JGi JAIN DEEMED-TO-BE UNIVERSITY | SCHOOL OF COMPUTER SCIENCE AND IT

Department of
Bachelor of Computer Applications

Ethical Hacking Fundamentals

Lab File – CA 08

Subject Code: 19BCA4C02L
Class: IInd Year IInd Semester

Prepared By:
Suman Garai
20BCAR0246

Aim :

Perform NMAP Scan on Metasploitable Web, IP Subnet using Kali Linux and Windows.

Requirements :

- Virtualisation Software
- Kali Linux 2021.4a
- Basics of Nmap
- Internet Connection

Objectives :

To Run different scans :

- ✓ TCP Null Scan
- ✓ UDP Port Scan
- ✓ Nmap Packet Trace

Procedure :

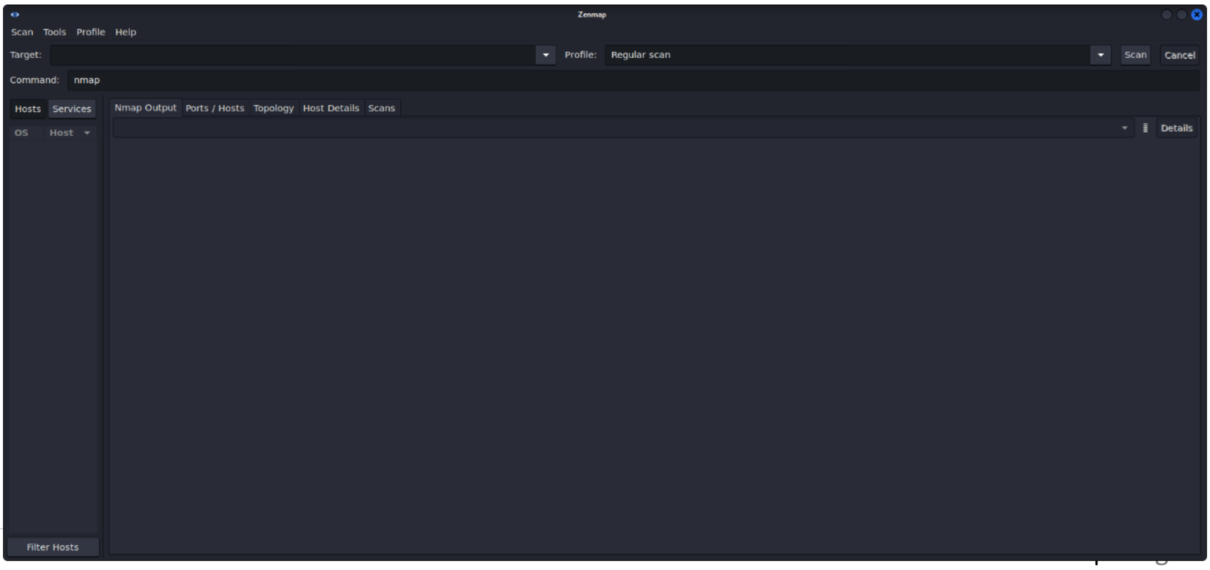
Basics

Zenmap is an Nmap frontend. It is meant to be useful for advanced users and to make Nmap easy to use by beginners. It was originally derived from Umit, an Nmap GUI created as part of the Google Summer of Code. This application runs in a container via kaboxer.

1> Open root terminal in kali linux, and run the command `sudo apt install zenmap-kbx` to install zenmap.

2> Launch the application by searching `zenmap` from Applications button in taskbar or typing `zenmap-kbx` in terminal.

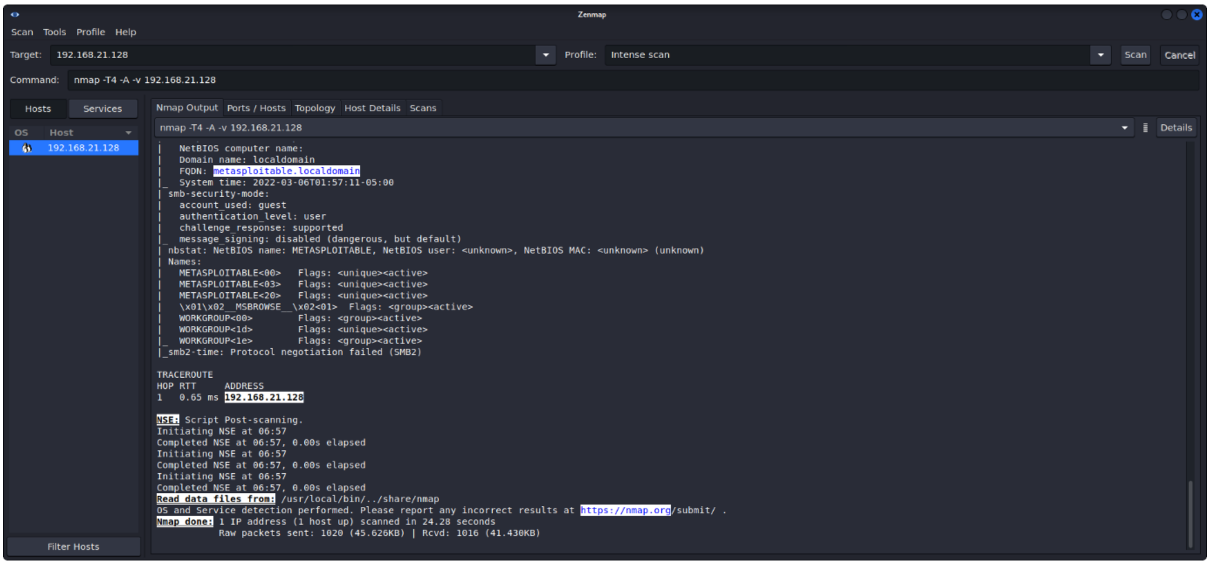
The window appears like this. There are areas where we can input target, command, use defined profiles, see rescan results and start scan button.



Profile: Regular scan

Command: nmap

Intesnse Scan (Demo)



Target: 192.168.21.128

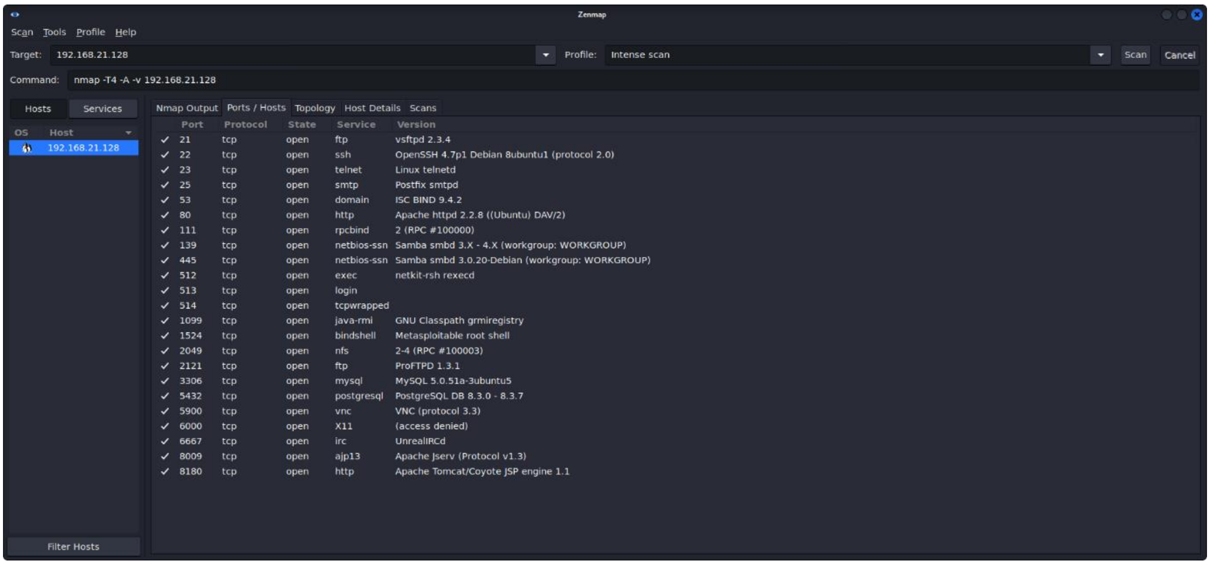
Profile: Intense scan

Command: nmap -T4 -A -v 192.168.21.128

```
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-03-06T01:57:11-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   0.65 ms 192.168.21.128

NSE: Script Post-scanning.
Initiating NSE at 06:57
Completed NSE at 06:57, 0.00s elapsed
Initiating NSE at 06:57
Completed NSE at 06:57, 0.00s elapsed
Initiating NSE at 06:57
Completed NSE at 06:57, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.28 seconds
           Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)
```

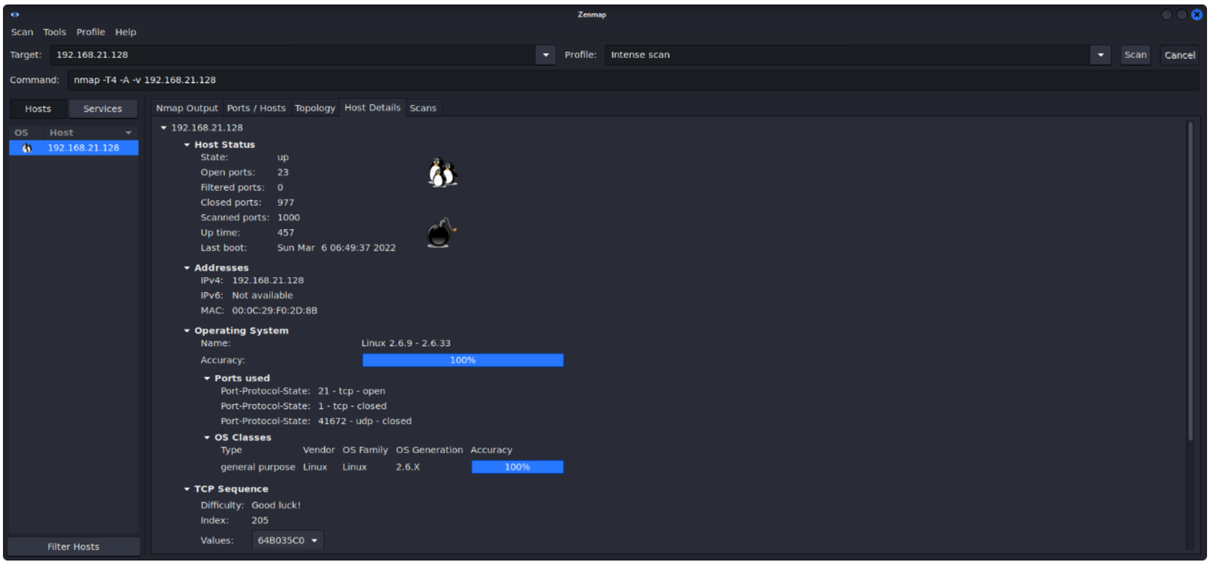


Target: 192.168.21.128

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.21.128

	Port	Protocol	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 3.0.20-Debian (workgroup: WORKGROUP)
✓	512	tcp	open	exec	netkit-rsh rexecd
✓	513	tcp	open	login	
✓	514	tcp	open	tcpwrapped	
✓	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



Target: 192.168.21.128

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.21.128

192.168.21.128

Host Status

State: up
Open ports: 23
Filtered ports: 0
Closed ports: 977
Scanned ports: 1000
Up time: 457
Last boot: Sun Mar 6 06:49:37 2022

Addresses

IPv4: 192.168.21.128
IPv6: Not available
MAC: 00:0C:29:F0:2D:8B

Operating System

Name: Linux 2.6.9 - 2.6.33
Accuracy: 100%

Ports used

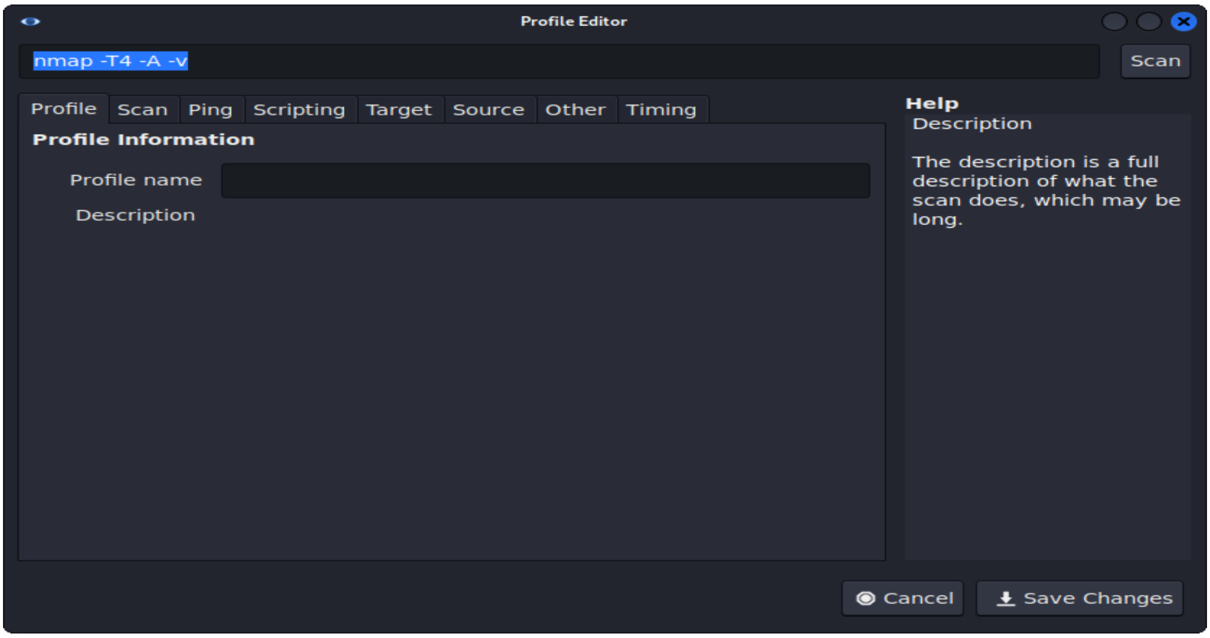
Port-Protocol-State: 21 - tcp - open
Port-Protocol-State: 1 - tcp - closed
Port-Protocol-State: 41672 - udp - closed

OS Classes

Type	Vendor	OS Family	OS Generation	Accuracy
general purpose	Linux	Linux	2.6.X	100%

TCP Sequence

Difficulty: Good luck!
Index: 205
Values: 64B035C0



```
nmap -T4 -A -v
```

Profile Information

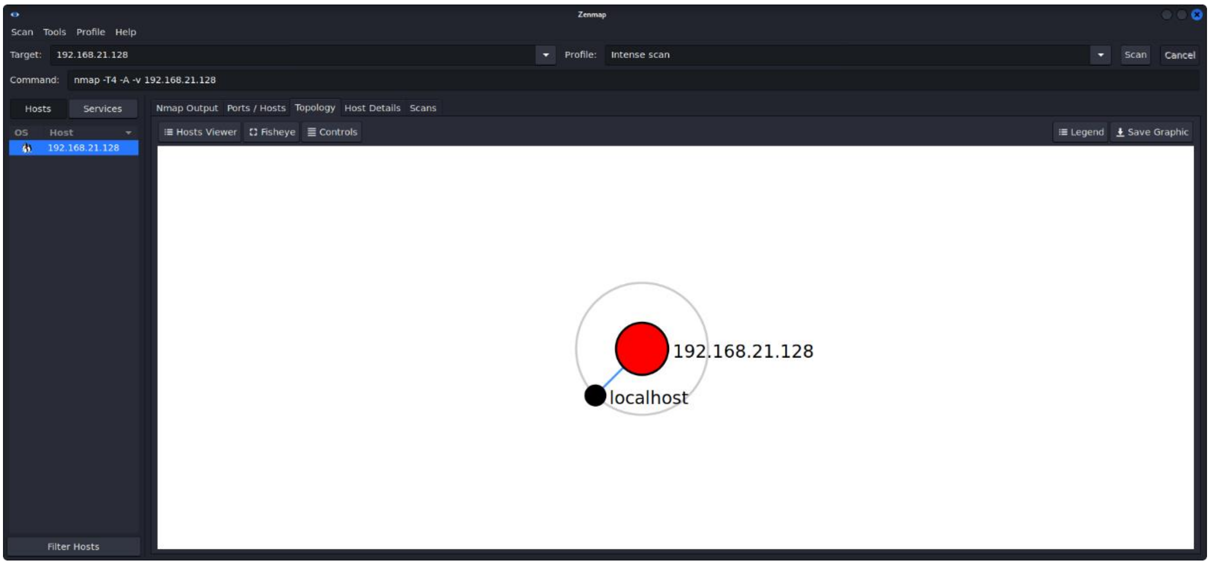
Profile name

Description

Help

Description

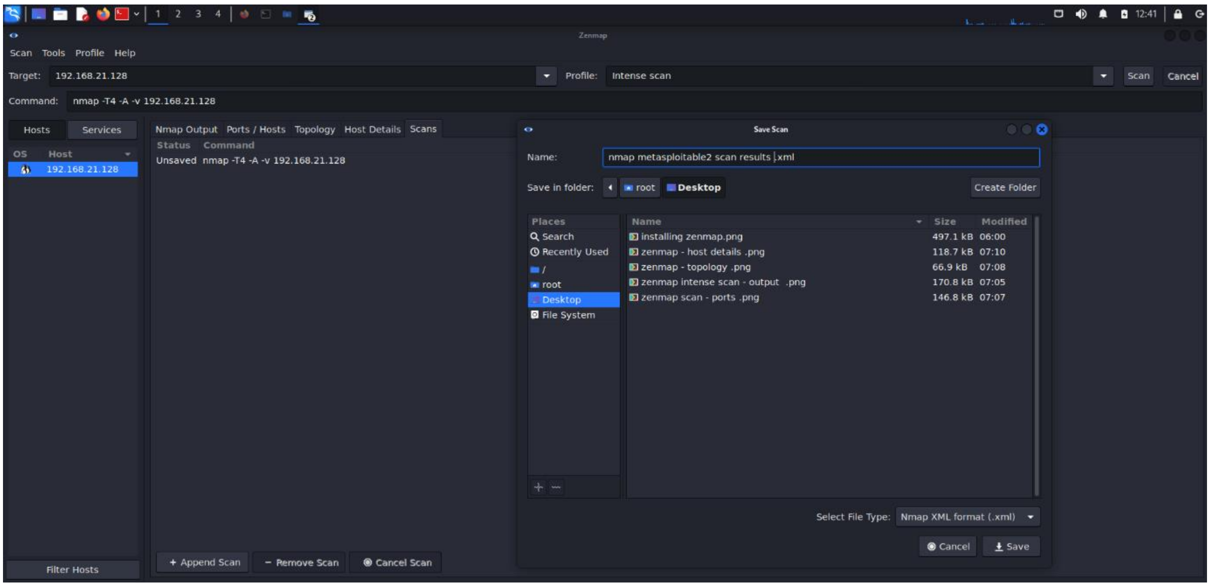
The description is a full description of what the scan does, which may be long.



Target: 192.168.21.128

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.21.128



Target: 192.168.21.128

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.21.128

Status	Command
Unsaved	nmap -T4 -A -v 192.168.21.128

Name: nmap metasploitable2 scan results .xml

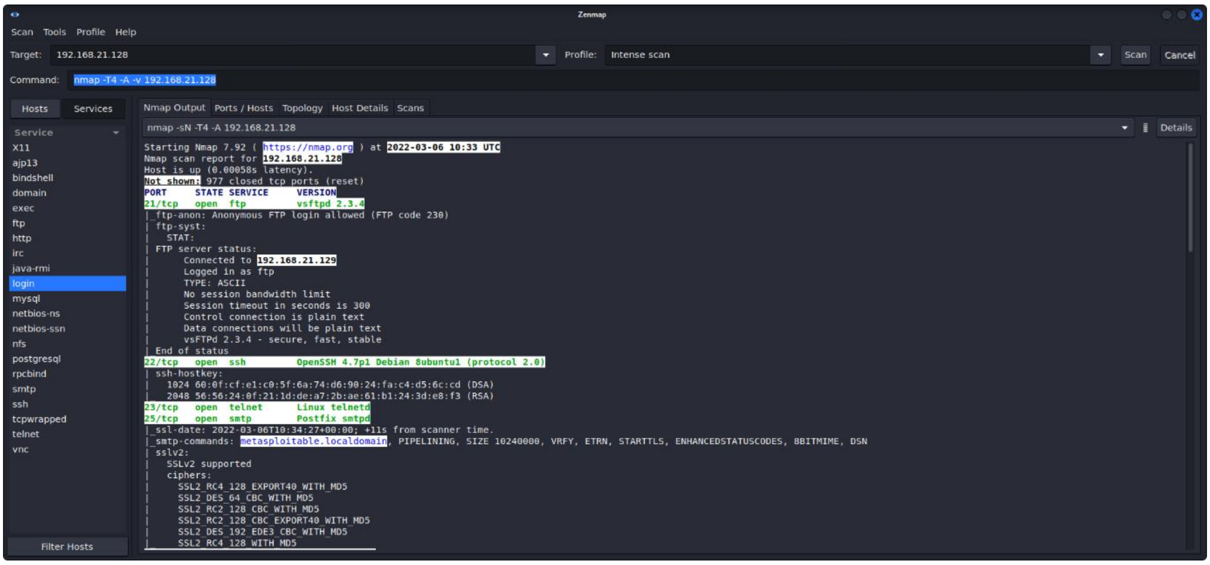
Save in folder: root Desktop

Name	Size	Modified
installing zenmap.png	497.1 kB	06:00
zenmap - host details .png	118.7 kB	07:10
zenmap - topology .png	66.9 kB	07:08
zenmap intense scan - output .png	170.8 kB	07:05
zenmap scan - ports .png	146.8 kB	07:07

Select File Type: Nmap XML format (.xml)

TCP Null Scan

Command: `nmap -sN -T4 -A <IP Address>`



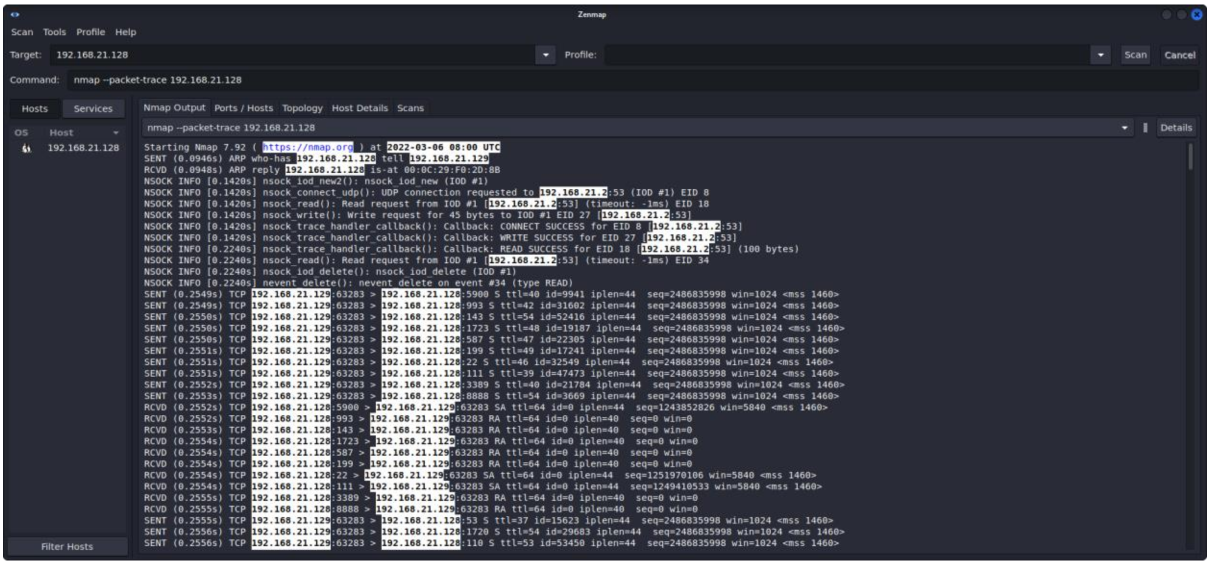
Target: 192.168.21.128
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.21.128

```
nmap -sN -T4 -A 192.168.21.128
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-06 10:33 UTC
Nmap scan report for 192.168.21.128
Host is up (0.00058s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.21.129
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2022-03-06T10:34:27+00:00; +11s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
```

NOTE: For more details regarding the information obtained, head over to: https://drive.google.com/file/d/1bV7ZlBRHPZdZwuZX4ZWswkkAmZ-utE5y/view?usp=sharing

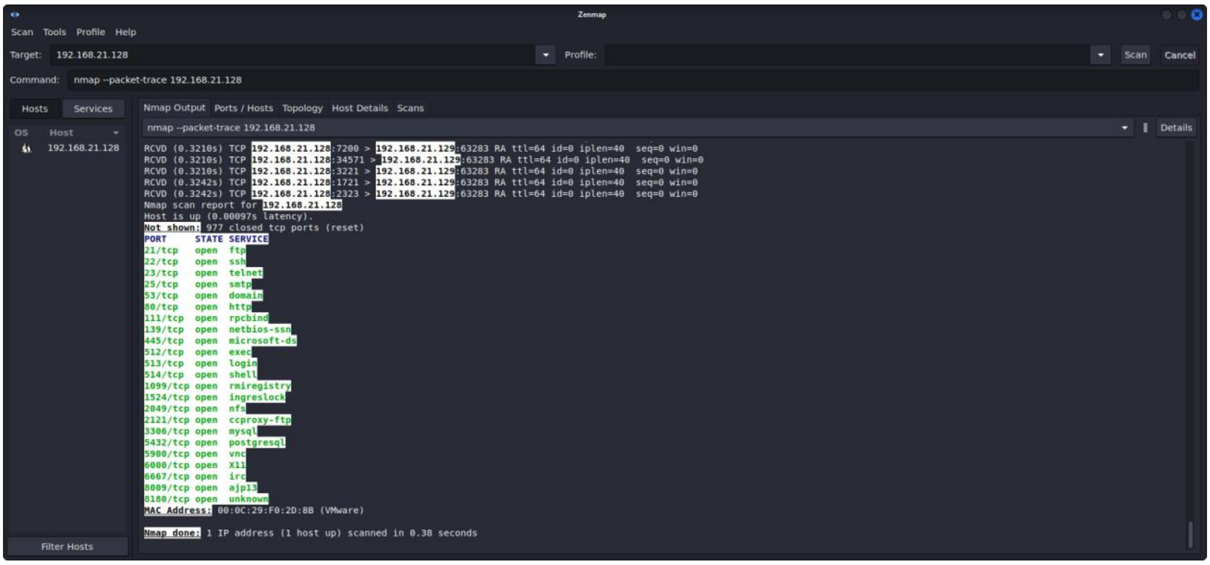
Packet Trace Scan

Command: `nmap --packet-trace <IP Address>`



Target: 192.168.21.128
Profile:
Command: nmap --packet-trace 192.168.21.128

```
nmap --packet-trace 192.168.21.128
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-06 08:00 UTC
SENT (0.0946s) ARP who-has 192.168.21.128 tell 192.168.21.129
RCVD (0.0948s) ARP reply 192.168.21.128 is-at 00:0C:29:F0:2D:8B
NSOCK INFO [0.1420s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.1420s] nsock_connect_udp(): UDP connection requested to 192.168.21.2:53 (IOD #1) EID 8
NSOCK INFO [0.1420s] nsock_read(): Read request from IOD #1 [192.168.21.2:53] (timeout: -1ms) EID 18
NSOCK INFO [0.1420s] nsock_write(): Write request for 45 bytes to IOD #1 EID 27 [192.168.21.2:53]
NSOCK INFO [0.1420s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.21.2:53]
NSOCK INFO [0.1420s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [192.168.21.2:53]
NSOCK INFO [0.2240s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [192.168.21.2:53] (100 bytes)
NSOCK INFO [0.2240s] nsock_read(): Read request from IOD #1 [192.168.21.2:53] (timeout: -1ms) EID 34
NSOCK INFO [0.2240s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.2240s] nevent_delete(): nevent_delete on event #34 (type READ)
SENT (0.2549s) TCP 192.168.21.129:63283 > 192.168.21.128:5900 S ttl=40 id=9941 iplen=44  seq=2486835998 win=1024 <mss 1460>
SENT (0.2549s) TCP 192.168.21.129:63283 > 192.168.21.128:993 S ttl=42 id=31602 iplen=44  seq=2486835998 win=1024 <mss 1460>
SENT (0.2550s) TCP 192.168.21.129:63283 > 192.168.21.128:143 S ttl=54 id=52416 iplen=44  seq=2486835998 win=1024 <mss 1460>
SENT (0.2550s) TCP 192.168.21.129:63283 > 192.168.21.128:1723 S ttl=48 id=19187 iplen=44  seq=2486835998 win=1024 <mss 1460>
SENT (0.2550s) TCP 192.168.21.129:63283 > 192.168.21.128:587 S ttl=47 id=22305 iplen=44  seq=2486835998 win=1024 <mss 1460>
SENT (0.2551s) TCP 192.168.21.129:63283 > 192.168.21.128:199 S ttl=49 id=17241 iplen=44  seq=2486835998 win=1024 <mss 1460>
SENT (0.2551s) TCP 192.168.21.129:63283 > 192.168.21.128:22 S ttl=46 id=32549 iplen=44  seq=2486835998 win=1024 <mss 1460>
SENT (0.2551s) TCP 192.168.21.129:63283 > 192.168.21.128:111 S ttl=39 id=47473 iplen=44  seq=2486835998 win=1024 <mss 1460>
SENT (0.2552s) TCP 192.168.21.129:63283 > 192.168.21.128:3389 S ttl=40 id=21784 iplen=44  seq=2486835998 win=1024 <mss 1460>
SENT (0.2553s) TCP 192.168.21.129:63283 > 192.168.21.128:8888 S ttl=54 id=3669 iplen=44  seq=2486835998 win=1024 <mss 1460>
RCVD (0.2552s) TCP 192.168.21.128:5900 > 192.168.21.129:63283 SA ttl=64 id=0 iplen=44  seq=1243852826 win=5840 <mss 1460>
RCVD (0.2552s) TCP 192.168.21.128:993 > 192.168.21.129:63283 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.2553s) TCP 192.168.21.128:143 > 192.168.21.129:63283 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.2554s) TCP 192.168.21.128:1723 > 192.168.21.129:63283 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.2554s) TCP 192.168.21.128:587 > 192.168.21.129:63283 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.2554s) TCP 192.168.21.128:199 > 192.168.21.129:63283 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.2554s) TCP 192.168.21.128:22 > 192.168.21.129:63283 SA ttl=64 id=0 iplen=44  seq=1251970106 win=5840 <mss 1460>
RCVD (0.2554s) TCP 192.168.21.128:111 > 192.168.21.129:63283 SA ttl=64 id=0 iplen=44  seq=1249410533 win=5840 <mss 1460>
RCVD (0.2555s) TCP 192.168.21.128:3389 > 192.168.21.129:63283 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.2555s) TCP 192.168.21.128:8888 > 192.168.21.129:63283 RA ttl=64 id=0 iplen=40  seq=0 win=0
SENT (0.2555s) TCP 192.168.21.129:63283 > 192.168.21.128:53 S ttl=37 id=15623 iplen=44  seq=2486835998 win=1024 <mss 1460>
SENT (0.2556s) TCP 192.168.21.129:63283 > 192.168.21.128:1720 S ttl=54 id=29683 iplen=44  seq=2486835998 win=1024 <mss 1460>
SENT (0.2556s) TCP 192.168.21.129:63283 > 192.168.21.128:110 S ttl=53 id=53450 iplen=44  seq=2486835998 win=1024 <mss 1460>
```



Target: 192.168.21.128
Profile:
Command: nmap --packet-trace 192.168.21.128

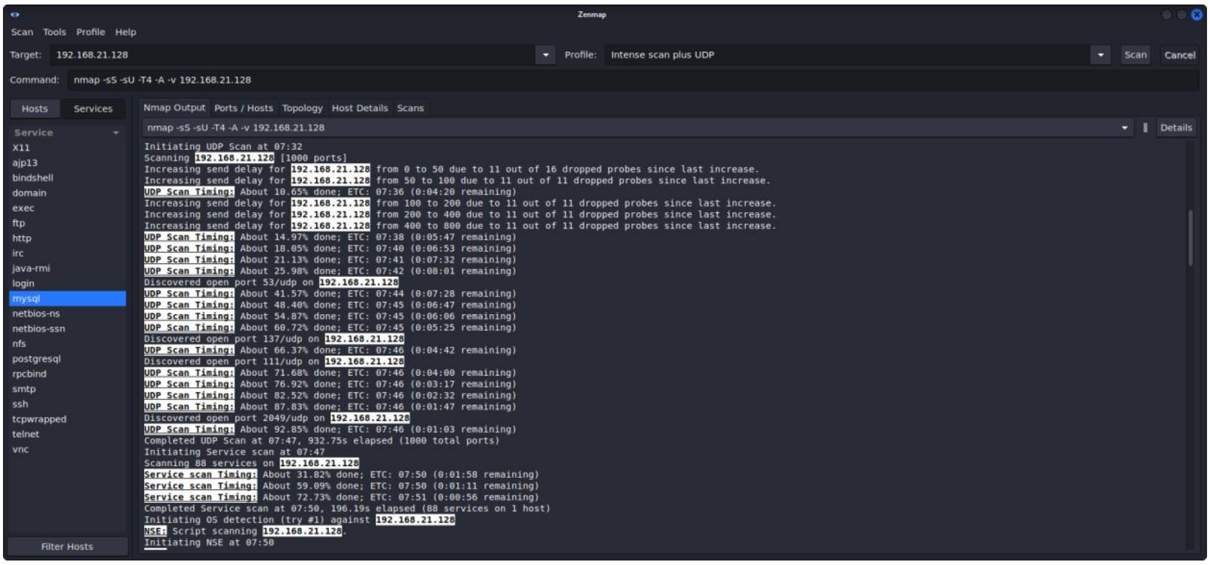
Host: 192.168.21.128

```
nmap --packet-trace 192.168.21.128
RCVD (0.3210s) TCP 192.168.21.128:7200 > 192.168.21.129:63283 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.3210s) TCP 192.168.21.128:34571 > 192.168.21.129:63283 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.3210s) TCP 192.168.21.128:3221 > 192.168.21.129:63283 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.3242s) TCP 192.168.21.128:1721 > 192.168.21.129:63283 RA ttl=64 id=0 iplen=40  seq=0 win=0
RCVD (0.3242s) TCP 192.168.21.128:2323 > 192.168.21.129:63283 RA ttl=64 id=0 iplen=40  seq=0 win=0
Nmap scan report for 192.168.21.128
Host is up (0.00097s latency).
Not shown: 977 closed tcp ports (reset)
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: 00:0C:29:F0:2D:8B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

UDP (Intense) Scan

Command: `nmap -sS -SU -T4 -A -v <IP Address>`



Target: 192.168.21.128
Profile: Intense scan plus UDP
Command: nmap -sS -sU -T4 -A -v 192.168.21.128

X11
ajp13
bindshell
domain
exec
ftp
http
irc
java-rmi
login
mysql
netbios-ns
netbios-ssn
nfs
postgresql
rpcbind
smtp
ssh
tcpwrapped
telnet
vnc

```
nmap -sS -sU -T4 -A -v 192.168.21.128
Initiating UDP Scan at 07:32
Scanning 192.168.21.128 [1000 ports]
Increasing send delay for 192.168.21.128 from 0 to 50 due to 11 out of 16 dropped probes since last increase.
Increasing send delay for 192.168.21.128 from 50 to 100 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 10.65% done; ETC: 07:36 (0:04:20 remaining)
Increasing send delay for 192.168.21.128 from 100 to 200 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 192.168.21.128 from 200 to 400 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 192.168.21.128 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 14.97% done; ETC: 07:38 (0:05:47 remaining)
UDP Scan Timing: About 18.05% done; ETC: 07:40 (0:06:53 remaining)
UDP Scan Timing: About 21.13% done; ETC: 07:41 (0:07:32 remaining)
UDP Scan Timing: About 25.98% done; ETC: 07:42 (0:08:01 remaining)
Discovered open port 53/udp on 192.168.21.128
UDP Scan Timing: About 41.57% done; ETC: 07:44 (0:07:28 remaining)
UDP Scan Timing: About 48.40% done; ETC: 07:45 (0:06:47 remaining)
UDP Scan Timing: About 54.87% done; ETC: 07:45 (0:06:06 remaining)
UDP Scan Timing: About 60.72% done; ETC: 07:45 (0:05:25 remaining)
Discovered open port 137/udp on 192.168.21.128
UDP Scan Timing: About 66.37% done; ETC: 07:46 (0:04:42 remaining)
Discovered open port 111/udp on 192.168.21.128
UDP Scan Timing: About 71.68% done; ETC: 07:46 (0:04:00 remaining)
UDP Scan Timing: About 76.92% done; ETC: 07:46 (0:03:17 remaining)
UDP Scan Timing: About 82.52% done; ETC: 07:46 (0:02:32 remaining)
UDP Scan Timing: About 87.83% done; ETC: 07:46 (0:01:47 remaining)
Discovered open port 2049/udp on 192.168.21.128
UDP Scan Timing: About 92.85% done; ETC: 07:46 (0:01:03 remaining)
Completed UDP Scan at 07:47, 932.75s elapsed (1000 total ports)
Initiating Service scan at 07:47
Scanning 88 services on 192.168.21.128
Service scan Timing: About 31.82% done; ETC: 07:50 (0:01:58 remaining)
Service scan Timing: About 59.09% done; ETC: 07:50 (0:01:11 remaining)
Service scan Timing: About 72.73% done; ETC: 07:51 (0:00:56 remaining)
Completed Service scan at 07:50, 196.19s elapsed (88 services on 1 host)
Initiating OS detection (try #1) against 192.168.21.128
NSE: Script scanning 192.168.21.128.
Initiating NSE at 07:50
```

NOTE: For more details regarding the information obtained, head over to: https://drive.google.com/file/d/1TtKczVb-4qil9Tn6F6oZcmnPoc1FtKXv/view?usp=sharing

Conclusion :

Nmap is a network scanner tool available both in CLI and GUI interfaces. Nmap is used to discover hosts and services on a computer network by sending packets and analysing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection. Tools used in this practical are Metasploitable and Linux CLI nmap. NMAP is used for identifying the available ports on the target machine. Further, using the available ports, we can exploit the available ports by identifying their exploits.