**CCNA ASSIGMENT**

**MODULE 4**

1. Explain Security Threat.

Security Threat is defined as a risk that which can potentially harm computer systems and organization. The cause could be physical such as someone stealing a computer that contains vital data. The cause could also be non-physical such as a virus attack. In these tutorial series, we will define a threat as a potential attack from a hacker that can allow them to gain unauthorized access to a computer system.

1. What is mitigation Techniques?

Mitigation, or Attack Mitigation, is the reduction in severity or seriousness of an event. In cybersecurity, mitigation is centred on strategies to limit the impact of a threat against data in custody.

Threats against data can come from outside attackers motivated by profit, activism, retribution, or mischief. Insider threats may have the same motives but could be tied to workplace issues resulting in people abusing their access privileges to inflict harm. In either case, it is the responsibility of a data owner to protect data from misuse, disclosure, theft, unauthorized exposure, wrongful transmission, and so on while still making the data useful and available to conduct business. To that end, a mitigation strategy should be strict in accordance with risk appetites and realistic enough to allow for the licit use of the data by those authorized.

1. Explain DoS Attacks.

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop.

1. Explain DDoS

DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

Motivations for carrying out a DDoS vary widely, as do the types of individuals and organizations eager to perpetrate this form of cyberattack. Some attacks are carried out by disgruntled individuals and hacktivists wanting to take down a company's servers simply to make a statement, have fun by exploiting cyber weakness, or express disapproval.

Other distributed denial-of-service attacks are financially motivated, such as a competitor disrupting or shutting down another business's online operations to steal business away in the meantime. Others involve extortion, in which perpetrators attack a company and install hostage ware or ransomware on their servers, then force them to pay a large financial sum for the damage to be reversed.

DDoS attacks are on the rise, and even some of the largest global companies are not immune to being "DDoS'ed". The largest attack in history occurred in February 2020 to none other than Amazon Web Services (AWS), overtaking an earlier attack on GitHub two years prior. DDoS ramifications include a drop in legitimate traffic, lost business, and reputation damage.

A DDoS attack aims to overwhelm the devices, services, and network of its intended target with fake internet traffic, rendering them inaccessible to or useless for legitimate users.

1. Explain IP spoofing

IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. It is a technique often used by bad actors to invoke DDoS attacks against a target device or the surrounding infrastructure.

Sending and receiving IP packets is a primary way in which networked computers and other devices communicate, and constitutes the basis of the modern internet. All IP packets contain a header which precedes the body of the packet and contains important routing information, including the source address. In a normal packet, the source IP address is the address of the sender of the packet. If the packet has been spoofed, the source address will be forged.

IP Spoofing is analogous to an attacker sending a package to someone with the wrong return address listed. If the person receiving the package wants to stop the sender from sending packages, blocking all packages from the bogus address will do little good, as the return address is easily changed. Relatedly, if the receiver wants to respond to the return address, their response package will go somewhere other than to the real sender. The ability to spoof the addresses of packets is a core vulnerability exploited by many DDoS attacks.

Spoofing is also used to masquerade as another device so that responses are sent to that targeted device instead. Volumetric attacks such as NTP Amplification and DNS amplification make use of this vulnerability. The ability to modify the source IP is inherent to the design of TCP/IP, making it an ongoing security concern.

1. What is social Engineering Attack?

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim’s trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

Baiting

As its name implies, baiting attacks use a false promise to pique a victim’s greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.

Scareware

Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraud ware.

Pretexting

Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.

Phishing

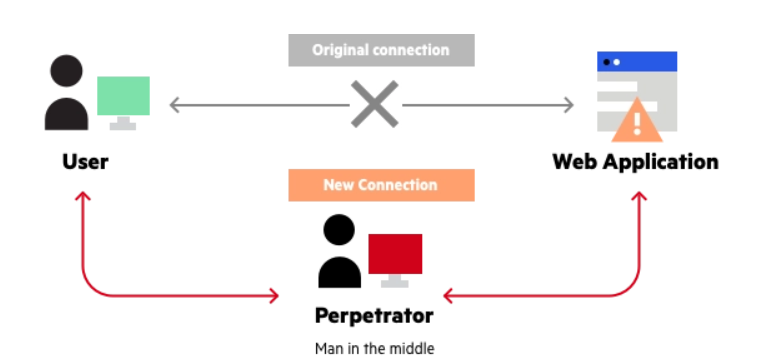
As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

Spear phishing

This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. Spear phishing requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They’re much harder to detect and have better success rates if done skilfully.

1. Explain Man-In-The Middle Attack.

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.



The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.

Information obtained during an attack could be used for many purposes, including identity theft, unapproved fund transfers or an illicit password change.

Additionally, it can be used to gain a foothold inside a secured perimeter during the infiltration stage of an advanced persistent threat (APT) assault.

Broadly speaking, a MITM attack is the equivalent of a mailman opening your bank statement, writing down your account details and then resealing the envelope and delivering it to your door.