Module 10 CCNA - Security threat landscape

• Beginner Question

1. Explain Security Threat

ANS: A security threat is a threat that has the potential to harm computer systems and organizations. The cause could be physical, such as a computer containing sensitive information being stolen. It's also possible that the cause isn't physical, such as a viral attack.

Types of Threats:

1. **Physical Threats:** A physical danger to computer systems is a potential cause of an occurrence/event that could result in data loss or physical damage. It can be classified as:

- **Internal:** Short circuit, fire, non-stable supply of power, hardware failure due to excess humidity, etc. cause it.
- **External:** Disasters such as floods, earthquakes, landscapes, etc. cause it.
- **Human:** Destroying of infrastructure and/or hardware, thefts, disruption, and unintentional/intentional errors are among the threats.

2. Non-physical threats: A non-physical threat is a potential source of an incident that could result in:

- Hampering of the business operations that depend on computer systems.
- Sensitive – data or information loss
- Keeping track of other's computer system activities illegally.
- Hacking id & passwords of the users, etc.

❖ ***non-physical threads:***

- *Malware*
- *Virus*
- *Worms*
- *Trojan*

2. What is mitigation Techniques?

ANS: They are a crucial part of risk management and can include various actions such as implementing safety measures, creating backup systems, diversifying investments, and more.

- **Risk Acceptance:** Acknowledging the risk and deciding to accept it without active engagement.
- **Risk Avoidance**: Changing plans to circumvent the risk entirely.
- **Risk Limitation:** Taking steps to reduce the likelihood or impact of the risk.
- **Risk Transference:** Shifting the risk to a third party, such as through insurance.
- **Risk Sharing:** Partnering with others to distribute the risk.
- **Risk Retention:** Deliberately retaining the risk for financial or strategic reasons.

• Intermediate Question

1. Explain DoS Attacks

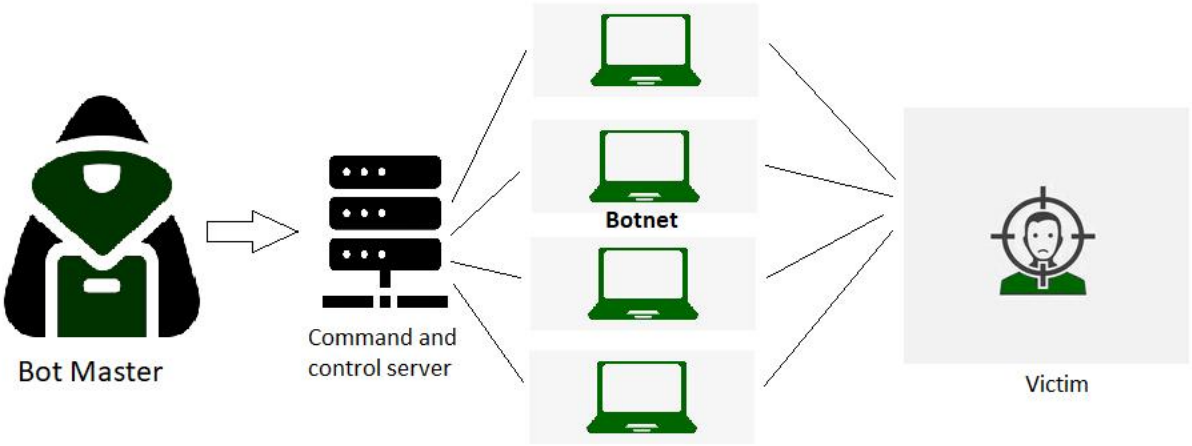
ANS: DoS stands for Denial of Service. It is a type of attack on a service that disrupts its normal function and prevents other users from accessing it. The most common target for a DoS attack is an online service such as a website, though attacks can also be launched against networks, machines, or even a single program.

2. Explain DDoS

ANS: Distributed Denial of Service (DDoS) is a type of DOS attack where multiple systems, which are Trojan infected, target a particular system which causes a DoS attack.

A DDoS attack uses multiple servers and Internet connections to flood the targeted resource.

A DDoS attack is one of the most powerful weapons on the cyber platform. When you come to know about a website being brought down, it generally means it has become a victim of a DDoS attack. This means that the hackers have attacked your website or PC by imposing heavy traffic. Thus, crashing the website or computer due to overloading.



3. Explain IP spoofing

ANS: With IP spoofing, intruder sends message to a computer system with an IP address indicating message is coming from a different IP address than its actually coming from. If intent is to gain unauthorized access, then Spoof IP address will be that of a system the target considers a trusted host. To successfully perpetrate an IP Spoofing attack, hacker must find IP address of a machine that the target System considers a trusted source. Hackers might employ a variety of techniques to find an IP address of a trusted host. After they have obtained trusted IP address they can then modify packet headers of their transmission so it appears that the packet coming from the host.

• Advance Question

1. What is social Engineering Attack?

ANS: Social engineering uses human weakness or psychology to gain access to the system, data, personal information, etc. It is the art of manipulating people. It doesn't involve the use of technical hacking techniques. Attackers use new social engineering practices because it is usually easier to exploit the victim's natural inclination to trust. For example, it is much easier to fool someone to give their password instead of hacking their password. Sharing too much information on social media can enable attackers to get a password or extracts a company's confidential information using the posts by the employees. This confidential information helped attackers to get the password of victim accounts.

2. Attack Explain Man-In-The Middle

ANS: Man In the Middle Attack implies an active attack where the attacker/Hacker creates a connection between the victims and sends messages between them or may capture all the data packets from the victims. In this case, the victims think that they are communicating with each other,

but in reality, the malicious attacker/hacker controls the communication i.e. a third person exists to control and monitor the traffic of communication between the two parties i.e. Client and Server.