Module 10 CCNA - Security threat landscape

1.Explain Security Threat

- A security threat is a risk or danger that can affect the confidentiality, integrity or availability of information, systems or assets. They can come from many sources, including malware, hacking, social engineering, denial of service attacks, data breaches, insider threats, physical threats, APTs, and the web. The site isn't bad. These threats can result in financial loss, reputational damage, privacy breach, or disaster. Organizations use measures such as firewalls, antivirus software, encryption, access controls, security awareness programs, and emergency response plans to mitigate security threats. Regular updates and vigilance are key to guarding against emerging threats.

2. What is mitigation Techniques?

- Mitigation techniques are strategies and measures used to reduce the impact and potential of threats to security. It includes risk assessment and management, defense in depth, access control, encryption, domain management, network partitioning, security awareness, detection and prevention, disaster response plans, regular backup and disaster recovery, and vulnerability scanning and access. Implementation With this technology, organizations can strengthen their security defenses and reduce vulnerabilities that attackers can exploit. It is important to constantly review and update technology to stay one step ahead of changing threats.

3. Explain DoS Attacks

- A Denial of Service (DoS) attack is a security attack designed to disrupt or disrupt the availability of a computer, network, or service. The main purpose of a DoS attack is to flood the target with too many illegal requests or too much traffic, making it unable to respond to legitimate requests.
- DoS attacks can be carried out in a variety of ways, including:

- **Bandwidth Attacks:** An attacker floods a target network or system with traffic, consuming all available bandwidth and causing chaos. This prevents legitimate users from accessing the network or service.
- **Resource Depletion Attack:** An attacker exploits a vulnerability in a target or application to consume its resources, such as CPU, memory, or disk space.This can cause the system to become unresponsive or crash, not serving legitimate users.

Module 10 CCNA - Security threat landscape

- **Connection Attacks:** An attacker overwhelms the target with a large number of partially open or incomplete connection requests, consuming the system's ability to manage new connections. This will result in a denial of service from legitimate users trying to connect.
- **Application Layer Attacks:** These attacks target specific applications or services by exploiting weaknesses in the application layer or software. Examples include an HTTP flood attack where an attacker floods a website with HTTP requests, or a DNS boost attack where an attacker uses an invalid DNS server to generate a targeted response stream.

4. Explain DDoS

- A Distributed Denial of Service (DDoS) attack is an advanced type of DoS attack in which multiple infected computers are flooded to a target, network, or service. Attackers control these infected computers, creating botnets to spread the effects of the attack. DDoS attacks can be volume-based, protocol-based, or protocol-based attacks designed to seize resources and disrupt a target's operations.
- DDoS attacks pose significant risks, including service disruption, financial loss and reputational damage. Mitigation of DDoS attacks requires a combination of technologies such as traffic jamming, rate limiting, traffic engineering, vulnerability detection, balancing, and network and application firewalls.
- A contingency response plan is required to detect, mitigate, and recover from DDoS attacks. While overall protection against DDoS attacks is difficult, organizations can increase their resilience by keeping systems up-to-date, implementing network security measures, and monitoring network connections for signs of attacks. Timely detection and mitigation is essential to reduce the impact of DDoS attacks and provide legitimate user service.

Module 10 CCNA - Security threat landscape

5.Explain IP spoofing

- IP spoofing is a technique in which an attacker manipulates an IP address in a network communication to deceive the recipient. By creating a fake IP address, they can hide their real identity, bypass access control, perform DDoS attacks, perform man-in-the-middle attacks and even treat the user illegally. It can pose a risk to network security and make it difficult for attackers to track and detect. IP spoofing is difficult to prevent due to vulnerabilities in theIP protocol, but mitigation measures can help reduce the risk. Ingress filtering can be used to block packets with fake IP addresses at the edge of the network.
- A more reliable authentication method than IP-based authentication should be used. Network monitoring tools such as IDS/IPS can detect and block suspicious or illegal traffic. Encryption and security protocols such as SSL/TLS protect the integrity and confidentiality of communications. Traffic analysis helps identify suspicious traffic that could indicate missing IP addresses or potential attacks.
- While complete protection is not always possible, a combination of these measures can improve network security and reduce the risks associated with IP spoofing.Regular updates and vigilance against emerging scam schemes are essential. Overall, a well-rounded combination of testing, monitoring and customer awareness is required to combat IP fraud and protect network infrastructure and communications.

6.What is social Engineering Attack?

- A social attack is a security attack that manipulates people's psychology to trick someone into disclosing, taking action, or allowing access to sensitive information because the system or resources are not valid. Unlike traditional hacking techniques that use malicious techniques, the attack architecture exploits people's weaknesses and credibility to gain unauthorized access or extract important information.
- Social media attacks can be used in many ways, including:

- **Phishing:** The attacker sends a malicious email, message, or phone call that appears to come from a trusted source, such as a bank or named organization. It is designed to trick people into revealing passwords, account numbers or other confidential information.

Module 10 CCNA - Security threat landscape

- **Spoofing:** An attacker creates a false status or personality to trick the victim into providing sensitive information or business.For example, they can build support technology, law enforcement, or colleagues to gain trust and gain information.
- **Traps:** Attackers leave physical devices such as infected USB drives or malware-laden CDs in public places where unauthorized people can see them. Curiosity causes victims to connect devices to their computers without knowing how to compromise their security.

- **Tailgating:** In this type of attack, an attacker follows an authorized person and enters a restricted area without authentication or permission.

- **Impersonation:** The attacker pretends to be someone else, such as an employee, customer, or contractor, in order to manipulate the victim into granting sensitive information or access.
- Social engineering attacks exploit human weaknesses such as trust, curiosity, fear, and inexperience. Data breaches can have serious consequences such as financial loss, identity theft and reputational damage.

7. Explain Man-In-The Middle Attack

- A man-in-the-middle (MitM) attack is a security attack in which an attacker intercepts and modifies communication between two parties that they believe are communicating directly with each other. The attacker is between the legitimate sender and receiver and is not allowed to transmit and control the data exchange.
- Below is a step-by-step description of a typical MitM attack:
- **Interruption of Communication:** The attacker has access to the communication channel between the victim and the receiver. This can be done in various ways, such as corrupting network equipment, exploiting vulnerabilities in software, or using malicious content.
- **Traffic monitoring:** The attackers monitored the communication by capturing and analyzing the data sent between the two parties.This allows them to store sensitive information without the knowledge of the sender or recipient.

Module 10 CCNA - Security threat landscape

- **Modifying Data**: Attackers can modify compromised data in real time, add their own malicious content, modify messages, or forward communications to other sites. These changes are often made in ways unknown to the parties involved.
- **Impersonation:** In some MitM attacks, an attacker impersonates one or both legitimate parties to gain trust. They can create fake websites, emails, or other communications that appear to be legitimate websites to trick users into revealing sensitive information.
- MitM attacks can have serious consequences such as access to confidential information, stolen credentials, financial loss and privacy breaches.