# MAJOR – SEP


## Name – Anjali Kuamri

## Email – anjalirajwar101@gmail.com

## College Name – BIT Sindri


## Cyber Security Major Project

**1.** Perform Scanning Module by using Nmap tool (Download from Internet) and scan kalilinux and Windows 7 machine and find the open/closed ports and services running on machine

Hacker Machine : Windows 10

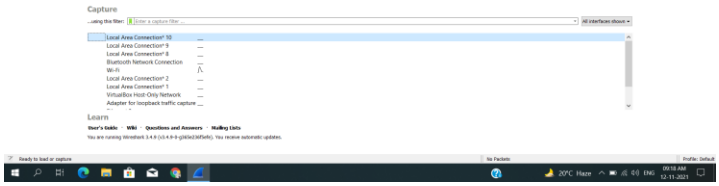
Victim machine : Kali Linux and Windows 7

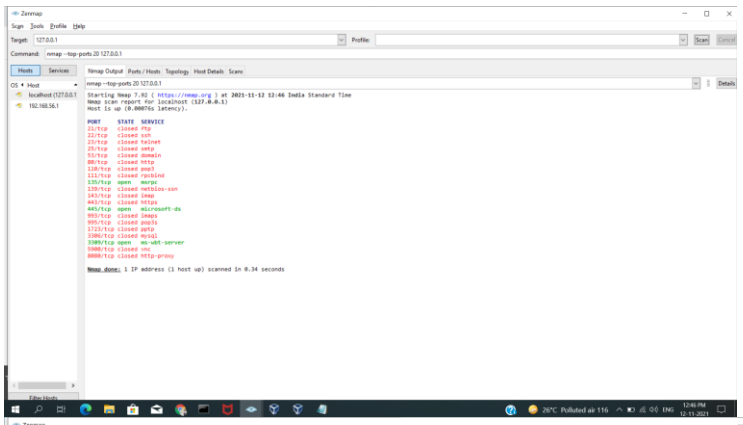
- Nmap can find information about the operating system running on devices. It can provide detailed information like OS versions, making it easier to plan additional approaches during penetration testing.

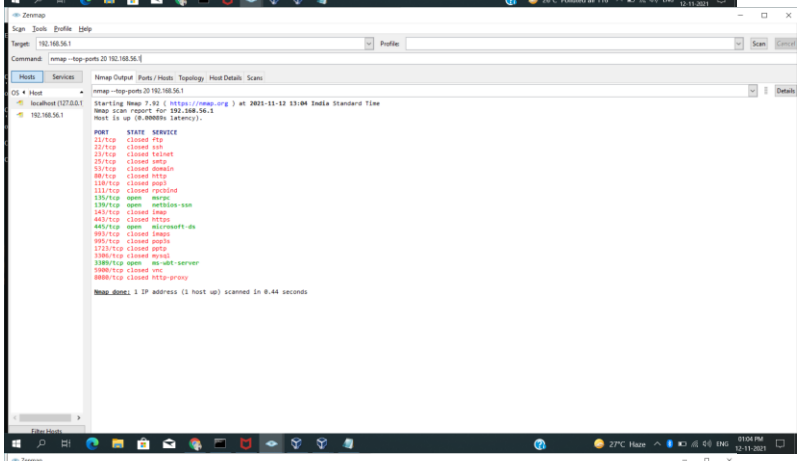
  To run a ping scan -> `nmap -sp 192.100.1.1/24`
  To run a host scan -> `nmap -sp <target IP range>`
  If you see anything unusual in this list, you can then run a DNS query on a specific host, by using -> `namp -sL <IP address>`

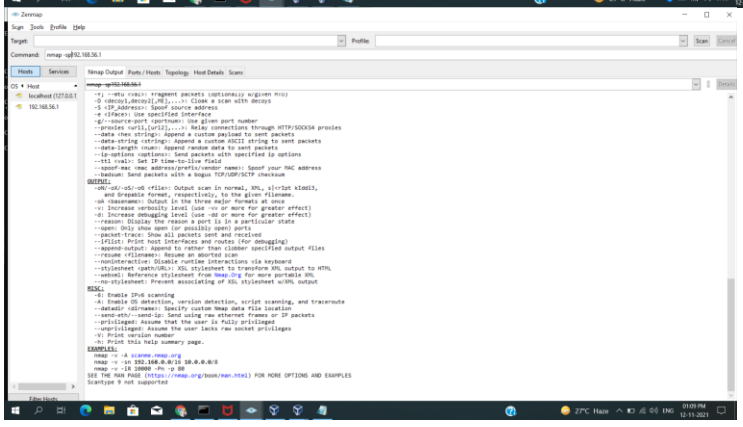
Host Scanning **->** nmap -sp <target IP range>
**OS Scanning** -> nmap –O <target IP>
**Scan The Most Popular Ports** -> nmap --top-ports 20 192.168.1.106
Disable DNS Name Resolution -> **nmap -sp -n 192.100.1.1/24**

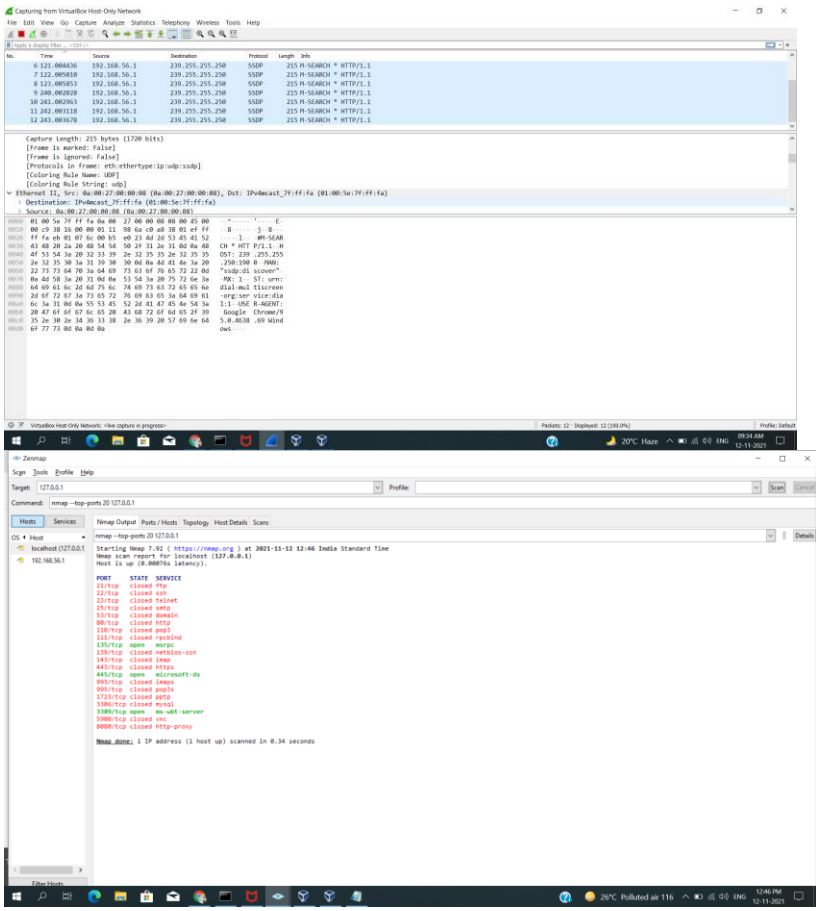

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Welcome to Wireshark
Open
C:\Users\anjal\Downloads\tftp_capture.pcapng (174 KB)

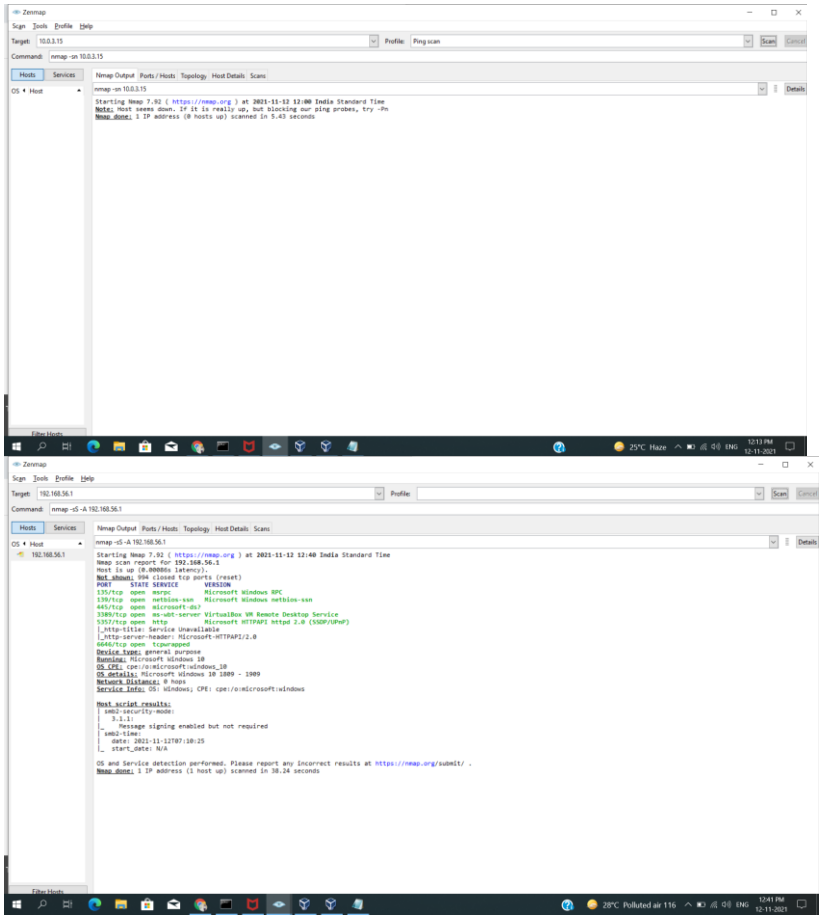

Capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Wi-Fi
Local Area Connection* 2
Local Area Connection* 1
VirtualBox Host-Only Network
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists


Zenmap
Target: 127.0.0.1
Command: nmap --top-ports 20 127.0.0.1
Nmap Output Ports / Hosts Topology Host Details Scans
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-12 12:46 India Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00075s latency).
PORT STATE SERVICE
21/tcp closed ftp
22/tcp closed ssh
23/tcp closed telnet
25/tcp closed smtp
53/tcp closed domain
80/tcp closed http
110/tcp closed pop3
111/tcp closed rpcbind
135/tcp open msrpc
139/tcp closed netbios-ssn
143/tcp closed imap
443/tcp closed https
445/tcp open microsoft-ds
993/tcp closed imaps
995/tcp closed pop3s
1723/tcp closed pptp
3306/tcp closed mysql
3389/tcp open ms-wbt-server
5900/tcp closed vnc
8080/tcp closed http-proxy
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds


Zenmap
Target: 192.168.56.1
Command: nmap --top-ports 20 192.168.56.1
Nmap Output Ports / Hosts Topology Host Details Scans
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-12 13:04 India Standard Time
Nmap scan report for 192.168.56.1
Host is up (0.00089s latency).
PORT STATE SERVICE
21/tcp closed ftp
22/tcp closed ssh
23/tcp closed telnet
25/tcp closed smtp
53/tcp closed domain
80/tcp closed http
110/tcp closed pop3
111/tcp closed rpcbind
135/tcp open msrpc
139/tcp open netbios-ssn
143/tcp closed imap
443/tcp closed https
445/tcp open microsoft-ds
993/tcp closed imaps
995/tcp closed pop3s
1723/tcp closed pptp
3306/tcp closed mysql
3389/tcp open ms-wbt-server
5900/tcp closed vnc
8080/tcp closed http-proxy
Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds


Zenmap
Command: nmap -sp 192.168.56.1
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sp 192.168.56.1
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
-S <IP_Address>: Spoof source address
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
--proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<1pt kIddI3,
and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
Scantype 9 not supported


Capturing from VirtualBox Host-Only Network
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
6 121.004436 192.168.56.1 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
7 122.005010 192.168.56.1 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
8 123.005853 192.168.56.1 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
9 240.002028 192.168.56.1 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
10 241.002963 192.168.56.1 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
11 242.003118 192.168.56.1 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
12 243.003678 192.168.56.1 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
Capture Length: 215 bytes (1720 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:ssdp]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Destination: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Source: 0a:00:27:00:00:00 (0a:00:27:00:00:00)
VirtualBox Host-Only Network: <live capture in progress>
Packets: 12 · Displayed: 12 (100.0%)
Profile: Default
20°C Haze
ENG
09:34 AM
12-11-2021
Zenmap
Scan Tools Profile Help
Target: 127.0.0.1
Profile:
Scan
Cancel
Command: nmap --top-ports 20 127.0.0.1
Hosts Services
OS Host
localhost (127.0.0.1
192.168.56.1
Nmap Output Ports / Hosts Topology Host Details Scans
nmap --top-ports 20 127.0.0.1
Details
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-12 12:46 India Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00076s latency).
PORT STATE SERVICE
21/tcp closed ftp
22/tcp closed ssh
23/tcp closed telnet
25/tcp closed smtp
53/tcp closed domain
80/tcp closed http
110/tcp closed pop3
111/tcp closed rpcbind
135/tcp open msrpc
139/tcp closed netbios-ssn
143/tcp closed imap
443/tcp closed https
445/tcp open microsoft-ds
993/tcp closed imaps
995/tcp closed pop3s
1723/tcp closed pptp
3306/tcp closed mysql
3389/tcp open ms-wbt-server
5900/tcp closed vnc
8080/tcp closed http-proxy
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
26°C Polluted air 116
ENG
12:46 PM
12-11-2021



**Nmap port scan command =** `nmap -p 80 X.X.X.X`

Basic Nmap Scan against IP or host = `nmap 1.1.1.1`

`nmap cloudflare.com`

Nmap Ping Scan = `nmap -sp 192.168.5.0/24`

Scan specific ports or scan entire port ranges on a local or remote server

= `nmap -p 1-65535 localhost`

= `nmap -p 80,443 8.8.8.8`

Scan multiple IP addresses

= `nmap 1.1.1.1 8.8.8.8`

```
= nmap 1.1.1.1,2,3,4
```

Scan IP ranges

= `nmap 8.8.8.0/28`

```
= nmap 8.8.8.1-14
```

```
= nmap 8.8.8.*
```

Scan the most popular ports

= `nmap --top-ports 20 192.168.1.106`

Scan hosts and IP addresses reading from a text file

= `nmap -iL list.txt`

Save your Nmap scan results to a file

= `nmap -oN output.txt securitytrails.com`

```
 = nmap -oX output.xml securitytrails.com
```

Disabling DNS name resolution

=

Scan + OS and service detection with fast execution

= `nmap -A -T4 cloudflare.com`

Detect service/daemon versions

= `nmap -sV localhost`

Scan using TCP or UDP protocols

=

CVE detection using Nmap

= `nmap -Pn --script vuln 192.168.1.105`

Launching DOS with Nmap

```
= nmap 192.168.1.105 -max-parallelism 800 -Pn --script http-slowloris --script-
args http-slowloris.runforever=true
```

## Launching brute force attacks

```
= nmap -sV --script http-wordpress-brute --script-args
'userdb=users.txt,passdb=passwds.txt,http-wordpress-brute.hostname=domain.com,
http-wordpress-brute.threads=3,brute.firstonly=true' 192.168.1.105

= nmap -p 1433 --script ms-sql-brute --script-args
userdb=customuser.txt,passdb=custompass.txt 192.168.1.105

= nmap --script ftp-brute -p 21 192.168.1.105
```

## Detecting malware infections on remote hosts

```
= nmap -sV --script=http-malware-host 192.168.1.105

= nmap -p80 --script http-google-malware infectedsite.com

= 80/tcp open  http

|_http-google-malware.nse: Host is known for distributing malware.
```

# Thank You...