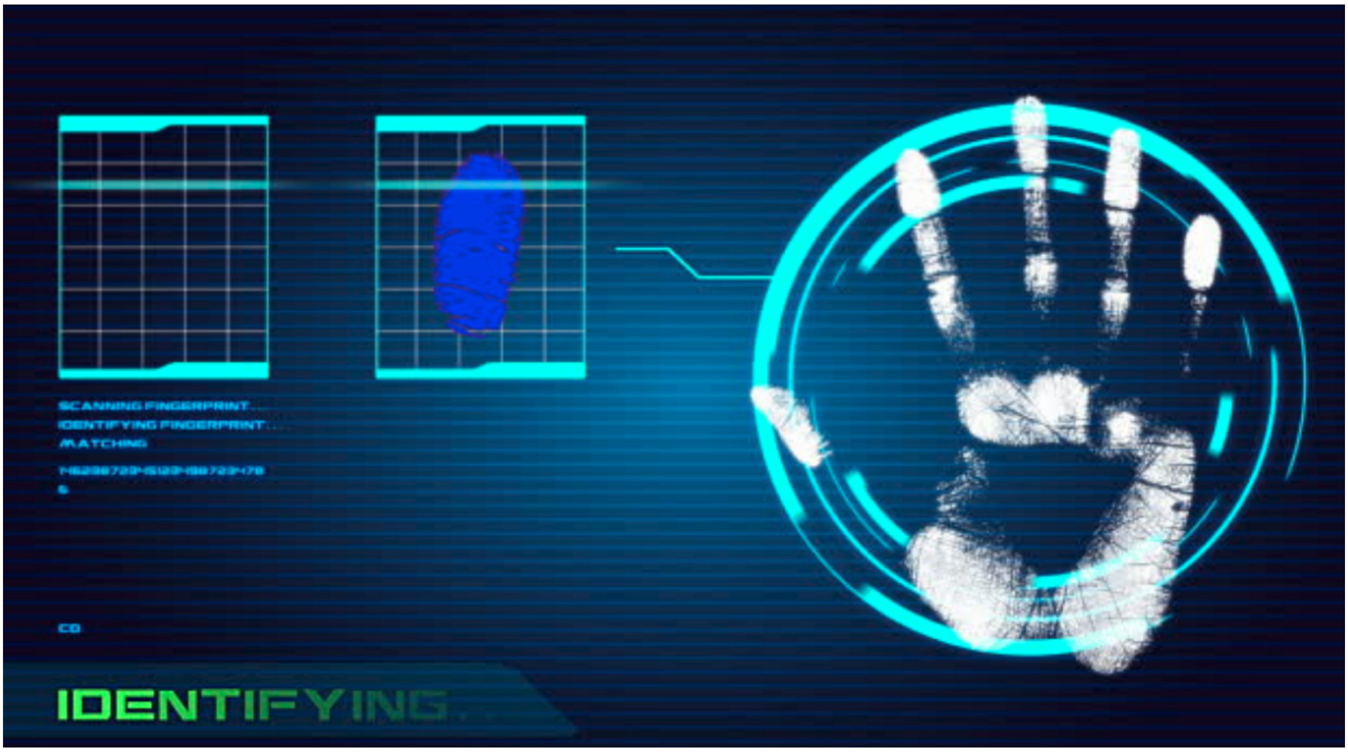
Network Penetration Testing-Part2

Piyush Patil
May 18 · 10 min read ★

After finishing information gathering, we will perform Scanning and Enumeration phase.



In this, we will cover scanning in detail. So what our main goal in scanning??

> *Hping3,*
>
> *Netcat*

· · ·

> *NMAP*

Nmap (“Network Mapper”) is a free and open source utility for network discovery and security auditing. It shows ports, services, os and also supports NSE which checks for vulnerabilities.

nmap -sn ip ==>ping sweep(it is also called host discovery to check weather host machine is alive or not, it is not a port scan)

nmap -sn ip | grep “Nmap scan” |cut -d” “ -f5 ==>Provide result in most visible format

——————————————————————————————

nmap -sn ip -oG sweep.txt =>store result into file

-oN Standard Nmap output

-oG Greppable format

-oX XML format

-oA Generate all above formats

nmap -sT ==>TCP connect scan

-sT and -sS is same but the only difference is -sT does 3-way handshake so it takes more time.

*Nmap send syn packet, if it gets syn ack then the port is open and if it gets reset then the port is close

If no response is received after several attempts,nmap can determine port is filtered.

———————————————————————————————

nmap -sU ==>UDP scan

Most of the services run on TCP but some services like DNS, SNMP, and DHCP communicate over UDP Protocol.

*If there is no reply from the port then the port is considered as open and if we receive ICMP destination unreachable packet then the port is closed.

———————————————————————————————

nmap -sV ip ==>Service version scan

———————————————————————————————

nmap -O ip ==>OS scan

-send TCP syn to port 443

-send TCP ack to port 80

-if the target is on the same subnetwork then send ARP packet otherwise send ICMP echo request.

-ICMP timestamp request

It is also called probing,

so when we use -Pn option we say that don’t probe machine, just scan it as it is considered that machine is online.

nmap -Pn ip =>very helpful in a real pentesting environment

——————————————————————————————

Timing Options:-

nmap -T4 ip

-T0 Paranoid: Very slow, used for IDS evasion

-T1 Sneaky: Quite slow, used for IDS evasion

-T2 Polite: Slows down to consume less bandwidth, runs ~10 times slower than the default

-T3 Normal: Default, a dynamic timing model based on target responsiveness nmap -F ip =>100 popular ports

nmap -p- ip =>scans for all ports 1–65535

nmap -p 80 ip =>scan for port 80

———————————————————————————————

nmap -v =>verbose

nmap -vv =>more verbose, you can keep adding v for more verbosity

———————————————————————————————

> ***NSE Script Engine***

nmap script-updatedb

———————————————————————————————

locate *.nse =>show all nmap scripts

cd /usr/share/nmap/scripts/ =>location of nmap scripts

ls -l | grep ssh

———————————————————————————————

NMAP Script Categories

nmap — script all $ip => it can take too much time

nmap — script vuln $ip =>Discovers common vulnerabilities

— —

Playing with FIREwall

option template time

-T0 Paranoid 5min

-T1 Sneaky 15sec

-T2 Polite 0,4 sec

-T3 Normal default

-T4 Aggressive 10 millisecond

-T5 Insane 5 millisecond

so it means if we use -T1 option, you can see the packets are sent every 15 seconds.

——————————————————————————————

Fragmentation⇒ spliting single packet into smaller packets

nmap -sS -f target_ip ==>we can use -f option to perform a scan with fragmented packets

Note that fragmentation option does not work with every kind of scan. For Example, it does not work with the options:

-sT

-sV

Beware: Modern IDSś are able to rebuild the fragmented packets note that you can not use the decoy attack with -sT and -sV scan

——————————————————————————————
—

Source Port ⇒ You can exploit a badly configured firewall that allows traffic coming from certain ports

For ex- Sysadmins may allow traffic coming from ports such as 53(DNS replies) or FTP(20)

nmap -sS — source-port 80 target_ip

· · ·

> *Unicornscan*

Fast network scanner ==>Use this when scanning UDP ports, it can be also used to scan TCP ports.

unicornscan 192.168.1.116 ==>normal scan

unicornscan -r200 -mT ip:port

Where;

-r200

indicates we want to send 200 packets per second

-mU

indicates we want to scan (m) using the UDP protocol

For the most common scanning, please find a cheat sheet below to assist you.

Other options:-

SYN : -mT

ACK scan : -mTsA

Fin scan : -mTsF

Null scan : -mTs

Xmas scan : -mTsFPU

Connect Scan : -msf -Iv

Full Xmas scan : -mTFSRPAU

scan ports 1 through 5 : (-mT) host:1–5

. . .

> *Amap*

In some cases administrator and applications may use non-standard ports and tools may not recognize it

Using nmap output file

```
amap -i nmap_file -o amap_output_file -m
```

(-m makes the file machine readable)

. . .

> *HPING3*

1. Testing ICMP: In this example, hping3 will behave like a normal ping utility, sending ICMP-echo and receiving ICMP-reply

```
hping3 -1 google.com
```

2. Traceroute using ICMP: This example is similar to famous utilities like tracert (windows) or traceroute (linux) who uses ICMP packets increasing every time in 1 its TTL value.

```
hping3 — traceroute -V -1 google.com
```

3. Checking port: Here hping3 will send a Syn packet to a specified port (80 in our example). We can control also from which local port will start the scan (5050).

```
hping3 -V -S -p 80 -s 5050 google.com
```

4. Traceroute to a determined port: A nice feature from Hping3 is that you can do a traceroute to a specified port watching where your packet is blocked. It can just be

receive a reply, that means the port is open. Normally firewalls send a RST+ACK packet back to signal that the port is closed..

```
hping3 -c 1 -V -p 80 -s 5050 -F google.com
```

7. Ack Scan: This scan can be used to see if a host is alive (when Ping is blocked for example). This should send a RST response back if the port is open.

```
hping3 -c 1 -V -p 80 -s 5050 -A google.com
```

8. Xmas Scan: This scan sets the sequence number to zero and set the URG + PSH + FIN flags in the packet. If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target discards the TCP Xmas scan, sending no reply.

```
hping3 -c 1 -V -p 80 -s 5050 -M 0 -UPF google.com
```

9. Null Scan: This scan sets the sequence number to zero and have no flags set in the packet. If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target discards the TCP NULL scan, sending no reply.

```
hping3 -c 1 -V -p 80 -s 5050 -Y google.com
```

10. Smurf Attack: This is a type of denial-of-service attack that floods a target system via spoofed broadcast ping messages.

```
hping3 -1 — flood -a VICTIM_IP BROADCAST_ADDRESS
```

11. DOS Land Attack

-d — data: data size

-S — syn: set SYN flag

-w — win: winsize (default 64)

-p — destport [+][+]<port> destination port(default 0) ctrl+z inc/dec

-s — baseport: base source port (default random)

· · ·

> *NETCAT*

Netcat can also be used as a port scanner by using the -z option and specifying a host and port range instead of a single port. This option checks the ports in range if there is a daemon listening without sending data. The following example will scan the ports 20 through 500 of 192.168.1.3 and list the open ones:

nc -z 192.168.1.3 20–500

To list the closed ports too include the -v option. For example:

nc -vz 192.168.1.3 20–500

Other options that can be used to speed up scanning are -n to prevent DNS lookup and -w 1 to limit the timeout to 1 second.

Reverse Engineering, Penetration Testing(Web, Mobile, IoT, Network, Infra)

Follow

More From Medium

Top on Medium

Top on Medium

Apparently I Was Nothing But A Woo-Girl

Michelle Ann in Fearless She Wrote

Nov 13 · 4 min read ★

4.91K

Top on Medium

How to Predict the End of a Relationship

Colleen Murphy in Mindful Muse

Nov 22 · 5 min read ★

2.3K