

NARASARAOPETA INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering

ETHICAL HACKING (IV - CSE) – I SEM

UNIT II

Footprinting: Footprinting, Types, Using ping and ns Lookup commands in Windows command line, Scanning: Scanning, Basics of Scanning, Basic Techniques of Scanning, Enumerating DNS using dns enum, Performing flag scan using hping3.

FOOTPRINTING

- Footprinting is the first phase of the information gathering process in ethical hacking and cybersecurity.
- Footprinting attacker can collect information like emails, contacts, domain name information and using social engineering even more sensitive data.
- The information gathered during footprinting can be used to plan and execute subsequent phases of a penetration test or security assessment.

Types:

1. Internal Footprinting

Footprinting performed inside the network is known as internal footprinting. In internal footprinting, attack may access internal network or is directly or indirectly connected to the internal network.

Following attacks or mechanism can be used for internal footprinting:

a. Dumpster Diving:

- Looking for sensitive information in garbage or dumps is known as dumpster diving.
- Sometimes, attacker may find a piece of paper or some important important documents from which sensitive information can be retrieved.
- When penetration testing or hacking is performed each and every possible aspect of gathering information is taken into consideration.

b. Shoulder Surfing:

Looking at shoulder or guessing the password by viewing a person typing or indirectly seeking into his hand movement to get password. Sometimes it provides quite sensitive information.

Shoulder surfing is a type of social engineering attack or eavesdropping technique in which an attacker observes or spies on the actions, data, or sensitive information of a person, often without their knowledge or consent.

The term "shoulder surfing" derives from the idea that the attacker is figuratively looking over the victim's shoulder to gain access to information.

c. Private Websites:

If attacker found any private websites of the target, it became treasure for him as he can gain bunch of sensitive information like employee and client details etc.

2. External Footprinting:

When attacker is not connected to the target network, in order to gather information, external footprinting is used. Generally, External Footprinting provides huge number of information about the data. There are lots of ways and possibilities to gather the information from outside of network.

Following attacks or mechanism can be used for External Footprinting:

1. Website:

Website of the target may contain some sensitive information or may be vulnerable. From the website, attacker can easily get the contact details like e-mails and phone numbers.

Using phone numbers, attacker can simply call and perform social engineering in order to gain sensitive information. Besides, attacker can also perform social engineering over e-mails.

2. Google:

Google is one of the biggest search engine and helping hand for a hacker. Sometimes simply googling about target can give much sensitive information like admin contents or about target profiles over social media.

Google help both actively and passively in gaining sensitive information. For ex, if you google for XYZ, you may get his picture, his address, about upcoming events or more of sensitive information about the target.

3. Whois:

Whois is a tool (both application and web application level) which is used to gather information about target domain like name server, domain records, admin contacts and other relative information.

Whois is one the major information provider and this information is used in writing penetration testing reports. It is a great database which contains records of almost every domain name.

www.whois.sc is one of the popular website to check whois information. How to use whois.sc:

1. Navigate to www.whois.sc .

- Provide the domain name.
- Crawl and look for required information (information will look like screenshot.)

The screenshot displays the DomainTools Whois Lookup interface. The top navigation bar includes links for HOME, RESEARCH, LOGIN, and SIGN UP. The main heading is "Whois Lookup" with a search bar containing "www.google.com". Below the search bar, the "Whois Record for Google.com" is shown. The record details are as follows:

Domain Profile	
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) +1.2086851750
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	9,487 days old Created on 1997-09-15 Expires on 2028-09-13 Updated on 2019-09-09
Name Servers	NS1.GOOGLE.COM (has 20,789 domains) NS2.GOOGLE.COM (has 20,789 domains) NS3.GOOGLE.COM (has 20,789 domains) NS4.GOOGLE.COM (has 20,789 domains)
IP Address	172.217.14.104 & other sites hosted on this server

On the right side, there is a sidebar with a "DomainTools Iris" advertisement and a "Tools" section. The tools listed include "Hosting History", "Monitor Domain Properties", "Reverse IP Address Lookup", "Network Tools", and "Visit Website".

4. Domain Name Server (DNS):

DNS footprinting can provide information same as of whois, sometimes attacker get sensitive information which lead to compromise of Domain of target.

5. Social Networking:

Public profiles on social network contain contact information and activity details. Target may be social engineered easily over social networking which lead to disclosure of sensitive information.

6. Social Engineering:

Social engineering is art of human exploitation. It is one of the major attack which leads to vast compromises. Social engineering may be tool based or human based. In tool based social engineering, tools like Phishing, tabnapping and Social Engineering toolkits are used. In human based social engineering, manipulating the target is used to gain sensitive information like client details, passwords, etc.

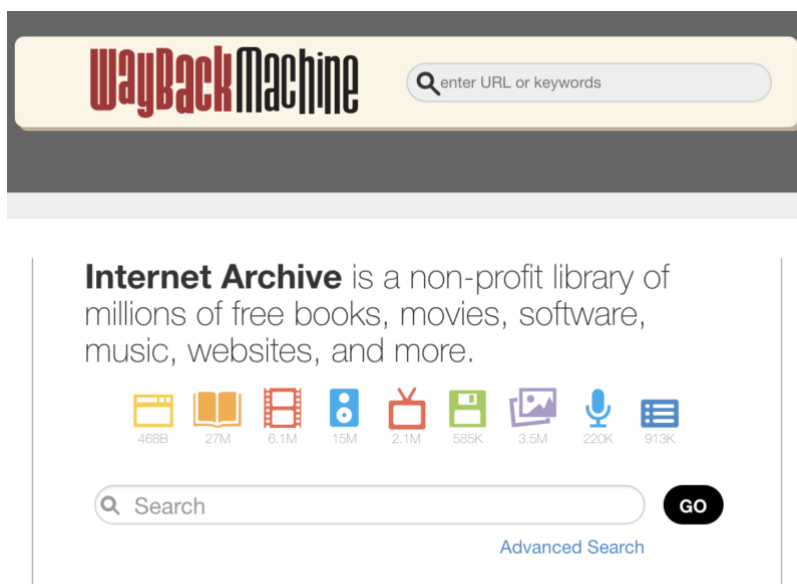
7. Archive Websites:

There are some websites over internet which keeps archives of almost every websites. Looking in archives can provide sensitive information about the target. Way Back Machine is one of the website which contains archives of websites.

Using Way Back Machine:

- Navigate to www.archives.org
- Input target domain.

check the archives, highlighted dates are dates when website is updated.(see in screenshot)



Footprinting using Tools:

Footprinting can be used using following tools:

1. Ping:

Ping is a command line tool used to check the target is live or not. Only if target is live, or not. Only if target is live, further exploitation can be done.

- Footprinting using the "ping" command is a basic but essential technique for gathering information about a target network or host.
- The "ping" command is available on most operating systems and is used to test the reachability and responsiveness of a network device.

Using Ping in windows command line:

- a) Open Command Prompt (CMD) in windows (press win+R and type cmd)
- b) Type “ ping target “ (replace target with IP or Website of target).

For ex: ping www.xyz.abc or ping 127.0.0.1

ping [options] target

Common Options:

- **-c count:** Specifies the number of packets to send before stopping (e.g., -c 4 to send 4 packets).
 - **-i interval:** Sets the time interval between sending packets in seconds (e.g., -i 1 for 1-second intervals).
 - **-t:** On Windows, this option sends continuous ping requests until manually stopped.
 - **-n:** On Windows, this option displays numeric IP addresses instead of resolving hostnames.
 - **-v:** Verbose output, showing additional information.
- c. Packets will be transferred between attacker and target. 0% loss indicates ping command completed and packets are successfully transferred.
- d. TTL stands for Time to live and generally 4 packets are transferred between attacker and target but it can be increased.
- e. To understand more about ping command, type ping -h or ping /? In terminal. It will open help for ping command. It can be used in linux as well.

```
C:\Users\HC>ping www.google.com

Pinging www.google.com [142.250.183.228] with 32 bytes of data:
Reply from 142.250.183.228: bytes=32 time=147ms TTL=118
Reply from 142.250.183.228: bytes=32 time=308ms TTL=118
Reply from 142.250.183.228: bytes=32 time=17ms TTL=118
Reply from 142.250.183.228: bytes=32 time=20ms TTL=118

Ping statistics for 142.250.183.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 308ms, Average = 123ms

C:\Users\HC>
```

Using "ping" for footprinting provides basic information about a target's online status and network latency but does not reveal detailed information about the target's infrastructure or vulnerabilities.

2. nsLookup:

nsLookup is a command line tool used to gather information about name server of target.

- nslookup, which stands for "Name Server Lookup," is a command-line tool used for querying Domain Name System (DNS) servers to obtain domain name or IP address information.
- DNS is a fundamental system that translates human-readable domain names (e.g., www.example.com) into IP addresses (e.g., 192.0.2.1), allowing computers to locate and communicate with each other on the internet. nslookup is available on most operating systems, including Windows, Linux, and macOS.

Using nsLookup in windows command line :

1. Open Command Prompt (CMD) in windows (press win+R and type cmd).
2. Type “ nslookup target “ (replace target with IP or Website of target).

For ex: nslookup www.xyz.abc or nslookup 127.0.0.1

nslookup [options] [hostname or IP address] [DNS server]

Common Options:

- [hostname or IP address]: The domain name or IP address you want to look up.

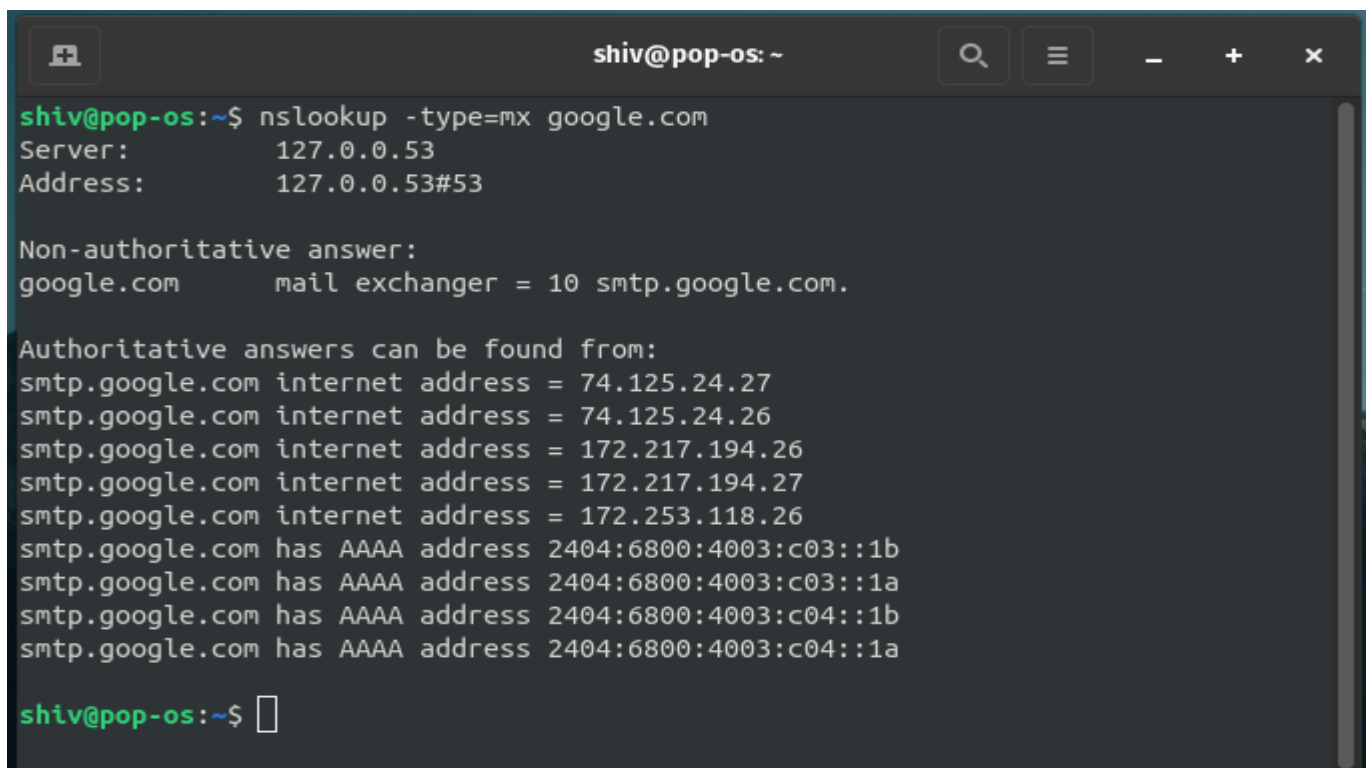
- [DNS server]: (Optional) The DNS server you want to query. If not specified, the default DNS server configured on your system will be used.
- -query=[type]: Specifies the type of DNS record to query. Common types include A (IPv4 address), AAAA (IPv6 address), MX (mail exchange), NS (name server), and TXT (text).
- -type=[type]: Same as -query. Specifies the type of DNS record to query.
- -class=[class]: Specifies the DNS class to use. The default is IN (Internet).
- -timeout=[seconds]: Sets the query timeout in seconds.
- -debug: Enables debugging mode, which displays detailed query and response information.
- -help or ?: Displays the help and usage information for nslookup.

3. To access interactive mode type nslookup and hit enter.

4. You can gather following information (shown in screenshot).

5. To understand more about ping command, type nslookup -h or nslookup /? in terminal. It will open help for ping command. It can be used in linux as well.

6. You can change for looking up mail server, SOA and different services. (mail server is shown in screenshot, for more check help command).



```

shiv@pop-os: ~$ nslookup -type=mx google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
google.com   mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:
smtp.google.com internet address = 74.125.24.27
smtp.google.com internet address = 74.125.24.26
smtp.google.com internet address = 172.217.194.26
smtp.google.com internet address = 172.217.194.27
smtp.google.com internet address = 172.253.118.26
smtp.google.com has AAAA address 2404:6800:4003:c03::1b
smtp.google.com has AAAA address 2404:6800:4003:c03::1a
smtp.google.com has AAAA address 2404:6800:4003:c04::1b
smtp.google.com has AAAA address 2404:6800:4003:c04::1a

shiv@pop-os: ~$ 

```

SCANNING

Scanning is phase of information gathering in which attacker gather more advanced information about the target like open ports and services running, operating system of the target, etc.

- Generally this phase gives us vulnerable point about the target. Information gathered by scanning is very important in performing actual HACK. It is important phase which help in gaining access into the system.
- In scanning, Port scanning, OS fingerprinting, DNS enumerating, etc. will be covered.

Attacker OSI Layer (Layer 3 & 4) Target Network

Between attacker and target the core OSI module layers, layer 3 which is Ipv4, ipv6 and icmp and layer 4 which is TCP and UDP is present. Transmission over a network is done through these layers. It is compulsory to understand the working of layer 3 and layer 4 of OSI module if attacker wish to penetrate over network layer.

Basics of Scanning:

1. Connectivity of Host :

To check whether the host is live or not, ping command is used (already covered in previous chapter), only if the host is up attacker can further perform the exploits.

2. Port Scanning :

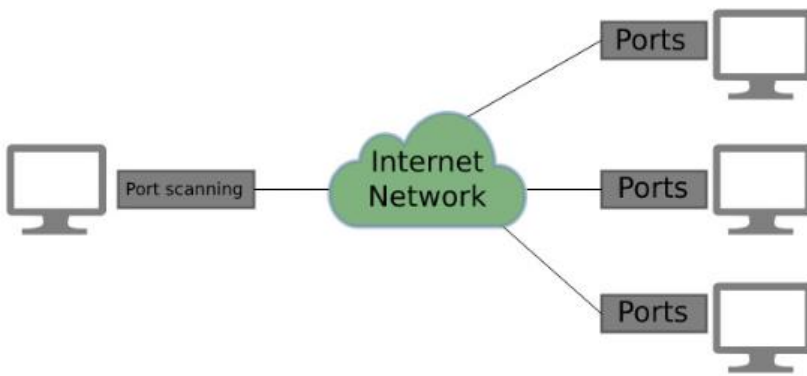
Port scanning is used to check for open ports and services running on them. Sometimes there are many ports open on the target system and some vulnerable services are running over them. It becomes easy to exploit into target system if we can list the vulnerable ports. Commonly used port scanning tools include Nmap, Nessus, and Masscan.

Types of Ports:

Open: The host replies and announces that it is listening and open for queries. An undesired open port means that it is an attack path for the network.

Closed: The host responds but notices that no application is listening. Hackers will scan again if it is opened.

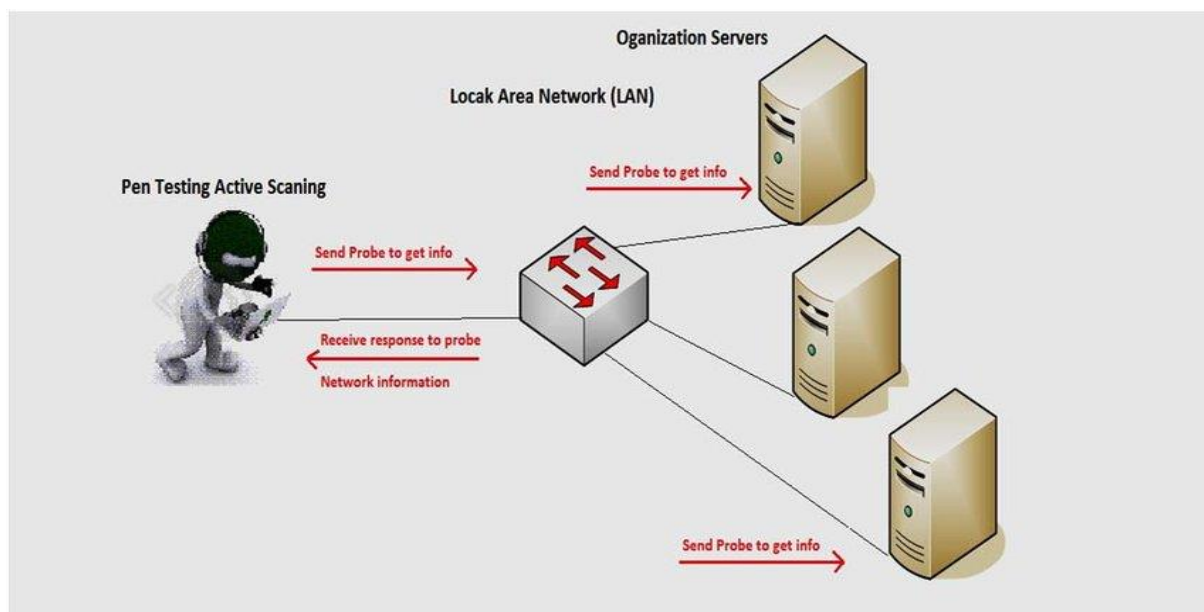
Filtered: The host does not respond to a request. This could mean that the packet was dropped due to congestion or a firewall.



Port scanning (NMAP)

3. Network Scanning

Network scanning is the technique of scanning the devices and systems in a network for vulnerabilities and inconsistencies. Its role is to help admins and ethical hackers find and fix vulnerabilities so that hacking attacks on the network can be avoided.



4. Vulnerability Scanning

It is the automated scanning of the systems in a network to find whether there are any vulnerabilities or loopholes.



5. ICMP Scanning

The role of ICMP scanning is to map network topology. It stands for Internet Control Message Protocol.

Basic techniques of scanning

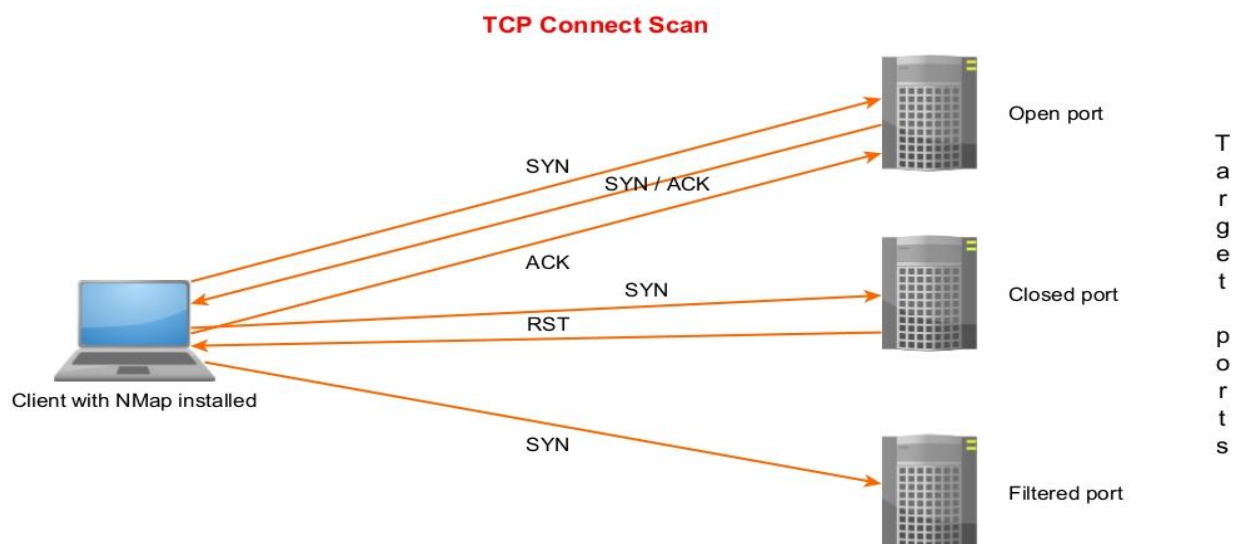
1. Ping Sweep :

Ping sweep is scanning a range of ip address one by one to check whether the target ip is alive or not. in this technique a range of ip address is defined in the same ping command just like : ping 123.43.23.45/24 , the whole range of ip address is scanned until or unless live target is found. This technique is mainly used when there is no specified target and hence targets the whole network to get live target.

```
root@kali:~/Desktop# nmap -sn 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 20:36 EDT
Nmap scan report for XiaoQiang (192.168.1.1)
Host is up (0.00097s latency).
MAC Address: 50:64:2B:CB:20:1B (Xiaomi Electronics,co.)
Nmap scan report for 192.168.1.2
Host is up (0.00017s latency).
MAC Address: 70:85:C2:8E:72:13 (ASRock Incorporation)
Nmap scan report for 192.168.1.3
Host is up (0.0081s latency).
```

2. Transmission control protocol (TCP):

Tcp contains flag, sniffing into tcp flags can provide information to a greater extent. There are following flags present in tcp. :



A. **SYN:** Synchronize, initiates the connection between two systems.

B. **FIN:** Finish, Indicates that transmission is finished.

C. **ACK**: Acknowledgement, Establish the connection

D. **RST**: Reset, used for resetting the connection established.

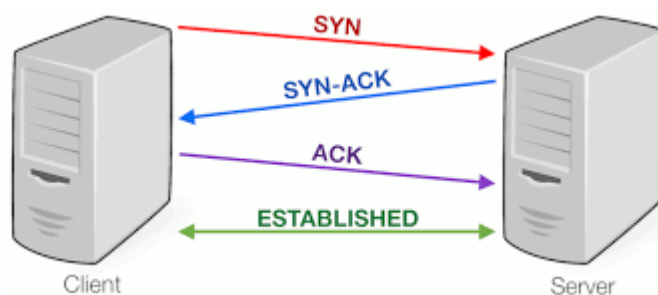
E. **URG**: Urgent, gives packet a priority to process immediately.

F. **PSH**: Push, instructs the target to respond with buffer data immediately.

3. 3-Way Handshake Mechanism :

3-way handshake is used for successful transmission of information or successful connection establishment. 3-way Handshake process :

- The system A will initiate a connection request to the server via a packer with only SYN FLAG.
- Server will reply back with packet having both SYN & ACK flag set.
- Now the client responds back to the server with a single ACK packet.
- zz If the above steps are completed without any problem or complication, then a TCP connection will be established b/w the client and server.



Some other scanning techniques:

1. Full Scan :

In Full Scan, Full TCP Connection is established between attacker and target. If the port is open then only connection will be established. If Port is closed, target becomes unreachable.

2. IDLE Scan :

In the idle scan, attacker performs scanning without sending a single packet from own ip address to the target. Zombies are used in IDLE Scan. Attacker spoofs the IPID of the zombie system (spoofed system which is under control of attacker) and SYN/ACK packets by the target are received by that zombie system. Zombie system replies with RST Packet.

3. Half open Scan

In Half Open Scan, Full TCP connection is not completed. Attacker send SYN packet to initiate the connection, if target responds back with ACK packet then attacker consider that target is listening and if target replies back with RST packet then target is not open or listening.

4. XMAS Scan

XMAS Scan don't work against any versions of windows, if tested on windows machine, it lists all the ports as closed. XMAS Scan Works only if the standard of tcp/ip implementation is used which is based on RFC793.

5. ICMP-ECHO Scan

ICMP-ECHO Scan is used to check whether all the hosts in the target network are live (up) or not by pinging them all. ICMP-Echo itself is not a port scanning technique directly.

6. UDP Scan

UDP Doesn't contains any flag. So what a TCP does UDP Don't and vice-versa. Though it don't contain any packet, udp is simple but at the same difficult to perform scan.

SCANNING USING TOOLS

Some of important scanning tools are demonstrated below :

A. Nmap :

Nmap is a powerful network mapping tool. It is mainly used to perform port scanning and os fingerprinting. Open Kali Linux terminal and type nmap -h . it will show the help window of Nmap.

1. Port Scanning Using Nmap :

- a) Open terminal in kali linux, type “ ifconfig”. It will show your internet address and mac address, to specifically check for Ethernet interface type “ ifconfig eth0 “.
- b) Open new terminal, type “ nmap -h “. It will open nmap help screen (as shown in screenshot).
- c) Name command structure is : nmap [scan type] [target] [target specification]

Common Nmap Scan type:

-sS or -sT: Performs a TCP SYN scan or TCP connect scan, respectively.

-sU: Performs a UDP scan to identify open UDP ports.

-p <ports>: Specifies the port(s) to scan, e.g., -p 1-100 to scan ports 1 through 100.

-A: Enables OS detection, version detection, and script scanning for detailed information about services.

-T<0-5>: Sets the timing template for scan speed (0 being slowest, 5 being fastest).

-oN <file>: Saves scan results to a text file.

-v or -vv: Increases verbosity for more detailed output.

-Pn: Treats all hosts as online, skipping host discovery.

d) For scanning the ports: `nmap -sT [target]` (for TCP Scan).

Example:

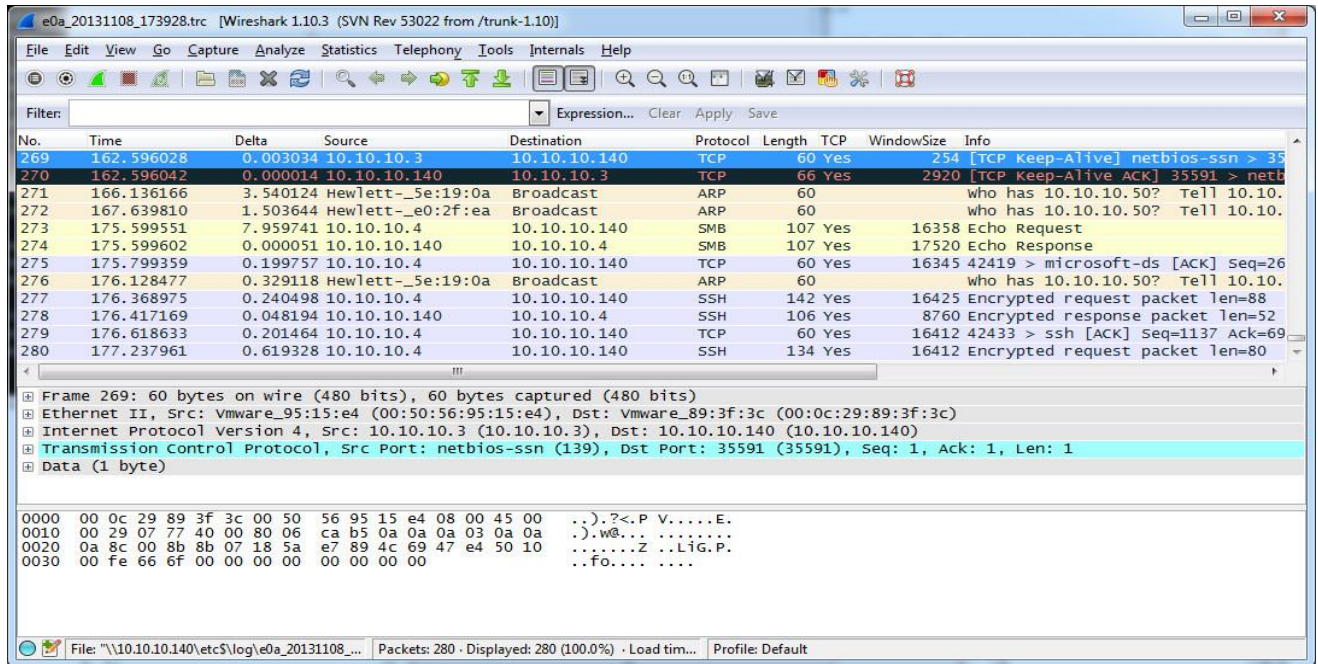
`nmap -sT 192.168.1.1-20`

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sT 192.168.192.131  
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-07-21 14:59 IST  
Nmap scan report for 192.168.192.131  
Host is up (0.00021s latency).  
Not shown: 991 closed ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49156/tcp open  unknown  
49157/tcp open  unknown  
MAC Address: (VMware)  
Nmap done: 1 IP address (1 host up) scanned in 14.86 seconds  
root@kali:~#
```

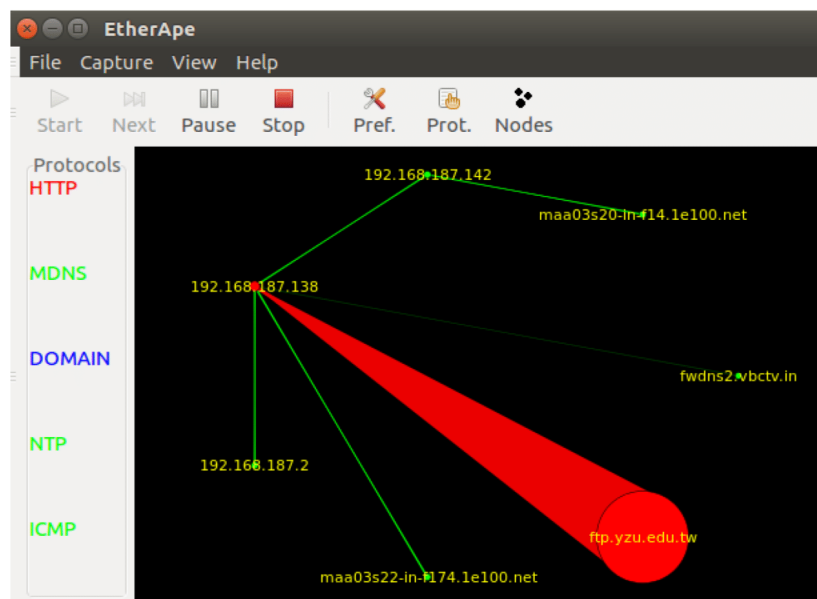
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -p 80,135,23,21 192.168.1.25  
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-07-27 17:14 IST  
Nmap scan report for 192.168.1.25  
Host is up (0.00034s latency).  
PORT      STATE SERVICE  
21/tcp    closed ftp  
23/tcp    closed telnet  
80/tcp    closed http  
135/tcp   open  msrpc  
MAC Address: 00:0C:29:62:DB:17 (VMware)
```

e) To check how nmap works, Etherape and Wireshark are used.

- f) To install the etherape, open new terminal and type “ apt-get install etherape”. Input Y for the additional space.
- g) Open a terminal and type “wireshark”. Wireshark windows will opens, now select the layers on which analysis has to take place. Click on start capturing. (shown in the screenshot.)



- h) Open a terminal and type “Etherape”. Once the packets starts exchanging, the network traffic will be illustrated in etherape. (see in screenshot.)



- i) Nmap will list all the ports open and this information is used to exploit the vulnerable ports.

2. OS Fingerprinting using Nmap :

- Open terminal in kali linux, type “ ifconfig”. It will show your internet address and mac address, to specifically check for Ethernet interface type “ ifconfig eth0 “.
- Open new terminal, type “ nmap -h “. It will open nmap help screen (as shown in screenshot).
- Name command structure is : nmap [scan type] [target] [target specification]
- For OS Fingerprinting : nmap -O [target] .

Additional Options:

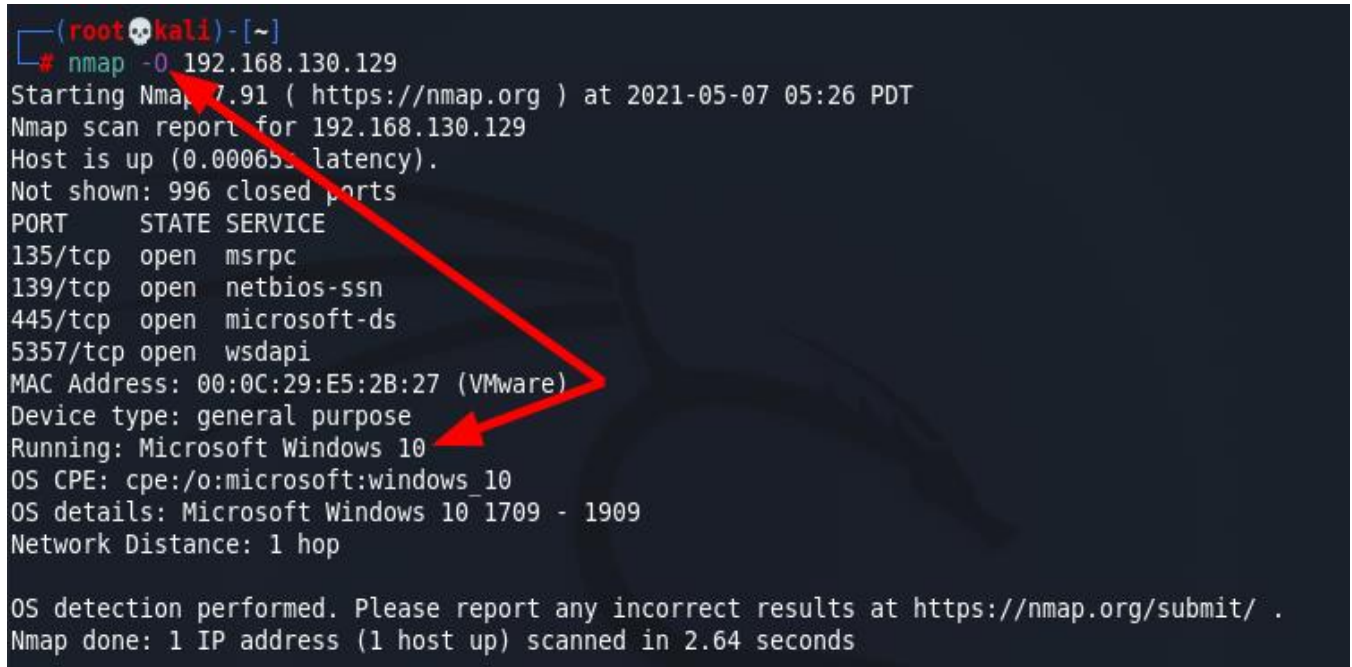
To enhance OS fingerprinting, such as:

-sV stands for Service version.

-A stands for Aggressive.

-T<0-5> to adjust the scan timing template.

- Nmap will list all the open ports along with the operating system running on target machine. It may be range or operating system like xp sp1 – sp3 or specified os. (shown in image)



```
(root@kali) ~# nmap -O 192.168.130.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-07 05:26 PDT
Nmap scan report for 192.168.130.129
Host is up (0.00065s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: 00:0C:29:E5:2B:27 (VMware)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.64 seconds
```

B. Dnsenum :

- Dnsenum is one the powerful dns enumeration tool, preinstalled in kali linux.
- It is often employed by ethical hackers and security professionals during the reconnaissance phase of security assessments and penetration testing to gather information about a target domain or network.
- Dnsenum is specifically designed to collect DNS-related data, such as subdomains, mail servers, and DNS records, which can be valuable for understanding an organization's online presence and identifying potential vulnerabilities.

Subdomain Enumeration:

- Dnsenum can be used to enumerate subdomains associated with a target domain. This process involves discovering additional subdomains beyond the main domain (e.g., subdomain.example.com).

Dnsenum will provide information about subdomains, IP addresses (A records), mail servers (MX records), and any TXT records associated with the domain. This information can be valuable for understanding the target's DNS configuration and online presence.

Basically its an perl script and it performs the following operations:

- 1) Gets the host's address (A record).
- 2) Gets the nameservers (threaded).

Nameservers help connect URLs with the IP address of web servers. Nameservers are an important part of the Domain Name System (DNS), which many people call the “phone book of the Internet”.

Nameservers play an important role in connecting a URL with a server IP address in a much more human-friendly way.

- 3) Gets the MX record (threaded).

A DNS 'mail exchange' (MX) record directs email to a mail server. The MX record indicates how email messages should be routed in accordance with the Simple Mail Transfer Protocol (SMTP, the standard protocol for all email).

- 4) Performs AXFR queries on nameservers and get BIND versions (threaded).

- 5) Gets extra names and subdomains via Google scraping (Google query = “allinurl: -www site:domain”).

- 6) Brute force subdomains from file, can also perform recursion on subdomain that have NS records (all threaded).

- 7) Calculates C class domain network ranges and perform whois queries on them (threaded).
- 8) Performs reverse lookups on net ranges (C class or/and whois net ranges) (threaded).
- 9) Writes to domain_ips.txt file ip-blocks.

Enumerating DNS using dnsenum :

- a. Open terminal in kali linux and type “ dnsenum -h “. Help screen will be shown up.
- b. Command for performing enumeration is “ dnsenum [target]”

For ex : dnsenum www.google.com

- e. Details of dns will be enumerated as shown in screenshot.
- f. There are many information gathering tools which are preinstalled in kali linux. (to check working of any tool, just type “ [tool name] -h” or “[tool name] /?”).

```
root@kali:~# dnsenum --enum google.com
dnsenum.pl VERSION:1.2.3
Host's addresses:
google.com. 62 IN A 74.125.130.100
google.com. 62 IN A 74.125.130.101
google.com. 62 IN A 74.125.130.102
google.com. 62 IN A 74.125.130.113
google.com. 62 IN A 74.125.130.138
google.com. 62 IN A 74.125.130.139
Name Servers:
ns1.google.com. 343227 IN A 216.239.32.10
ns2.google.com. 343227 IN A 216.239.34.10
ns3.google.com. 343227 IN A 216.239.36.10
ns4.google.com. 343227 IN A 216.239.38.10
Mail (MX) Servers:
aspmx.l.google.com. 17 IN A 74.125.129.27
alt1.aspmx.l.google.com. 38 IN A 74.125.142.26
alt3.aspmx.l.google.com. 178 IN A 173.194.68.27
alt4.aspmx.l.google.com. 163 IN A 74.125.131.27
alt2.aspmx.l.google.com. 293 IN A 74.125.137.27
```

C. Hping3 :

Hping 3 is a powerful tool which is pre-installed in kali linux. Hping is used for advanced ping, packet crafting, flooding the target by dos and many other uses. To take the overview of hping tool, open terminal in kali linux and type “ hping3 -h “. It will open help screen of hping tool. There are many options for performing various attacks. (shown in screenshot)

- hping3 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies.
- Packet crafting is a technique that allows network administrators to probe firewall rule-sets and find entry points into a targeted system or network.
- hping3 is a network tool able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies.
- hping3 handles fragmentation, arbitrary packets body and size and can be used in order to transfer files encapsulated under supported protocols.

Performing flag scan using hping3 :

1. Open terminal in kali linux and type “ wireshark”. Wireshark will be opened and choose interface on which packet sniffing is to be performed. Click on Start Capture and minimize the window.
2. Open new terminal and type “ hping -S [target]”.
3. Once the command is completed, maximize the Wireshark window and analyse the packets, all the captured packets will be SYN Packet. (shown in screenshot.)
4. Practise for various attack vectors of hping3. It is one of the important tools which is also useful in later stages.

\$ sudo hping3 [options] hostname

Some important options in hping3 command are as follows:

- **-c, --count:** specify the number of packets to be sent
- **-8, --scan:** Scan mode
- **-9, --listen:** Listen mode
- **-a, --spoof:** Spoof source address
- **-t, --ttl:** set TTL (time to live) of outgoing packets

1. Send TCP packets to a host

```
$ sudo hping3 192.168.56.102
```

```
golinux@ubuntu-PC:~$ sudo hping3 192.168.56.102
HPING 192.168.56.102 (enp0s9 192.168.56.102): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=7.0 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=1 win=0 rtt=16.3 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=2 win=0 rtt=16.2 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=3 win=0 rtt=16.3 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=4 win=0 rtt=8.6 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=5 win=0 rtt=16.3 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=6 win=0 rtt=16.0 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=7 win=0 rtt=16.3 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=8 win=0 rtt=16.0 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=9 win=0 rtt=15.8 ms
^C
--- 192.168.56.102 hping statistic ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 7.0/14.5/16.3 ms
```

2. Send SYN packets to the target

To send SYN packets to the target IP address, you can use the `-S` or `--syn` option.

```
$ sudo hping3 -S 192.168.56.102
```

```
golinux@ubuntu-PC:~$ sudo hping3 -S 192.168.56.102
HPING 192.168.56.102 (enp0s9 192.168.56.102): S set, 40 headers + 0 data bytes
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=6.7 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=1 win=0 rtt=6.6 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=2 win=0 rtt=6.0 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=3 win=0 rtt=5.9 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=4 win=0 rtt=5.0 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=5 win=0 rtt=4.1 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=6 win=0 rtt=3.8 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=7 win=0 rtt=3.8 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=8 win=0 rtt=3.9 ms
len=46 ip=192.168.56.102 ttl=64 DF id=0 sport=0 flags=RA seq=9 win=0 rtt=3.0 ms
^C
--- 192.168.56.102 hping statistic ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 3.0/4.9/6.7 ms
```

3. Send ICMP packets to the target:

```
$ sudo hping3 -1 192.168.56.102
```

Or `$ sudo hping3 --icmp 192.168.56.102`

4. Send UDP packets to target

You can use the `-2` or `--udp` option to send UDP packets to the target host.

```
$ sudo hping3 -2 192.168.56.102 (Or) $ sudo hping3 --udp 192.168.56.102
```

5. Specify the number of packets:

The `-c` or `--count` option lets you specify the number of packets to be sent.

```
$ sudo hping3 -c num 192.168.56.102 (Or) $ sudo hping3 --count num 192.168.56.102
```

