

Révision

Chap1.1: CyberSecurity & CIA Triad

Overview of Attacks and Breaches

Top Cybersecurity Threats in 2024

Change Healthcare Breach

A large-scale data breach exposed personal and medical information of 100 million Americans, raising concerns about data protection in the healthcare sector. Attackers likely exploited inadequate security protocols.

WarmCookie Malware

This malware spreads through deceptive links, using social engineering to compromise users. It aims to steal sensitive data and deliver payloads to infected systems.

Fortinet Zero-Day Exploitation

Hackers exploited unpatched vulnerabilities in FortiManager, affecting enterprise networks and demonstrating the importance of rapid vulnerability management.

LockBit Ransomware on macOS

An adapted version of LockBit ransomware specifically targeted macOS systems, representing an expansion of ransomware's scope beyond traditional Windows environments

'Business' of hacking

There are a few broad categories for attacker groups: organized crime, corporate espionage, hacktivism, cyber warfare/terrorism, and those just looking for pure monetary gain. We can compare the different lines of business within the hacking industry and see how financially lucrative each business is.

Cybersecurity ethics

Cybersecurity practices have as their aim the securing—that is, the keeping safe—of data, computer systems and networks (software and hardware). While those data, systems, and networks might have some economic or other value

in and of themselves, what cybersecurity practices primarily protect are the integrity, functionality, and reliability of human institutions/practices that rely upon such data, systems, and networks. And in protecting those institutions and practices, cybersecurity professionals in turn are protecting the lives and happiness of the human beings who depend upon them.

Information Security

Information security (or infosec) refers to the protection of data resources from unauthorized access, attack, theft, or damage. Data may be vulnerable because of the way it is stored, the way it is transferred, or the way it is processed. The systems used to store, transmit, and process data must demonstrate the properties of security.

Secure information has three properties, often referred to as the CIA Triad:

- Confidentiality means that certain information should only be known to certain people.
- Integrity means that the data is stored and transferred as intended and that any modification is authorized.

- Availability means that information is accessible to those authorized to view or modify it.

Cybersecurity Framework

Within the goal of ensuring information security, cybersecurity refers specifically to provisioning secure processing hardware and software. Information security and cybersecurity tasks can be classified as five functions, following the framework developed by the National Institute of Standards and Technology (NIST)

- Identify: develop security policies and capabilities. Evaluate risks, threats, and vulnerabilities and recommend security controls to mitigate them.
- Protect: procure/develop, install, operate, and decommission IT hardware and software assets with security as an embedded requirement of every stage of this operations life cycle.
- Detect : perform ongoing, proactive monitoring to ensure that controls are effective and capable of protecting against new types of threats.
- Respond: identify, analyze, contain, and eradicate threats to systems and data security.

- Recover: implement cybersecurity resilience to restore systems and data if other controls are unable to prevent attacks

Chap2.1 Network Fundamentals

Data Networking Introduction

What is Data Networking?

Data networking involves technologies and systems that connect individuals and devices, enabling the sharing of stories, knowledge, opinions, and experiences. The internet is the backbone of this communication, often referred to as a "network of networks." By understanding networking, you can grasp how the internet works and its impact on our daily lives.

Primary Network Types:

- LAN (Local Area Network)
- WAN (Wide Area Network)
- PAN (Personal Area Network)
- MAN (Metropolitan Area Network)

Each network type serves different purposes and operates within specific ranges, which we will explore below.

Personal Area Network (PAN)

A Personal Area Network (PAN) covers a very small area, such as a room.

Common PAN technologies include:

- Wireless: Bluetooth and Wi-Fi
- Wired: USB connections

Examples include:

- Communication between smartphones and wireless headsets
- Printers, keyboards, and other peripheral devices interacting with computers

Although small, PANs are vital for individual device communication.

Local Area Network (LAN)

A Local Area Network (LAN) spans a small geographic area, typically ranging from 1 to 5 kilometers. Examples include:

- Homes, offices, schools, and small groups of buildings

LANs often use:

- Wired connections: Ethernet cables
- Wireless connections: Wi-Fi (e.g., 802.11a, 802.11b, 802.11g, 802.11n)

Key protocols include Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI). LANs connect computers, servers, and peripherals, enabling fast and efficient communication within the network.

Metropolitan Area Network (MAN)

A Metropolitan Area Network (MAN) connects multiple LANs over a larger geographic area, such as a city, with ranges of 50-60 kilometers. Key features:

- Backbone lines (often optical fiber) enable high-speed data transfer
- Protocols: RS-232, X.25, Frame Relay, and ATM

MANs are ideal for connecting local networks within urban areas.

Wide Area Network (WAN)

A Wide Area Network (WAN) spans large geographic regions, ranging from 100 to 1000 kilometers or more. Examples include:

- Networks connecting cities, regions, or even countries

WANs utilize a variety of devices, such as routers, switches, firewalls, and modems. Communication often occurs via microwave satellites. Common WAN protocols include Frame Relay, X.25, ISDN, and Point-to-Point Protocol (PPP).

OSI Model: The Seven Layers of Networking

The Open Systems Interconnection (OSI) model is a conceptual framework that organizes networking into seven distinct layers:

1. Physical Layer: Handles physical equipment (e.g., cables and switches) and bit transmission.
2. Data Link Layer: Manages data transfer within the same network, using frames for communication.
3. Network Layer: Facilitates data transfer between different networks and determines routing paths.
4. Transport Layer: Ensures end-to-end communication, flow control, and error correction.

5. Session Layer: Manages communication sessions between devices, including synchronization.
6. Presentation Layer: Prepares data for application use by handling encryption, compression, and translation.
7. Application Layer: Interfaces directly with user data through applications like web browsers and email.

The OSI model helps troubleshoot network issues by isolating problems within specific layers, streamlining the debugging process.

IP Addressing Basics

An IP address is a 32-bit identifier for devices on a network, written in two notations:

- Dotted Decimal Notation: E.g., 192.168.0.1
- Hexadecimal Notation: E.g., 0xC0A80001

Classful Addressing:

- Class A: 1.0.0.1 to 126.255.255.254 (Large networks)
- Class B: 128.1.0.1 to 191.255.255.254 (Medium networks)

- Class C: 192.0.1.1 to 223.255.254.254 (Small networks)
- Class D: 224.0.0.0 to 239.255.255.255 (Multicast)
- Class E: 240.0.0.0 to 255.255.255.254 (Experimental)

Each IP address has a Network ID and a Host ID based on its class.

Subnetting:

Subnetting divides a network into smaller sub-networks by extending the default mask. For example:

- Class C Network: 204.17.5.0
- Subnet Mask: 255.255.255.224 (creates 8 subnets, each with 30 usable addresses)

Subnetting allows efficient use of IP addresses and enhanced network management.

Chap2.2 Network Topologies

Topic	Key Details
-------	-------------

Physical Topology	- Based on geographic location. - Divided by offices or branches (e.g., New York LAN, Headquarters LAN).
------------------------------	---

Logical Topology	- Based on operational/security requirements. - Achieved via VLANs or ACLs (e.g., Network device management VLAN, Database server VLAN).
-----------------------------	---

Bus Network Topology	Description: Single cable connects all devices. Advantages: Simple, cost-effective for small networks. Disadvantages: Single point of failure, high traffic decreases performance, outdated.
--	--

Star Network Topology	Description: Central switch connects all devices. Advantages: Easy management, fault tolerance for individual nodes. Disadvantages: Central switch failure cripples the network, expensive.
---	---

Ring Network Topology	Description: Nodes connected in a circular format. Advantages: Low packet collision risk, high-speed data transmission. Disadvantages: Vulnerable to node/link failure, scalability issues, downtime needed for changes.
---	--

Mesh Network Topology	Description: Nodes interconnected (full or partial). Advantages: Reliable, no single point of failure, secure. Disadvantages: Expensive, complex setup, high configuration requirements.
---	--

Flat Networks	- Simple structure where all devices communicate freely. - Common in small businesses and homes. - Disadvantage: Lacks internal security, vulnerable to breaches.
---------------------------------	---

Segmented Networks	- Uses routing and segmentation to restrict node connections. - Improves security by isolating compromised machines. - Examples: Guest networks, departmental isolation.
--------------------------------------	--

Relation to Security	- More segmentation enhances breach resistance and containment. - Limits malware spread and allows time for response. - Modern security focuses on damage control over 100% prevention.
-----------------------------	---

Mitigation Techniques	- Routing, segmentation, internal firewalls, and IoT separation. - Techniques like NAT, QoS throttling, and jump boxes. - Companies with heavy segmentation limit damage from attacks and invest in backups for quick recovery.
------------------------------	---

Chap2.3 Network reconnaissance

The process of mapping out the attack surface is referred to as network reconnaissance and discovery. Reconnaissance techniques can be used by threat actors, but they can also be used by security professionals to probe and test their own security systems, as part of a security assessment and ongoing monitoring.

Topology discovery (or "footprinting") means scanning for hosts, IP ranges, and routes between networks to map out the structure of the target network. Topology discovery can also be used to build an asset database and to identify non-authorized hosts (rogue system detection) or network configuration errors.

Basic topology discovery tasks can be accomplished using the command line tools built into Windows and Linux. The following tools report the IP configuration and test connectivity on the local network segment or subnet.

- **ipconfig**—shows the configuration assigned to the network interface(s) in Windows.
- **ifconfig**—show the configuration assigned to the network interface(s) in Linux.
- **ping**—probe a host on a particular IP address or host name using Internet Control Message

- **Protocol (ICMP).** You can use ping with a simple script to perform a sweep of all the IP addresses in a subnet.

The following example will scan the 10.1.0.0/24 subnet from a Windows machine:

```
for /l %i in (1,1,255) do @ping -n 1 -w 100 10.1.0.%i | find /i "reply"
```



- **arp**—display the local machine's Address Resolution Protocol (ARP) cache. The ARP cache shows the MAC address of the interface associated with each IP address the local host has communicated with recently. This can be useful if you are investigating a suspected spoofing attack. For example, a sign of a man-in-the-middle attack is where the MAC address of the default gateway IP listed in the cache is not the legitimate router's MAC address.

ROUTE AND TRACEROUTE

The following tools can be used to test the routing configuration and connectivity with remote hosts and networks.

- **route**—view and configure the host's local routing table. Most end systems use a default route to forward all traffic for remote networks via a gateway router. If the host is not a router, additional entries in the routing table could be suspicious.
- **tracert**—uses ICMP probes to report the round trip time (RTT) for hops between the local host and a host on a remote network. tracert is the Windows version of the tool.
- **tracert**—performs route discovery from a Linux host. traceroute uses UDP probes rather than ICMP, by default.
- **pathping**—provides statistics for latency and packet loss along a route over a longer measuring period. pathping is a Windows tool; the equivalent on Linux is mtr.

In a security context, high latency at the default gateway compared to a baseline might indicate a man-in-the-middle attack. High latency on other hops could be a sign of denial of service, or could just indicate network congestion.

Tools

Tool/Concept	Description	Key Features/Commands
IP Scanners	Tools for host discovery and mapping network topology.	Examples: Microsoft System Center (authorized scans with SNMP), Nmap (stealth scanning, port scanning).
Nmap	Open-source IP scanner for network reconnaissance, service discovery, and OS fingerprinting.	- Host discovery: nmap -sn suppresses port scans. - TCP SYN scan: nmap -sS (fast, half-open scan). - UDP scan: nmap -sU.

		- Port range: nmap -p. - Service/version detection: nmap -sV. - OS fingerprinting: nmap -o or -A.
Netstat/ss	Command-line tools for viewing active network connections and service states on a local machine.	Useful for checking service misconfigurations, malware, or unauthorized connections. ss is the modern alternative to netstat in Linux.
Nslookup/ Dig	Query DNS records to identify misconfigurations or vulnerabilities like zone transfers.	Example: nslookup <domain> (Windows), dig <domain> (Linux).

theHarvester	OSINT tool for gathering public data about a domain, including emails and subdomains.	Install: <code>sudo apt install theharvester.</code> Run: <code>theHarvester -d <domain> -b <source>.</code> Save results: <code>theHarvester -d <domain> -b google -f results.html.</code>
dnsenum	DNS reconnaissance tool for analyzing records and finding IP ranges or hidden subdomains.	Install: <code>sudo apt install dnsenum.</code> Run: <code>dnsenum <domain>.</code> Use brute force with: <code>dnsenum --dnsserver <dns_server_ip> --threads 5 --subfile subdomains.txt <domain>.</code>

scanless	Anonymous port scanning tool using third-party services.	Install: <code>pip3 install scanless.</code> Run: <code>scanless -t <domain>.</code> Choose service: <code>scanless -t <domain> -s <service_name>.</code>
curl	Command-line client for HTTP requests and web application testing.	Examples: - Basic GET: <code>curl -v http://<domain>.</code> - POST request: <code>curl -X POST -d "username=admin&password=12345" http://<domain>/login.</code> - Handle redirects: <code>curl -L http://<domain>.</code>
Nessus	Commercial vulnerability scanner for	Install: <code>sudo dpkg -i Nessus-<version>.deb.</code>

	identifying software vulnerabilities.	Start service: sudo systemctl start nessusd.service. Run scans via web UI at https://<your_ip>:8834.
Reconnaissance Tools	Tools like Kali Linux and ParrotOS bundle multiple utilities for security assessments.	Examples: theHarvester, dnsenum, scanless, curl.

2.4 Packet Capture and Analysis

Packet and Protocol Analysis

- **Packet Analysis:** Examines individual frames in captured network traffic for detailed inspection.
- **Protocol Analysis:** Uses statistical tools to analyze sequences of packets (packet traces).

Sniffer Tools for Capturing Traffic

- Sniffers can capture traffic from a **host** or a **network segment** using:

- **SPAN Port (Mirror Port):** Configures a switch to copy frames from source to destination ports.
- **TAP (Test Access Port):** A device inserted into the cable to copy traffic. Available as passive or active versions.

Sniffers are typically placed inside firewalls or near critical servers to identify malicious traffic. However, deploying multiple sensors requires adequate resources due to the large volume of data generated.

tcpdump (Command-Line Packet Capture)

- Basic usage: `tcpdump -i eth0` (captures traffic on the specified interface).
- Save packets to a file: `-w` option; Read from a file: `-r` option.
- **Filters:**
 - **Type:** e.g., `host`, `net`, `port`.
 - **Direction:** e.g., `src` (source) or `dst` (destination).
 - **Protocol:** e.g., `tcp`, `udp`, `icmp`.

Combine filters with Boolean operators (`and`, `or`, `not`). Example:

```
tcpdump -i eth0 "src host 10.1.0.100 and (dst port 53 or dst port 80)"
```

Wireshark (Graphical Packet Analysis Tool)

- **Features:**

- Three-pane view:

1. **Packet List:** Summary of frames.
2. **Packet Details:** OSI layer and protocol details.
3. **Packet Bytes:** Raw frame data in hex/ASCII.

- Supports live capture or analysis of saved **.pcap** or **.pcapng** files.
 - Powerful **display filters** and customizable coloring rules for easier analysis.

- **Follow TCP Stream:** Reconstructs packet contents for a TCP session.

- **PCAPNG Format:** Improved format with more metadata; supported by Wireshark and tcpdump.

Wireshark provides a comprehensive way to decode and analyze network traffic, making it a preferred choice for in-depth protocol analysis.

Active defence: 3.1 Firewalls

A **firewall** is a network security solution designed to monitor, filter, and control incoming and outgoing traffic based on predefined security rules.

Types of Firewalls

1. **Hardware Firewall:**

- Physical device placed between internal and external networks.
- Handles high traffic volumes, suitable for large organizations.
- More reliable but expensive and complex to configure.

2. Software Firewall:

- An application installed on a server or device.
- Easy to deploy for small businesses or individuals.
- Less efficient than hardware firewalls for handling heavy traffic.

3. Packet-Filtering Firewall (Stateless):

- Examines individual packets based on basic rules (IP address, port, protocol).
- Simple but vulnerable to advanced attacks like spoofing.

4. Stateful Inspection Firewall:

- Tracks the state of network connections (e.g., TCP, UDP sessions).
- Enables filtering based on the context of packets.

5. Next-Generation Firewall (NGFW):

- Combines traditional features with advanced inspection (application analysis, intrusion detection, etc.).
- Includes content analysis, malware detection, and application control.

Key Features

- **Address Filtering:** Blocks or allows specific IP addresses or ranges.
- **Port and Protocol Filtering:** Controls communication through specific ports/protocols (HTTP, FTP, etc.).
- **Deep Packet Inspection (DPI):** Analyzes packet content to detect threats (malware, attacks).
- **NAT (Network Address Translation):** Masks internal IP addresses using a public address.
- **VPN (Virtual Private Network):** Ensures secure connections for remote users.

Advantages of a Firewall

- Protects against unauthorized access.
- Reduces exposure to DDoS attacks, malware, and exploit vulnerabilities.
- Provides centralized control over network access.

Limitations

- Does not protect against internal threats or attacks from compromised devices.
- Requires proper configuration to avoid vulnerabilities.

Active defence: 3.1 IDS

Intrusion Detection System (IDS)

An **Intrusion Detection System (IDS)** is a cybersecurity tool designed to monitor network traffic and systems for suspicious activity or policy violations. Unlike a firewall, which blocks unauthorized access, an IDS identifies and alerts administrators about potential threats.

Types of IDS

1. Network-Based IDS (NIDS):

- Monitors network traffic on specific segments.
- Detects attacks such as DDoS, port scanning, or malware spreading.
- Example: Snort, Suricata.

2. Host-Based IDS (HIDS):

- Monitors activities on a specific host (server or workstation).
- Tracks system logs, file integrity, and user activities.
- Example: OSSEC, Tripwire.

3. Hybrid IDS:

- Combines features of both NIDS and HIDS.
- Offers comprehensive monitoring for both network and hosts.

Detection Methods

1. **Signature-Based Detection:**

- Relies on predefined attack patterns or signatures.
- Effective against known threats but cannot detect zero-day attacks.

2. **Anomaly-Based Detection:**

- Uses machine learning or baselines to detect unusual behavior.
- Can identify new or unknown attacks but may produce false positives.

3. **Heuristic/Behavioral Detection:**

- Analyzes patterns of behavior to flag malicious activity.
- Useful for identifying advanced persistent threats (APTs).

Key Features

- **Alerting:** Notifies administrators in real time about detected intrusions.
- **Logging:** Maintains detailed records of detected activities for analysis.

- **Integration:** Can work alongside firewalls, SIEMs, and other tools for enhanced security.
- **Traffic Analysis:** Monitors protocols, payloads, and metadata to identify threats.

Advantages of IDS

- Detects threats that firewalls may miss (e.g., insider attacks).
- Provides visibility into network and system behavior.
- Enhances incident response by providing forensic data.

Limitations

- **Passive Role:** IDS only alerts and does not actively block threats (unlike IPS).
- **False Positives:** May generate unnecessary alerts for benign activities.
- **Resource-Intensive:** Requires proper configuration and maintenance to avoid performance issues.

Active defence: 3.1 IPS

An Intrusion Prevention System (IPS) is a security tool designed to actively monitor, detect, and prevent malicious activities on a network. Unlike an IDS,

which only identifies and alerts about threats, an IPS takes immediate action to block or mitigate those threats.

Types of IPS

1. **Network-Based IPS (NIPS):**

- Monitors and protects the entire network.
- Deployed at critical points, such as between the internet and internal networks.
- Example: Cisco Firepower, Palo Alto Networks.

2. **Host-Based IPS (HIPS):**

- Protects individual devices or hosts by analyzing application behavior, logs, and system changes.
- Example: Symantec Endpoint Protection.

3. **Hybrid IPS:**

- Combines features of both NIPS and HIPS for comprehensive security.

Detection Methods

1. **Signature-Based Detection:**

- Identifies known attack patterns using predefined signatures.

- Fast and accurate against established threats but ineffective for zero-day attacks.

2. Anomaly-Based Detection:

- Monitors for deviations from normal traffic patterns or behaviors.
- Effective for detecting unknown threats but prone to false positives.

3. Policy-Based Detection:

- Enforces predefined security policies, such as blocking certain protocols or IP ranges.
- Useful in environments with strict compliance requirements.

4. Heuristic/Behavioral Detection:

- Uses advanced algorithms to detect abnormal behavior or advanced persistent threats (APTs).

Key Features

- **Active Blocking:** Automatically blocks malicious traffic or activity in real time.
- **Threat Intelligence:** Utilizes updated databases of threat signatures and indicators of compromise (IoCs).

- **Traffic Inspection:** Examines packet headers, payloads, and metadata to identify threats.
- **Integration:** Works alongside firewalls, SIEMs, and other security tools for comprehensive protection.

Advantages of IPS

- **Real-Time Prevention:** Acts immediately to stop threats before they cause harm.
- **Reduced Human Intervention:** Automates the mitigation process, saving time for security teams.
- **Advanced Threat Detection:** Protects against a wide range of threats, including malware, DDoS attacks, and zero-day vulnerabilities.
- **Compliance Support:** Helps organizations meet regulatory requirements by enforcing security policies.

Limitations

- **False Positives:** May block legitimate traffic if not configured properly.
- **Performance Impact:** Deep packet inspection can slow down network traffic if the IPS is overloaded.
- **Resource Dependency:** Requires regular updates to threat signatures and policies to remain effective.

Active defence: 3.2 SIEM

A Security Information and Event Management (SIEM) system is a comprehensive tool used to collect, analyze, and manage security data from across an organization's network, providing real-time visibility into potential threats and incidents.

Core Functions of a SIEM

1. Log Collection and Aggregation:

- Collects log data from various sources like firewalls, IDS/IPS, servers, endpoints, and applications.
- Centralizes data for easier analysis.

2. Event Correlation:

- Analyzes collected data to identify patterns and correlate events that may indicate malicious activity.
- Example: Multiple failed login attempts followed by a successful login from an unusual IP.

3. Real-Time Alerts:

- Generates alerts for detected threats or anomalies, allowing security teams to respond quickly.

4. Threat Detection and Analysis:

- Uses predefined rules, machine learning, and threat intelligence to detect known and emerging threats.

5. Incident Management and Response:

- Helps security teams prioritize and investigate incidents efficiently.
- Can integrate with automation tools for faster response.

6. Compliance Reporting:

- Provides reports and audit trails to meet regulatory requirements (e.g., GDPR, HIPAA, PCI-DSS).

Benefits of SIEM

- **Centralized Visibility:**

- Unifies security data from multiple sources, enabling a complete view of the organization's security posture.

- **Advanced Threat Detection:**

- Detects complex attacks that might go unnoticed by standalone security tools.

- **Enhanced Response Time:**

- Provides actionable insights and automates certain responses to reduce mean time to respond (MTTR).

- **Regulatory Compliance:**

- Simplifies compliance with automated reporting and data retention features.

Key Features

- **Integration:**

- Works with various security tools like firewalls, IDS/IPS, endpoint detection, and cloud services.

- **Threat Intelligence:**

- Leverages global threat feeds to recognize emerging threats.

- **Dashboards and Visualization:**

- Offers user-friendly interfaces to visualize security metrics and alerts.

- **Log Retention:**

- Stores logs for long-term analysis and compliance requirements.

Challenges of SIEM

1. **High Cost:**

- Licensing, deployment, and operational costs can be significant.

2. **Complexity:**

- Requires expertise to configure, tune, and manage effectively.

3. False Positives:

- May generate numerous alerts, including non-critical ones, leading to alert fatigue.

4. Scalability:

- Large organizations may require extensive resources to scale SIEM capabilities effectively.

Examples of Popular SIEM Solutions

- **Splunk Enterprise Security**
- **IBM QRadar**
- **Microsoft Sentinel**
- **Arcsight**
- **Elastic SIEM**

Attacks, Threats, Vulnerabilities & Architecture

1. Common Threat Actors and Motivations

Threat actors are entities that perform malicious actions against systems or networks. They are categorized by motivations and capabilities:

- **Hacktivists:** Ideologically motivated; disrupt services or deface websites.
- **Cybercriminals:** Financially motivated; use ransomware, phishing, and fraud.
- **Nation-States:** Espionage and sabotage; target critical infrastructure, intellectual property.
- **Insiders:** Employees or contractors with malicious intent or negligence.
- **Script Kiddies:** Low-skilled attackers using pre-written tools.
- **Terrorist Groups:** Politically or ideologically motivated to cause large-scale harm.

2. Common Threat Vectors and Attack Surfaces

A **threat vector** is a path used by attackers to exploit vulnerabilities, while the **attack surface** is the total exposure to potential attacks.

- **Threat Vectors:**
 - Phishing emails
 - Malware-laden websites

- Insecure APIs
- Physical breaches (e.g., USB drives)
- Exploiting weak passwords
- **Attack Surfaces:**
 - **Digital:** Open ports, unpatched software, IoT devices.
 - **Physical:** Workstations, access to servers.
 - **Human:** Social engineering, insider threats.

3. Explain Threat Intelligence Sources

Threat intelligence helps organizations anticipate, identify, and mitigate threats.

- **Sources:**
 - Open-source intelligence (OSINT): Publicly available data (blogs, forums).
 - Commercial feeds: Paid intelligence from providers (e.g., Recorded Future).
 - Information Sharing and Analysis Centers (ISACs): Sector-specific threat sharing.
 - Government sources: CERTs, FBI alerts.

- Dark web monitoring: Tracking threat actor activities.

4. Types of Vulnerabilities

Vulnerabilities are weaknesses in systems that attackers exploit.

- **Technical:**

- Unpatched software
- Misconfigured systems
- Weak encryption

- **Human:**

- Social engineering
- Lack of awareness

- **Physical:**

- Inadequate physical security measures

- **Zero-Day Vulnerabilities:**

- Exploits discovered before a patch is available.

5. Indicators of Malicious Activity

Indicators (IOCs) are clues that suggest a potential or active cyberattack.

- **Network Indicators:**

- Unusual outbound traffic
- Traffic to known malicious IPs
- **Endpoint Indicators:**
 - Unauthorized file changes
 - Unknown processes
- **Behavioral Indicators:**
 - Login attempts outside normal hours
 - Use of administrative accounts in unexpected ways.

6. Mitigation Techniques Used to Secure the Enterprise

Organizations deploy multiple layers of security to prevent and mitigate threats.

- **Technical Controls:**
 - Firewalls, IDS/IPS, endpoint security.
- **Access Controls:**
 - Role-based access control (RBAC), multi-factor authentication (MFA).
- **Regular Updates:**
 - Patch management for OS and applications.

- **Backups:**
 - Regularly backup data and store offsite.
- **User Training:**
 - Teach staff to recognize phishing and social engineering.

7. New Defensive Techniques

Emerging technologies and strategies in cybersecurity:

- **Zero Trust Architecture (ZTA):**
 - Never trust, always verify; granular access control.
- **Extended Detection and Response (XDR):**
 - Integrates multiple data sources for comprehensive detection.
- **Threat Hunting:**
 - Proactively search for threats in systems.
- **AI/ML Security Tools:**
 - Automates detection of anomalies and malicious activities.

8. Identifying Social Engineering

Social engineering exploits human behavior to manipulate victims.

- **Tactics:**

- Phishing (emails, messages).
- Pretexting (fake identities to gain trust).
- Baiting (luring with USBs, fake rewards).
- Tailgating (following someone into secure areas).
- **Prevention:**
 - Awareness training.
 - Verify unknown requests.
 - Implement policies like clean desk and MFA.

9. Malware Analysis

Malware analysis determines the functionality and impact of malicious code.

- **Types of Malware:**
 - Viruses, worms, ransomware, trojans, spyware, adware.
- **Analysis Techniques:**
 - **Static Analysis:** Examine code without execution.
 - **Dynamic Analysis:** Execute malware in a sandbox environment.
- **Key Tools:**
 - IDA Pro, Ghidra, Cuckoo Sandbox.
- **Prevention:**

- Use updated antivirus and endpoint detection tools.
- Employ behavioral analysis to detect anomalies.

Architecture & Design II

1. Implementing Authentication Controls

Authentication controls verify the identity of users or systems and ensure proper access.

- **Principles:**

- Something you know: Passwords, PINs.
- Something you have: Smart cards, tokens.
- Something you are: Biometrics.
- Somewhere you are: Geolocation-based authentication.
- Something you do: Behavioral patterns, typing cadence.

- **Best Practices:**

- Enforce strong password policies (length, complexity, expiration).
- Use Multi-Factor Authentication (MFA).
- Implement account lockout thresholds for repeated failed attempts.

2. Implement Authentication Technologies

Technologies help enforce secure authentication in modern systems.

- **Single Sign-On (SSO):**
 - One set of credentials provides access to multiple systems.
 - Reduces password fatigue and improves security.
- **Federated Identity Management:**
 - Uses a trusted third party to authenticate users across organizations (e.g., SAML, OAuth).
- **Certificate-Based Authentication:**
 - Uses digital certificates for secure logins (e.g., PKI).
- **Token-Based Authentication:**
 - Temporary tokens for session-based access (e.g., OAuth2, JWT).
- **Biometric Authentication:**
 - Ensures access based on unique physical or behavioral characteristics.

3. Biometrics

Biometric technologies are highly secure and difficult to replicate but have privacy and usability concerns.

- **Types of Biometrics:**

- **Physical:**

- Fingerprint scanning
 - Iris or retinal recognition
 - Facial recognition

- **Behavioral:**

- Voice recognition
 - Typing patterns

- **Challenges:**

- False positives/negatives.
 - Privacy concerns around biometric data storage.
 - Spoofing (e.g., using masks for facial recognition).

- **Benefits:**

- Stronger than passwords.
 - Non-transferable and unique to each user.

4. Implementing Cybersecurity Resilience

Cybersecurity resilience ensures business continuity even during attacks or disruptions.

- **Key Principles:**

- **Redundancy:** Backups for critical systems and data.
- **Incident Response:** Documented processes to address breaches.
- **Disaster Recovery Plans (DRP):** Systems to recover from disasters quickly.
- **Business Continuity Plans (BCP):** Ensure critical services remain operational.

- **Resilience Techniques:**

- Regular testing of backups and recovery plans.
- Implement high availability (HA) solutions like load balancing and failover clusters.
- Use immutable backups to prevent ransomware tampering.

5. Physical Security

Physical security protects systems, data, and personnel from physical threats.

- **Key Components:**

- **Access Controls:**
 - Locks, badges, and smart cards to secure facilities.
 - Use of surveillance cameras and monitoring.

- **Environmental Controls:**
 - Fire suppression systems.
 - Climate controls to prevent overheating.
- **Perimeter Security:**
 - Fences, guards, and barriers to deter unauthorized access.
- **Best Practices:**
 - Enforce security zones with restricted access levels.
 - Implement intrusion detection systems for physical breaches.
 - Train staff to report and respond to suspicious activities.

Cryptography & Secure Solution

Implementation I

1. Cryptography in General

Cryptography is the science of securing information by transforming it into an unreadable format for unauthorized users while ensuring authorized users can access it.

- **Core Goals (CIA):**

- **Confidentiality:** Protects data from unauthorized access (encryption).
- **Integrity:** Ensures data has not been tampered with (hashing).
- **Availability:** Data is accessible to authorized users when needed.
- **Authentication:** Verifies the identity of users.
- **Non-Repudiation:** Prevents denial of actions (digital signatures).
- **Key Concepts:**
 - **Encryption:** Converting plaintext to ciphertext (e.g., AES, RSA).
 - **Decryption:** Reverting ciphertext back to plaintext.
 - **Keys:** Secret values used in encryption/decryption.

2. Cryptography for Signature

Digital signatures verify the authenticity and integrity of data.

- **How It Works:**
 - A private key encrypts the signature, while the corresponding public key decrypts it.
 - The hash of the data is signed and compared at the receiver's end to ensure the data hasn't been altered.
- **Use Cases:**

- Signing emails and documents.
- Verifying the legitimacy of software updates.
- Ensuring secure online transactions.
- **Popular Algorithms:**
 - RSA
 - Digital Signature Algorithm (DSA)
 - Elliptic Curve Digital Signature Algorithm (ECDSA)

3. Cryptography Pros and Cons / Advanced Cryptographical Techniques

Pros of Cryptography:

- **Data Protection:** Strong encryption prevents unauthorized access.
- **Authentication:** Ensures trust in communications and systems.
- **Compliance:** Meets legal and industry regulations for data protection.
- **Flexibility:** Can secure both stored and transmitted data.

Cons of Cryptography:

- **Complexity:** Implementation errors can create vulnerabilities.
- **Performance Overhead:** Can slow down systems if poorly optimized.
- **Key Management Issues:** Loss or compromise of keys can lead to data breaches.

- **Potential for Abuse:** Encryption can be misused by malicious actors for illicit activities.

Advanced Cryptographic Techniques:

- **Quantum Cryptography:** Uses quantum mechanics to achieve secure communication (e.g., Quantum Key Distribution - QKD).
- **Homomorphic Encryption:** Allows computations on encrypted data without decryption.
- **Zero-Knowledge Proofs:** Enables one party to prove knowledge of information without revealing it.
- **Post-Quantum Cryptography:** Algorithms resistant to quantum computing threats.

4. Modern Cryptography

Modern cryptography is based on rigorous mathematical algorithms and is categorized into symmetric and asymmetric systems.

Symmetric Cryptography (Shared Key):

- Uses the same key for encryption and decryption.
- Fast and efficient for large data (e.g., AES, DES).
- Limitation: Key distribution is challenging.

Asymmetric Cryptography (Public/Private Key):

- Uses a pair of keys: one for encryption (public) and one for decryption (private).
- Suitable for secure communications and key exchange (e.g., RSA, ECC).
- **Limitation:** Slower than symmetric cryptography.

Hashing:

- A one-way function used for data integrity (e.g., SHA-256, MD5).
- Often combined with encryption for secure message authentication.

5. Implementing Secure Protocols

Secure protocols use cryptography to protect data during transmission and ensure trusted communication.

Key Secure Protocols:

- **TLS/SSL (Transport Layer Security):** Encrypts web communications (HTTPS).
- **IPsec (Internet Protocol Security):** Secures data at the network layer.
- **SSH (Secure Shell):** Encrypts remote login sessions.
- **S/MIME (Secure/Multipurpose Internet Mail Extensions):** Secures email communication.

Implementation Best Practices:

- Use the latest cryptographic standards (e.g., TLS 1.3).
- Enforce strong key management policies.
- Regularly update software to patch vulnerabilities.
- Disable deprecated algorithms (e.g., MD5, SHA-1).