Module : 27 Ech - Information Gathering

1) The CIA Triad is a fundamental concept in information security that stands for Confidentiality, Integrity, and Availability.

- Each component plays a critical role in ensuring the protection of data and systems.

2) A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

- Its primary purpose is to create a barrier between a trusted internal network and untrusted external networks, such as the internet.

3) Vulnerability Assessment (VA)

- Focus: Identifying potential weaknesses and vulnerabilities in systems, networks, and applications.
- Methodology: Primarily uses automated tools to scan for known vulnerabilities, misconfigurations, and outdated software. May also involve some manual analysis.
- Output: A report listing identified vulnerabilities, their severity levels, and recommended remediation steps.
- Goal: To provide a broad overview of an organization's security posture and highlight areas that need attention.

- Frequency: Can be performed regularly (e.g., weekly or monthly) due to its automated nature.
- Penetration Testing (PT)
- Focus: Simulating real-world cyberattacks to identify exploitable vulnerabilities and assess the potential impact of a successful attack.
- Methodology: Involves ethical hackers manually attempting to exploit vulnerabilities, using various techniques and tools to gain unauthorized access.
- Output: A report detailing the exploited vulnerabilities, the methods used to exploit them, the potential impact, and recommendations for strengthening defenses.
- Goal: To provide a deeper understanding of an organization's security risks and identify weaknesses that automated tools might miss.
- Frequency: Typically performed less frequently (e.g., annually or after significant system changes) due to its time-consuming and resource-intensive nature.

4) HIDS (Host-based Intrusion Detection System)

- Focus: Monitors individual devices (hosts) like computers, servers, or endpoints for suspicious activity.
- Location: Installed directly on the host it protects.

- Data Source: Analyzes logs, system calls, file changes, and other activities within the host.
- Detection: Primarily uses signature-based detection (comparing known attack patterns) and anomaly-based detection (identifying deviations from normal behavior) on the host.
- NIDS (Network-based Intrusion Detection System)
- Focus: Monitors network traffic for suspicious activity across the entire network or a specific segment.
- Location: Strategically placed within the network (e.g., at network entry/exit points, subnets).
- Data Source: Analyzes network packets and traffic patterns.
- Detection: Uses both signature-based and anomaly-based detection to identify suspicious network behavior.

5) SSL (Secure Sockets Layer) encryption is a crucial security protocol that protects your data as it travels across the internet.

- SSL encryption scrambles your data into an unreadable format before it's sent.
- Only the intended recipient with the correct "key" can unscramble and read it.
- This ensures that even if someone intercepts the data, they can't understand it.

6) Data leakage is the unintentional or unauthorized release of sensitive information to individuals or entities who should not have access to it.

- This can occur in various ways, often due to human error, technical vulnerabilities, or malicious intent.

7) A Brute Force Attack is a method used by attackers to gain access to a system or account by systematically trying all possible combinations of passwords or encryption keys until the correct one is found.

- Strong Password Policies
- Account Lockout Mechanisms
- Multi-Factor Authentication (MFA)
- Use of CAPTCHA
- Regularly Update Passwords
- Monitor and Respond to Suspicious Activity

8) A Man-in-the-Middle (MITM) Attack is a type of cyberattack where an attacker secretly intercepts and potentially alters the communication between two parties who believe they are directly communicating with each other.

- The attacker positions themselves between the sender and receiver, capturing and possibly modifying the data being exchanged.
- This can lead to sensitive information being stolen, such as login credentials, financial information, or personal data.
- Use Strong Encryption
- Secure Wi-Fi Networks
- Verify Certificates
- Implement Multi-Factor Authentication (MFA)
- Regular Software Updates
- DNS Security
- Network Segmentation

9) A Cross-Site Scripting (XSS) attack is a type of security vulnerability found in web applications.

- It allows attackers to inject malicious scripts into web pages viewed by other users.
- These scripts can then execute in the user's browser, leading to various harmful consequences, such as data theft, session hijacking, and defacement of web pages.
- Input Validation and Sanitization:
- Output Encoding
- Content Security Policy (CSP)
- Escaping Data

- HTTPOnly and Secure Cookies
- Security Frameworks and Libraries
- Regular Security Testing

10) A Botnet is a network of compromised computers (also known as "bots" or "zombies") that are controlled by a malicious actor, often referred to as a "botmaster" or "bot herder."
- These infected devices are used to carry out various cybercriminal activities without the knowledge or consent of their owners.

11) SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols designed to provide secure communication over a computer network.
- SSL (Secure Sockets Layer)
- SSL was created to secure data transmission between web servers and browsers by encrypting the data. It ensures that any data transferred remains private and unaltered.
- SSL 3.0 is considered outdated and insecure due to known vulnerabilities.
- TLS (Transport Layer Security)

- TLS is the successor to SSL and provides similar encryption and security features but with improved algorithms and security measures.
- TLS 1.2 and TLS 1.3 are the most widely used versions today, with TLS 1.3 offering the best security features and performance.

12) Virus

- A virus is a type of malicious software that attaches itself to a legitimate program or file and spreads from one computer to another. It can replicate itself and infect other files or systems when the infected host file is executed.

13) Phishing is a type of cyberattack in which attackers attempt to deceive individuals into providing sensitive information, such as login credentials, financial information, or personal details, by pretending to be a trustworthy entity. The attackers often use email, text messages, or fake websites to carry out their schemes.

- Be Skeptical of Unsolicited Emails
- Check URLs
- Keep Security Software Updated

14) Encryption is the process of converting plain text or readable data into an encoded format called ciphertext.

- This transformation is done using an algorithm and a key. The purpose of encryption is to protect data from unauthorized access, ensuring that only authorized parties can read it.
- Encryption is widely used to secure sensitive information, such as financial transactions, personal data, and communications.
- Decryption is the process of converting ciphertext back into its original plain text or readable format. This is achieved using a decryption algorithm and a key.
- Decryption allows authorized parties to access and understand the protected information. For decryption to work, the key used must match the one used during encryption.

15) A Distributed Denial of Service (DDoS) Attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of internet traffic.

- Unlike a standard Denial of Service (DoS) attack, a DDoS attack uses multiple compromised devices (often referred to as a botnet) to generate the excessive traffic.

- Infection and Control
- Traffic Flooding
- Resource Exhaustion

16) A zero-day vulnerability refers to a security flaw in software or hardware that is unknown to the vendor or developer.
- Because the vulnerability is undiscovered, there are no existing patches or fixes available to address it.
- The term "zero-day" signifies that developers have had zero days to fix the issue before it is discovered and potentially exploited by attackers.

17) Network sniffing is the process of monitoring and capturing data packets traveling over a network.
- This can be done for both legitimate and malicious purposes.
- Network sniffing tools, also known as packet sniffers or network analyzers, can intercept and log network traffic to analyze the data being transmitted.

18) A Security Operations Center (SOC) is a centralized unit within an organization responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents and threats.

- The SOC operates continuously, ensuring the organization's IT infrastructure, systems, applications, and data remain secure from cyberattacks and breaches.

19) The importance of forensics in cyber security.

- Incident Response and Investigation
- Legal and Regulatory Compliance
- Prevention and Mitigation
- Attribution and Accountability

20) Future Trends in Cybersecurity

- Artificial Intelligence (AI) and Machine Learning (ML)
- Zero-Trust Architecture
- Quantum Computing
- Increased Focus on Cloud Security
- Supply Chain Security
- Remote Work Security
- Important Skills for Cybersecurity Professionals
- Scripting:
- Networking and System Administration:

- Cloud Security:
- Security Tools and Technologies
- Incident Response

21) Intrusion Detection System (IDS)

- IDS is designed to detect and alert on suspicious activities or potential security breaches within a network.
- It monitors network traffic in real-time, analyzing it against a database of known threat signatures or anomalous behavior patterns.
- IDS is a passive system that generates alerts when it detects suspicious activity. It does not take action to block or mitigate the threat.
- Intrusion Prevention System (IPS):
- IPS is designed to detect, prevent, and mitigate potential security threats in real-time.
- It actively monitors network traffic and can take immediate action to block or prevent malicious activities based on predefined rules and policies.
- IPS is an active system that can automatically block, quarantine, or mitigate threats without requiring manual intervention.