Ethical Hacking

Module-5

- **Explain MAC spoofing and Email spoofing.**

✓ **MAC spoofing: -**

MAC spoofing is a technique that can be used to fool the operating system into believing it has received an ARP request from another machine. This allows the attacker to gain access to a victim's network without being detected.

✓ **Email spoofing: -**

Email spoofing is a threat that involves sending email messages with a fake sender address. Email protocols cannot, on their own, authenticate the source of an email. Therefore, it is relatively easy for a spammer or other malicious actors to change the metadata of an email.

- **Explain Kali Linux tool SYN Flooding Attack using Metasploit.**

TCP SYN flood is a type of Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.

- ✓ First, select your target's IP address. (ping www.website.com)
- ✓ So now I know the victim's IP Address nnn.nnn.nnn.hhh
- ✓ Launching Metasploit by typing msfconsole -q in your kali terminal
- ✓ Msf6 > use auxiliary/dos/tcp/synflood
- ✓ Msf6> show options
- ✓ Now you can see you have all the available options that you can set.
- ✓ To set an option just you have to typeset and the option name and option.
- ✓ You have to set two main options
- ✓ RHOST= target IP Address
- ✓ RPORT=target PORT Address

Set RPORT nnn.nnn.nnn.hhh

Set RPORT PP (PORT no)

- ✓ To launch the attack just type.
- ✓ Exploit
- ✓ to see the packets, you can open Wireshark.

- **Find online email encryption service.**
  - ✓ https://proton.me/mail

- **Types of Firewalls.**
  - ✓ packet filtering firewall.
  - ✓ circuit-level gateway.
  - ✓ application-level gateway (aka proxy firewall)
  - ✓ stateful inspection firewall.
  - ✓ next-generation firewall (NGFW)

- **Explain Evading Firewalls.**

Firewalls and IDS intend to avoid malicious traffic from entering into a network but certain techniques can be used to send intended packets to the target and evade IDS/Firewalls.

- ✓ Packet Fragmentation- send fragmented probe packets to the intended target, which re-assembles it after receiving all the fragments.
- ✓ Source Port Manipulation- manipulate the actual source port with the common source port to evade IDS/firewall
- ✓ IP address spoofing /Decoy IP- generate or manually specify the IP address of the decoy so that the IDS/firewall cannot determine the actual IP.
- ✓ Create custom packets: - Send custom packets to scan the intended target beyond the firewalls.
- ✓ Spoofing MAC address: - Spoofing our MAC address to hide our actual identity.