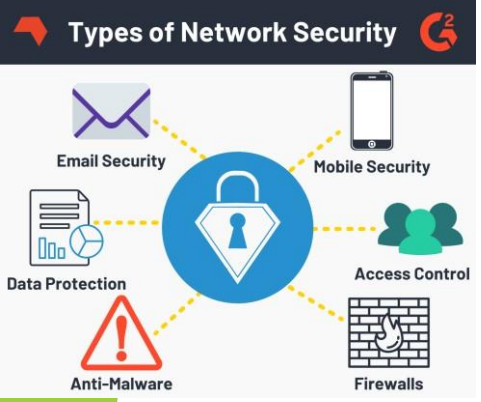

NIS
(Network and Information Security)
&
SIC
(Security In Computing)

Last Time

- What is attack ?
- What are the types of attacks ?
- What is active Attack
- What is passive attack
- Example of Active Attack
- Example of passive attack
- What is DoS attack
- What is Three way handshake
- What is SYN flood attack
- What is Ping-of-death attack
- What is DDoS

Sniffing

- Sniffer is an application that can capture network packets. Sniffers are also known as network protocol analyzers.
- Objective of Sniffing is to steal:
  - Password (from Email, Web Site, FTP, TELNET, etc.)
  - Email Text
  - Files in tranfer
- A network sniffer is a software or hardware that is used to observe the traffic, it passes through a network on shared broadcast media.
- These devices can be used to view all traffic, or it can target a specific protocol, service, or even string of characters like logins.
- Network administrators for monitoring network performance can use network sniffers. They can be used to perform traffic analysis. For example, in order to determine what type of traffic is most commonly carried on the network and to determine which segments are mot active.

Sniffing

- They can also be used for network bandwidth analysis and to troubleshot certain problems such as duplicate MAC addresses.
- Contents of the email messages can be viewed by the sniffers which travel across the network
- **Packet Sniffing:-** It is a passive attack, attacker does not hijack the conversation but he will observe the packets as they passed by.
- In order to prevent sniffing:-
  - The information that is travelling can be encoded
  - The transmission link can be encoded.

Spoofing

- Spoofing is making data similar to it has come from a different source. This is possible in TCP/IP because of the friendly assumptions behind the protocols
- The assumption at the time of protocol development is that an individual who is having access to the network layer will be privileged users who can be trusted.
- When a packet is sent from one system to another, it includes not only the destination IP address and port but the source IP address as well. This is one of the several forms of spoofing.
- **Spoofing Email**
  - E-mail spoofing can be easily accomplished, and there are several different ways to do it and programs that can assist you in doing so.
  - E-mail Spoofing refers to a mail that appears to have been originated from one source but, it was actually send from another source. Best example of Email spoofing is Spam Mail and Junk mails.
  - There are simple ways to determine that an e-mail message was probably not sent by the source, but most users do not question their e-mail and will accept it.

Spoofing

- **URL Spoofing:-**
  - An attacker acquires a URL to close to the one they want to spoof so, that e-mail sent from their system appears to have come from the official site.
  - For example, if attackers wanted to spoof XYZ Corporation, which owned XYZ.com, the attackers might take access to the URL XYZ.Corp.com. An individual receiving a message from the spoofed corporation site would not normally suspect it to be spoof but would take it to be official.

Man-in-Middle Attack

- A man-in-middle Attack, generally occurs when attackers are able to place themselves in the middle of two other hosts that are communicating in order to view and/or modify the traffic
- This will do by making sure that all communication going to or from the target host is routed through the attackers host.
- Then the attacker can be able to observe all traffic before transmitting it and can actually modify or block traffic. To the target host, communication is occurring normally, since all expected replies are received.

Replay

- A replay attack is an attacker captures a portion of a communication between two parties and retransmits it after some time.
- For example, an attacker might replay a series of commands and codes used in a financial transaction in order to cause the transaction to be conducted multiple times.
- The best way to prevent replay attacks is with encryption, Cryptographic authentication, and time stamps.

TCP/IP Hijacking

- TCP/IP hijacking is the process of taking control of an already existing session between a client and a server.
- Main benefit to an attacker of hijacking over attempting to enter a computer system or network is that the attacker doesn't have to avoid any authentication mechanisms, since the user has already authenticated and established the session.
- When the user completed its authentication sequence, the attacker can then take the session and carry similar to the attacker, and not the user, had authenticated with the system.
- To prevent the user from noticing anything unusual the attacker may decide to attack the users system and perform DoS attack on it, so that the user and the system, will not notice any unusual traffic that is taking place.

Thank you for Hearing with Patience