#################################\*\*\*DAY-1\*\*\*###################################

**NMAP:**

**Network Mapper**: To gather info about target.

Nmap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques, version detection (determine service protocols and application versions listening behind ports), and TCP/IP fingerprinting (remote host OS or device identification).

->Host Discovery/Ports Discovery/Version or Service Discovery/OS Discovery ---------**PORTS[0-65535]**

->Debian -> apt install nmap -y -------------------------------Centos -> yum install nmap -y

**# Ports:-**

a) Well Known [0-1024]

b) Registered [1025-49151]

c) Dynamic/Open [49152-65535

# **TCP flags** -🡪 SYN,ACK,RST,PSH,FIN,URG

# **3 way handshake**

M1 --------SYN--------> M2

M1 <------SYN/ACK------ M2

M1 --------ACK--------> M2

|<--------TUNNEL------->|

**# COMMANDS:-**

# nmap –help

# nmap <option><type\_of\_scan> <target>

+ Host Discovery

# nmap -sn target [-s means scan and -n means never do dns resolution]

# # nmap -sn 192.168.206.133

# nmap -sn 192.168.206.133 192.168.206.11

# nmap -sn 192.168.206.133 10.0.0.1

# nmap -sn 192.168.206.1-133

# nmap -sn 192.168.206.1-133 --exclude 192.168.206.10

# nmap -sn 192.168.206.0/24

# nmap -sn 192.168.206.0/24 10.0.0.0/8

# nmap -sn domain.tld

# nmap -sn domain.tld example.com

# nmap -sn -iL ips.txt

-i [Input]

-L [List]

**State of Ports:-** open/closed/filtered/open-filtered/closed-filtered

**1) TCP Scan: [ Full Open Scan ]**

Attacker ---------SYN:8080-------> Target

Attacker <---------SYN/ACK-------- Target

Attacker ----------ACK-----------> Target

**Commands for full open scan:- [ -s means scan and T means TCP scan ]**

# nmap -sT 192.168.1.1

# nmap -sT 192.168.1.1 -p80

# nmap -sT 192.168.1.1 -p80,443

# nmap -sT 192.168.1.1 -p80-100

# nmap -sT 192.168.1.1 -p- [Entire range 65535 ports]

**2) SYN Scan: [ Half Open Scan ]**

-------------------------------

Attacker ---------SYN:8080-------> Target

Attacker <---------SYN/ACK-------- Target

Attacker ----------RST-----------> Target

# nmap -sS target

**Wireshark:**

**+ Show only SMTP (port 25) and ICMP traffic:**

tcp.port eq 25 or icmp

**+ Show only traffic in the LAN (192.168.x.x), between workstations and servers – no Internet:**

ip.src == 192.168.0.0/16 && ip.dst == 192.168.0.0/16

**3) Service/Version Scan:-**

# nmap -sSV target

80/tcp open http Apache-2.2.2

**4) OS Scan:** # nmap -O target

**# REPORT:- -> Format in xml/nmap/gnmap**