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

Dheeraj Sir Ditiss, [Dec 18, 2023 at 7:12 PM]

VAPT:

-----

Vulnerability Assessment: Finding weakness/Loopholes

Penetration testing: Exploit

Report Management:

------------------ PoC [ Proof-of-concept ]

Patch Management:

----------------- Fix/patch

Dheeraj Sir Ditiss, [Dec 18, 2023 at 7:12 PM]

++++++++++++++++++++++++++++++++++++

Network VAPT

WAPT

API Testing/GraphQL

Cloud Pentesting

Souce Code Analysis

Android Pentesting

++++++++++++++

Dheeraj Sir Ditiss, [Dec 18, 2023 at 7:13 PM]

**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).

+ Hosts Discovery

+ Ports Discovery

+ Service/Version Discovery

+ OS Discovery

+ Bypass Scan protection against firewalls

+ NSE to scan in depth

ZENMAP - GUI

NMAP - CLI

[Debian]

# apt install nmap -y

[CentOS/RHEL]

# yum install nmap -y

PORTS: [0-65535]

a) Well Known [0-1024]

b) Registered [1025-49151]

c) Dynamic/Open [49152-65535]

Dheeraj Sir Ditiss, [Dec 18, 2023 at 7:13 PM]

TCP/UDP

**TCP Flags:**

SYN,ACK,RST,PSH,FIN,URG

**3 way handshake [RTO]**

````````````

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

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

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

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

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

Dheeraj Sir Ditiss, [Dec 18, 2023 at 7:13 PM]

HELP

# nmap --help

**Syntax:**

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

**Host Discovery:**

````````````

# nmap -sn target

-s [Scan]

-n [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]

Port Discovery:

````````````

**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

+ Targets:

# nmap -sT 192.168.1.1

-s [Scan]

T [TCP Scan]

**NOTE: By default NMAP scan 1000 ports.**

+ Port:[-p]

-----------

# 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]

+ Debug:

--------

Press 'space bar' to debug it.

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

Dheeraj Sir Ditiss, [Dec 18, 2023 at 7:13 PM]

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

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

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

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

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

# nmap -sS target

+++++++++++++++++++++++++++++++++++++++++++++

Dheeraj Sir Ditiss, [Dec 18, 2023 at 7:13 PM]

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

Dheeraj Sir Ditiss, [Dec 18, 2023 at 7:14 PM]

**3) Service/Version Scan:**

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

# nmap -sSV target

80/tcp open http Apache-2.2.2

4) OS Scan:

-----------

# nmap -O target

Dheeraj Sir Ditiss, [Dec 18, 2023 at 7:14 PM]

Report:

-------

Format: .xml, .nmap, .gnmap

**# nmap -sSV target -oX filename**

-oN filename

-oG filename

-oA filename

-o : output

X : .xml

N : .nmap

G : .gnmap

A : All Formats

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

How to convert XML to HTML

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

# apt install xsltproc -y

# xsltproc nmap-scan.xml -o scan-report-nmap.html