

3. Scanning Networks



ETHICAL HACKING



Theory

Scanning

Scanning is a process of identifying network and service-related information by communicating with the target. Scanning helps in identifying IP/Hostnames, Ports, Services running on ports, Live hosts, Vulnerable services running on the target network.

Types of Scanning

Different number of scanning procedures are used with the objective to identify hosts, ports, and services in the target network. One of the most common types scanning methods that are available.

Network Scanning

During the network scanning process, attackers gather a list of IP addresses of computers that are live on the target network. The job of the attacker will be easy if he/she can analyze the network structure and services running on each machine.

List of Network Scanners

- Angry IP Scanner
- Advanced IP Scanner
- Netdiscover
- Autoscanner
- hping3
- Nmap

List of Network Scan Methods

- Ping Sweep
- Arp Scan

What Are Ports and Port Numbers

Ports are virtual entry points to any digital device; devices can communicate with one to another using port, there are virtually 65535 ports available in every device, those can be identified with port numbers, ranging from 0 to 65535.

0	1023	Well known ports
1024	49135	Random ports
49136	65535	Experimental ports

Port Scanning

Port scanning is a technique where the attacker will send communication probes to targets to see how the target is responding to them, based on the

response attacker will determine what ports are open and several other port details, like service running on the port numbers, and OS the target is running.

List of Port scanners

- Nmap
- SuperScan
- Strobe
- Zenmap

List of Port Scan methods

- SYN Scan/Stealth Scan/
- TCP Connect Scan
- ACK Scan
- XMAS Scan
- FIN Scan
- NULL Scan
- OS Detection Scan
- Script Scan
- UDP Scan
- Service Detection Scan

Few Well-Known Ports

Application	Port Number(s)	Application	Port Number(s)
FTP	20–21	DNS	53
Telnet	23	IRC	194
SMTP	25	POP3	110
DNS	53	SNMP	161
HTTP	80	HTTPS	443
SSH	22	NetBIOS	139
TFTP	69	SQL	156

For details on other port numbers and services refer [RFC-1700](https://www.rfc-editor.org/rfc/rfc1700)

Live Host identification scan

Identifying the turned-on computers by sending ICMP packets or ARP packets or some other kind of packets is called Live Host Identification Scan.

ICMP

ICMP stands for Internet Control Messaging Protocol; this is widely used for internet communication troubleshooting or to generate errors related to IP operations, this will send packets to the target machine and will see whether the packets are delivered or not.

TCP

Transmission Control Protocol (TCP), which is a widely used protocol for data transmission over a network. This protocol establishes a reliable connection between two hosts before transmitting data, to ensure that data transmitted over the network reaches the destination without fail. TCP also known as a connection-oriented protocol, establishes a reliable connection between sender and receiver. TCP provides error and flow control mechanisms which help in orderly transmission of data and retransmission of lost packets.

UDP

UDP stands for User Datagram Protocol, which is connectionless protocol, mostly used for connections that can tolerate data loss. UDP is used by applications on the internet that offer voice and video communications, which can suffer some data loss without adversely affecting the quality. UDP does not provide error and flow control mechanisms because of which it does not require a connection before transmitting data over the network.

TCP 3-way Handshake

To start a proper TCP conversation, the sender and receiver perform 3-way handshake before exchanging data over the network. It is a process used by two hosts to agree upon some protocol stack to start sharing data. Following image represents the process of 3-way handshake.



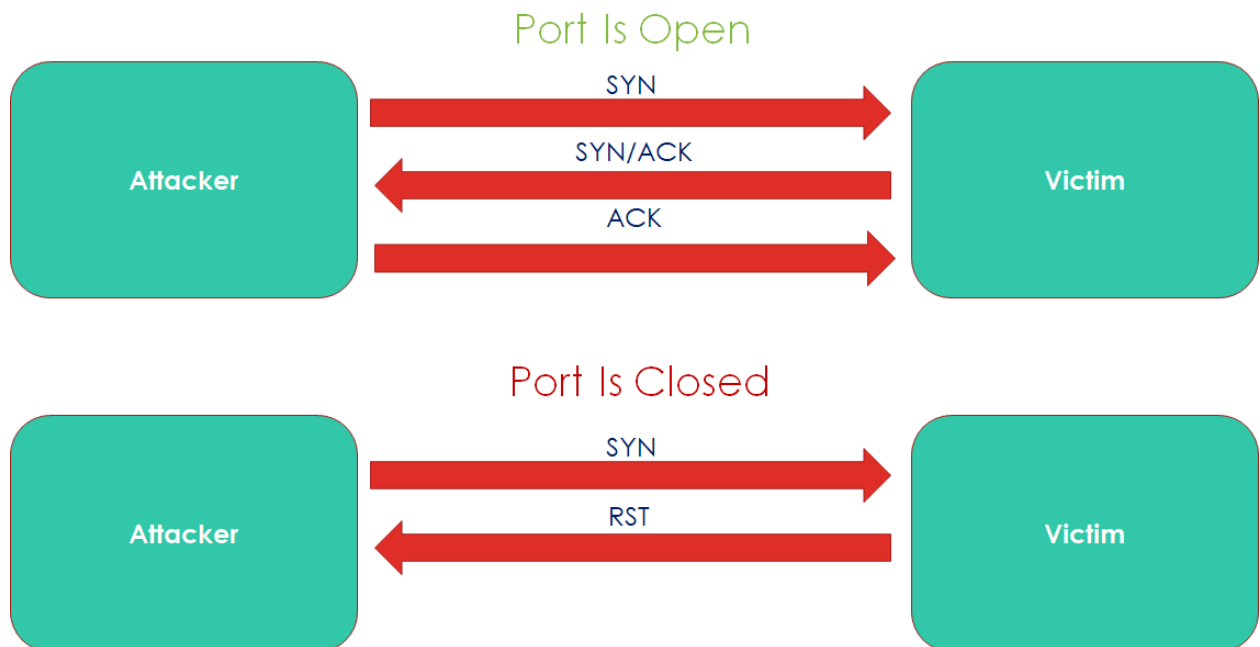
TCP COMMUNICATION FLAGS

1. **SYN** (Synchronize): SYN flags will be used to initiate a data transfer at the start of a communication process.
2. **ACK** (Acknowledgement): ACK flags will be used to send the receipt of successful packet transmission.
3. **FIN** (Finish): FIN flags will be used to close or finish an existing packet transmission. No more packets to be received.
4. **RST** (Reset): RST flags will be used to terminate or reset a connection.
5. **URG** (Urgent): Data in this flagged packet should be processed immediately.
6. **PSH** (Push): Sends all buffered data immediately.

Types of Port Scanning Techniques

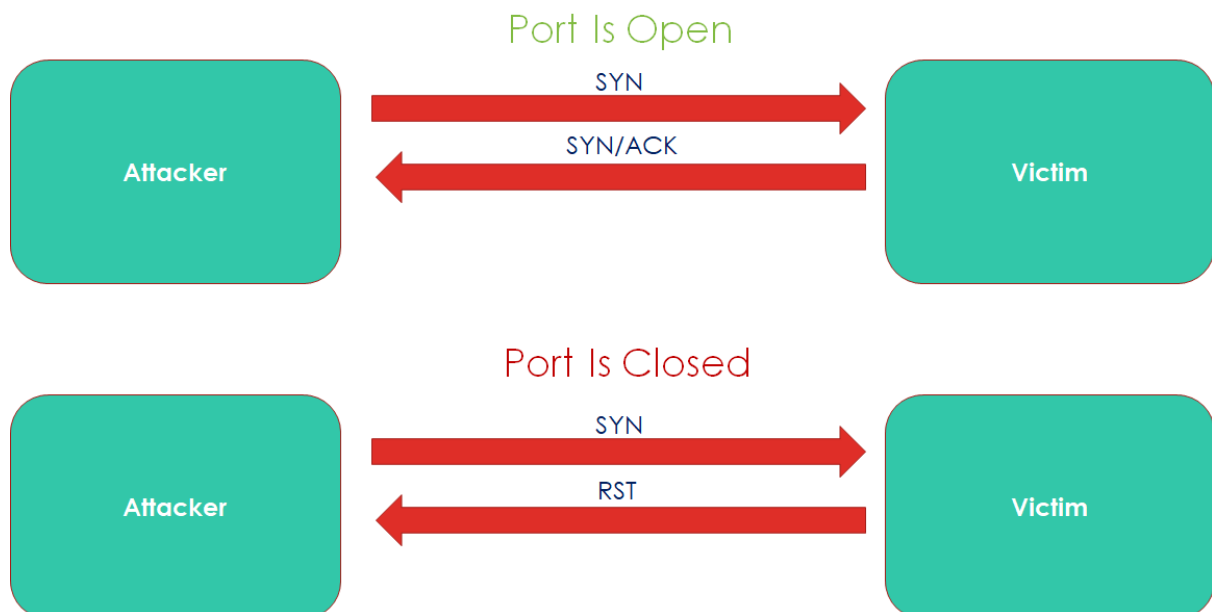
- **TCP Connect Scan / Full Open Scan**

Nmap directly communicates with the operating system to establish a connection with the target machine and port by issuing the connect system call.



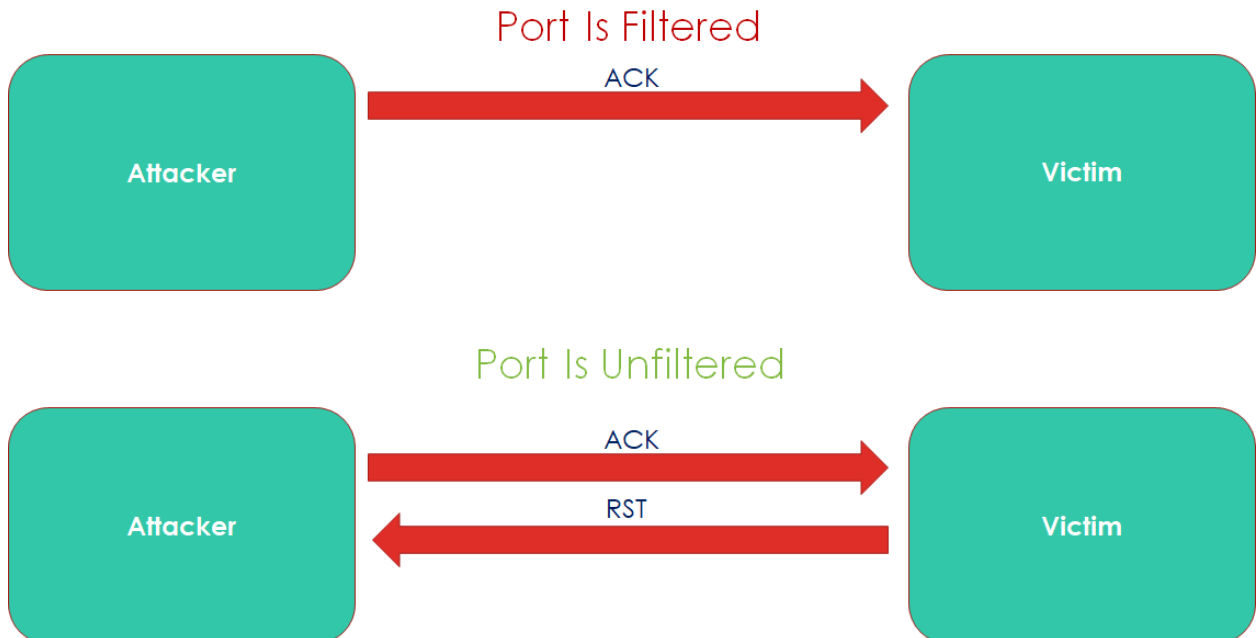
- **SYN Scan / Half-Open Scan / Stealth Scan**

SYN scan is the most popular scan option. It can scan thousands of ports in a short period on a fast network not hampered by restrictive firewalls.



- **ACK Scan/Firewall Detection**

This scan is different from others scanning operations discussed before; it never determines open ports. It is used to identify firewall rules, determining the type of firewall and identify filtered ports.



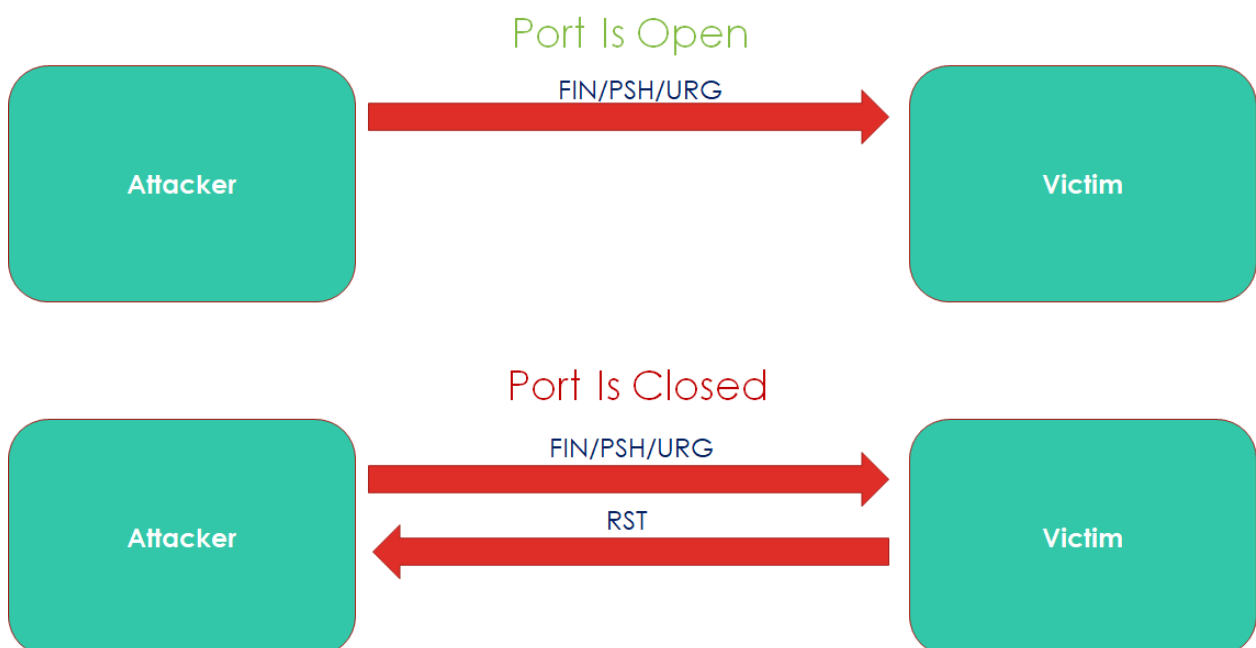
- **XMAS Scan**

The Xmas-Tree scan sends a TCP packet with the following flags:

URG — Indicates that the data is urgent and should be processed immediately

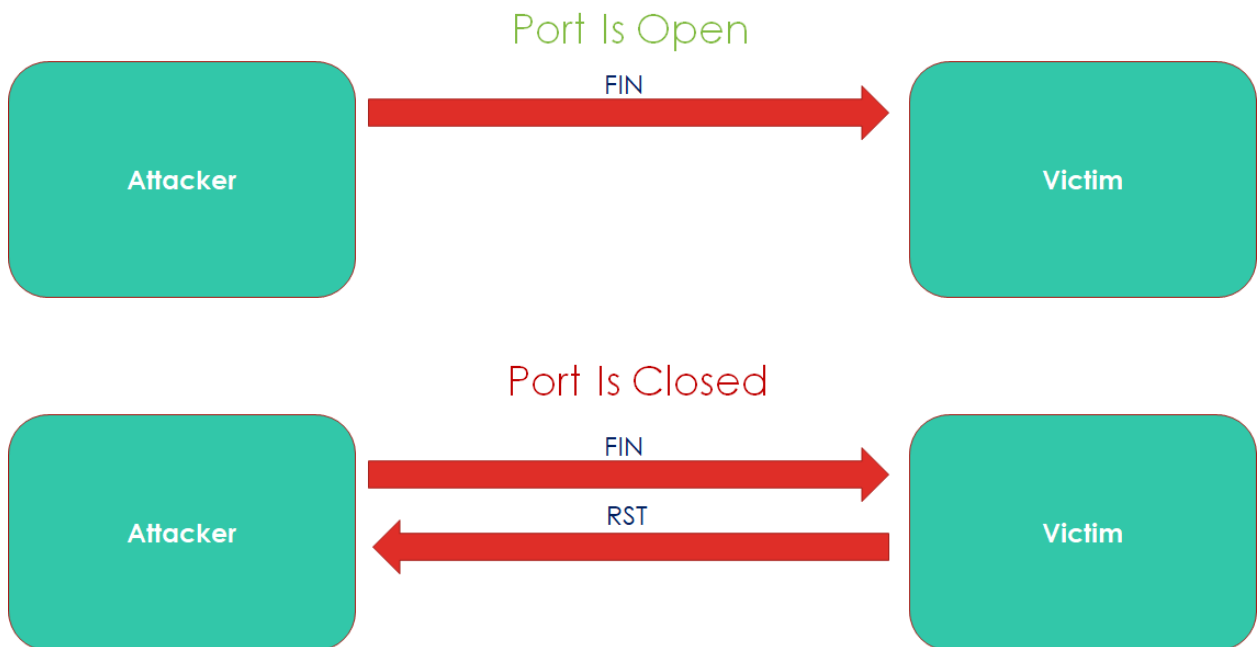
PSH — Forces data to a buffer

FIN — Used when finishing a TCP session



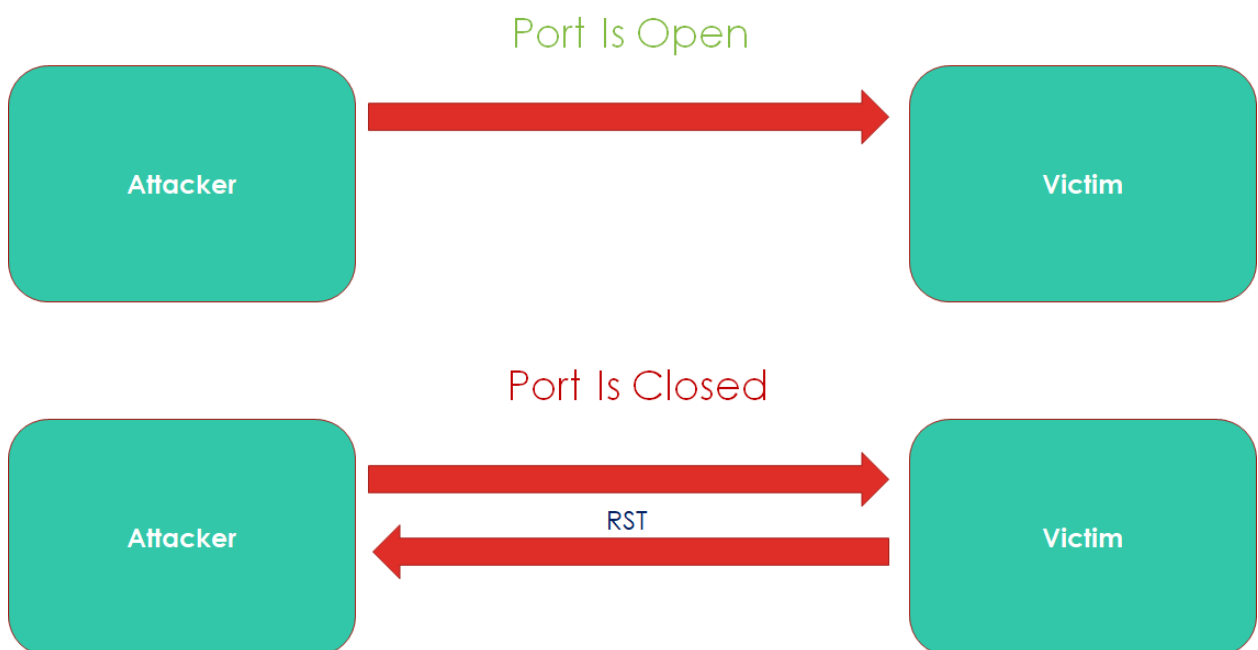
- **FIN Scan**

FIN scan, which attempts to close a connection that isn't open. The operating system generates an error if service is not running on target port. If a service is listening, the operating system will silently drop the incoming packet. Therefore, no response indicates a listening service at the port.



- **NULL Scan**

A data packet with zero flag values will be sent to a TCP port. (In a regular TCP communication, at least one bit or flag is set). In TCP connect / SYN scans, a response indicates an open port, but in a NULL scan, a response indicates a closed port.



Importance of Scanning

Scanning will provide an exact outline of the network structure of the target workspace. It is beneficial for hacking target servers or individual computers. Scanning will provide a blueprint of entire network and details about devices running on the network, information related to network topology and helps in deciding what operating system is running on target computers.

Countermeasures

- Block ICMP and UDP inbound.
- Disable unused ports with support of policy settings.
- Block internal IP addresses from coming inbound.
- Change system and application banners to counter software detection attacks.
- Always use a genuine operating system, update it frequently.
- Use IDS & IPS to detect and prevent attacks.
- Use “duckduckgo” or “StartPage” search engine to protect privacy.



Practicals

INDEX

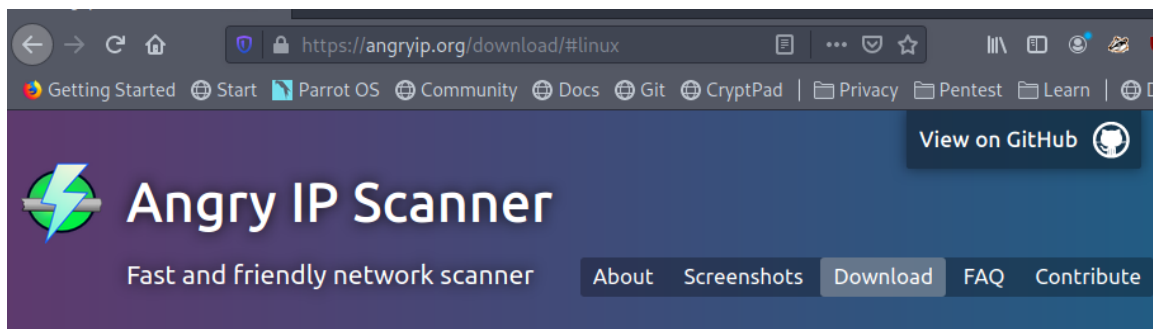
S. No.	Practical Name	Page No.
1	Network Scanning with Angry IP Scanner	1
2	Network Scanning With netdiscover	6
3	Ping Sweeping with nmap	7
4	Port Scanning with nmap	8



Practical 1: Network Scanning with Angry IP Scanner

Description: In this practical we will discuss how to install Angry IP scanner and how to perform scanning using this tool. It is a graphical tool that is used to perform scanning on a range of Private IPs or Public IPs using different protocols. It is also useful to perform port scanning on IPs and we can export results to a file for report purposes.

Step 1: To download Angry IP scanner, visit following link <https://angryip.org/download/> And download a suitable package, for Parrot Linux download .deb package (based on your installation 32 bit or 64bit)



Download for Windows, Mac or Linux

Windows

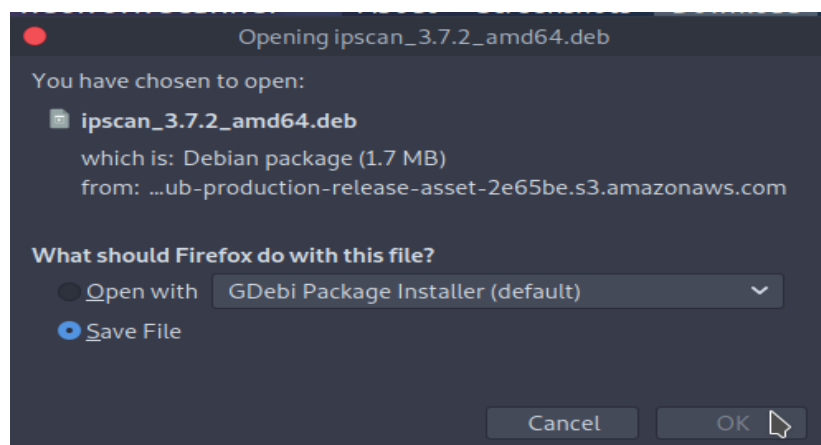
Mac OS

Linux

Download version 3.7.2 below or [browse more releases](#) or [even older releases](#).

- [DEB Package](#) for Ubuntu/Debian/Mint, 64-bit
- [RPM Package](#) for Fedora/RedHat/Mageia/openSUSE, 64-bit
- [DEB Package](#) for Ubuntu/Debian/Mint, any architecture (e.g. 32-bit or ARM)
- [Executable Jar](#) - you need to provide your own swt.jar to classpath

Step 2: Save the file if it is asking



Step 3: Then open a terminal and go to **Downloads** location (/root/Downloads/)

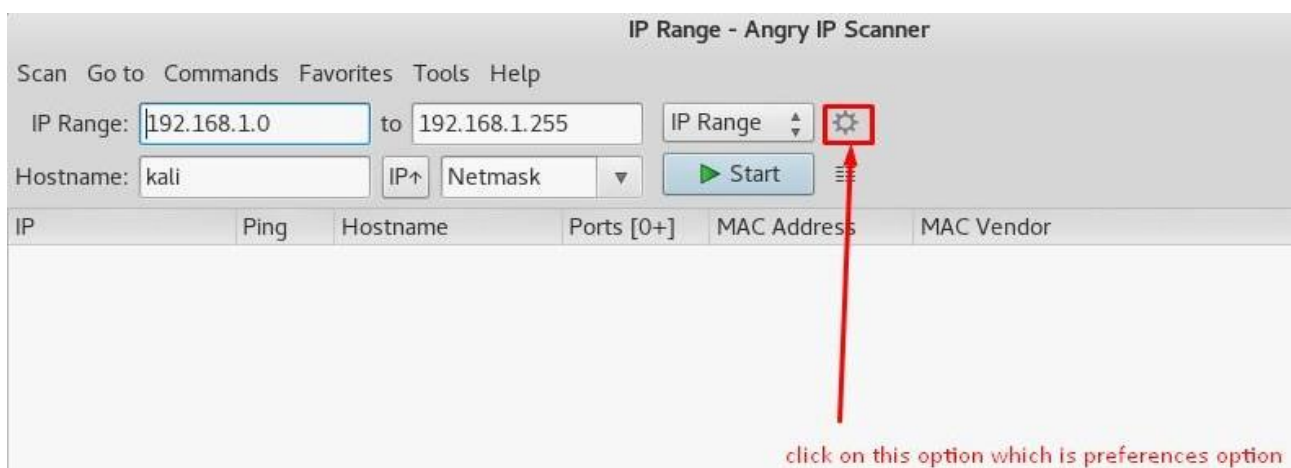
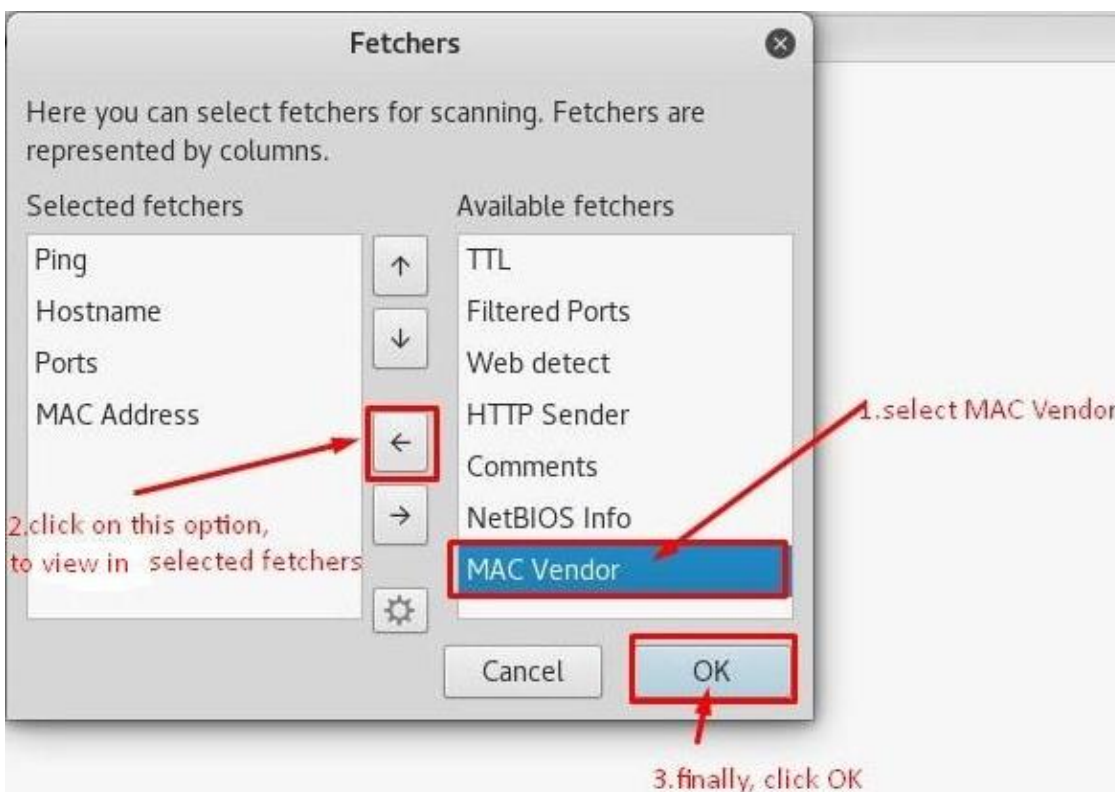
```
[user@parrot-virtual]~$ cd Downloads/
[user@parrot-virtual]~/Downloads$ ls
ipscan_3.7.2_amd64.deb
```

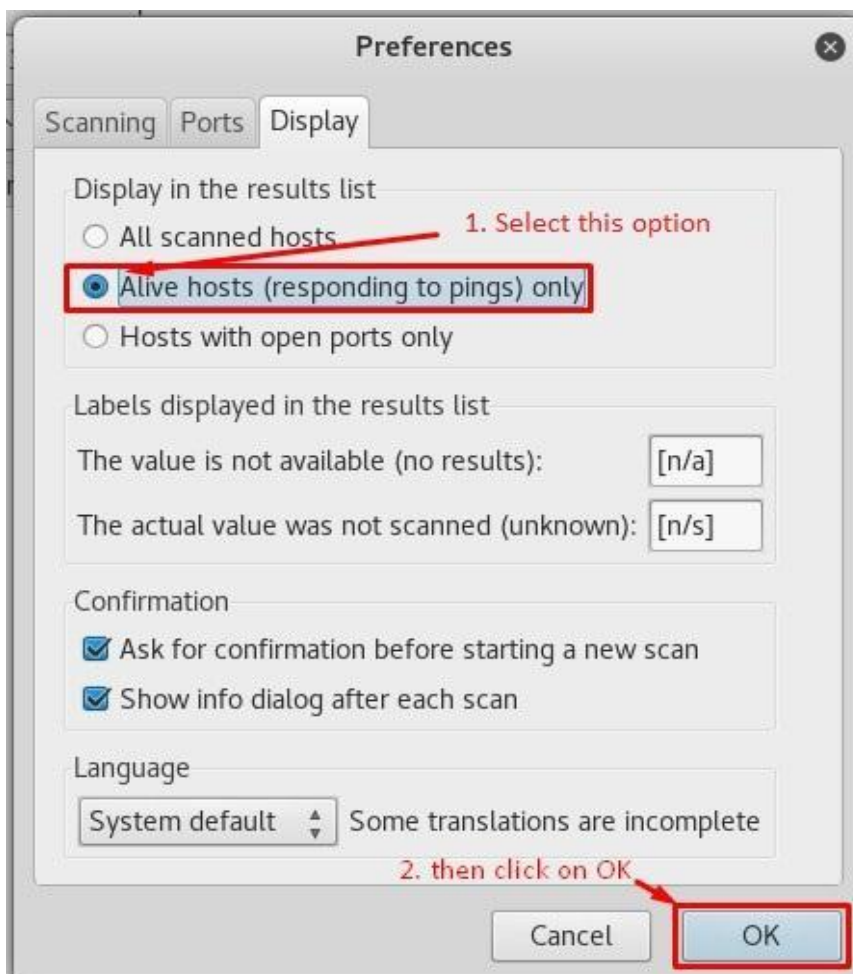
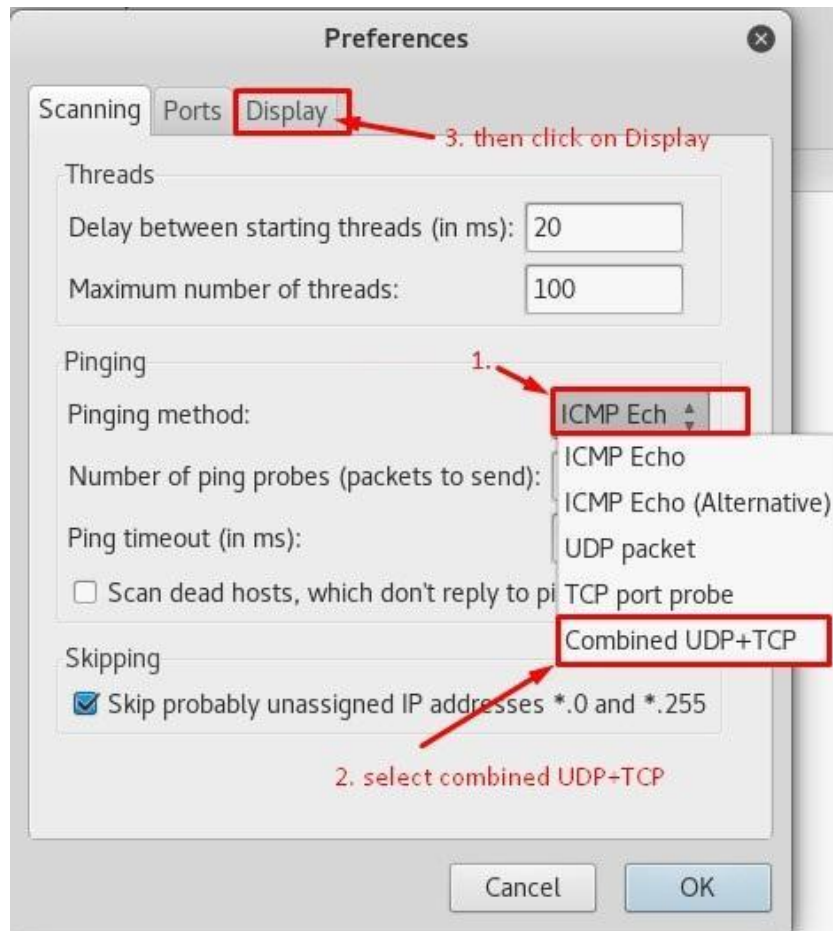
Step 4: we can see the downloaded file in the **Downloads** directory; we can install it by executing the following command

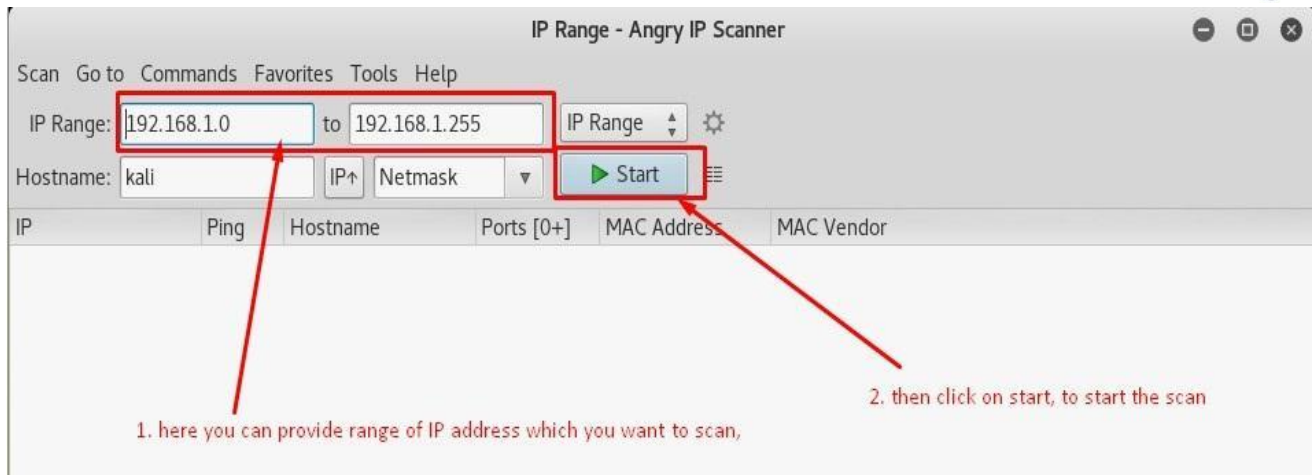
```
[user@parrot-virtual]~/Downloads$ sudo dpkg -i ipscan_3.7.2_amd64.deb
[sudo] password for user:
Selecting previously unselected package ipscan.
(Reading database ... 421442 files and directories currently installed.)
Preparing to unpack ipscan_3.7.2_amd64.deb ...
Unpacking ipscan (3.7.2) ...
Setting up ipscan (3.7.2) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for bamfdaemon (0.5.4-2) ...
Rebuilding /usr/share/applications/bamf-2.index...
Processing triggers for mime-support (3.64) ...
```

Step 5: After installation, search for **Angry IP scanner** in installed applications and start Angry IP scanner. The application looks as shown below. Follow the steps to perform scanning and discover devices.

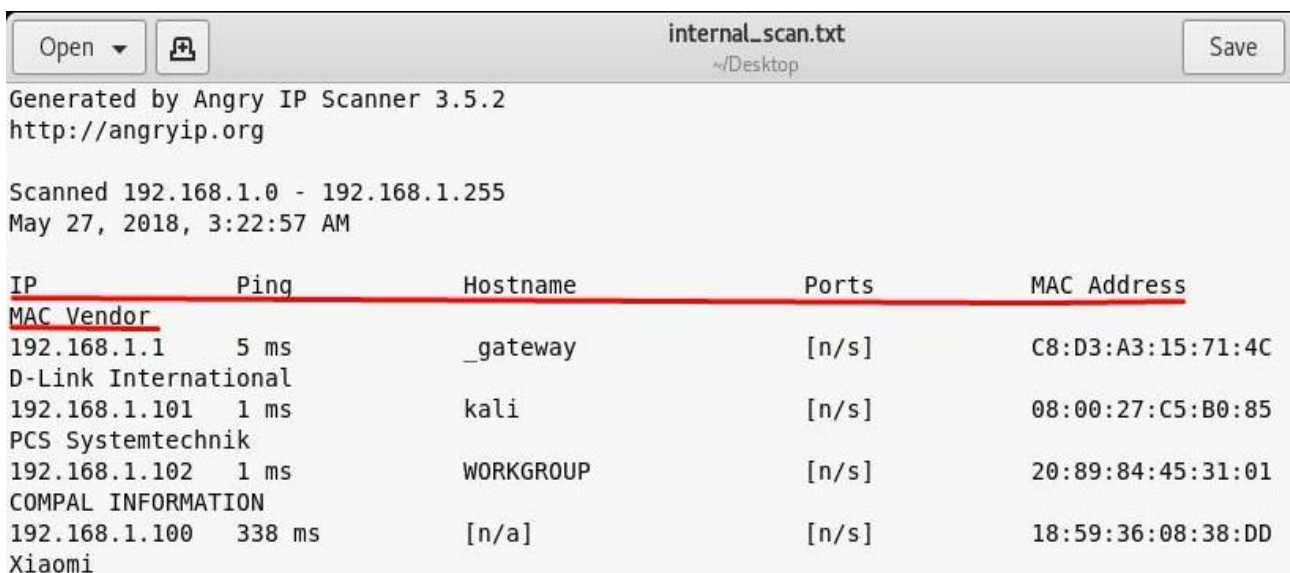








Step 5: Export the scan results to a text file. We can use this output file to feed it to another VA tools or port scanner tools.



Practical 2: Network Scanning With netdiscover

Description: Netdiscover is another terminal based network scanner used to perform scanning on local networks. It uses arp protocol to perform scanning. Major drawback in this tool is if a group of people perform at the same time it won't give correct results.

Prerequisites: Netdiscover tool installed in your system

Step 1: In Parrot Linux terminal type the following command **netdiscover -i <interface name>**

- for example: **netdiscover -i eth0**

```
[user@parrot-virtual]-[~/Downloads]
$ sudo netdiscover -i eth0
```

```
Currently scanning: 172.26.131.0/16 | Screen View: Unique Hosts
55 Captured ARP Req/Rep packets, from 7 hosts. Total size: 3300
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.21.1	00:e0:2d:9c:04:12	1	60	InnoMediaLogic, Inc.
192.168.43.1	7c:46:85:19:65:f4	27	1620	Motorola (Wuhan) Mobility Technologies Communication Co.
192.168.43.247	00:e0:2d:9c:04:12	23	1380	InnoMediaLogic, Inc.
192.168.43.205	08:00:27:ae:17:53	1	60	PCS Systemtechnik GmbH
192.168.43.222	08:00:27:28:0b:85	1	60	PCS Systemtechnik GmbH
192.168.43.67	04:79:70:db:7e:b6	1	60	HUAWEI TECHNOLOGIES CO.,LTD
172.16.254.1	00:e0:2d:9c:04:12	1	60	InnoMediaLogic, Inc.

Practical 3: Ping Sweeping with nmap

Description: Nmap is an open source scanning tool that performs scanning on large networks and gives results within less time. In this practical we use nmap to network scanning over a range of IP addresses, it can scan both private and public IPs. we can save the results in different file formats also.

Prerequisites: nmap tool installed in your system

Step 1: In Parrot Linux terminal type the following command

- **nmap -sn 192.168.1.1/24**

```
[user@parrot-virtual]~  
$ route -n  
Kernel IP routing table  
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface  
0.0.0.0          192.168.43.1    0.0.0.0          UG    100    0      0 eth0  
192.168.43.0     0.0.0.0         255.255.255.0    U     100    0      0 eth0  
[user@parrot-virtual]~  
$ nmap -sn 192.168.43.1/24  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 09:52 BST  
Nmap scan report for 192.168.43.71  
Host is up (0.00031s latency).  
Nmap scan report for 192.168.43.205  
Host is up (0.0057s latency).  
Nmap scan report for 192.168.43.222  
Host is up (0.0036s latency).  
Nmap scan report for windows (192.168.43.247)  
Host is up (0.0022s latency).  
Nmap done: 256 IP addresses (4 hosts up) scanned in 12.72 seconds
```

Practical 4: Port Scanning with nmap

Description: Nmap is a multi-purpose tool, we can perform different actions using this tool. In this practical we will explore different options nmap have to perform port scanning on the target IPs and different scanning customizations. Using nmap we can get which ports are open in target IP, what are the services running on ports and it's versions, target OS details, firewall detection etc.

Scan 1: Regular Scan (SYN stealth scan or half open scan)

- **Syntax:** nmap <target IP or domain>
 - **Ex:** nmap 192.168.0.137
 - nmap -sS example.com

```
[user@parrot-virtual]~$ sudo nmap -sS 192.168.43.205
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 09:55 BST
Nmap scan report for 192.168.43.205
Host is up (0.00026s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:AE:17:53 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.95 seconds
```

Note: Even if we take a domain name, nmap will not scan the website, it will scan the computer (server) hosting that website.

Scan 2: TCP connect scan (Full Connect Scan)

- **Syntax:** `nmap -sT <target IP or domain>`
 - **Example:** `nmap -sT example.com`
 - `nmap -sT 192.168.0.137`

```
[root@parrot-virtual]~[/home/user/Documents/Sublist3r]
#nmap -sT hackthissite.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 09:24 BST
Nmap scan report for hackthissite.org (137.74.187.104)
Host is up (0.18s latency).
Other addresses for hackthissite.org (not scanned): 2001:41d0:8:ccd8:137:74:187:103 2001:41d0:8:ccd8:137:74:187:100 2001:41d0:8:ccd8:137:74:187:102 2001:41d0:8:ccd8:137:74:187:101 2001:41d0:8:ccd8:137:74:187:104 137.74.187.102 137.74.187.103 137.74.187.101 137.74.187.100
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
443/tcp    open  https
Nmap done: 1 IP address (1 host up) scanned in 46.09 seconds
```

Note: If you get any error saying host may be down or disabled ICMP try adding `-Pn` to the command

- **Example:** `nmap -sT -Pn example.com`

Scan 3: Service Detection scan or Version Detection scan

- **Example:** `nmap -sV example.com`
- `nmap -sV 192.168.0.137`

```
[user@parrot-virtual]~[~]
$sudo nmap -sV 192.168.43.205
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 09:57 BST
Nmap scan report for 192.168.43.205
Host is up (0.00017s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login
514/tcp   open  shell?
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port514-TCP:V=7.80%I=7%D=9/29%Time=5F72F70B%P=x86_64-pc-linux-gnu%r(NUL
SF:L,35,"\\x01Couldn't\\x20get\\x20address\\x20for\\x20your\\x20host\\x20\\(parrot
SF:-virtual\\)\\n");
```

Scan 4: OS Detection Scan

- **Syntax:** `nmap -O <target IP or domain>`
 - **Example:** `nmap -O example.com`
 - `nmap -O 192.168.0.137`

```
[user@parrot-virtual]~$ sudo nmap -O 192.168.43.205
```

```
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 02:25:98:60:ED:4F (Unknown)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
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 2.45 seconds
```

Based on open and closed ports, this scan finds out the OS running on target ip.

NOTE: this scan needs atleast 2 open and 2 closed ports to identify OS.

Scan 5: FIN scan (FIN Flag)

- **Syntax:** `nmap -sF <target IP or domain>`
 - **Example:** `nmap -sF example.com`
 - `nmap -sF 192.168.0.137 -v`

```
[user@parrot-virtual]~$ sudo nmap -sF 192.168.43.222
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 10:47 BST
Nmap scan report for 192.168.43.222
Host is up (0.00017s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
80/tcp    open|filtered http
8080/tcp  open|filtered http-proxy
MAC Address: 08:00:27:28:0B:85 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
[user@parrot-virtual]~$ sudo nmap -sF 192.168.43.78
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 10:47 BST
Nmap scan report for 192.168.43.78
Host is up (0.00049s latency).
All 1000 scanned ports on 192.168.43.78 are open|filtered
MAC Address: 08:00:27:5E:51:D4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.30 seconds
```


Scan 6: XMAS scan (FIN, PSH, URG Flags)

- **Syntax:** `nmap -sX <target IP or domain>`
 - **Ex:** `nmap -sX example.com`
 - `nmap -sX 192.168.0.137 -v`

```
[user@parrot-virtual]~$ sudo nmap -sX 192.168.43.222
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 10:48 BST
Nmap scan report for 192.168.43.222
Host is up (0.00053s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
80/tcp    open|filtered http
8080/tcp  open|filtered http-proxy
MAC Address: 08:00:27:28:0B:85 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds
[user@parrot-virtual]~$ sudo nmap -sX 192.168.43.78
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 10:48 BST
Nmap scan report for 192.168.43.78
Host is up (0.00038s latency).
All 1000 scanned ports on 192.168.43.78 are open|filtered
MAC Address: 08:00:27:5E:51:D4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.25 seconds
```

Scan 7: NULL scan (No Flags)

- **Syntax:** `nmap -sN <target IP or domain>`
 - **Ex:** `nmap -sN example.com`
 - `nmap -sN 192.168.0.137 -v`

```
[user@parrot-virtual]~$ sudo nmap -sN 192.168.43.78
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 11:08 BST
Nmap scan report for 192.168.43.78
Host is up (0.00033s latency).
All 1000 scanned ports on 192.168.43.78 are open|filtered
MAC Address: 08:00:27:5E:51:D4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.23 seconds
[user@parrot-virtual]~$ sudo nmap -sN 192.168.43.222
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 11:09 BST
Nmap scan report for 192.168.43.222
Host is up (0.00025s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
80/tcp    open|filtered http
8080/tcp  open|filtered http-proxy
MAC Address: 08:00:27:28:0B:85 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds
```

Scan 8: Aggressive scan

- **Syntax:** `nmap -A <target IP of domain>`
 - **Ex:** `nmap -A example.com`
 - `nmap -A 192.168.0.137 -v`
- You can add `-v` at the end of any command to see the verbose (in detailed) information

```
[user@parrot-virtual]~$ sudo nmap -A 192.168.43.222
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 11:41 BST
Nmap scan report for 192.168.43.222
Host is up (0.00082s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 1024 94:d2:06:69:a7:f4:4e:be:6b:16:29:2c:73:0a:f0:11 (DSA)
|_ 2048 1e:57:bb:51:fe:bd:e5:00:b8:14:96:8d:e3:4e:a4:20 (RSA)
|_ 256 d5:7d:37:b2:3d:87:1c:ac:fb:f0:a6:e2:c2:e1:c8:d4 (ECDSA)
|_ 256 af:f8:0e:fe:49:07:f5:4c:91:f5:53:f3:73:63:a8:9b (ED25519)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: VulnMachine
8080/tcp   open  http     nginx 1.4.6 (Ubuntu)
|_ http-favicon: Drupal CMS
|_ http-generator: Drupal 7 (http://drupal.org)
|_ http-robots.txt: 33 disallowed entries (15 shown)
|_ /includes/ /misc/ /modules/ /profiles/ /scripts/
|_ /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
|_ /INSTALL.pgsql.txt /install.php /INSTALL.txt /LICENSE.txt
|_ /MAINTAINERS.txt /update.php
|_ http-server-header: nginx/1.4.6 (Ubuntu)
|_ http-title: Welcome to Drupal | Drupal
MAC Address: 08:00:27:28:0B:85 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.82 ms  192.168.43.222
```

Scan 9: UDP port scan

- **Syntax:** `nmap -sU <target IP or domain>`
 - **Example:** `nmap -sU example.com`
 - `nmap -sU 192.168.0.137`

```
[user@parrot-virtual]~$ sudo nmap -sU 192.168.43.222
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 11:09 BST
Nmap scan report for 192.168.43.222
Host is up (0.00064s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
68/udp    open|filtered dhcpc
MAC Address: 08:00:27:28:0B:85 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1088.12 seconds
```

Scan 10: Custom port scanning

- **Syntax:** `nmap -p <port range> <target IP or domain>`
 - **Ex:** `nmap -p 80 example.com`
 - `nmap 192.168.0.137 -p 80-85`
 - `nmap 49.204.90.43 -p 80,81,85,21,443`

```
[user@parrot-virtual]~$ sudo nmap -p 21,80 192.168.43.222
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 11:10 BST
Nmap scan report for 192.168.43.222
Host is up (0.00048s latency).

PORT      STATE SERVICE
21/tcp    closed ftp
80/tcp    open  http
MAC Address: 08:00:27:28:0B:85 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
[user@parrot-virtual]~$ sudo nmap -p 80 192.168.43.222
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 11:11 BST
Nmap scan report for 192.168.43.222
Host is up (0.00055s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:28:0B:85 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

```
[user@parrot-virtual]~$ sudo nmap -p 21-80 192.168.43.222
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 11:11 BST
Nmap scan report for 192.168.43.222
Host is up (0.00018s latency).
Not shown: 58 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:28:0B:85 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```


Scan 11: Traceroute scan with nmap

- **Syntax:** nmap --traceroute <target IP or domain>
- **Ex:** nmap --traceroute example.com
- nmap --traceroute 192.168.0.137 -v

```
[user@parrot-virtual]~  
$sudo nmap --traceroute hackthissite.org  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 11:13 BST  
Nmap scan report for hackthissite.org (137.74.187.102)  
Host is up (0.093s latency).  
Other addresses for hackthissite.org (not scanned): 2001:41d0:8:ccd8:137:74:187:  
104 2001:41d0:8:ccd8:137:74:187:102 2001:41d0:8:ccd8:137:74:187:101 2001:41d0:8:  
ccd8:137:74:187:103 2001:41d0:8:ccd8:137:74:187:100 137.74.187.100 137.74.187.10  
3 137.74.187.101 137.74.187.104  
Not shown: 997 filtered ports  
PORT      STATE SERVICE  
22/tcp    closed ssh  
80/tcp    open  http  
443/tcp   open  https  
  
TRACEROUTE (using port 80/tcp)  
HOP RTT      ADDRESS  
1   3.85 ms   192.168.43.1  
2   ...  
3   86.10 ms  10.72.171.75  
4   86.13 ms  172.25.124.210  
5   75.93 ms  172.25.124.207  
6   85.83 ms  hackthissite.org (137.74.187.102)  
  
Nmap done: 1 IP address (1 host up) scanned in 17.91 seconds
```