JGi JAIN DEEMED-TO-BE UNIVERSITY

SCHOOL OF COMPUTER SCIENCE AND IT

Department of

Bachelor of Computer Applications

Ethical Hacking Fundamentals

Lab File – CA 09

Subject Code: 19BCA4C02L

Class: IInd Year IInd Semester

Prepared By:

Suman Garai

20BCAR0246

Aim :

Practical to perform enumerating services on user network using Nmap [Any 5 scan].

Requirements :

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

Objectives :

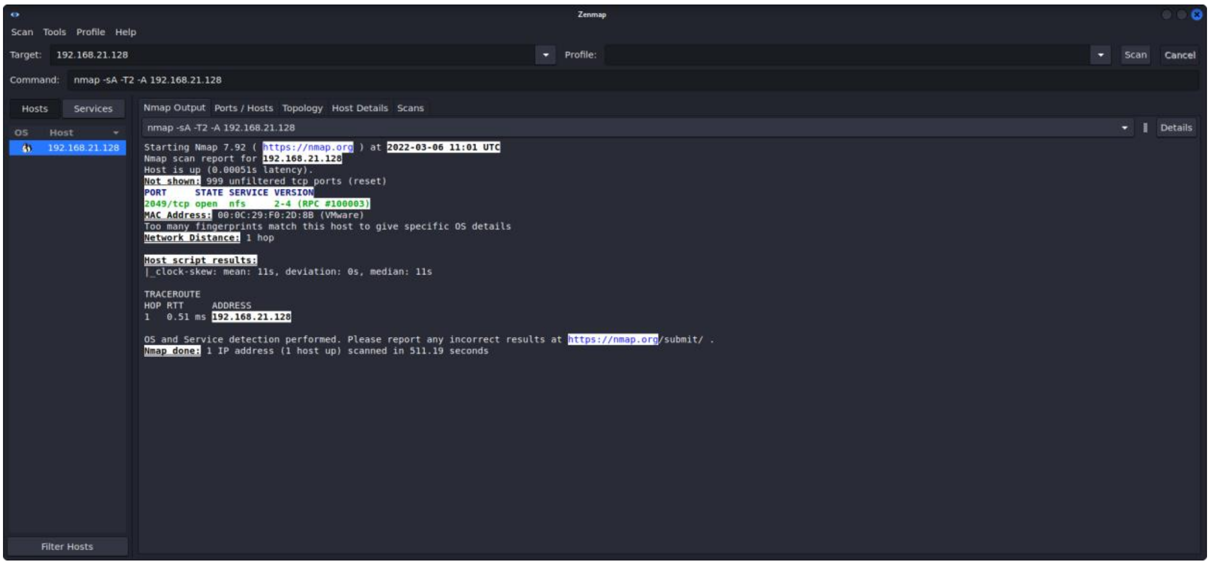
To Run different scans :

- ✓ TCP ACK Port Scan
- ✓ TCP Connect Scan
- ✓ TCP Maimon Scan
- ✓ Version Detection Scan
- ✓ Fin Scan

Procedure :

TCP ACK Port Scan

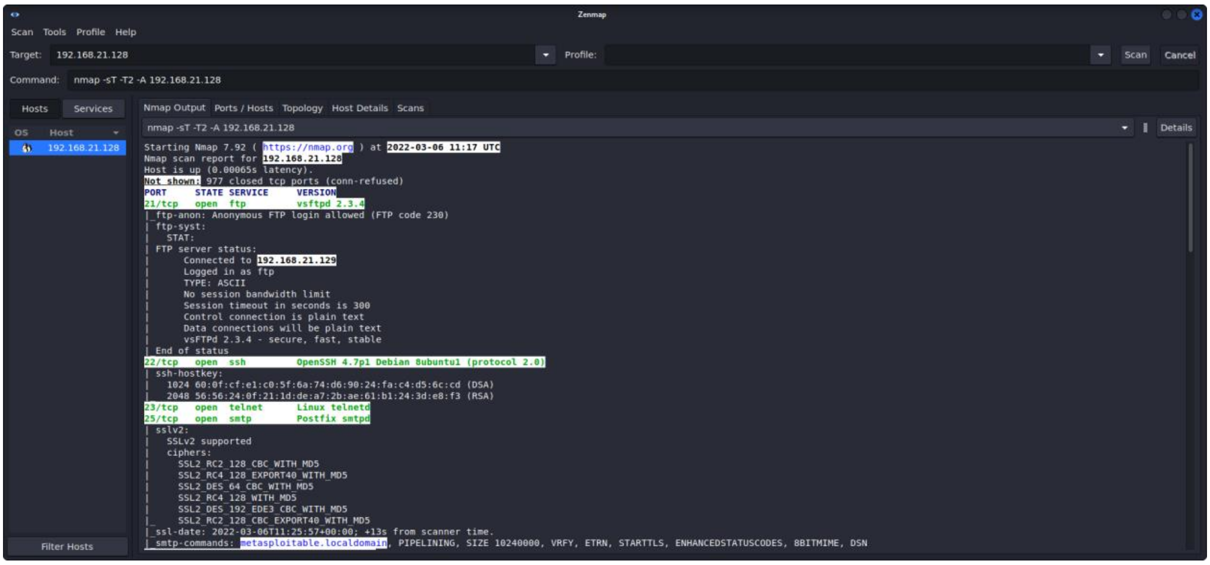
Command: `nmap -sA -T2 -A <IP Address>`


Zenmap
Scan Tools Profile Help
Target: 192.168.21.128
Profile:
Scan
Cancel
Command: nmap -sA -T2 -A 192.168.21.128
Hosts
Services
OS Host
192.168.21.128
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sA -T2 -A 192.168.21.128
Details
Filter Hosts

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-06 11:01 UTC
Nmap scan report for 192.168.21.128
Host is up (0.00051s latency).
Not shown: 999 unfiltered tcp ports (reset)
PORT     STATE SERVICE VERSION
2049/tcp open  nfs     2-4 (RPC #100003)
MAC Address: 00:0C:29:F0:2D:8B (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Host script results:
|_clock-skew: mean: 11s, deviation: 0s, median: 11s

TRACEROUTE
HOP RTT     ADDRESS
1   0.51 ms 192.168.21.128

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 511.19 seconds
```

TCP Connect Scan

Command: `nmap -sT -T2 -A <IP Address>`



Target: 192.168.21.128

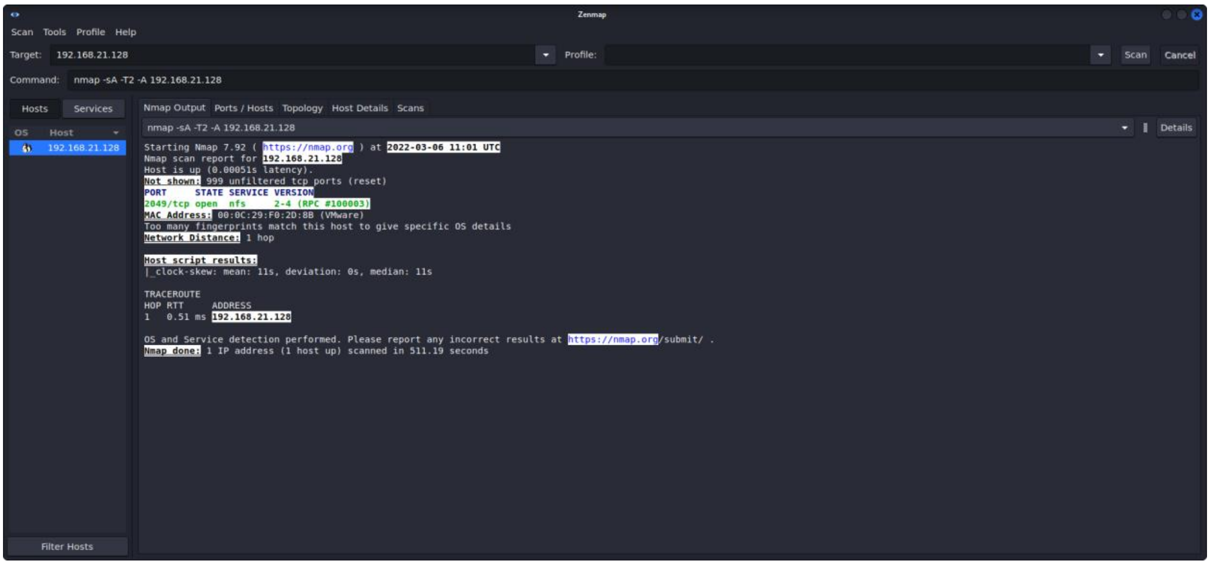
Command: nmap -sT -T2 -A 192.168.21.128

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-06 11:17 UTC
Nmap scan report for 192.168.21.128
Host is up (0.00065s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ssl-date: 2022-03-06T11:25:57+00:00; +13s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
```

NOTE: For more details regarding the information obtained, head over to: https://drive.google.com/file/d/1mDal9rrzByahercesW7C4yndI8LZS7FD/view?usp=sharing

TCP Maimon Scan

Command: `nmap -sM -T3 -A <IP Address>`



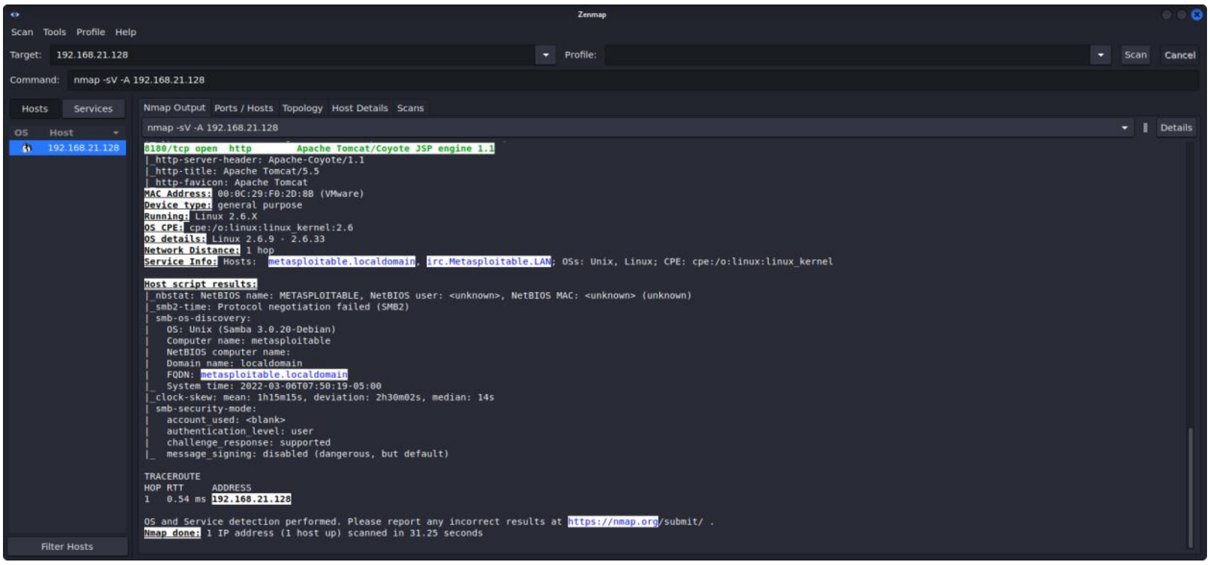
Target: 192.168.21.128

Command: nmap -sA -T2 -A 192.168.21.128

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-06 11:01 UTC
Nmap scan report for 192.168.21.128
Host is up (0.00051s latency).
Not shown: 999 unfiltered tcp ports (reset)
PORT     STATE SERVICE VERSION
2049/tcp open  nfs     2-4 (RPC #100003)
MAC Address: 00:0C:29:F0:2D:8B (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Host script results:
|_clock-skew: mean: 11s, deviation: 0s, median: 11s

TRACEROUTE
HOP RTT     ADDRESS
1   0.51 ms 192.168.21.128

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 511.19 seconds
```

Version Detection Scan

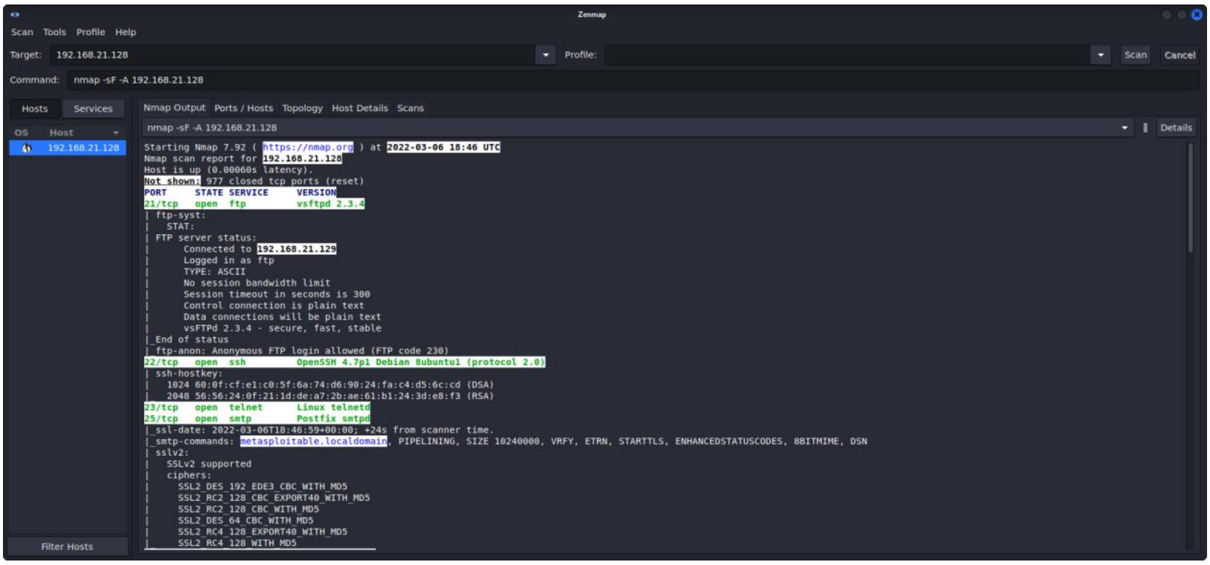
Command: `nmap -sV -A <IP Address>`



```
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
| http-favicon: Apache Tomcat
MAC Address: 00:0C:29:F0:2D:8B (VMware)
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-03-06T07:50:19-05:00
|_clock-skew: mean: 1h15m15s, deviation: 2h30m02s, median: 14s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.54 ms 192.168.21.128

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 31.25 seconds
```

Fin Scan

Command: `nmap -sF -A <IP Address>`



```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-06 18:46 UTC
Nmap scan report for 192.168.21.128
Host is up (0.00060s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| 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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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: 2022-03-06T18:46:59+00:00; +24s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
```

NOTE: For more details regarding the information obtained, head over to: https://drive.google.com/file/d/11yLVgHPBsjzDnhssDW7Iq9l2rxzZMhLT/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.