**DAY 20**

**PART-1**

Few techniques the hackers use in order to create some email id for instant account creation and bypassing the account registration restriction.

🡪temp-mail.org

🡪10minutemail.net

How hackers grab documents that are uploaded in a website which are publicly accessible using data grabbing techniques.

1. Google dorks

2. FOCA(Fingerprinting Organization using Collected Archieves)

🡪Meta data of the documents

🡪Grabbing all the links to the documents

🡪Gather network information of the target domain

🡪Basic vulnerabilities can be analysed

🡪Eleven paths FOCA

FOCA uses three search engines: **Google, Bing, Exalead**

How hackers grab the publicly available documents which were deleted in the website previously.

It can be 3 or 4 years.

Internet archieve:

Web archieve

Internet bot:

🡪wayback machine

1. The developer should enable restriction to the website using a file called robots.txt

2. This file should be uploaded in the root of the website

3. robots.txt

User-agent: ia\_archive

Disallow:/

How hackers spoof their mac address in kali linux/ubuntu:

\*macchanger

macchanger -s eth0

To change mac address:

1. ifconfig eth0 down

2. macchanger -r eth0

3. ifconfig eth0 up

To restore mac address:

1. ifconfig eth0 down

2. macchanger -p eth0

3. ifconfig eth0 up

In Ubuntu:

🡪apt-get install net-tools

🡪sudo apt-get install macchanger

**PART-2**

DOS/DDOS attack:

DOS is an attack used to deny the legitimate users access to a resource such accessing a website, emails, connecting to a network.

In DOS/DDOS attack the attacker will send unlimited data packets to the server which makes the server to deny the service to its intended users.

DOS attacks work in two different layers of OSI model

1. Source is hacker

2. Destination is web server

3. Web server is running http service on port 80

4. We know in tcp, ports perform TCP 3-way handshake in order to connect and communicate

1. Source will send a SYN packet to the destination

2. Destination will respond with a SYN+ACK packet

3. Source will again send a ACK packet to destination

If the destination is not accepting:

1. Source will send a SYN packet to the destination

2. Destination will respond with a RST packet

\*If the source is not responding with ACK packet the destination will wait for 60-70 seconds

DOS attack:

1. Attacker will send a SYN packet to the destination.

2. Destination will respond with a SYN-ACK packet.

3. Attacker will not respond with any packet.

4. The destination waits for at least 60-70 seconds

Symptoms of DOS attack:

1. Slow performance of device/services

2. Increase in spam emails

3. Unavailability of a service

4. Loss of access to websites

5. Disconnection of wireless and wired networks

Tools:

1. **XERXES**

2. **METASPLOIT**

3. **HPING3**

🡪hping3 -S –flood <target\_ip> -a <spoof\_ip>

XERXES:

Github 🡪 Dev0uss

🡪git clone

🡪gcc cerces.c -o ATTACK

🡪./ATTACK <ip\_address> <port>