Module 10 CCNA - Security threat landscape

Security Threats:

Security threats refer to potential risks or vulnerabilities that can compromise the confidentiality, integrity, or availability of data, systems, or networks. Here are some common security threats:

Malware: Malicious software (viruses, worms, Trojans) that can damage or steal data.

Phishing: Deceptive emails or messages to trick users into revealing sensitive information.

Denial of Service (DoS): Overwhelming a system or network to disrupt its normal functioning.

Insider Threats: Malicious actions by authorized users (employees, contractors).

Data Breaches: Unauthorized access to sensitive data.

Social Engineering: Manipulating people to divulge confidential information.

Zero-Day Exploits: Attacks exploiting unknown vulnerabilities.

Ransomware: Encrypting data and demanding payment for decryption.

Man-in-the-Middle (MitM): Intercepting communication between parties.

Physical Attacks: Theft, destruction, or tampering with hardware.

Mitigation Techniques:

Organizations use various strategies to minimize or eliminate security threats. Here are some key mitigation techniques:

Risk Assessment: Identify vulnerabilities and assess their impact.

Incident Response Plan (IR): Develop a plan to handle security incidents.

User Training: Educate employees about security best practices.

Network Monitoring: Continuously monitor network traffic for anomalies.

Strong Password Policies: Enforce complex passwords and regular changes.

Patch Management: Keep software and systems up to date.

Encryption: Protect data in transit and at rest.

Access Controls: Limit user privileges based on the principle of least privilege.

Firewalls and VPNs: Secure network connections.

Threat Intelligence: Stay informed about emerging threats.

Backup and Recovery: Regularly back up critical data.

Physical Security Measures: Secure physical access to servers and devices.

DoS Attacks (Denial of Service Attacks):

A Denial-of-Service (DoS) attack aims to disrupt the normal functioning of a service, system, or network by overwhelming it with traffic or resource requests.

Key points:

Objective: Make a resource (e.g., website, server) unavailable to legitimate users.

Methods:

Flooding Attacks: Overwhelm the target with excessive traffic.

Resource Exhaustion: Exploit vulnerabilities to consume system resources (CPU, memory, bandwidth).

Impact:

Loss of revenue for businesses.

Damage to reputation.

Financial losses due to mitigation efforts.

Disruption of critical services (e.g., healthcare, emergency services).

Examples:

Ping of Death: Sending oversized ICMP packets to crash a system.

Teardrop Attack: Manipulating fragmented IP packets to crash the target.

Buffer Overflow Attacks: Exploiting software vulnerabilities.

Prevention:

Implement DDoS protection solutions.

Keep systems up-to-date with security patches.

DDoS (Distributed Denial of Service):

A Distributed Denial of Service (DDoS) attack is an amplified form of DoS attack.

Characteristics:

Multiple Systems: Uses a botnet (multiple compromised systems) to flood the target.

Overwhelming Traffic: Exceeds the target’s processing capabilities.

Masking Identity: Hides the malicious source.

Types of DDoS attacks:

Volumetric Attacks: Flood the network or server with excessive traffic.

Fragmentation Attacks: Manipulate packet fragments.

Application Layer Attacks: Target specific applications (e.g., HTTP, DNS).

Protocol Attacks: Exploit weaknesses in network protocols.

IP Spoofing:

IP spoofing involves creating Internet Protocol (IP) packets with a forged source address.

Purpose:

Hide the sender’s identity.

Impersonate another computer system.

Vulnerability exploited by DDoS attacks:

Spoofed source addresses make it difficult to block malicious requests.

Law enforcement and cybersecurity teams struggle to trace attackers.

Prevention:

Ingress Filtering: Examines incoming IP packets and rejects suspicious ones.

BCP38 (Best Common Practice): Implements ingress filtering to prevent spoofed packets.

Social Engineering Attack:

A social engineering attack is a cyberattack that relies on psychological manipulation of human behavior to:

Disclose sensitive data.

Share credentials.

Grant access to personal devices.

Otherwise compromise digital security.

Social engineering attacks exploit human error and often begin on a personal level.

Common types include:

Phishing: Deceptive emails, SMS, or messages to trick users into revealing information.

Whaling: Targeting high-level executives with personalized attacks.

Baiting: Luring victims with enticing offers (e.g., free software downloads).

Business Email Compromise (BEC): Impersonating executives to request funds or sensitive data.

Smishing: Phishing via SMS (text messages).

Pretexting: Creating a fabricated scenario to extract information.

Honeytrap: Using attractive bait to compromise victims.

Tailgating/Piggybacking: Physically following someone to gain unauthorized access.

Man-in-the-Middle (MITM) Attack:

A man-in-the-middle attack occurs when an attacker secretly relays and possibly alters communication between two parties who believe they are directly communicating.

Key points:

The attacker intercepts messages between victims.

Victims think they are communicating directly but are unaware of the attacker’s presence.

Examples:

Active eavesdropping: Intercepting Wi-Fi communication.

Impersonation: Attacker masquerades as each endpoint.

Prevention:

Mutual authentication (e.g., TLS certificates).

Ingress filtering to detect and prevent spoofed packets