.0.0.0
- 172.16.0.0
- 192.168.0.0

DNS (Domain Name System): used for domain name resolution

- DNS resolves hostnames to IP Address

DNS Servers host data in zones (databases)

- Zones include multiple records

DNS Zones includes records such as:

- A Records: for IPv4 Addresses
- AAAA Records: for IPv6 Addresses
- MX Records: identify mail servers and the one with lowest preference is the primary mail server

DNS uses TCP port 53 for zone transfers
DNS uses UDP port 53 for DNS client queries
DNSSEC adds RRSIG (Resource Record Signature), which provides data integrity and authentication and helps prevent DNS poisoning attacks

DNS Poisoning (DNS Cache Poisoning): when attackers successfully modify the DNS cache with a bogus IP Address to a malicious website

- Countermeasure: DNSSEC (Domain Name System Security Extension)-RRSIG
    - A suite of extensions to DNS that validate DNS responses

Nslookup (Name Server Lookup): used troubleshoot problems related to DNS

- You can look up if a DNS Server can resolve specific hostname and FQDNs (Fully Qualified Domain Name) to an IP Address

Dig: command-line-tool that replaces nslookup in linux systems

- Dig is the linux version of nslookup (Windows)

Nslookup and dig are two command-line tools used to test DNS

- Microsoft systems include nslookup and Linux systems include dig
- The can be used to query specific records such as mail servers
- When a system has multiple mail servers, the lowest number preference identifies the primary mail server

Quality of Service (QoS): refers to the technologies running on a network that measure and control different types

- It allows admins to prioritize certain types of traffic over other types of traffic
- Ex) gaming stream may not be as prioritized as VoIP

Unicast: one-to-one traffic

- One host sends traffic to another host using a destination IP Address
- Other hosts may see the packet, but wont process b/c it isn't addressed to them

Broadcast: one-to-all traffic

- one host sends traffic to all other hosts on the subnet, using broadcast address such as 255.255.255.255

Port Security includes disabling unused ports and limiting the number of MAC Addresses per port

- a more advanced implementation to restrict each physical port to only a single specific MAC Address

Broadcast storm and loop prevention such as STP (Spanning Tree Protocol) or RSTP (Rapid STP) is necessary to protect against switching loop problems, such as those caused when two ports of a switch are connected together

STP and RSTP provide:

- broadcast storm prevention for switches
- loop prevention for switches

BPDU (Bridge Protocol Data Unit)

- STP sends BPDU messages in a network to detect loops
- When loops are detected, STP shuts down or blocks traffic from switch ports sending redundant traffic

Edge port: a switch port connected to a device, such as a computer, server, or printer

Implicit deny: in the context of ACLs, it indicates that all traffic that isn't explicitly allowed is implicitly denied

Routers and stateless firewalls (or packet-filtering firewalls) perform basic filtering with an ACL (Access Control List)

- ACLs identify what traffic is allowed and what traffic is blocked
- An ACL can control traffic based on networks, subnets, IP Addresses, ports and some protocols
- Implicit deny blocks all access that has not been explicitly granted
- Routers and firewalls use implicit deny as the last rule in the access control list

ACLs on Routers can filter:

- IP Addresses and Networks
- Ports
- Protocol Numbers (ex. During an attack ICMP protocol 50 blocked)

Default Gateway: the IP Address of a router on a network and typically provides a path to the internet

Firewalls: filter incoming and outgoing traffic for a single host or network

Host-Based Firewalls

- Servers or workstations use this
- Monitors traffic passing through the NIC and can prevent intrusions into the computer via the NIC

Network-Based Firewall is usually a dedicated hardware system with additional software installed to monitor, filter, and log traffic

- Usually have two NICs

Host-Based Firewalls provide protection for individual hosts, such as servers or workstations

- A host-based firewall provides intrusion protection for the host
- Linux systems support xtables for firewall capabilities
- Network-based firewalls are often dedicated servers and provide protection for the network

Stateless Firewall

- Based off ACL to identify allowed and blocked traffic
- Uses implicit deny to block traffic
- Rules Look Like:
    - Permission: PERMIT/ALLOW/DENY
    - Protocol: TCP or UDP
    - Source: IP Address
    - Destination: IP Address
    - Port/Protocol

Firewalls use a denyanyany, denyany, or a dropallstatement at the end of the ACL to enforce an implicit deny strategy

- The statement forces the firewall to block any traffic that wasn't previously allowed in the ACL
- The implicit deny strategy provides a secure starting point for a firewall

Stateful Firewall

- Inspects traffic and makes decisions based on the traffic context or state
- Keeps track of established sessions
- Common Issue: if ACL misconfigured, it can allow almost all traffic into the traffic (ex. If ACL doesn't include an implicit deny rule)

Web Application Firewall (WAF)

- Designed to protect web applications (A web server hosts the web application)
- You need WAF AND network-based firewall, not completely secure on own

A stateless firewall blocks traffic using an ACL, and a stateful firewall blocks traffic based on the state of the packet within the session

- Web application firewalls (WAF) provide strong protection for web servers
- They protect against several different types of attacks, focusing on web application attacks

Intranet = internal network

- Peoples use the intranet to communicate and share content with each other

Extranet = part of network that can be accessed by authorized entities outside of the network

Network perimeter: provides a boundary between the intranet and internet

A screened subnet (DMZ-Demilitarized Zone) is a buffer zone between the internet and intranet network

- It allows access to services while segmenting access to the internal network
- In other words, internet clients can access the services hosted on servers in the screened subnet, but the screened subnet provides a layer protection for the intranet (internal network)

Network Address Translation Gateway (NAT)

- Protocol that translates Public IP Addresses to Private IP Addresses and Private Addresses back to Public IP Addresses
- A common form of NAT is Port Address Translation (PAT), network address and port translation
- Dynamic NAT uses multiple public IP Addresses, while static NAT uses a single public IP Address

Red networks = classified
Black networks = unclassified

An air gap isolates one network from another by ensuring there is physical space (literally a gap of air) between all systems and cables

- Physical isolation ensures that one network isn't connected to another network
- SCADA (Supervisory Control and Data Acquisition) Systems typically are industrial control systems for power plants and water treatment facilities
- SCADA operate in their own network, and are isolated from any other network

VLANs (Virtual Local Area Networks) separate or segment traffic on physical networks, and you can create multiple VLANs with a single Layer 3 switch

- A VLAN can logically group several different computers together or logciallly separate computers without regard to their physical location
- VLANS are also used to separate traffic types, such as voice traffic on one VLAN and data traffic on a separate VLAN

East-West Traffic

- Refers to traffic between servers
- On diagrams, servers are shown horizontally

North-South Traffic

- Refers to traffic between clients and servers
- On diagrams, clients are shown above and below servers

<u>Proxy Server (Forward Proxy Servers)</u>

- Forward requests for services from clients within an organization to the internet, retrieves the contents from the internet, and then returns the data to the client
- Most proxy servers act as proxy for HTTPS and HTTP services
- Proxy located on edge of network, bordering the internet and the intranet
- When internet request received, it stores the data (cache) so next time the request is made, it doesn't' have to request from internet
- Cache = temporary storage

Transparent proxy: will accept and forward requests without modifying them

- Simplest to setup and it provides caching

Non-Transparent proxy: can modify or filter requests

- Often used by organizations to restrict what employees can access with URL

Regular proxy:

- Sits in front of client

Reverse Proxy: accepts requests from the internet, typically for a single web server

- Protects web servers
- Sits in front of webserver and caches

A proxy server forwards requests for services from a client

- It provides caching to improve performance and reduce Internet bandwidth usage
- Transparent proxy servers accept and forward requests without modifying them

- Non-transparent proxy servers use URL filters to restrict access to certain sites
- Both types can log user activity

Unified Threat Management (UTM) vs Firewall

A UTM appliance combines multiple security controls into a single appliance
- They can inspect data streams and often include URL filtering, malware inspection, and content inspection componenets
- - many UTMs include a DDoS mitigator to block DDoS attakcs

Common Issue: misconfigured content filter can accept too much spam or block legitimate packets

Jump Server (Jump Box)

A Jump Server is placed between different security zones and provides secure access from devices in one zone to devices in the other zone
- It can provide secure access to devices in a screened subnet from an internal network

- Admins can use a jump server to access servers in a screened subnet through the jump server

SNMP (Simple Network Management Protocol Version 3)

Administrators use SNMPv3 to manage and monitor network devices, and SNMP uses UDP ports 161 and 162
- SNMPV3 encrypts credentials before sending them over the network and is more secure than earlier versions

**SNMP used to easily check up on the network devices (routers, switches, firewalls etc.) to assess their functionality

---

END OF CHAPTER 3

Chapter 4: Securing the Network

IDS: monitor networks and send alerts to admin when suspicious events arise in the network
IPS: react to attacks in progress and prevent them from reaching systems and networks

HIDS (Host-Based Intrusion Detection System): can monitor all traffic on a single host system such as a server or a workstation

- In some cases, it can detect malicious activity missed by antivirus software, which is why many organizations install it on every workstation as an extra layer of security
- HIDS can also monitor some applications and protect local resources such as operating system file
- HIDS can monitor network traffic reaching its NIC and the network's traffic

- **IDS can detect malicious activity that passes anti-virus software

NIDS (Network-Based Intrusion Detection System Sensors/or Collectors) console is installed on a network appliance

- Sensors are installed on network devices such as switches, routers, or firewalls to monitor network traffic and detect network-based attacks
- It can also use taps or port mirrors to capture traffic
- A NIDS CANT monitor encrypted traffic and CANT monitor traffic on individual hosts

NIDS are sensors/or collectors that admins install on network devices such as switches, routers, or firewalls

- These sensors gather information and report to a central monitoring network appliance hosting a NIDS console
- CANT detect anomalies on individual systems or workstations unless causing significant difference in network traffic

Port Tap/Mirroring/Spanning: allows admins to configure the switch to send all traffic the switch receives to a single port

- This can be then used as a tap to send all switch data to a sensor or collector and forward this to a NIDS console

Signature-Based Detection: IDS use a database of known vulnerabilities or attack patterns
Heuristic/Behavioural-Based Detection: uses a normal operating network condition as a baseline, and when it detect abnormal activity to that baseline, it sends off an alert

- Effective Against Zero-Day Attacks

SYN Attack: like a friend extending his hand shake with you, you extending your hand in response, and then at the last moment, the friend pulls his hand away

- After a while you'll stop attempting to handshake if they keep pulling away, but not a computer
- In a SYN attack, the attacker sends multiple SYN attacks but never follows through with the third (last) step of sending the ACK packet, leading to open connections for the server which can ultimately disrupt services

IDS Aggregator: stores log entries from dissimilar systems

- IDS can analyze log entries to provide insight into trends
- These trends can detect a pattern of attacks and provide insight into improving a networks' protection

Signature-Based Detection Identifies issues based on known attacks or vulnerabitlies

- Signature-Based Detection Systems can detect known anomalies
- Heuristic or Behaviour-Based IDS (called anomaly-based) can detect unknown anomalies
- They start with a performance baseline of normal behavior and then compare network traffic against this baseline
- When traffic differs significantly from the baseline, the system sends an alert

A false positive incorrectly indicates an attack is occurring when an attack is not active

- A false positive increases admin workload
- A false negative is when an attack is occurring, but the system doesn't detect and report it
- Admins often set the IDS threshold high enough that it minimizes false positives, but low enough that it does not allow false negatives

IPS is placed inline (traffic passes through) with the traffic and can detect, react to, and prevent attacks

- IDS monitors and responds to an attack
- It is **NOT INLINE** but instead collects data passively (also known as out-of-band)

An intrusion prevention system (IPS) is a preventative control

- It is placed inline with traffic
- An IPS can actively monitor data streams, detect malicious content, and stop attacks in progress
- It can also be used internally to protect private networks

Honeypot: sweet-looking server to attackers

- Left open or appears to have been locked down sloppily, allowing an attacker relatively easy access
- Intent is to divert attacker from live network
- May contain bogus information such as fabricated credit card transaction data
- Used to gather intelligence on the attacker

Honeynet: group of honeypots in a separate network or zone, but accessible from an organization's primary network

- Created by organizations using multiple virtual servers contained within a single physical server
- Servers act as honeypots, and the honeynet mimics the functionality of a live network

Honeypots and honeynets attempt to deceive attackers and disrupt attackers

- They divert attackers from live networks and allow security personnel to observe current methodologies attackers are using
- A honeyfile is a file with a name that will attract the attacker's attention (password.txt)

Telemetry: collecting information such as statistical data and measurements and forwarding it to a centralized system for processing

Fake Telemetry: corrupts the data sent to monitoring system and can disrupt a system

Wireless Access Point (AP): connects wireless clients to a wired network

- May have routing capabilities as wireless routers

SSID (Service Set Identifier): the wireless network name that wireless networks are identified by

MAC filtering can restrict access to a wireless network to specific clients

- However, an attacker can use a sniffer to discover allowed MAC addresses and circumvent this form of network access control
- It's relatively simple for an attacker to spoof a MAC Address

MAC Cloning: refers to the process of changing the MAC address on a PC or other device, with the same MAC address as the WAN port on an Internet-facing router

- Or changing MAC Address to the MAC Address of an authorized system

A site survey examines the wireless environment to identify potential problem areas

- A heat map shows wireless coverage and dead spots if they exist

<u>Wireless footprinting</u>: gives you a detailed diagram of wireless access point, hotspots, and dead spots within an organization

Wi-fi Analyzer: identifies activity on channels within the wireless spectrum and analyze activity in 2.4GHz and 5GHz frequency ranges

Omnidirectional antennas: transmit and receive signals in all directions at the same time

- the most commonly used wireless antennas on both Aps and wireless devices

directional antenna: transmits signals in a single direction and receives signals back from the same direction

- has greater gain and can transmit signals over greater distances b/c focused on one direction

WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) were weak cryptographic protocols for wireless networks

- not used anymore b/c easy to exploit

WPA2: can operate in either open, pre-shared key (PSK), or Enterprise modes

- Open Mode: doesn't use any security
- PSK Mode: users access wireless network anonymously with PSK or passphrase, which supports authorization and not authentication (identifying ones identity via credentials)
- Enterprise Mode: forces uses to authenticate via credentials using 802.1X server

RADIUS server: you enter the IP addresses assigned to the 802.1X server
RADIUS port: you enter the port used by the RADIUS server

- The official default port for RADIUS is 1812 → must input same exact port used by server

Shared Secret: similar to user password, but not that

WPA-PSK uses a pre-shared key and does not provide individual authentication

- Open mode doesn't use any security and allows all users to access the AP
- Enterprise mode is more secure than Personal mode, and it provides strong authentication
- Enterprise mode uses an 802.1x server (implemented as a RADIUS server) to add authentication

WPA2 supports CCMP (based on AES) and replaced earlier wireless cryptographic protocols

- WPA3 uses Simultaneous Authentication of Equals (SAE) instead of a pre-shared key (PSK) used with WPA2

IEEE802.1X: port-based authentication protocol that requires users or devices to authenticate when they connect to a wireless access point or a specific physical port

- Prevents rogue devices from connecting to networks

Enterprise mode requires 802.1X servers

- EAP-FAST supports certificates
- PEP and EAP-TTLS require a certificate on the 802.1X server
- EAP-TLS also uses TLS, but it requires certificates on both 802.1X servers and each of the clients
- An 802.1X server provides port-based authentication, ensuring that only authorized clients cannot to a device or a network
- It prevents rogue devices from connecting

Captive portals: technical solution that forces clients using web browsers to complete a specific process before it allows them access to network

- Ex) free internet access requires accepting acknowledgment
- Ex) paid internet
- Ex) IEEE 802.1X Server

Disassociation attack effectively removes a wireless client from a wireless network, forcing it to reauthentication

- WPS allows users to easily configure a wireless device by entering an eight-digit PIN
- A WPS attack guesses all possible PINs until it finds the correct one
- It will typically discover the PIN within hours and use it to discover the passphrase

Wi-Fi Protected Setup (WPS): allows users to configure wireless devices without typing in the passphrase by entering short 8 digit pin or by sampling pressing button on router to connect automatically

- Makes process of connecting to router seamless, but has its obvious flaws

Rogue access points are often used to capture and exfiltrate data

- An evil twin is a rogue access point using the same SSID (or similar SSID) as a legitimate access point
- A secure AP blocks unauthorized users, but a rogue access point provides access to unauthorized users

In evil twin, attackers can use a Wireless Access Card in their laptop to act as an AP

- Site surveys by admins can help detect rogue, evil twin Aps

Jamming: type of DoS attack where attacker transmit noise or another radio signal on the same frequency used by a wireless network, interfering with wireless transmission and can seriously degrade performance

- To overcome, increase power levels of the AP
- Or to overcome, use different wireless channels

IV (Initialization Vector) Attacks: an IV is a number used by encryption systems

- Wireless IV attack attempt to discover the pre-shared key after first discovering the IV
- Some wireless protocols use IV by combining it with the pre-shared key to encrypt data in transit

(NFC) Near Field Communication: group of standards used by mobile devices that allow them to communicate with other mobile devices when they are close to them

- Primary indication of NFC attacks is unauthorized charges on credit card
- Attackers can use their own NFC readers to capture packets when two other devices are sharing with one another
- Airdrop
- Payment

RFID Attacks

- Radio-Frequency Identification (RFID) systems include an RFID reader and RFID tags placed on objects
- Used to track and manage inventory and assets, including objects and animals
- Tags don't have power source, they use electronics that allow them to collect and use power to transmits data stored on the device
    - Used for:
        - Sniffing or Eavesdropping: b/c RFID transmit data over air, attacker can collect it by listening → need to knoe RFID system's frequency and have a receiver tuned to that frequency
        - Replay:
        - DoS: jamming or flooding

Bluejacking is the unauthorized sending of text messages to a nearby Bluetooth device

- Bluesnarfing is the unauthorized access to, or theft of information from, a Bluetooth device
- Ensuring devices cannot be paired without manual user intervention prevents attacks, and placing them in Faraday cages will prevent pairing

BlueJacking vs BlueSnarfing
Wireless Replay Attack: attacker captures data sent between two entities, modifies it, and then attempts to impersonate one of the parties by replaying the data

War Driving: the practice of looking for a wireless network

- Attackers use war driving in large cities to look for networks with weak signals to exploit, using directional antennas
- Can be used by admins to detect rogue Aps or evil twins

War Flying: is the practice of war driving using private planes or drones

Administrators use war driving techniques as part of a wireless audit

- A wireless audit checks a wireless signal footprint, power levels, antenna placement, and encryption of wireless traffic
- Wireless audits using war driving can detect rogue access points and identify unauthorized users
- War flying is similar to war driving, but it uses planes or drones instead cars

A virtual private network (VPN) provides remote access to a private network via a public network

- VPN appliances are dedicated devices used for VPNs
- They include all the services needed to create a secure VPN supporting many clients

IPsec is a secure encryption protocol used with VPNs

- Encapsulating Security Payload (ESP) provides confidentiality, integrity, authentication (CIA) for VPN traffic
- IPsec uses Tunnel mode for VPN traffic and can be identified with protocol ID 50 for ESP
- It uses IKE over port 500
- A full tunnel encrypts all traffic after a user has connected to a VPN
- A split tunnel only encrypts traffic destined for the VPN's private network

RADIUS server used by Direct-Access VPN server to validate the credentials of a user across the internet that wants remote access

- The RADIUS server may use an LDAP server to validate credentials of user

Tunnel mode: encrypts the entire IP packet, including both the payload and the packet headers

- Benefit of tunnel mode is that its IP Address used within the internal network is encrypted and not visible to anyone who intercepts the traffic
- Attacker that sniffs packets can see the source IP address from client and destination address to the VPN server, but not the internal IP Address information (hidden)

Transport Mode: only encrypts payload and used in private networks, not VPNs

IPsec Provides Security in Two Ways:

1) Authentication: IPsec includes an Authentication Header (AH) to allow each of the IPsec conversation hosts to authenticate with each other before exchanging data
    - AH provides authentication and integrity, using port 51

2) Encryption: IPsec includes Encapsulating Security Payload (ESP) to encrypt the data and provide confidentiality
    - ESP includes AH so it provides CIA, using port 50

VPN Spit Tunnel: VPN admins determine what traffic should use the encrypted tunnel

- Ex) possible to configure the tunnel to only encrypt traffic going to private IP Addresses used in private network

VPN Full Tunnel: all traffic goes through encrypted tunnel while the user is connected to the VPN

L2TP (Layer 2 Tunneling Protocol): used in VPN for secure transport, but does not encrypt data

Network Access Control (NAC) includes methods to inspect clients for health (malware infection), such as having up-to-data antivirus software, and can restrict access of unhealthy clients to a remediation network

- You can use NAC for VPN clients and internal clients
- NAC uses agents (applications/services) to check health of clients
- These agents are downloaded onto the client PC and collects information, reporting back to the NAC system the results

PAP (Password Authentication Protocol) authentication uses a password or a PIN

- A significant weakness is that PAP sends the information across a network in cleartext, making it susceptible to sniffing attacks
- CHAP (Challenge Handshake Authentication Protocol) is more secure than PAP b/c doesn't send passwords over the network in cleartext

In CHAP, both client and server know a shared secret (similar to password) used in the authentication process

- Client hashes secret and combines it with a nonce (number used once) provided by server

RADIUS and TACACS+ provide centralized authentication

- RADIUS only encrypts the password by default, but can be used with EAP to encrypt entire sessions
- TACACS+ encrypts the entire session by default and can be used with Kerberos
    - Used for AAA

AAA Protocol

Authentication: verifies user identification
Authorization: determines if a users should have access
Accounting: tracks user access with logs

CHAP (Challenge Handshake Authentication Protocol) and PAP (Password Authentication Protocol) Authentication uses password/pin to authenticate

- CHAP secure by converting password/pin into ciphertext
- PAP not secure b/c done in plaintext

IPSEC uses AH + ESP to main security

- AH (Authentication Header): provides integrity and authentication between the two hosts before sharing the contents of the ESP payload (Encapsulated + Encrypted)

END OF CHAPTER 5

Chapter 5: Securing Hosts and Data

Virtualization: popular technology used in data centers that allow you to host one or more virtual systems, or virtual machines (VMs) on a single system

Hypervisor: software that creates, runs, and manages the VMs
- VMware, Oracle VM VirtualBox

Host: the physical system hosting the VM in the host

Guest: operating systems running on the host system are guests or guest machines

Host Scalability: refers to ability to resize the computing capacity of VM

Host Elasticity: refers to ability to dynamically change resources assigned to VM based on load

Container virtualization: runs services or applications within isolated containers or application cells
- Host's operating system or kernel run the service or app within each of the containers
- None of the services or apps can interfere with other containers and their apps/services

VM vs Container
- Container uses fewer resources and can be more efficient than VM hypervisor
- Con of Container: must use the operating system of the host
    - Ex) if host is running Linux, all containers must run Linux

VM Escape: allows an attacker to access the host system from within the virtual system
- Successful VM escape gives attacker unlimited control over host system and each virtual system within the host

VM Sprawl: occurs when an organization has many VMs that aren't' appropriately managed

Virtualization allows multiple virtual servers to operate on a single physical server providing increased cybersecurity resilience with lower operating costs
- Keeping systems up to date with current patches is the best protection from VM escape attacks

Virtual Machines are simply files and as a result, are easy to replicate or restore
VM Snapshot: provides you with a copy of a VM at a moment in time, which can be used as a backup

Persistent Virtual Desktop: changes can be made so next time user logs-in the changes are remain

Non-Persistent Virtual Desktop: you can make changes to VM, but as soon as you log off it goes back to baseline → used in organizations

Hardening: the practices of making an operating system (OS) or application more secure from its default installation → helps eliminate vulnerabilities from default configurations, misconfigurations, and weak configurations

A master image provides a secure starting point for systems

- Administrators sometimes create them with templates or with other tools to create a secure baseline
- They then use integrity measurements to discover when a system deviates from the baseline

Patch Management procedures ensure that operating systems, applications, and firmware are up to date with current patches

- This protects systems against known vulnerabilities
- Change management defines the process and accounting structure for handling modifications and upgrades
- The goals are to reduce risks related to unintended outages and provide documentation for all changes

Administrators often test updates in a sandbox environment such as a virtual machines

- A sandbox provides an isolated environment

Change Management Provides Two Keys:

1) To ensure changes to IT systems do not result in unintended outages
2) To provide an accounting structure or method to document all changes

An application approved list is a list of authorized software, and it prevents users from installing or running software that isn't on the list

- An application block list is a list of unauthorized software and prevents users from installing or running software on the list

Approved Lists (Whitelists)
Block Lists (Deny/Black Lists)

Allow List: list of applications authorized to run on a system
Block List: a list of applications the system blocks

Application Programming Interface (API): a software component that gives developers access to features or data within another application, a service, or an operating system

- Common for developers to user APIs with web applications, IoT devices and cloud-based services
- APIs are vulnerable to attacks

Ex) Amazon provides tracking data by using web service-based APIs provided by different shippers

To Prevent API Attacks:

a) Authentication: to prevent unauthorized access
b) Authorization:
c) Transport Level Security: API should use strong TLS when transferring any traffic over Internet

Microservices: code modules designed to do one thing really well
Ex) Amazon tracking ID will give you update on package

A self-encrypting Drive automatically encrypts and decrypts data on a drive without user intervention

- An Opal-compliant drive requires users to enter credentials to unlock the drive when booting the system

Boot Integrity: processes verify the integrity of the operating system and boot loading systems

- Can verify key operating system files haven't been changed

Measured boot: goes through enough of the boot process to perform these checks without allowing a user to interact with the system

- If it detects system has lost integrity and can no longer be trusted, system wont boot

BIOS (Basic Input/Output): hardware chip that executes software that provides computer with basic instructions on starting → runs basic checks, locates operating system, then boots

- Firmware

Firmware: combination of hardware and software
A Trusted Platform Module (TPM): hardware chip included on many laptops and mobile devices

- TPM **stores** cryptographic keys used for encryption

- It provides full disk encryption and supports a secure boot process and remote attestation
- TPM includes a unique RSA asymmetric key burned into the chip that provides a hardware root of trust
- TPM can generate, store, and protect other keys used for encrypting and decrypting disks

Boot Attestation: TPM captures signatures of key files used to boot the computer and store a report of the signatures securely within the TPM
Remote Attestation: TPM captures key signatures but sends to remote system for storage and checks when booting again for integrity

Attestation = “evidence or proof of something”

TPM has RSA private key for asymmetric encryption and can be used to support authentication

A Hardware Security Module (HSM) is a removable or external device that can generate, store, and manage RSA keys used in asymmetric encryption

- Many server-based applications use an HSM to protect keys
- A microSD HSM is an HSM device installed on a microSD chip and can be installed on any device with a microSD or SD slot

DLP (Data Loss Prevention): technique and technologies to prevent data loss

- Ex) blocking USB flash drives and control removeable media

Rights Management (Digital Rights Management): refers to the technologies used to provide copyright protection for copyrighted works

USB Data Blocker: prevents someone from writing any data to a USB drive

Data exfiltration is the unauthorized transfer of data out of a network

- Data Loss Prevention (DLP) techniques and technologies can block the use of USB devices to prevent data loss and monitor outgoing email traffic for unauthorized data transfer

The primary methods of protecting the confidentiality of data are with encryption and strong access controls

- Database column encryption protects individual fields within a database

Applications such as web-based email provided over the Internet are Software as a Service (SaaS) cloud-based technologies

- Platform as a Service (PaaS) provides customers with a fully managed platform, including hardware, operating systems, and limited applications
- The vendor keeps systems up to date with current patches

Infrastructure as a Service (IaaS) provides customers with access to hardware in a self-managed platform

- Anything as a Service (XaaS) refers to cloud-based services other than SaaS, PaaS, or IaaS
    - Includes services such as communications, databases, desketops, storage, security, and more
    - CSP typically manages all the resources keeping everything operational and up to date
    - Information Technology (IT) as a service is another way of thinking XaaS

Private Clouds are only available for one organization

- Third-Party companies provide public cloud services, and public cloud services are available to anyone
- Two or more organizations with shared concerns can share a community cloud
- A hybrid cloud is a combination of two or more clouds

A Managed Security Service Provider (MSSP) is a third-party vendor that provides security services for an organization

- A Managed Service Provider (MSP) provides an IT services needed by an organization, including security services provided by an MSSP

CSP Responsibilities

SaaS: Data, applications, runtime, middleware, OS, virtualization, servers, storage, networking
PaaS: customer responsible for data and applications
IaaS: customer responsible for Data, Applications, Runtime, Middleware, OS

On-Premise: organization has complete control over cloud-based resources and security implementations

- Know exactly where data stored

Off-Premise: CSP stores data and organization not sure exactly where it is

- Affects organization's ability to protect the CIA of their data

Cloud-Access Security Broker (CASB): software tool or service deployed between an organization's network and CSP

- Provides security by monitoring traffic and enforcing security policies

A Cloud-Based DLP can enforce security policies for data stored in the cloud, such as ensuring that Personally Identifiable Information (PII) is encrypted

A cloud access security broker (CASB) is a software tool or service deployed between an organization's network and the cloud provider
- It provides security by monitoring traffic and enforcing security policies
- Next-Generation Secure Gateway (SWG) provides proxy services for traffic from clients to Internet sites, such as filtering URLs and scanning for malware

Next-Generation Secure Gateway (SWG): a combination of a proxy server and stateless firewall

Software-Defining Network (SDN): uses virtualization technologies (APIs) to route traffic instead of using hardware routers and switches

Routers uses OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol) to help route traffic
- SDN can use these protocols as well

SDV (Software-Defined Visibility)
- Refers to technologies used to view all network traffic
- Ensures all traffic is viewable and can be analyzed

Edge Computing: the practice of storing and processing data close to the device
- Ex) car detects obstacle and stops immediately using ultrasonic sensors

Cloud Security Alliance (CSA): promotes best practices related to cloud

Corporate-Owned Personally Enabled (COPE) devices are owned by the organization, but employees can use them for personal reasons
- A bring your own device (BYOD) policy allows employees to connect their own personal devices to the corporate network
- A choose your own device (CYOD) policy includes a list of provided devices that employees can purchase and connect to the network
- Corporate Owned Policy: organization purchases devices and issues them to employees

Infrared Connection: line-of-sight wireless technology used by TV remotes

Ad Hoc Network: wireless devices connect to each other without an AP
Ad Hoc: latin for "as needed"

Mobile Device Management (MDM) tools help enforce security policies on mobile devices

- This includes the use of storage segmentation, containerization, and full device encryption to protect data
- Containerization is useful when using the BYOD model
- They also include enforcing strong authentication methods to prevent unauthorized access

Unified Endpoint Management (UEM): ensure systems are kept up to date with current patches, have antivirus software installed with up-to-date definitions, and are secured using standard security practices

Remote wipe sends a signal to a lost or stolen device to erase all data

- Geolocation uses Global Positioning System (GPS) and can help locate 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 organization's property
- GPS tagging adds geographical data to files such as pictures
- Context-aware authentication uses multiple elements to authenticate a user and a mobile device

Jailbreaking removes all software restrictions from an Apple device

- Rooting modifies an Android device, giving users root-level access to the device
- Overwriting the firmware on an Android device with custom firmware is another way to root an Android device
- Sideloading is the process of installing software on an Android device from a source other than an authorized store

Tethering and mobile hotspots allow devices to access the Internet and bypass network controls

- Wi-Fi Direct is a standard that allows devices to connect without a wireless access point or wireless router
- MDM tools can block access to devices using tethering, mobile hotspot, or Wi-Fi Direct to access the Internet

In a hotspot, your phone acts somewhat as a router

Three Embedded Systems:

1) Field Programmable Gate Array (FPGA): programmable integrated circuit (IC) installed on a circuit board
- Starts off with no configurations, but when turned on, it transfers a configuration program from a configuration memory chip or external processer
- Memory chip os non-volatile flash memory, allowing it to retain the programming, even without power

2) Arduino: microcontroller board with its circuit board containing CPU, RAM, ROM (Read-Only Memory)
- Doesn't need OS, b/c it uses firmware
- Used mainly for simple repetitive tasks
- Ex) monitor temperature, and show results using LED light

3) Raspberry Pi: microprocessor-based mini-computer
- Uses Raspberry Pi OS to run
- More extensive capabilities than Arduino
- Ex) instead of just monitoring and displaying temperature, it can send signals to (HVAC) systems to control temperature

A supervisory control and data acquisition (SCADA) system has embedded systems that control an industrial control system (ICS) such as one used in power plant or water treatment facilities
- Embedded systems are also used for many special purposes, such as medical devices, automotive vehicles, aircraft and unmanned aerial vehicles (UAVs)

System on a chip (SoC): an integrated circuit that includes all the functionality of a computing system within the hardware
- Typically contains an application contained within onboard memory, such as read-only memory (ROM), electrically erasable programmble ROM (EEOROM), or flash memory
- Many mobile computing devices have SoC

An embedded system is any device that has a dedicated function and uses a computer system to perform that function
- It includes any devices in the Internet of Things (IoT) category, such as wearables and home automation system
- Some embedded systems use a system on a chip (SoC)

Communication Considerations

a) 5G
b) Narrow-Band: narrow band signals have a very narrow frequency range
    - Commonly used in two-way radio systems such as walkie-talkies
c) Baseband Radio: include frequencies that are very near zero
    - Used when transferring data over a cable rather than over air
d) Subscriber Identity Module (SIM) Card: mobile devices with internet capabilities use SIM cards to connect with cellular provider
    - SIM card has a unique serial number
        - User pays a subscription fee for access, and the cellular provider grants access as long as the SIM card's serial number matches a valid account
e) Zigbee: suit of communication protocols used for smaller networks
    - Designed to be simpler to use and cheaper than other wireless protocols
    - Relatively low data rate, low power consumption, strong security, including data encryption
    - Battery life of two years or more

Infrastructures as code: refers to managing and provisioning data centers with code to define VMs and virtual networks

- Reduces complexity of creating virtual objects by allowing admins to run a script to create them

---

END OF CHAPTER 5

Chapter 6: Threats Vulnerabilities, Common Attacks

Advanced Persistent Threat (APT) refers to an organized and sophisticated group of threat actors
- Nation-states (governments) sponsor them and give them specific targets and goals
- Criminal syndicates are groups of individuals involved in crime and their primary motivation is money

APT members = “state actors”

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

A script kiddie is an attacker who uses existing computer scripts or code to launch attacks
- Script kiddies typically have very little expertise, sophisitication, and funding
- A hacktivist launches attacks as part of an activist movement or to further a cause
- An insider is anyone who has legitimate access to an organization’s internal resources, such as an employee of a compney
- DLP solutions can prevent users from writing data to external media devices

Two Successful and Common Attack Vectors:
- Email
- Social Media

Shadow IT refers to unauthorized systems or applications installed on a network without authorization or approval

A logic bomb executes in response to an event, such as when a specific application is executed, or a specific time arrives

A backdoor provides another way to access a system
- Many types of malware create backdoors, allowing attackers to access systems from remote location
- Employees have also created backdoors in applications and systems

Malware includes a wide variety of malicious code, including viruses, worms, Trojans, ransomware, and more

- A virus is malicious code that attaches itself to an application and runs when the application is started
- A worm is self-replicating and doesn't need user interaction to run

Rogueware = scareware

A Trojan appears to be something useful but includes a malicous component, such as installing a backdoor on a user's system

- Many Trojans are delivered via drive-by downloads
- They can also infect systems from fake antivirus software, pirated software, games, and browser extensions

Drive-By Download Step:

1) Attacker compromises a website to gain control of it
2) Attackers install a Trojan embedded in the website's code
3) Attackers attempt to trick users into visiting the site → sometimes they simply send the link to thousands of users via email, hopting that some of the click the link
4) When a user visit, the website attempts to download the trojan onto the users' system

Remote Access Trojan (RAT)

- Allows attackers to control systems from remote locations
- - often delivered via drive-by-downloads, or malicious attatchments on emails
- Some RATs automatically collect log keystrokes, usernames, passwords, incoming and outgoing email, chat sessions, browser history, screenshots

Keylogger: attempt to capture a user's keystrokes

- Keystrokes are stored in a file and either sent to an attacker immediately, or saved until the attacker retrieves the file

Keylogger can be thwarted by two-factor authentication

Keyloggers capture a user's keystrokes and store them in a file

- This file can be automatically sent to an attacker or manually retrieved depending on the keylogger
- Spyware monitors a user's computer and often includes a keylogger

Rootkits have system-level or kernel access and can modify system files and system access

- Rootkits hide their running processes to avoid detection with hooking techniques
- Tools that can inspect RAM can discover these hidden hooked processes

Botnets are groups of computers controlled by attackers, and computers in a botnet check in with command and control servers periodically for instructions

- Attackers frequently use botnets to launch DDoS attacks

Bot herder: the criminal behind the botnet (net of zombies)

Command-Control (C2): the zombies/malware try to connect to a C2 resource for instructions

<u>Types of Botnets:</u>

IRC (Internet Relay Chat) the bot herder provides C2 instructions
P2P (Peer-To-Peer) Botnets: the bots look for other infector computers and can act as C2 instructions

- Makes harder to shut down by law enforcement

Ransomware is a type of malware that takes control of a user's system or data

- Cryptomalware encrypts the user's data
- Criminals then attempt to extort payment from the victim
- Ransomware often includes threats of damaging a user's system or data if the victim does not pay the ransom, and attackers increasingly target hospitals, citiies, and other larger organizations

PUP (Potentially Unwanted Programs): programs that a user may not want, even if a user consented to download it

- Some of these unwanted programs are legitimate, but some are malicious, such as Trojans

7-zip is a popular compression tool, but using from any other site than the official may include PUPs

Fileless viruses (Fileless Malware) run in memory instead of from a file on a disk

- They are often scripts that are injected into legitimate programs
- They can also be hidden in vCards
- They are files written to disk

Techniques use by Filelesss Malware:

a) Memory Code Injection: malware injects code into legitimate applications using known and unpatched vulnerabilities in these applications
b) Script-based Techniques: two common examples are SamSam ransomware and Operation Cobalt Kitty
    - SamSam used encrypted code that is only decrypted when run, making it difficult to detect
    - Operation Cobalt Kitty used Powershell to target an organization for almost six months, starting with a spear-phishing email
c) Window Registry Manipulation: malware uses a Windows process to write and execute code into the Registry

vCard: file format used for electronic business cards

- Ex) used for business code with freedom of text
- So instead of exchanging business cards to build contact list, they send malware

Potential Indicators of Malware Attack:

- Extra traffic
- Data exfiltration
- ****Encrypted traffic**
- Traffic to specific IP
- Outgoing spam

Social engineering uses social tactics to trick users into giving up information or performing actions they wouldn't normally take

- Social engineering attacks ca occur in perons, over the phone, while surfing the Internet, and via email

A social engineer can gain unauthoruzed information just by looking over someone's shoulder

- This might be in person, such as when a user is at a computer or remotely using a camera
- Screen filters help prevent shoulder sufing by obscuring people's view unless they are directly in front of the monitor

Hoax: a message, often circulated through email, which tells of impending doom from a virus or other security threat that simply doesn't exist

Tailgating is a social engineering tactic that occurs when one user follows closely behind another user without using credentials

- Access control vesibules (sometimes called mantraps) allow only a single person to pass at a time
- Sophisticated mantraps can identify and authenticate indivdiulals befor allowing access
- Dumpster divers search through trash looking for information
- Shredding or burning papers instead of throwing them away mitigates this threat

Zero-day exploits take advantage of vulnerabilities that don't have available patches

- It could be b/c vendors don't know about the vulnerability or haven't written patches to fit it yet
- Zero-day exploits can evade up-to-date antivirus software

Zero-day vulnerability: a vulnerability or bug that is unknown to trusted sources, such as operating system and antivirus vendors

Typo Squatting (URL Hijacking): when someone buys a domain name that is close to a legitimate domain name for malicious purposes

Elicitation: act of getting information without asking for it directly

- Used in social engineering
    - Active listening
    - Reflecting questioning: demonstrates active listening and encourages target to talk more
    - False Statements: attacker gives false statement, hoping that victim corrects him
    - Bracketing: attackers get specific information by stating a specific number or range of numbers, hoping that victim tells them the exact precise number

Pretexting: added to the beginning of a conversation to make request more believable
Prepending: simply appending something to the beginning of something else

- Ex) [IMPORTANT} <Email Header>)

Hybrid warfare: military strategy that blends conventional warfare with unconventional methods to influence people (ex. Fake news)

- Battles aren't fought on battlefields alone

Spam: unwanted or unsolicited email

SPIM (Spam Over Instant Messaging): unwanted messages sent over instant messaging (IM) channels

Phishing: the practice of sending emails to users with the purpose of tricking them into revealing personal information or clicking on a link

Spam is unwanted email

- Phishing is malicious spam
- Attackers attempt to trick users into revealing sensitive or personal information or clicking on a link
- Links within email can also lead unsuspecting users to install malware

A spear phishing attack targets specific groups of users

- It could target employees within a company or customers of a company
- Digital signatures provide assurances to recipients about who sent an email and can reduce the success of spear phishing
- Whaling targets high-level executive or impersonates high-level executies

Voice over IP (VoIP) Technology: allows the attacker to spoof caller ID< making it appear as though the call came from a real company

Vishing is a form of phishing that uses the phone system or VoIP

- Some vishing attempts are fully automated
- Others start as automated calls, but an attacker takes over at some point during the call
- **Smishing** is a form of phishing using text messages

Drive-by-download installs itself on the user's computer without the user's knowledge

<u>Blocking Malware and Other Attacks:</u>

- Spam filter on mail gateway
- Anti-Malware software on mail gateways
- All systems have anti-malware software installed
- Boundaries or Firewalls

Spam filters: although they are good, companies will always be a little lenient and not too rigid b/c they don't want to block emails from legitimate sources, so some spam will still be passed through

Antivirus software detects and removes malware, such as viruses, Trojans, and worms

- Signature-based antivirus software detects known malware based on signature definitions
- Heuristic-based software detects previously unknown malware based on behaviour

Heuristic-Based Software: attempts to detect viruses that were previously unknown and do not have signatures

- Runs questionable code in a sandbox or virtualized environment specifically designed to protect the live environment while observing the code's behavior

Cuckoo Sandbox: open source automated software analysis system

- Its primary purpose is to analyze suspicious files, such as suspected malware
- You need to submit files to cuckoo sandbox, then it runs in a VM and creates a report on its activity

Many of the reasons that social engineers are effective are b/c they use psychology-based techniques to overcome users' objections

- These techniques include representing themselves as authority figures, using intimidation, faking scarcity, creating a sense of urgency, establishing familiarity, and creating a sense of trust

---

END OF CHAPTER 6

Chapter 7: Protecting Against Advanced Attacks

Kill Chain: military concept related to an attack

- It starts with the identification of a target, dispatching resources to the target, someone deciding to attack and giving the order, and it ends with the destruction of the target

Cyber Kill Chain (7 Steps):

1) Recon
2) Weaponization
3) Delivery
4) Exploitation
5) Installation
6) Command and Control (C2)
7) Actions on Objectives

<u>Diamond Model of Intrusion Analysis</u>

Intrusion Analysis Looks at Four Key Components for every Intrusion Event:

1) **Adversary**: adversaries identified by email addresses, handles in online forums, memberships in APT groups and other identification
2) **Capabilities**: refers to malware, exploits, and other hacker tools uses in the intrusion
3) **Infrastructure**: refers to the Internet domain names, email addresses, and IP Addresses used by adversary
4) **Victim:** identified by their names, email addresses, or network identifiers

Attack frameworks help cybersecurity professionals understand the tactics, techniques, and procedures used by attackers

- The cyber kill chain includes seven elements tracking an attack from reconnaissance to performing actions to achieve the attacker's objections
- The Diamond Model of Intrusion
- Analysis identifies four key components of every intrusion event
- MITRE ATT&CK is a matrix of ten tactics and techniques use to achieve each

A distributed denial-of-service (DDoS) attack is an attack from multiple computers against a single target

- DDoS attacks typically include sustained, abnormally high network traffic and usage of memory and processor time resulting in resource exhaustion
- In addition to network attacks, DDOS attacks can also impact applications and operational technology (OT) systems such as industrial control systems

Spoofing: occurs when one person or entity impersonates or masquerades as someone or something else

- Ex) email addresses, IP Addresses, MAC Addresses
- Often used to change the sender addresses to appear as a legitimate source for victim recipient

An on-path attack (also known as man-in-the-middle or man-in-the browser attack) is a form of active eavesdropping

- It captures data from two other computers in a session
- When secure channels are used, the on-path system may use certificates that aren't' issues by a CA and will generate certificate warnings
- SSH gives a warning if previously established keys have changed

Secure Socket Layer (SSL) Stripping: attacks a HTTPS connection to a HTTP connection

- HTTPS uses TLS instead of SSL, so you can think of this as TLS Stripping

Layer 2: transfers data frames between systems, and one of the primary protocols on this layer is the Address Resolution Protocol (ARP)

ARP poisoning attacks attempt to mislead systems about the actual MAC address of a system

- ARP poisoning is sometimes used in on-path attacks

ARP Cache: ARP memory for IP Addresses of each MAC Address in network

ARP Uses Two Primary Messages:

1) ARP Request: the ARP request broadcasts the IP address asking, "Who has this IP Address"
2) ARP Reply: the computer with IP Address in the ARP request responds with its MAC Address

- The computer that sent the ARP request, caches the MAC address for the IP
- Many OS that hear the ARP reply also cache the MAC Address

Vulnerability of ARP: very trusting, will trust any device that gives ARP reply

- Attacker can send an ARP reply with a bogus MAC address for the default gateway
- If all computers cache the bogus MAC Address for the default gateway, none of them can reach it, and it stops all traffic out of the network

MAC Flooding: an attack against a switch that attempts to overload it with different MAC addresses associated with each physical port causing its MAC Address table to overflow

- At some point, the switch runs out of memory to store all the MAC Addresses and enters a fail-open state

Countermeasure: switches have flood guards to limit the amount of memory used to store MAC Addresses for each port

- Sending alerts when near max

MAC Cloning: changing a system's MAC Address to another MAC Address

A DNS poisoning attack attempts to modify or corrupt DNS data

- **Pharming** is also an attack on DNS, and it manipulates the DNS name resolution process
- A primary indicator of both attacks is that a user tries to go to one website but is taken to a different website

In a domain hijacking attack, an attacker changes a domain name registration without permission from the owner

Domain reputation: helps ISPs determine the likelihood that an email is being sent by a legitimate organization

DNS sinkhole: a DNS server that gives incorrect results for one or more domain names

- With DNS sinkhole, you won't be able to reach the site of preference
- Investigative authority use DNS sinkholes to disrupt botnets and malware
- Infected computers frequently check in with command and control servers, and the malware includes the domain names of these servers
    - Authorities reverse engineer the malware to discover these domain names, and they coordinate the DNS owners to redirect traffic destined for these domain names

Replay attacks capture data in a session to impersonate one of the parties in the session

- Timestamps and sequence numbers are effective countermeasures against replay attacks

Secure Coding Concepts

OWASP (Open Web Application Security Project): non-profit foundation that is focused on improving the security of software

- Online community produces free documentation, tools, methodologies, technologies to improve web applications security

Code Reuse: saves time and helps prevent the introduction of new bugs

- Developers are encouraged to reuse code that is reputable already and vigorously tested
- Third-Party Libraries and Software Development Kits (SDKs)
    - Used in JavaScript for Web Development

Dead code: code that is never executed or used

- Logic error also creates dead code
    - Ex) if variable x has value of 12, it is squared, but if x is null, it returns an error and exits function

The lack of input validation is one of the most common security issues on web-based applications

- Input validation verifies the validity of inputted data before using it, and 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 injection, and cross-site scripting attacks

Code Sanitizer: programming tool that detects bugs in the form of undefined or suspicious behavior by a compiler/user inserting code at runtime

Race Condition: when two or more modules of an application, or two or more applications, attempt to access a resource at the same time

- Ex) buying plane, concert tickets at the same time
    - Countermeasure: locking selection for period of time

Time of Check to Time of Use (TOCTOU) Race Condition/ State Attack: this is when an attacker tries to race the operating system to do something malicious with data after the operating system verifies access is allowed, but before the operating system performs a legitimate action at the time of use

Error and exception handling helps protect the operating system's integrity and controls the error shown to users

- Applications should show generic error messages to users but log detailed information

Code Obfuscation: attempts to make code unreadable by changing simple variable names into xsdkf or something, where only the developer will understand

Compiler: converts code written in programming language into binary executable file

Cookies

- When user visits a website, the website creates a cookie and writes it to the user's system
- This cookie is a small text file and can include anything that web developers choose to write
- When user returns to website, the web application reads the cookie and uses it to enhance the user experience
    - Attacks can sometimes read cookie and exploit various vulnerabilities

Secure cookie: ensures cookie send only over secure HTTPS

Static code analysis examines the code without running it

- In a manual review, a developer goes through the code line by line, looking for vulnerabilities
- Dynamic code analysis checks the code while it is running
- **Fuzzing techniques** send random strings of data to applications looking for vulnerabilities

Secure Development Environment Stages

a) Development: software developers use isolated development environment to create the application
b) Test: testing environment doesn't simulate a full productive environment
c) Staging: simulates the production environment and is used for late-stage testing
    - Provides complete but independent copy of production environment
d) Production: application goes live as final product
e) Quality Assurance (QA): ongoing process used throughout software lifetime

A secure development environment includes multiple stages

- Stages are completed in separate nonproduction environments
- **Quality assurance methods are used in each of the stages

SQL (Structured Query Language): used to communicate with databases

- SQL statements read, insert, update, and delete data to and from a database
- Many websites use SQL to interact with database
- Database is often stored as tables with rows and columns

Normalization: organizing data tables and columns to reduce redundant data and improve overall database performance

Normalization is a process used to optimize databases

- While several normal forms are available, a database is considered normalized when it conforms to the first three normal forms:
    - First Normal Form (1NF):
        - Each row within a table is unique and identified with primary key
        - Related data is contained in a separate table
        - None of the columns include repeating groups
    - Second Normal Form:
        - Applies to tables that have a composite primary key, where two or more columns make up the full primary key
        - It is in 1NF
        - Non-primary key attributes are completely dependent on the composite primary key
    - Third Normal Form:
        - Helps eliminate unnecessary redundancies within a database
        - It is 2NF, this implies that it is also in 1NF
        - All columns that aren't primary keys are only dependent on the primary key

SQL Injection Attack: the attacker enters additional data into the webpage form to generate different SQL statements

Attackers use SQL injection attacks to pass queries to back-end databases through web servers

- Many SQL injection attacks use the phrase ' or '1'='1' to trick database server into providing information
- Input validation techniques and stored procedures help prevent SQL injection attacks

Stored Procedure: group of SQL statements that perform data validation of input SQL before it is executed on legitimate table to prevent potential SQL Attacks

- Mini-program

<u>Provisioning/Deprovisioning</u>

Provisioning: giving user accounts privileges
Deprovisioning: removing user account's privileges

Integrity measurement = quality of code and how extensively and effectively the code was tested throughout the development life cycle

Common Indicators of Malware Infections:

- You cant update system
- Antivirus software is disabled
- System runs slower than normal
- Internet traffic increases on its own
- Programs appear to start on their own
- A system randomly crashes or freezes
- Pop-ups or security warnings begin to appear
- Your browser home page or default search engine changes
- A ransom demand appears along with the inability to access data or a system

Powershell: Windows' task-based command line that uses cmdlets scripting language

Bash (Bourne-Again Shell): Unix's command line

PowerShell cmdlets use a verb-noun structure such as Invoke-Command

- Bash scripts typically call either /bin/bash or /bin/sh
- If logs show verb-noun cmdlets or calls to bash or sh, it may be a potential attack indicator

Macro: a short instruction that will run a longer set of instructions

- Useful at automating repetitive functions

VBA (Visual Basic for Applications): runs an internal programming language within Microsoft applications

- Disabled in Microsoft Office Applications b/c easy for attackers to create malicious macros and VBA

OpenSSL: software library used to implement SSL and TLS protocols

- Suit of tools that simplify SSH as well

SSH: used to connect remote systems

Zero-Day exploits are undocumented and unknown to the public

- The vendor might know about it but has not yet released a patch to address it
- The best indicator of a zero-day attack is erratic or unexpected behavior on an attacked system

Memory Leak: a bug in a computer application that causes the application to consume more and more memory the longer it runs

- Typically occurs with applications reserve memory for short-term use, but fail to release
- Can cause OS to crash

Buffer Overflow: occurs when an application receives more input, or different input, than it expects

- Result: error that exposes system memory that would otherwise be protected and inaccessible
- Normally application only has access to specific are of memory, the buffer
- Buffer overflow allows access to memory locations beyond the application's buffer, enabling an attacker to write malicious code into this memory area

Buffer overflows occur when an application receives more data than it can handle or receives unexpected data that exposes system memory

- Buffer overflow attacks often include NOP instructions (such as x90) followed by malicious code
- When successful, the attack causes the system to execute the malicious code
- Input validation helps prevent buffer overflow attacks

Reference/pointer = memory location of an object or variable
Deference = setting a reference/pointer to null for garbage collection

DLL (Dynamic Link Library) = compiled set of code that an application can use without re-creating code

- Ex) Math-based DLL → square root

DLL Injection: an attack that injects a DLL into a system's memory and causes it to run

- Attacker connects to DLL and then executes its malicious functions

LDAP (Lightweight Directory Access Protocol) Injection: specifies the formats and methods used to query databases of objects such as users, computers and other objects within a network

Directory Traversal: specific type of injection attack that attempts to access a file by including the full directory path or traversing the directory structure on a computer

Cross-Site Scripting (XSS) attacks: allows attackers to capture user information such as cookies

- Input validation techniques at the server help prevent XSS attacks
- Cross-Site Request Forgery Attacks often include a question mark to modify the URL

XSS: web application vulnerability that allows attackers to inject scripts into webpages

- Reflected XSS/Non-Persistent: attacker crafts malicious email and then encourages user to click it
    - Malicious URL is often placed within a phishing email, but could also be placed on a public website → link in comment section

- Stored XSS/Persistent: instead of user sending the malicious code to the server, it is stored in a database or other location trusted by web application
    - The web application can retrieve the malicious code later, such as when admin logs onto website

Cross-Site Request Forgery (XSRF/CSRF): an attacker where an attacker tricks a 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) link → clicking it goes straight to google and searches 'apples' without you having to enter and search apple manually

Server-Side Request Forgeries (SSRF): exploit how a server processes external information

- Some web applications read data from an external URL and use it when creating webpage
- If attacker can modify the external URL, they can potentially inject malicious code into the webpage

Client-Side Request Forgeries: if an attacker can inject code into the client-side webpage after server has crafted it and sent it to the user

- Common way is through cookies

Cross-Site Request Forgery (XSRF) scripting causes users to perform actions on websites, such as making purchases, without their knowledge

- In some cases, it allows an attacker to steal cookies and harvest passwords

Refactoring Code: process of rewriting the code's internal processing without changing its external behavior

- Usually done to correct problems related to software design

Shimming: provides the solution that makes it appear that older drives are compatible

AI vs Machine Learning (ML)

AI (Artificial Learning): intelligence that machines can demonstrate

- AI starts with basic machine learning techniques, but then expands itself by applying the knowledge to learn more and act on the new knowledge
- AI is like humans:
    - Learns what works and keeps doing it
    - Learns what doesn't work and stops doing it
    - Try new things

ML (Machine Learning): refers to technologies that help computer systems improve experience

ML is a part of AI, but AI is the broader umbrella

Adversarial AI: attempts to fool AI models by supplying it deceptive input

- Wrong rules etc.

Goal of AI Evolution is to be like or greater than humans…How:

- Ability to discover
- Ability to infer
- Ability to reason

Machine Learning (ML): involves predictions and decisions based on data

- Statistical analysis to come to decision
- The more data given, the more accurate decisions made
- Machine "Learning" → learns

Types of ML:

a) Supervised
    - More human involvement
b) Unsupervised
    - Find things not explicitly stated

Sub Field of ML = Deep Learning

Deep Learning:

- Involves things like neural networks, involve nodes and statistical relations between nodes to model the way our mind works

Visual Basic for Application: Window's native programming language used to create Windows Applications

- Disabled for Microsoft Office Applications => for obvious reasons

When Will AI Become Like Humans:

- Ability to discover
- Ability to infer
- Ability to reason

END OF CHAPTER 7

Chapter 8: Using Risk Management Tools

Risk: the likelihood that a threat will exploit a vulnerability
- Vulnerability = weakness
- Threat = potential danger
- Impact = magnitude of harm that can be caused if a threat exploits a vulnerability

Threats
- Malicious Human Threats
- Accidental Human Threats
- Environmental Threat

IP (Intellectual Property) Theft: includes things like copyright, patents, trademarks, trade secrets

Legacy System: any outdated computing system, hardware, or software that is still in use
- Vulnerable b/c vendor no longer develops patches to protect security of system/software

Multiparty = third-party

Vulnerabilities
- Default Configurations
- Lack of Malware Protection
- Improper/Weak Patches
- Lack of Firewalls
- Lack of Organizational Policies

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

Types of Risk:
- Risk Awareness: acknowledging that risk exists and addresses them via mitigation
- Inherent Risk: risks that exist before controls are in place to manage risk
- Residual Risk: amount of risk that remains after control are implemented
- Control Risk: the risk that exists if in-place controls do not adequately manage risks
- Risk Appetite: the amount of risk an organization is willing to accept

Risk Management Strategies:

- Avoidance: organization not providing a specific service or not participating in risky activity
- Mitigation: organization implements controls to reduce risk vulnerabilities or impact of threat
- Acceptance: when cost of control outweighs a risk
- Transference: organization transfers risk to another entity or at least shares the risk with another entity
- Cybersecurity Insurance: helps protect businesses and individuals from losses related to Cybersecurity incidents such as data breaches and network damage
    - Traditional insurance do not typically protect cybersecurity-related incidents

It is **not possible to eliminate risk**, but you can take steps to manage it

- An organization can avoid a risk by not providing a service or not participating in a risky activity
- Insurance transfers the risk to another entity
- You can mitigate risk by implementing controls, but when the cost of the controls exceeds the cost of the risk, an organization accepts the remaining, or residual risk

Risk Assessment: quantifies and qualifies risk

Risk Control Assessment: examines an organization's known risks and evaluates the effectiveness of in-place controls

Risk Control Self-Assessment: a risk control assessment conducted by employees

Quantitative Risk Assessment: measures the risk of using a specific monetary amount

- SLE (Single Loss Expectancy): the cost of any single loss
- ARO (Annual Rate of Occurrence): the ARO indicates how many times the loss will occur in a year
- ALE (Annual Loss Expectancy): the value of (SLE x ARO)

A quantitative risk assessment uses specific monetary amounts to identify cost and asset values

- The SLE identifies each loss's amount, the ARO identifies the number of failures in a year, and the ALE identifies the expected annual loss
- You calculate the ALE as SLE x ARO
- A qualitative risk assessment uses judgement to categorize risks based on the likelihood of occurrence and impact

A qualitative risk assessment: uses judgment to categorize risks based on the likelihood of occurrence (LOC)/probability of impact

- Ex) Low, Medium, High → but you can assign them as 1, 5, 10, respectively

Report: the final phase of risk assessment

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

A risk register is a comprehensive document listing known information about risks such as the risk owner

- It typically includes risk scores along with recommended security controls to reduce the risk scores
- A risk matrix plots risks onto a graph or chart, and a risk heat map uses color-coding to plot the risks

Supply chain: all the elements required to produce and sell a product

- Includes all the processes required to create and distribute a finished product

Threat Hunting: the process of actively looking for threats within a network before an automated tool detects and reports on the threat

- Important part of threat hunting is gathering data via threat intelligence to determine threat's capabilities, motives, goals, and resources

Threat feed: provides subscribers with up-to-date information on current threats
TTPs (Adversary Tactics, Techniques, Procedures): refers to attacker's method when exploiting a target

Threat Intelligence Fusion: combines all this data to create a picture of likely threats and risks for an organization

MD5: weak hash algorithm

Offline password cracker: using password databases (recovered-hash), to crack password
Online password cracker: using brute force to guess password

Password crackers attempt to discover passwords and can identify weak passwords, or poorly protected passwords

- Network scanners can detect all the hosts on a network, including the operating system and services or protocols running on each host

Service vs Port Scan

Service scan: similar to port scan, but it goes a step further, and verifies protocol or services used on a port

Port scan: checks for open ports on a system and gives hints about what protocols or services are running

OS Detection: analyzing IP Addresses to identify the OS

- Known as “TCP/IP Fingerprinting”

CVSS (Common Vulnerability Scoring System): 0-10

Common Vulnerabilities from Weak Configurations:

a) Open Ports and Services:
    - Open ports can signal a vulnerability
    - Ex) all web servers do not FTP, so if TCP port 20 and 21 are open, it indicates potential vulnerability

b) Unsecured Root Accounts
    - Weak admin passwords
c) Default Accounts and Passwords
d) Default Settings
e) Unpatched Systems
f) Open Permissions
g) Unsecure Protocols
h) Weak Encryption
i) Weak Password
j) Sensitive Data Sent Over Network

A vulnerability scanner can identify vulnerabilities, misconfigured systems, and the lack of security controls such as up-to-date patches

- Vulnerability scans are **passive** and have little impact on a system during a test
- In contrast, a pen-test is **intrusive** and can potentially compromise a system

A false positive from a vulnerability scan indicates that a scan detected a vulnerability, but the vulnerability doesn't exist

- Credentialed scans run under the context of a valid account and can get more detailed information on targets, such as the software versions of installed applications
- They are typically more accurate than non-credentialed scans and result in fewer false positives

A penetration system is an active test that can assess deployed security controls and determined the impact of a threat

- It starts with reconnaissance and then tries to exploit vulnerabilities by attacking or simulating an attack

Rules of Engagement: specifies the boundaries of a test before an individual is given to pen-test an organization for improving security

Reconnaissance/Footprinting: the pen-tester attempts to learn as much as possible about a network

-

a) Passive Recon: collects information about a targets system, network, or organization using OSINT
    - theHarvester→ CLI used for passive pentest
    - Passive Recon doesnt not use any tools to send information to targets and analyze the responses, however can include tools to gather infomraiton from systems other than the target

Recon Tools:

IP Scanner (Ping Scanner): searches a network for active IP Addresses

- Sends an ICMP ping to a range of IP Addresses in a network
- Firewalls can block ICMP packets

Nmap: network scanner from command prompt that identifies all the active hosts on a network, their IP Addressees, the protocols and services running on each of these hosts, and the host's operating system

Netcat (nc): CLI tool that admins use for remotely accessing Linux systems

- Banner Grabbing: identifying target's OS
- Can be used for transferring files and checking for open ports

Scanless: python CLI to perform port scans

- Uses an online website to perform scans so that scans don't come from attacker's IP address, but from the website's IP Address

Dnsenum: enumerates (lists) DNS records for domains (all DNS records for particular domain)

Nessus: vulnerability scanner

Hping: used to send pings using TCP, UDP, or ICMP

- Used to search for open ports on remote systems

Sn1per: robust automated scanner used for vulnerability assessments and to gather information on targets during pen testing

Curl (Client URL Command): used to transfer and retrieve data to and from servers such as web servers

Penetration tests include passive methods and active network reconnaissance and discovery methods

- Passive reconnaissance uses open source intelligence methods, such as social media and an organization's website
- Network reconnaissance and discovery methods use tools such as network scanners to gain information on the target

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

- Ex) Tester may enable SSH and create a method used to log on to a system using SSH

Attacker uses credentials to exploit a user's computer and then uses the compromised computer to move laterally

After exploiting a system, penetration testers use privilege escalation techniques to gain more access to target systems

- Pivoting is the process of using an exploited system to target other systems

Unknown environment testers have zero prior knowledge of a system prior to a penetration test (Black-Box Test)

- Known environment testers have full knowledge of the environment (White-Box), and partially-known environment testers have some knowledge (Gray-Box)

Cleanup: one of the last steps of pen-testing

- Includes removing all traces of a pen tester's activities
- Attackers should use a log to track their activity not rote memory

Bug Bounty: provides monetary incentive for security researchers to discover bugs, or vulnerabilities

A vulnerability scanner is passive and non-intrusive and has little impact on a system during a test

- In contrast, a pen test is active and intrusive, and can potentially compromise a system
- A pen-test is more invasive than a vulnerability scan

Red teams attack using known TTPs and blue teams defend against these attacks

- Members of the purple team can perform as either red team members or blue team members
- White team personnel set the rules and oversee testing

Packet Capture: refers to capturing network packets transmitted over a network
Packet Replay: refers to sending packets back out over the network

Protocol Analyzer/Sniffing: used to capture packets

- Can be used by admins or attackers to analyze and modify packet headers and their payloads
- They typically modify them before sending them back out as a packet replay

Administrators use a protocol analyzer to capture, display, and analyze packets sent over a network

- It is useful when troubleshooting communications problems between systems
- It is also useful to detect attacks that manipulate or fragment packets
- A capture shows information such as the type of traffic (protocol), flags, source and destination IP Addresses, and source and destination MAC Addresses
- The NIC must be configured to use promiscuous mode to capture all traffic

Tcpreplay: suite of utilities used to edit packet captures and then send the edited packets over the network

- Includes tcpreplay, prep, write and more

An admin can modify packets to mimic known attack and then send to IDS to test

Tcpdump Command: CLI protocol analyzer similar to wireshark (windows-based)

- Tcpdump in linux

NetFLow: feature available on routers and switches that collect IP traffic statistics and send them to NetFlow collector

- NetFlow collector receives the data and stores it, and analysis software on the NetFlow collector allows admins to view and analyze the network activity

Protocol Analyzer vs NetFlow

- Protocol analyzer allow you to capture and view all data, including headers and payloads of individual packets
- NetFlow doesn't include payload data and doesn't even include individual packet headers
    - Only records counts, or stats related to data device receives

NetFlow Data

- Timestamps identifying start and finish time of flow
- Input interface identifier (on router or switch)
- Out interface identifier (will be zero if a packet is dropped)
- Source information (source IP Address and port number)
- Destination information (destination IP address and port)
- Packet count and byte count
- Protocols (TCP, UDP, ICMP and any other Layer 3 Protocol)

Framework: provide guidance to professionals on how to implement security in various systems

ISO Standards:

ISO 27001: identifies requirements to become certified
ISO 27002: provides organizations with best practical guidance
ISO 27701: provides organizations with guidance to comply with global privacy standards, such as EU GDPR

SOC 2 Type 1: Type 1 Report describes an organization's systems and covers the design effectiveness of security controls on a specific data, such as March 30

- Design Effectiveness: how well the security controls address the risks, but not mitigate

SOC 2 Type 2: Type 2 Report describes an organization's systems and covers security controls' operational effectives over a range of dates, such as 12 months

- Operational Effectiveness: how well the security controls worked when mitigating risks during the range of dates
- Type 2 gives a higher level of assurance than SOC 2 Type 1

When using credit cards, a company would comply with the Payment Card Industry Data Security Standard (PCI DSS)

- Many organizations use the Risk Management Framework (RMF) and the Cybersecurity Framework (CMF) to identify and mitigate risks

Reference Architecture: a document or set of documents that provides a set of standards

IDS uses information from existing frameworks to detect attacks

Metasploit: has data on over 1600 exploits and includes methods to develop, test, and use exploit code

BeEF (Browser Exploitation Framework): focuses on identifying web browser vulnerabilities

- Successful attacks allow testers to launch attacks from within an exploited web browser

W3af (Web Application Attack and Audit Framework): focuses on web application vulnerabilities

- Goal is to find and exploit web application vulnerabilities and makes this information known to others

---

END OF CHAPTER 8

Chapter 9: Implementing Controls to Protect Assets

Physical security control: something you can physically touch, such as hardware lock, fence, identification badge, security camera

Many organizations use camouflage techniques (industrial camouflage)

- Used to hide buildings, parts of a building, and other items

Proximity card electronics:

- Contains a capacitor and coil that accepts charge from a proximity card reader
- When card comes close to reader, the reader excites the coil and stores a charge in the capacitor
- Once charged the card transmits the information to the reader using radio frequency

Proximity cards are credit card-sized access cards

- Users pass the card near a proximity card reader, and the card reader then reads data on the card
- Some access control points use proximity cards with PIN information

Door access systems include physical locks, cipher locks, and biometrics

- Physical locks can help prevent access to secure areas by unauthorized individuals
- Cable locks are effective threat deterrents for small equipment such as laptops and some workstations
- When used properly, they prevent losses due to theft of small equipment

Physical cipher lock: have four or five buttons labeled with numbers

- 1, 2, 3, 4

Manual cipher lock: requires user to manually twist the knob after entering the code

- May require two buttons pressed at the same time

Con: does not identify user and code can be given to anyone

Cable lock: lock a computer to a piece of furniture

- Most cable locks have a four-digit combo
- If you remove the cable lock without the combo, it will likely destroy the laptop

Two-person Integrity: a security control that requires the presence of at least two authorized individuals to perform a task

- For handling COMSEC (Communication Security) and keying material
- Keying Material: refers to materials used to encrypt and decrypt classified communication
- Two-person integrity prevents any individual person to access COMSEC keying material

Robot Sentries: move and record all activity by people entering and leaving

- Use laser light detection sensors and 3D mapping to learn and navigate the environment

Video surveillance provides reliable proof of a person's location and activity

- It can identify who enters and exits secure areas and can record theft of assets
- Many cameras include motion detection and object detection capabilities
- CCTV systems can be used as a compensating control in some situations

CCTV (Closed-Circuit Television) System: transmits signals from video camera to monitors that are similar to TVs

- Can also deter threats
- Records for playback
- Cameras can be connected to motion detection systems, turning on only when motion is detected

Sensors monitor the environment and can detect changes

- They can detect motion, noise, moisture, temperature changes, and more

Moisture detection: located within flood zones and use moisture detection methods to detect flood events allowing to turn on water pumps before water causes damage

Fencing, Lighting, and Alarms all provide physical security

- They are often used together to provide layered security
- Motion detection methods are also used with these methods to increase their effectiveness
- Infrared detectors detect movement by objects of different temperatures

Drones/Unmanned Aerial Vehicles (UAV): both a physical security method, but can also be a threat

Barricades provide stronger barriers than fences and attempt to deter attackers

- Bollards are effective barricades that can block vehicles

Effective Asset Management:

a) Architecture and Design Weaknesses: help reduce architecture and design weaknesses by ensuring purchases go through an approval process
b) System Sprawl and Undocumented Assets: system sprawl occurs when an organization has more systems than it needs, and the system it owns are underutilized
    - Asset management begins before hardware is purchased and helps prevent system sprawl by evaluating purchase

RFID (Radio-Frequency Identification) Methods can track movement of devices

- If someone doesn't pay, the RFID device transmits and sounds alarm

Defense in Depth ("Layered Security"): refers to the security practice of implementing several layers of protection

One way of applying layered security is diversity via different vendors, technologies, controls:

a) Vendor Diversity: the practice of implementing security controls from different vendors to increase security
    - If using two different firewalls and attack finds vulnerability in one, the other is still secure

b) Technology Diversity: the practice of using different technologies to protect an environment
    - Biometrics, CCTV, locks

c) Control Diversity: use of different security control types such as technical, physical, administrative controls
    - Technical controls: firewalls, IDS/IPS, proxy
    - Physical controls:
    - Administrative Controls: vulnerability testing, pen-testing

A faraday cage can be a large room or box, and it prevents signals from emanating beyond the enclosure

- An air gap is a physical security control that ensures that a network is physically isolated from other networks, including the internet

Hot and Cold Aisles: help regulate the cooling in data centers with multiple rows of cabinets

- The back of all the cabinets in one row faces the back of all the cabinets in an adjacent row
- B/c the hot air exits out of the back of the cabinet, the aisle with backs facing each other is the hot aisle
- Cool air is pumped through the floor to this cool aisle using perforated floor tiles in the raised flooring→ this is the cold aisle
    - in some designs, cold air is pumped through the base of the cabinets

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

- computer sees the USB as a human interface device (keyboard, mouse), allowing an attacker to send commands to computer

Malicious Flash Drive: includes malware configured to infect a computer when it is plugged into computer

Credit Card Skimming: practice of capturing credit card data at the point of sale

- allows the payment to go through, but also capture the credit card data

Card Cloning: making a copy of a credit card using data captured from a magnetic strip

- difficult to do b/c of chips in card that are encrypted

<u>Fire Components: Heat, Oxygen, Fuel, Chain Reaction</u>

Fire Extinguishers try to eliminate one of these:

Removing Heat: using chemical agents or water to remove the heat
Remove the Oxygen: using CO_2 to displace the oxygen → popular method b/c harmless to electrical equipement
Remove the Fuel: → not popular method
Disrupt the Chain Reaction: some chemicals can disrupt the chain reaction of fires to stop them

Also note, in case of fire, if card reader damaged, there is an alternative route to safety

<u>Protecting Cable Distribution</u>

- Cable Trough: long metal containers that make it inaccessible for attacker to manipulate wires
- Important to keep cables away from EMI (Electromagnetic Interference) source

Only Constant: Computers, subsystems and networks will fail

- Not a matter of “if” but rather “when”

Redundancy: adds duplication to critical system components and networks and provides fault tolerance

- If a critical component has a fault, the duplication allows the service to continue as if a fault never occurred

Fault tolerance: a system with fault tolerance can suffer a fault, but it can tolerate it and continue to operate

Organizations add redundancy to eliminate single point of failure (SPOF):

- Disk redundancies using RAID
- NIC redundancy with NIC teaming
- Server redundancies by adding load balancers
- Power redundancies by adding generators or an UPS
- Site redundancies by adding hot cold, or warm sites

A single point of failure (SPOF) is any component whose failure results in the failure of an entire system

- Elements such as RAID, load balancing, UPSs, and generators remove many single points of failure
- RAID is an inexpensive method used to add fault tolerance and increase availability
- If only one person knows how to perform specific tasks, that person can become a single point of failure (SPOF)

Examples of SPF:

a) Disk: if a server uses a single drive, the system will crash if the single drive fails
    - Redundant array of inexpensive disks (RAID) provide fault tolerance for hard drives and is a relatively inexpensive method of adding fault tolerance
b) Server: if a server provides a critical service and its failure halts the service, it is a SPF
    - Load balancing provides fault tolerance for critical servers
c) Power: if organization only has one source of power for critical systems, the power is SPF
    - Power generators and Uninterruptible power supplies (UPS) provide fault tolerance for power outages
d) Personnel: if there are tasks in organization that only one person can perform → the person is SPF

Any system has four primary resources: processor, memory, disk, network interface

- Disk is the slowest and most susceptible to failure

RAID (Redundant Array of Inexpensive Disks) Subsystem

- Provides fault tolerance for disks and increases system availability
- Even if disk fails, most RAID subsystems can tolerate the failure, and the system will continue to operate

RAID-0 (Striping)

- Doesn't provide any redundance or fault tolerance
- Includes two or more physical disks
- Files stored in RAID-0 are spread across each of the disks
- Benefit is increased read and write performance
- If you have three 500-GB drives, you have 1500 GB (1.5TB) of storage space

RAID-1 (Mirroring)

- Uses two disks
- Data written to one disk is also written to other disk
- If one disk fails, the other still has all the data
- Disk Duplexing: You configure so both disks have a disk controller obsoleting disk controller as a SPF

RAID-2, 3, 4 rarely used

RAID-5 and RAID-6 (Striping)

- RAID-5 is three or more disks that are striped together, similar to RAID-0

RAID subsystem, such as RAID-1, RAID-5, and RAID-6 provide fault tolerance and increased data availability

- RAID-1 and RAID-5 can survive the failure of one disk, and RAID-6 can survivie the failure of two disks

RAID-10

- Combines mirroring and striping
- Minimum number of drives is 4, and in 2's → so 6, or 8, 10 drives etc.

Disk Multipath

- Multipath Input/Output (I/O) is another fault tolerance method for disks
  - Used to separate data transfer path to and from the storage hardware
  - If one of the paths fail, the second path handles the transfer
  - If both paths are operational, it provides increased performance

High Availability: refers to systems and services that needs to remain operational with almost zero downtimes

- It's possible to achieve 99.999 % uptime ➔ "The Five Nines"

Load balancing increases the overall processing power of a services by sharing the load among multiple servers

- Configurations can be active/passive or active/active
- Scheduling methods include round-robin and source IP address affinity
- ***Source IP Address affinity*** scheduling ensures clients are redirected to the same server for an entire session so ensure session persistence

Source Affinity: sends requests to the same server based on the requestor's IP Address and provides the user with session persistence

- Ex) if user wants to access webpage, the load balancer records their IP Address and sends to say server 3, when the user interacts with page and sends another request to webpage, the balancer identifies the IP Address and sends request to server 3 again
- Source affinity effectively sticks users to a specific server ensuring session persistence

Active/Passive Load Balancing Configuration

- One server is active and other is inactive, if active server fails, the inactive server takes over
- b/c both servers have access to shared storage, there is no loss of data

NIC Teaming: allows you to group two or more physical network adapters into a single software-based virtual network adapter

- provides increased performance b/c NIC Team handles all the individual NIC's bandwidth as if the NIC team is a single physical network adapter
- NIC Team uses load-balancing algorithms to distribute outgoing traffic
- It also eliminates any physical NIC from being a SPOF

Power Redundancies

- You can use uninterruptible power supplies (UPS), generators, managed power distribution units (PDU) to provide both fault tolerance and high availability

UPS (Uninterruptible Power Supplies): provides short-term power and protect against power fluctuations

- Allow systems to stay powered on for short period of time until longer-term power supplied

Dual Supply: a second power supply that can power a device if the primary power supply fails

Generators: provide long-term power during extended outages

- During natural disasters such as floods and hurricanes, great

PDU (Power Distribution Units): distribute power to devices

- Monitor the voltage, current and power consumption and reports these measurements to admins

Backups

Tape is the most common media for backups b/c it stores more data and is cheaper than other medias:

- Disk: access to data in disk much quicker than in tape
    - Disk can be located on servers or simple USB disk drives

- **NAS (Network-Attached Storage):** dedicated computer used for file storage and is accessible on network
    - Can have multiple drives and runs a stripped down Linux system

- SAN (Storage-Area Network): provides block-level data storage
    - Used by organizations for real-time replication of data
    - As soon as data changes in its primary location, it is replicated to SAN

- Cloud: many companies like Microsoft and Google provide free limited cloud storage

Online backups: via cloud
Offline backups: via tape, disk, NAS, SAN → more control

Hot Backup: backing up data while it is operational

Types of Backups:

a) Full Backup: full (or normal) back up of all the selected data
b) Differential Backup: backs up all the data that has changed or is different since last full backup
c) Incremental Backup: backs up all the data that has changed since the last full or incremental backup
d) Snapshot and Image Backup: captures the data at a point in time → "image backup"

If you have unlimited time and money, the full backup alone provides the fastest recovery time

- Full/Incremental Strategies reduce the amount of time needed to perform backups
- Full/Differential Strategies reduce the amount of time needed to restore backups

Test Restores are the best way to test the integrity of a company's backup data

- Backup media should be protected with the same level of protection as the data on the backup
- Geographic considerations for backups include storing backups off-site, choosing the best location, and considering legal implications and data sovereignty

Test Restore: restoring the data from a backup and verifying its integrity

Data Sovereignty: refers to legal implications of storing data off-site, say in another country, where data is subject to different country laws

The BIA (Business Impact Analysis) identifies mission-essential functions and critical systems that are essential to the organization's success

- It also identifies maximum downtime limits for these systems and components, various scenarios that can impact these systems and components, and the potential losses from an incident

The Recovery Time Objective (RTO) identifies the maximum amount of time it should take to restore a system after an outage

- It is derived from the maximum allowable outage time identified in the BIA
- The Recovery Point Objective (RPO) refers to the amount of data you can afford to lose

The Mean Time Between Failures (MTBF) provides a measure of a system's reliability and would provide an estimate of how often the systems will experience outages

- The Mean Time To Repair (MTTR) refers to the time it takes to restore a system

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

Recovery Site: an alternative processing site that an organization uses for site resiliency

- If one site suffers a catastrophic event, an alternative site can be used

A hot site includes personnel, equipment, software, and communication capabilities of the primary site with all the data up to date

- A hot site provides the shortest recovery time compared with warm and cold sites
- It is the most effective disaster recovery solution, but it is also the most expensive to maintain

Warm Site: → Goldilocks Solution

- Hot sites are generally too expensive for most organizations, and cold sites sometimes take too long to configure for full operation
- Warm sites are the happy medium between the two concerns

A 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
- For cold sites, the organization brings all the equipment required for recovery
- A 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

Mobile Site: self-contained transportable unit with all the equipment needed for specific requirements

Mirrored Site: identical to the primary location and provide 100 percent availability

- They use real-time transfer to send modifications from primary location to mirrored site
- Although a hot site can be up and operational within an hour, the mirrored site is always up and operational

A disaster recovery plan (DRP) identifies how to recover critical systems after a disaster and often prioritizes services to restore after an outage

- Testing validates the plan
- The final phase of disaster recovery includes a review to identify any lessons learned and may include an update of the plan

Disaster Recovery Plan (DRP) identifies how to recover critical systems and data after a disaster

- DRP is a part of a business's overall business continuity plan

You can validate business continuity plans through testing

- Tabletop exercises are discussion-based only and are typically performed in a conference setting
- Walk-throughs provide training to personnel prior to a tabletop exercise or to create a formal tabletop exercise plan
- Simulations are hands-on exercises

END OF CHAPTER 9

Chapter 10: Understanding Cryptography and PKI

Hashing: creates a fixed-length string of bits or hexadecimal characters that **CANT be reversed** to recreate original data

- Secure Hash Algorithm (SHA-3) is the most common hashing algorithm used
- No matter how many times you create a hash for a file, it will always create the same value, if the file is the same

Stream cipher: encrypt data 1 bit at a time
Block cipher: encrypts data in blocks

Steganography: provides a level of confidentiality by hiding data within other files

- Ex) embedding data within the white space of a picture file

Digital Signature: provides authentication, non-repudiation, and integrity

Hashing verifies integrity for data such as email, downloaded files, and files stored on a disk

- A hash is a number created with a hashing algorithm

Checksum: small piece of data, sometimes 1 or 2 bits, that is used to quickly verify the integrity of data

- Not intended to be cryptographically secure, just a quick indication of integrity
- Hashes are much longer numbers and used in strong cryptographic implementation

16-Digit Credit Card Number:

- First 6 Digits = Institution of Bank
- Next 9 Digits = Represents Account Number
- 16^{th} Digit = check digit/check sum

Two popular hashing algorithms used to verify integrity are MD5 and SHA-256

- HMAC (Hash-Based Message Authentication Code) Verifies both the integrity and authenticity of a message with the use of a shared secret
- Other protocols such as IPsec and TLS use HMAC-MD5 and HMA-SHA256

MD5 (Message Digest 5) -> since 1992

- Common hashing algorithm that produces a 128-bit hash
- Experts found significant vulnerabilities in 2004
- Still used as a quick checksum to verify file integrity for email, files stored on disk, files downloaded from internet, executable files etc.

SHA (Secure Hashing Algorithm)

- SHA-0: not used
- SHA-1: creates 160-bit hash → no longer used b/c of weakness found
- SHA-2: SHA-256 and SHA 512 (256 and 512 represent the bit size)
- SHA-3 (created outside of US National Security Agency (NSA))

MD5: used for verify file integrity
SHA: also used to verify file integrity

HMAC (Hash-Based Message Authentication Code)

- Used as a fixed-length string of bits **similar** to MD5 and SHA, but also uses a shared secret key to add some randomness to the result and only the sender and receiver know the secret key
- Provides both integrity and authenticity of messages

Ex) server sending message using HMAC-MD5:

- First creates a hash of message using MD5
- Then uses a secret key (HMAC) to complete another calculation on hash
- Server then sends the message and the HMAC-MD5 hash to the second server
- Second server performs the same calculations and compares the received HMAC-MD5 hash with its result

Hashing is a one-way function that creates a string of characters

- You cannot reverse the hash to re-create the original file
- Passwords are often stored as hashes instead of storing the actual password
- Additionally, applications often salt passwords with extra characters before hashing them

Email applications automatically create and compare the hashes

Two Golden Hash Rules:

1) The hash will always be the same no matter how many times you calculate it
2) Hashing verifies the file has retained integrity

- Hashing provides the assurance of integrity in data

If you can recognize the hashing algorithms such as MD5, SHA, and HMAC, it will help you answer some exam questions

- For example, if a question asks what you would use to encrypt data and it lists three hashing algorithms, you can quickly eliminate them b/c hashing algorithms don't encrypt data

Company Password Databases store passwords as hashes and turn user log-in passwords to hashes to verify their identity

Hash Collision: when the hashing algorithm creates the same hash from different input

- MD5 is suspectable to hash collisions, which is why it isn't used now

Online attack guess the password of an online system

- Offline attacks guess the password stored within a downloaded file, such as a database
- Logs will show a large volume of failed logon attempts as **Event ID 4625** and/or several accounts being locked out as **Event ID 4740**
- Spraying attacks attempt to avoid account lockout policies, but logs will still show a large volume of failed logon attempts, but with a time lapse between each entry

Dictionary Attack: uses a dictionary of words and attempts every word in the dictionary to see if it works

- The original password attack
- Modern version, includes other common passwords in database as well, such as 1234

Brute-Force Attack: attempts to guess all possible character combinations

Password Spraying Attack: a special type of brute force or dictionary attack designed to avoid being locked out

- An automated program starts with a large list of targeted user accounts, it then picks a password and tries it against every account in the list
- It then picks another password and loops through the list again

Pass-the-Hash Attack: attacker discovers the hash of the user's password and then uses it to log onto the system as the user

- Any authentication protocol that passes the hash over the network in an unencrypted format is susceptible to this attack

Password Hashes Storages:

- SAM (Security Account Manager) Database
- LSASS (Local Security Authority Subsystem) Process
- CredMan (Credential Manager) Store

Passwords are typically stored as hashes

- A pass the hash attack attempts to use an intercepted hash to access an account
- They attacks can be detected in Event ID 4624 with a Logon Process of NtLmSSP and/or an Authentication Package of NTLM (New Technology LAN Manager)

Birthday attacks exploit collisions in hashing algorithms

- A hash collision occurs when the hashing algorithm creates the same hashes from different passwords
- Salting adds random text to passwords before hashing them and thwarts many password attacks, including rainbow table attacks (table of hashes)

Birthday Attack

- Names after the birthday paradox in mathematical probability theory
- States: for every 23 people, there is a 50% chance that 2 of them have the same birthday
- In birthday attacks, attacker attempts to create a password that produces the same hash as the user's actual password

Rainbow Table Attacks: attackers attempt to discover the password from the hash

- A rainbow table is a huge database of possible passwords with the precomputed hashes for each
    - The application guesses a password
    - The application hashes the guessed password
    - The application compares original password hash with guessed password hash…if they match, application now knows password

Salting Passwords: helps prevent rainbow table attacks and other password attacks

- A salt is a set of random data such as two additional characters
- Salting adds these additional characters to password before hashing it

Key Stretching: instead of just salting a password before hashing it, key stretching applies cryptographic stretching algorithm to salted password

Bcrypt, PBBKDF2, 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

Encryption provides confidentiality and helps ensure that data is viewable only by authorized users

- This applies to any data at rest (such as data stored in a database) or data in transit being sent over a network

Encryption Method Elements:

- Algorithm: performs mathematical calculations on data
    - This is always the same
- Key: a number that provides variability for the encryption
    - Either kept private and/or changed frequently

Symmetry encryption uses the same key to encrypt and decrypt data

- For example, when transmitting encrypted data, symmetric encryption algorithms use the same key to encrypt and decrypt data at both ends of the transmission media
- RADIUS uses symmetric encryption

Symmetric Encryption/ Secret-Key / Session-Key Encryption

- Uses the same key to encrypt and decrypt data
- If key is 3 → all letters move forward 3 letters

Symmetric Key Analogy = House Key

- No matter you has a copy, they can enter or lock the house, just like data

ROT13 (Rotation 13): uses key 13

Block cipher: encrypts data in specific-sized blocks, such as 64-bit blocks or 128-bit blocks

- Block cipher creates large files or messages into these blocks and then encrypts each individual block separately

Stream Cipher: encrypts data as a stream of bits or bytes rather than dividing it into blocks

Stream ciphers encrypt data in a single bit, or a single byte, at a time in a stream

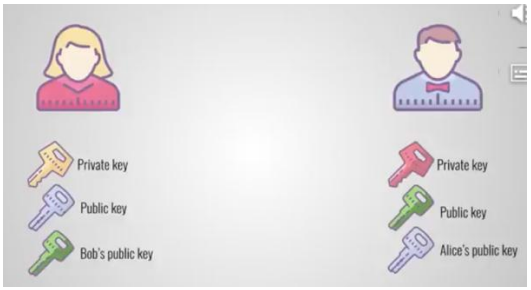
- Block ciphers encrypt data in a specific-sized block such as 64-bit or 128-bit blocks
- Stream ciphers are more efficient than block ciphers when encrypting data in a continuous stream

AES (Advanced Encryption Standard) is a strong symmetric block cipher that encrypts data in 128-bit blocks

- AES uses 128-bit, 192-bit, or 256-bit keys
- 3DES (Triple Data Encryption Standard) was originally designed as a replacement for DES, but NIST selected AES as the current standard
- However, 3DES is still used in some applications, such as when legacy hardware doesn't support AES

Asymmetric Encryption

- Uses two keys in a matched pair to encrypt and decrypt data – a public key and a private key
    - Public key: encrypts information, only matching private key can decrypt
    - Private key: encrypts information, only matching public key can decrypt the same information
    - Private keys are kept private and public keys are freely shared by embedding them in a shared certificate



Rayburn Box

- Rayburn box is a lockbox that allows people to securely transfer items over long distances and it has two keys
    - One key can lock the box but can't unlock it
    - The other key can unlock the box, but can't lock it
        - Only one copy of private key exists
        - Multiple copies of public key exist

Only a private key can decrypt information encrypted with a matching public key

- Only a public key can decrypt information encrypted with a matching private key
- A key element of several asymmetric encryption methods is that they require a certificate and a PKI

Rayburn Box can be used for authentication: if box is built so only individual with private key can lock it, but anyone with public key can decrypt → you know message was by individual

Certificates

- Key element of asymmetric encryption
- A certificate is a digital document that typically includes the public key and information on the owner of the certificate
- Certificate Authorities (CA) issue and manage certificates

Certificates are an important part of asymmetric encryption

- Certificates include public keys 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

Elements of Certificate:

a) Serial Number: serial number uniquely identifies the certificate
    - The CA uses this serial number to validate a certificate
    - If CA revokes the certificate, it publishes serial number in a certificate revocation list (CRL)
b) Issuer: identifies the CA that issued the certificate
c) Validity Dates: expiration date
d) Subject: identifies owner of certificate
e) Public key: asymmetric encryption uses the public key in combination with matching private key
f) Usage: some certificates only for encryption or authentication

Ephemeral: refers to something that lasts a short time

- Ephemeral key has a short lifetime and is re-created for each session

Static key: semipermanent and stays the same over a longer period of time

- Benefit: CA can validate them

Ephemeral key pair: includes private ephemeral key and public ephemeral key

- Systems use these key pairs for a single session and then discard them

Certificates Use 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, such as a year

Perfect Forward Secrecy: an important characteristic that ephemeral keys comply with in asymmetric encryption

Elliptic Curve Cryptography (ECC): uses mathematical equations to formulate an elliptical curve and then graphs points on the curve to create keys

Digital signatures commonly used to sign emails

- Digital Signature Algorithm (DSA) uses key pairs managed by PKI with the public key distributed in a certificate
- ECDSA (Elliptical Curve Digital Signature Algorithm) can also be used for digital signatures

Digital Signature

- Sender encrypts message with private key (Digital Signature) the only one with private key
- This creates non-repudiation b/c we know they are the only ones who can encrypt the message
- Anyone with the sender's public key can decrypt and as a recipient you know that the message is coming from the legitimate source

Quantum Cryptography: uses a qubit, which can have two values at the same time

Quantum Key Distribution (QKD): allows two parties to establish a shared key, similarly to how asymmetric encryption is used to allow two parties to establish a shared key used with symmetric encryption

- Ex) two people in different cities can use QKD to establish a quantum connection and share a symmetric key, and use to share encrypted data

Post-Quantum Cryptography: refers to cryptographic algorithms that are likely to be resistant to attack using a quantum computer

Smaller devices and IoT devices either don't have the ability to implement strong cryptography, or if they do, it severely limits their performance

Lightweight cryptography refers to cryptographic methods that can be deployed on smaller devices such as wireless devices and IoT devices

- Homomorphic encryption allows data to remain encrypted while it is being processed

The way any individual algorithm is strengthened is by increasing the length of a key

Three common encryption modes of operation used with encryption are authenticated, counter, and unauthenticated

- Authenticated encryption provides both confidentiality and authenticity
- Counter (CTR) mode is a form of authenticated encryption and CTR modes allow block ciphers to function as stream ciphers
- Unauthenticated mode provides confidentiality, but not authenticity

Imagine Homer is visiting a website using TLS:

- His computer and the website establish a session and share symmetric keys
- One key is used to encrypt the webpages before sending them
- The second key is used with a hash function on the ciphertext to create a MAC (Message Authentication Code)
- Note that at this point only the website and Homer's computer know these keys
- 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
- If the recalculated MAC is the same as the sent MAC, it provides authenticity by proving that the data was sent by the website and that the data hasn't changed
- The first key is then used to decrypt the ciphertext

Steganography

Steganography: hides data inside other data → hiding data in plain sight

- It doesn't encrypt data, just hides data (obfuscation) → make something unclear or difficult to understand)

Three Main Types of Steganography Files:

1) Audio files
2) Image files
3) Video files

Audio Steganography

- Takes advantage of limitations of human ear
    - Human ear can only detect sound frequencies ranging from 20Hz and 20KHz
    - Humans can't detect sounds between 18KHz and 20KHz, but microphones can
        - These sounds are called "audio beacons" used to identify user activity

Some audio beacons are used by marketers within stores, they track the location of shoppers as they move through a large store, apps then send ads or coupons based on the shopper's location

Image Steganography

- Practice of hiding data within files such as .jpeg and .gif files
    - Done via manipulating bits of a file or by hiding data in white space
- Many files have unused spaced (white space) at the end of file clusters

Video Steganography

- An extension of image steganography and it embeds messages into videos
- Drawback: can create noise into audio

Steganography hides messages or other data within a file

- Security professionals use hashing to detect changes in files that may indicate the use of steganography
- The three methods of steganography are audio, image, and video

Email Signatures

- The sender's private key encrypts (or signs)
- The sender's public key decrypts

Email Encryption

- The recipient's public key encrypts
- The recipient's private key decrypts

Website Encryption

- The website's public key encrypts
- The website's private key decrypts

Knowing which key encrypts and which key decrypts will help you answer those questions on the exam

- For example, just by knowing that a private key is encrypting, you know that it is being used for a digital signature

Cryptography provides two primary security methods for email:

- Digital Signatures (Not same as Digital Certificate)
- Encryption

A digital signature is an encrypted hash of a message

- The sender's private key encrypts the hash of the message to create the digital signature
- The recipient decrypts the hash with the sender's public key
- If successful, it provides authentication, non-repudiation, and integrity
- Authentication identifies the sender
- Integrity verifies the message has not been modified
- Non-repudiation prevents senders from later denying they sent an email

Digital signatures need certificates, and certificates include the sender's public key

In a digital signature, the sender uses the sender's private key to encrypt the hash of the message and the recipient uses the sender's public key to decrypt the hash of the message

- The public key is often distributed in an **S/MIMIE.p7s** formatted file

Emails send encrypted hash and unencrypted message

- Encrypted hash is to validate authentication, non-repudiation, integrity

Encrypting Email with Only Asymmetric Encryption:

1) Lisa retrieves a copy of Bart's certificate that contains his public key
2) Lisa encrypts the email using Bart's public key
3) Lisa sends the encrypted email to Bart
4) Bart decrypts the email with his private key

The recipient's public key encrypts when encrypting an email message and the recipient uses the recipient's private key to decrypt an encrypted email message

Digital Signature Encryption is opposite of Asymmetric Encryption

- In Digital Signature, sender encrypts digital signature using its private key and it is decrypted by recipient whom uses the sender's public key
- In Asymmetric Encryption, the recipient uses its private key to decrypt a message that was encrypted by the sender using the recipient's public key

Encrypting Email using Both Symmetric and Asymmetric Encryption

- Most email applications use asymmetric encryption to privately share a session key
- They use symmetric encryption to encrypt the data with this session key

1) Lisa's system identifies a symmetric key to encrypt her email via AES symmetric algorithm, say key 53
2) Lisa encrypts the email contents with symmetric key 53

3) Lisa retrieves copy of barts certificate that contains his public key
4) She uses bart's public key to encrypt the symmetric key 53
5) Lisa sends the encrypted email and the encrypted symmetric key to bart
6) Bart decrypts the symmetric key with his private key
7) He then decrypts the email with the decrypted symmetric key

Email Encryption Summary

- Symmetric Encryption used to encrypt email messages
- Symmetric Encryption Key is encrypted with recipient's public key by sender
- Encrypted Symmetric Key is decrypted by recipient's private key to obtain the symmetric key
- Symmetric Key unencrypt message

Unauthorized users who intercept the email sent by Lisa won't be able ot read it b/c it's encrypted with the symmetric key

- Additionally, they can't read the symmetric key b/c it's encrypted with Bart's public key and only Bart's private key can decrypt it

S/MIME (Secure/Multipurpose internet Mail Extensions): one of the most popular standards used to digitally sign and encrypt email

- Most email applications that support encryption and digital signatures use S/MIME

Transport encryption methods encrypt data in transit on internet and internal networks to ensure transmitted data remains confidential

TLS is the replacement for SSL

- TLS requires certificates issued by certificate authorities (CAs)
- TLS encrypts HTTPS traffic, but it can also encrypt other traffic

TLS (Transport Layer Security) and SSL (Secure Sockets Layer) are encryption protocols that have been commonly used to encrypt data sent over the internet

- Any SSL/TLS is just referring to TLS b/c SSL is vulnerable → not used

TLS used to encrypt HTTPS, but also FTPS

- Provides certificate-based authentication and encrypts data with a combination of both symmetric and asymmetric encryption during a session
    - It uses asymmetric encryption for key exchange (to privately share session key)

- Uses symmetric encryption to encrypt data displayed on the webpage and transmitted during the session
    - Similar to Email Encryption I guess

<u>Encrypting HTTPS using TLS</u>

1) Client begins by requesting HTTPS session (entering URL or clicking on HTTPS link)
2) Server responds by sending the server's certificate
    - The certificate includes the server's public key
    - The matching private key is on the server and only accessible by the server
3) The client creates a symmetric key and encrypts it with the server's public key
    - Imagine the symmetric key is 53, the client encrypts the symmetric key 53 using the web server's public key creating ciphertext @#$@
        - This symmetric key will be used to encrypt data in the HTTPS session, so it is sometimes called a session key
4) The client sends the encrypted session key @#$@ to the webserver
    - Only the server's private key can decrypt this
        - If attackers intercept encrypted key, they won't be able to decrypt it b/c they don't' have access to the server's private key
5) The server receives the encrypted session key and decrypts it with the server's private key → at this point, both the client and the server know the session key
6) All the session data is encrypted with this symmetric key using symmetric encryption

Symmetric Keys are called session keys in web exchange b/c it's used to encrypt session data

Downgrade Attack: forces system to downgrade its security and then the attacker exploits the lesser security control

- If client cant use TLS, the server would downgrade its security and use SSL

One way to ensure SSL not used is to ensure SSL is disabled

Administrators should disable weak cipher suits and weak protocols on servers

- When a server has both strong and weak cipher suits, attackers can launch downgrade attacks bypassing the strong cipher suite and exploiting the weak cipher suite

Blockchain: a distributed, decentralized, public ledger

- Public record-keeping technology
- Block: refers to pieces of digital information (the ledger)
- Chain: refers to public database
- Blockchain: database of public records

Each block has three parts:

- Information about transaction, such as date, time, amount
- Information about parties involved

- Unique hash that distinguishes the block from other blocks

Block is added to block chain after four things happen:
- Transaction verified by network of computers
- Transaction is accurately recorded in a block
- Block is assigned a unique hash

Block also contains hash of most recent block added before it, creating that chain b/c each block has its own hash and the hash of the previous block

In bitcoin:
Minors: the network of computers that verify and record transactions

Security vs Resource (cost)

When encrypting and decrypting, quick algorithm preferred
When salting and hashing, slow algorithm preferred to thwart attackers

Entropy: refers to the randomness of a cryptographic algorithm
- The higher level of randomness, the higher level of security

Pseudo-random number generator: uses deterministic algorithm
- In other words, given the same input, a pseudo-random number generator will produce the same output

True-random number generators use environmental factors such as atmospheric noise or cosmic background radiation as inputs

Weak Keys: short or small keys
- Even if you have the strongest algorithm, it can be cracked with weak key

Longevity: refers to how long you can expect to use an algorithm
- Related to expected improvements in processing power

Symmetric keys should NOT be reused

Important Cryptographic Concepts for EXAM:

Supporting integrity: hashing protocols are used to support integrity
- Verifying data not changed by unauthorized users

Supporting Confidentiality: encryption protocols are used to provide confidentiality
- Prevents unauthorized users from accessing data

Supporting Non-repudiation: digital signatures are used to support non-repudiation
- Ex) email message hash encryption

Supporting high resiliency: refers to security of an encryption key even if an attacker discovers parts of it

Supporting Obfuscation: steganography is used to support obfuscation, allowing data to hide in plain sight

Supporting low power devices: using lightweight cryptography algorithms

Supporting low latency:

Public Key Infrastructure (PKI): group of technologies used to request, create, manage, store, distribute, and revoke digital certificates
- Asymmetric encryption depends on use of certificates for a variety of purpose such as protecting email, and protecting internet traffic with TLS

Benefit of PKI: allows two people or entities to communicate securely without knowing each other previously

Certificate Authority (CA): issues, manages, validates, and revokes certificates
- DigiCert, Symantec, Comodo or even a small single service running on a server within a private network

CA are trusted by placing a copy of their root certificate into a trusted root CA store
- The root certificate is the first certificate created by the CA that identifies it, and the store is just a collection of these root certificates
- If the CA's root certificate is place in the store, all certificates issued by this CA are trusted

Certificate Chaining: combines all the certificates from the root CA down to the certificate issued to the end user

OpenSSL: software library accessible via CLI in Linux to create key pairs in one command, allowing you to export the public key to a file in a second command

You typically request certificates using a certificate signing request (CSR)

- The first step is to create the **RSA-based private key**, which is used to create the public key
- You then include the private key using the CSR and the CA will embed the public key in the certificate
- The private key is not sent to the CA

- RSA algorithm is used to create the private key, and the private key is used to sign the certificate signing request for a public key to creates public key infrastructure

Can revoke certificates for several reasons such as when the private key is compromised or the CA is compromised

- The Certificate Revocation List (CRL) includes a list of revoked certificates and is publicly available
- An alternative to using a CRL is the Online Certificate Status Protocol (OCSP), which returns answer such as good, revoked, or unknown

OCSP (Online Certificate Status Protocol): quicker way and less traffic for clients to validate CA

Validating Certificate:

a) Expired
b) Certificate Not Trusted: see if the certificate was issued by a trusted CA
    - Ex) Windows look in the Trusted Root Certification Authority Store and the intermediate certification Authorities store shown
    - If the system doesn't have a copy of the CA's certificate, it indicates certificate not trusted
c) Certificate Revoked: clients also validate certificates through the CA to ensure they haven't' been revoked

Common Way:

1) Client initiates a session requiring a certificate, such as an HTTPS session
2) The server responds with a copy of the certificate that includes the public key
3) The client queries the CA for a copy of the CRL
4) The CA responds with a copy of the CRL

Certificate stapling is an alternative to OCSP

- The certificate presenter (such as a web server) appends the certificate with a timestamped digitally signed OCSP response from the CA
- This reduces OSCP traffic to and from the CA
- Public key pinning helps prevent attackers from impersonating a website with a fraudulent certificate

- The web server sends a list of public key hashes that clients can use to validate certificates sent to clients in subsequent sessions

Online Certificate Status Protocol (OCSP): another method to validate certiricate
- Allows client to query the CA with serial number of certificate
- CA responds with answer “good”, “revoked”, “unknown → could be forgery”

Public Key Pinning: security mechanism designed to prevent attackers from impersonating a website using fraudulent certificates

Public key pinning: once a host’s certificate or public key is known, the certificate or public key is associated or ‘pinned’ to the host

Key Escrow: process of placing a copy of a private key in a safe environment

CER is an ASCll format for certificates and DER is a binary format
- PEM is the most used certificate format and can be used for just about any certificate type
- P7B certificates are commonly unused to share public keys
- P12 and PFX certificates are commonly used to hold the private key

CER: ASCII format used to create certificate
DER: binary format used to create certificate
PEM: most used format to create certificate
- Versatile

END OF CHAPTER 10

Chapter 11: Implementing Policies and Mitigate Risks

Personnel Policies

- Companies develop policies to define and clarify issues related to personnel, includes personnel behavior, expectations and possible consequences

Acceptable Use Policy

- Describes the purpose of computer systems and networks, how users can access them, and the responsibilities of users when they access the system
- Many companies monitor user activities, such as websites they visit and what data is sent via email

Mandatory Vacation Policies require employees to take time away from their job

- These policies help to deter fraud and discover malicious activities while the employee is away

Separation of Duties prevents any single person or entity from controlling all the functions of a critical or sensitive process by dividing the tasks between employees

- This helps prevent potential fraud, such as if a single person prints and signs checks

Least privilege specifies that individuals or processes are granted only those rights and permissions needed to perform their assigned tasks or functions

- By implementing the least privilege policy, it limits potential losses if any individual or process or compromised

Job rotation policies require employees to change roles regularly

- Employees might change roles temporarily, such as for three to four weeks, or permanently
- This helps ensure that employees cannot continue with fraudulent activity indefinitely

Clean Desk Policy requires users to organize their areas to reduce the risk of possible data theft

- It reminds users to secure sensitive data and may include a statement about not writing down passwords

Background Checks investigate the history of an individual prior to employment and, sometimes, during employment

- They may include criminal checks, credit checks, and an individual's online activity
- Onboarding is the process of granting new employees access to resources
- Offboarding removes this access often by disabling or deleting a user's account
- Offboarding also includes collecting everything issued to the employee

NDA (Non-Disclosure Agreement)

- Used between two entities to ensure that proprietary data is not disclosed to unauthorized entities

Supply Chain: includes all the elements required to produce and sell products and services

- Organizations sometimes require vendor diversity to provide cybersecurity resilience

EOL (End of Life): refers to the date when a product will no longer be offered for sale
EOSL (End of Life Service): indicates the date when you expect a lack of vendor support b/c vendors no longer create patches or upgrades to resolve vulnerabilities for the product

Supply chain and vendor policies typically provide guidance on how to limit access to given vendors

- An SLA (Service Level Agreement) between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels
- A MOU (Memorandum of Understanding) expresses an understanding between two or more parties indicated their intention to work together toward a common goal
- A MSA (Measurement Systems Analysis) evaluates the processes and tools used to make measurements

BPA (Business Partner Agreement): written agreement that details the relationship between business partners, including their obligations toward the partnership

- Identifies the shares of profits or losses each partner will take, their responsibilities to each other, and what to do if a partner chooses to leave partnership
- Benefit: helps settle conflicts when they arise

Term of Agreement: refers to period that an agreement shall be in effect

- Often a clause in a legal document such as NDAs, SLAs, BPAs

An incident response policy defines a security incident and incident response procedures

- Incident response procedures start with preparation to prepare for and prevent incidents
- Preparation helps prevent incidents such as malware infections
- Personnel review the policy periodically and in response to lessons learned after incidents

Common Elements of Incident Response Plan:

1) Definition of Incident Types: help employees identify the difference between an event and an actual incident
2) Incident Response Team (IRT): composed of employees with expertise in different areas
3) Roles and Responsibilities: many incident response plans identify specific roles for an incident response team along with their responsibilities

Communication Plan is part of the incident response plan and provides direction on how to communicate issues related to an incident

Common Communication Plan Elements:

1) First Responders: initial responders, help-desk technicians, should know when to inform incident response entities of an incident and who to contact
2) Internal Communication: IRT should know when to inform senior personnel of an incident → not necessary to report an attempted DDoS attack that was blocked by automated response systems
3) Reporting Requirements: often, security incidents need to be reported to external entities such as law enforcement
    - If customer data is exposed, customers need to be notified
4) External Communication: should be clear who can talk to external entities such as media
5) Law Enforcement: law enforcement personnel provide significant help after an incident
6) Customer Communication: In some cases, laws dictate when an organization must inform customers of a data breach

Equifax: in 2017, massive data breach exposed personal information of 147 million people

- Close to $billion dollar reparation fee

Consequences of Data Breaches:

- If Intellectual Property (IP) or trade secrets and software algorithms are stolen, organization suffers direct losses
- If personal information about customers accessed, impersonation by attackers can take place causing lawsuits and monetary settlements, causing more direct losses

Stakeholder Management: refers to creating and maintaining positive relationships with stakeholders

- Stakeholders are: owners, stock owners, employees, creditors, suppliers, and more

The first step in the incident response process is preparation

- After identifying an incident, personnel attempt to contain or isolate the problem to protect critical systems while maintaining business operations
- Eradication attempts to remove all malicious components from an attack, and recovery returns a system to normal operation
- Reviewing lessons learned allows personnel to analyze the incident and the response to prevent a future occurrence

Common Phases of Incident Response Process:

1) Preparation: provides guidance to personnel on how to response to an incident
2) Identification: all events are not security incidents, so personnel take the time to verify potential incidents
3) Containment: once identified as a security incident, security personnel attempt to isolate or contain it (Quarantining)
4) Eradication: removing malware and components from attack (installed malware software)
5) Recovery: admin return all affected systems to normal operations
6) Lessons Learned: security personnel take the time to learn valuable lessons, and changes may take place to network infrastructure or approach or policy

SOAR (Security Orchestration, Automation, and Response) platforms use internal tools to respond to low-level security events automatically, reducing administrator workload

- A SOAR playbook provides a checklist of things to check for suspected incidents
- A SOAR runbook implements the paybook checklist using available tools within the organization

Runbook: implement the guidelines documented in the playbooks using the available tools within an organization

- It can automatically respond to potential incidents
- Ex) automatically forward an email with attachment to sandbox and detonate safely to analyze if secure or not

Digital Forensics

A tag is placed on evidence items when they are identified

- A chain of custody provides assurances that evidence has been controlled and properly handled after collection
- It documents who handled the evidence and when they handled it
- A legal hold is a court order to preserve data as evidence
    - Data retention policies hold so if it says to delete emails older than 6 months, that's okay
    - If admin did not follow policy and has emails older than 6 months still but now has a legal hold, they cant delete it and it will be examined

Data Breach Notification Law: require organizations to notify customers about a data breach and take steps to mitigate the loss

- When the data is stored in the cloud, this could require notification based on several different laws

Order of Volatility: refers to the order in which you should collect evidence

- Volatile: means that it is not permanent
- When collecting digital evidence, begin by collecting data that is most volatile to least volatile

A processor can only work on data in RAM, so all the data in RAM indicates what the system was doing

Order of Volatility from Most to Least:

1) Cache: data in cache memory, including processor cache and hard drive cache is removed as new data is used
2) RAM: data in RAM used by OS and applications
3) Swap/Pagefile: a swap file is on the system disk drive, it is an extension of RAM and is stored on the hard drive
    - Pagefile not typical file, and system rebuilds the pagefile when rebooting, so more volatile than other files stored on hard drive
4) Disk: data files are stored on local disk drives, they remain there even after rebooting a system
5) Attached Devices: such as USB will also hold data when a system is powered off
6) Network: networks typically have servers and shared folders accessible by users and used to store log files

When collecting data for forensics analysis, you should collect it from the most volatile to the least volatile

- The order of volatility is cache memory, regular RAM, swap file (or paging file), hard drive data, and data stored on network systems

Forensics Artifacts: pieces of data on a device that regular users are unaware of, but digital experts can identify and extract

- Web History: includes both pages visited and searched
- Recycle Bin: you view the content of deleted files and the metadata of deleted files
- Windows Error Reporting: these often give insight into what programs were running when a system crashed
- Remote Desktop Protocol (RDP) Cache: provides useful information if an attacker moves laterally through a network, or when an attacker is connecting to a system from an Internet server

OS Forensics: refers to collecting data from OS

- Cache
- RAM
- Swap File
- Artifacts

Forensics experts capture data using tools that don't modify it during the capture process

- Some commonly used tools used to capture data on disks and within memory are the dd command (data duplicator), memdump (memory dumper), WinHex, FTK imager
- Autopsy provides a graphical tool to run many of the commands in The Sleuth Kit
- Hashes and checksums prove the provenance of data

Memdump: dumps any addressable memory space ot the terminal or redirce the output to a dump file

WInHex: Windows-based used for evidence gathering, data analysis, editing, recovery of data, and data removal

- It can work with data on all drives, such as hard drives, CDs, DVDs, it can also work directly with memory

FTK Imager: can capture an image of a disk as a single file, or multiple files and save thej image in various formats

- Also gives option of creating images of individual folders or files

Autopsy: graphical user interface (GUI) digital forensics platform

Provenance: refers to tracing something back to its origin

- In digital forensics, hashing and checksums allow you to prove the analyzed copy of data is the same original data

eDiscovery (Electronic Discovery): the identification and collection of electronically stored information

- includes files of any kind, voice mail, social media entries, and website data

Data Recovery: refers to restoring lost data, such as restoring a corrupt file from a backup

- even without backups, it's often possible to recover data that a user has intentionally or accidentally deleted

Public Data is available to anyone

- sensitive data is any kind of data that needs to be protected against unauthorized data
- confidential data information is kept secret among a certain group of people
- Proprietary Data is data related to ownership, such as patents or trade secrets
- Financial information provides a picture of an organization's financial health

Intelligence: the ability to learn by acquiring new knowledge and skills
Digital Intelligence: refers to knowledge and information which has value to investigate personnel and has been gathered using digital forensics methods and techniques

Strategic Intelligence: refers to collecting, processing, and analyzing information to create long-term plans and goal

Counterintelligence Activities: assume that attackers are also using strategic intelligence methods

- Refers to any activities designed to prevent or thwart spying, intelligence gathering, or attacks

Top Secret: if data in this category is disclosed to unauthorized entities, it could cause exceptionally grave damage to national security

Secret: if data in this category is disclosed to unauthorized entities, it could cause serious damage to national security

Confidentiality: if data in this category is disclosed to unauthorized entities, it could cause damage to national security

Sensitive data: any data that isn't public and that the organization wants to protect against unauthorized access

Public data: available to anyone

Private data: information about an individual that should remain private (PII, health info)

Confidential Data: information that organization intends to keep secret among a certain group of people

Proprietor: owner
Proprietary Data: owned by an individual, group, or an organization

- Includes patents, trade secrets, software algorithms, designs

Personally Identifiable Information (PII) includes information such as full name, birth date, biometric data, and identifying numbers such as SSN

- Personal health information is PII, which includes medical or health information
- Organizations have an obligation to protect PII and typically identify procedures for handling and retaining PII in data policies

Data Governance: refers to the processes an organization uses to manage, process, and protect data

- Some data governance methods help ensure or improve the quality of data
- Other methods are driven by regulations and laws
- Proper data governance practices ensure that critical data elements are identified

HIPPA (Health Insurance Portability and Accountability Act): mandates that organizations protect health information

GLBA (Gramm-Leach Bliley Act): requires financial institutions to provide consumers with a privacy notice explaining what information they collect and how it is used

SOX (Sarbanes-Oxley Act): requires executives within an organization to take individual responsibility for the accuracy of financial reports

GDPR (General Data Protection Regulation): this European Union directive mandates the protection of privacy data for individuals who live in the EU

Critical Data: data that is critical to the success of a mission within an organization

Data Minimalization: a principle requiring organizations to limit the information they collect and use

Data Masking: refers to modifying data to hide the original content

Data Anonymization: modifies data to protect the privacy of individuals by removing all PII within a data set

Pseudo-Anonymization: replaces PII and other data with pseudonyms or artificial identifiers

- If unauthorised personnel gain access to data, they won't be able to identify people in data set

Data Tokenization: replaces sensitive data elements with token

- Token is a substitute value used in place of the sensitive data
- Tokenization system can convert token back into its original form
- Ex) used in credit card mobile payments → important thing is that credit card data not used at POS, tokens are

Data Masking hides sensitive data by permanently replacing it with inauthentic data

- Anonymization attempts to permanently remove all PII within a data set to protect the privacy of individuals
- Pseudo-Anonymization replaces data elements within a data set with pseudonyms or artificial identifiers
- Tokenization replaces data elements with a token, or substitute value

Data Retention Policy: identifies how long data is retained, and sometimes specifies where it is stored

Data Sanitization: method ensures that data is removed or destroyed from any devices before disposing of the device

Common Methods of Destroying Data and Sanitize Media:

- File Shredding: repeatedly overwriting space where file is located with 1s and 0s
- Wiping: refers to process of completely removing all remnants of data on a disk
- Erasing and Overwriting: SSDs require a special process for sanitization
    - Some organization require personnel to physically destroy SSDS as only option
- Paper Shredding
- Burning: in an incinerator
- Pulping: additional step to paper shredding
- Pulverization: process of physically destroying media to sanitize it –
    - Sledge hammer
- Degaussing: very powerful electronic magnet that if a disk is passed through it, the degaussing field renders the data on tape and magnetic disk drives unreadable
- Third-Party Solutions to Destroy

CBT (Computer-Based Training)

User training helps keep personnel up to date on security policies and current threats

- CBT is on computers or online and allows students to learn at their own pace
- Phishing simulations mimic the type of phishing campaigns used by attackers and allow an organization to safely check to see if employees will respond to phishing emails
- Gamification adds game-design elements into training to increase user participation and interaction

Role-Based training ensures that employees receive appropriate training based on their roles in the organization

- Data owners are responsible for ensuring adequate security controls are in place to protect the data
- The data controller determines why and how personal data should be processed
- The data processor uses and manipulates the data on behalf of the data controller
- A data custodian/steward is responsible for routine daily tasks such as backing up data
- The data protection officer acts as an independent advocate for customer data

NIC Teaming: group two or more physical NICs into a single logical network device called a bond
ABAC (Attribute-Based Access Control): based on attributes that identify subjects and objects within a policy
DAC (Discretionary Access Control): an owner and the owner establishes access for the object
MAC (Mandatory Access Control): uses labels assigned to subjects and objects
RBAC (Role-Based Access Control): assigns rights and permissions
STP (Spanning Tree Protocol) and RSTP (Rapid Spanning Tree Protocol) prevent switch loop problems
MSSP (Managed Security Service Provider): third-party vendor that provides security for an organization

---

END OF CHAPTER 11

End of Notes

Congratulations on reaching the end of this material! This marks another step forward in your journey toward achieving your certification goals. Stay focused, trust in your preparation, and approach the challenges ahead with confidence.

Remember, success is the result of dedication, perseverance, and belief in yourself. You've got this!

Best wishes for your continued success.

Support

If you found this course helpful and would like to support me, you can buy me a coffee! Your support helps me create more valuable content. 😊 Check it out here: buymeacoffee.com/bobsingh