

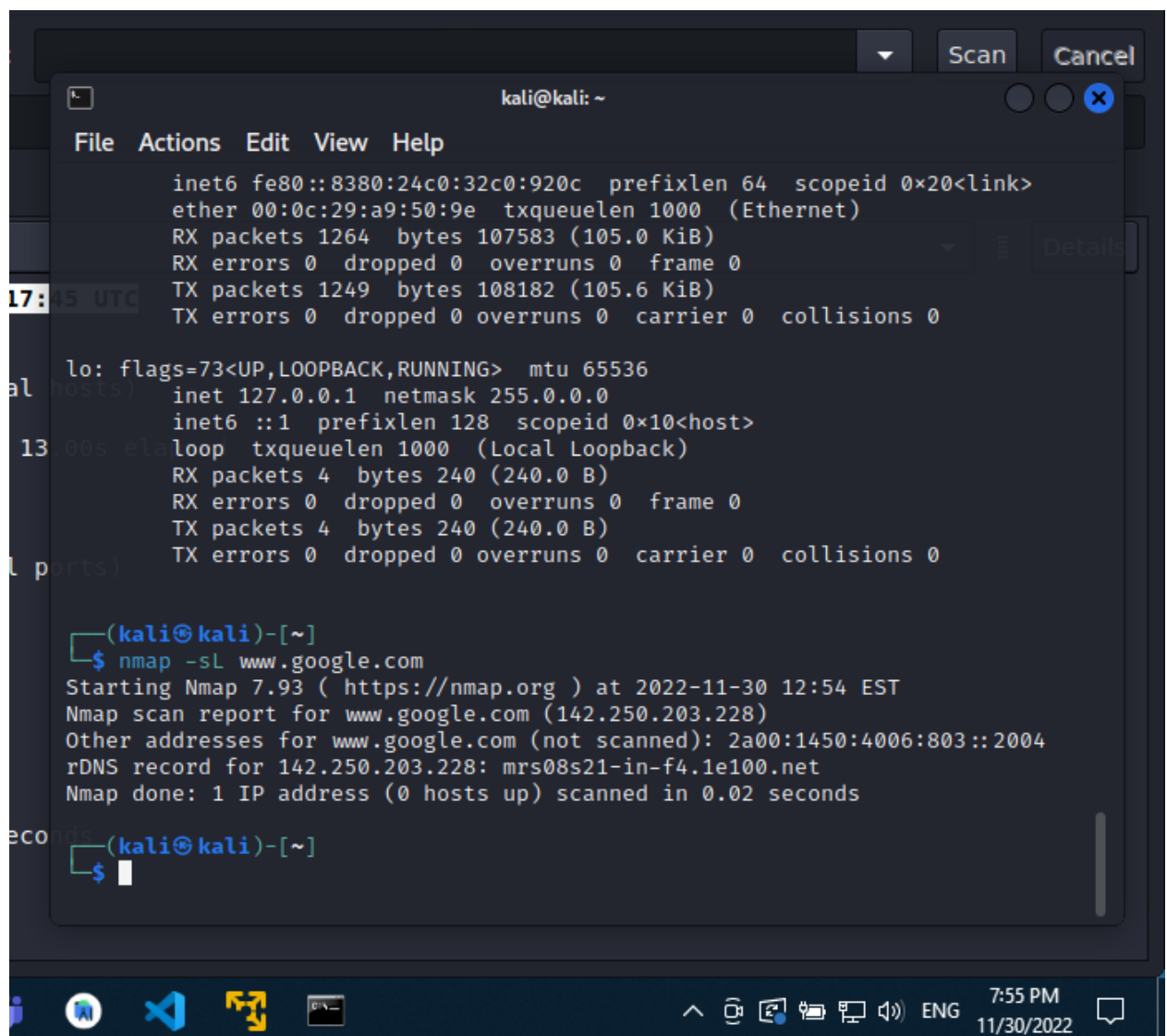
Questions and Discussion:

1. What is Host Discovery?

Host discovery in Nmap is the operation of collecting information about the host in terms of the respective network. It's called "ping scan". Nmap xcan use other functionalities like "ping" or "built-in" script to search for ports, services, and running servers on respective IPs using TCP and UDP.

Some functionalities of Host Discovery in Nmap:

- List Scan: A list scan generally lists the possible host without sending any packets to the targeted host.



```
kali@kali: ~  
File Actions Edit View Help  
    inet6 fe80::8380:24c0:32c0:920c prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:a9:50:9e txqueuelen 1000 (Ethernet)  
    RX packets 1264 bytes 107583 (105.0 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1249 bytes 108182 (105.6 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$ nmap -sL www.google.com  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-30 12:54 EST  
Nmap scan report for www.google.com (142.250.203.228)  
Other addresses for www.google.com (not scanned): 2a00:1450:4006:803::2004  
rDNS record for 142.250.203.228: mrs08s21-in-f4.1e100.net  
Nmap done: 1 IP address (0 hosts up) scanned in 0.02 seconds  
  
(kali@kali)-[~]  
$
```

- Ping Sweep: Ping sweep discovers on the basis the host is powered on.

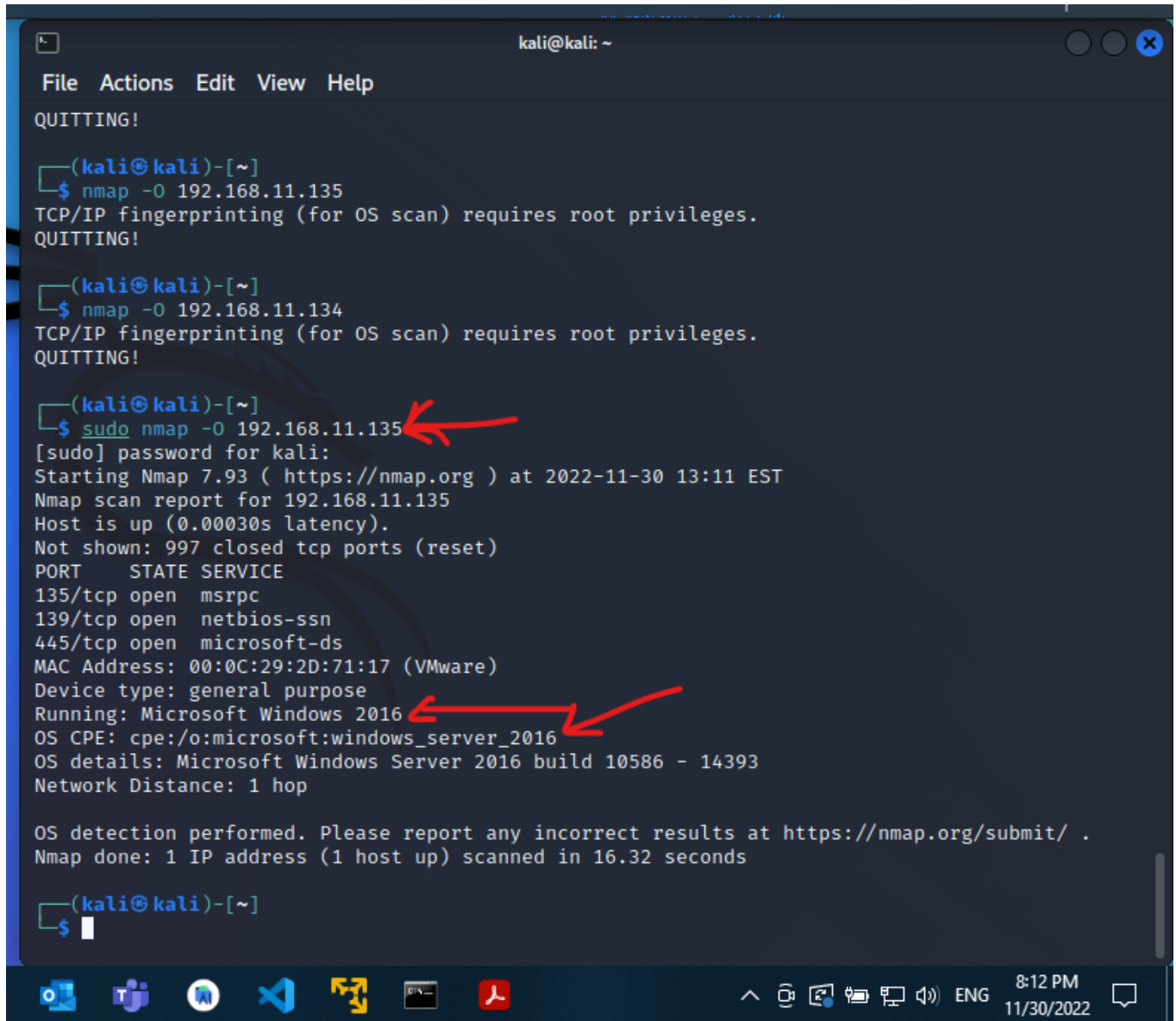
```
(kali㉿kali)-[~]  
$ nmap -sP www.google.com  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-30 12:56 EST  
Nmap scan report for www.google.com (142.250.203.228)  
Host is up (0.041s latency).  
Other addresses for www.google.com (not scanned): 2a00:1450:4006:803::2004  
rDNS record for 142.250.203.228: mrs08s21-in-f4.1e100.net  
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds  
  
CO (kali㉿kali)-[~]  
$
```

- Disable ARP Ping: Nmap mostly uses ARP ping to discover the other host in the network. To disable ARP Ping, use option --disable-arp-ping.

```
(kali㉿kali)-[~]  
$ nmap -sn www.google.com --disable-arp-ping  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-30 12:58 EST  
Nmap scan report for www.google.com (172.217.171.196)  
Host is up (0.044s latency).  
Other addresses for www.google.com (not scanned): 2a00:1450:4006:800::2004  
rDNS record for 172.217.171.196: mrs09s06-in-f4.1e100.net  
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds  
  
O (kali㉿kali)-[~]  
$
```

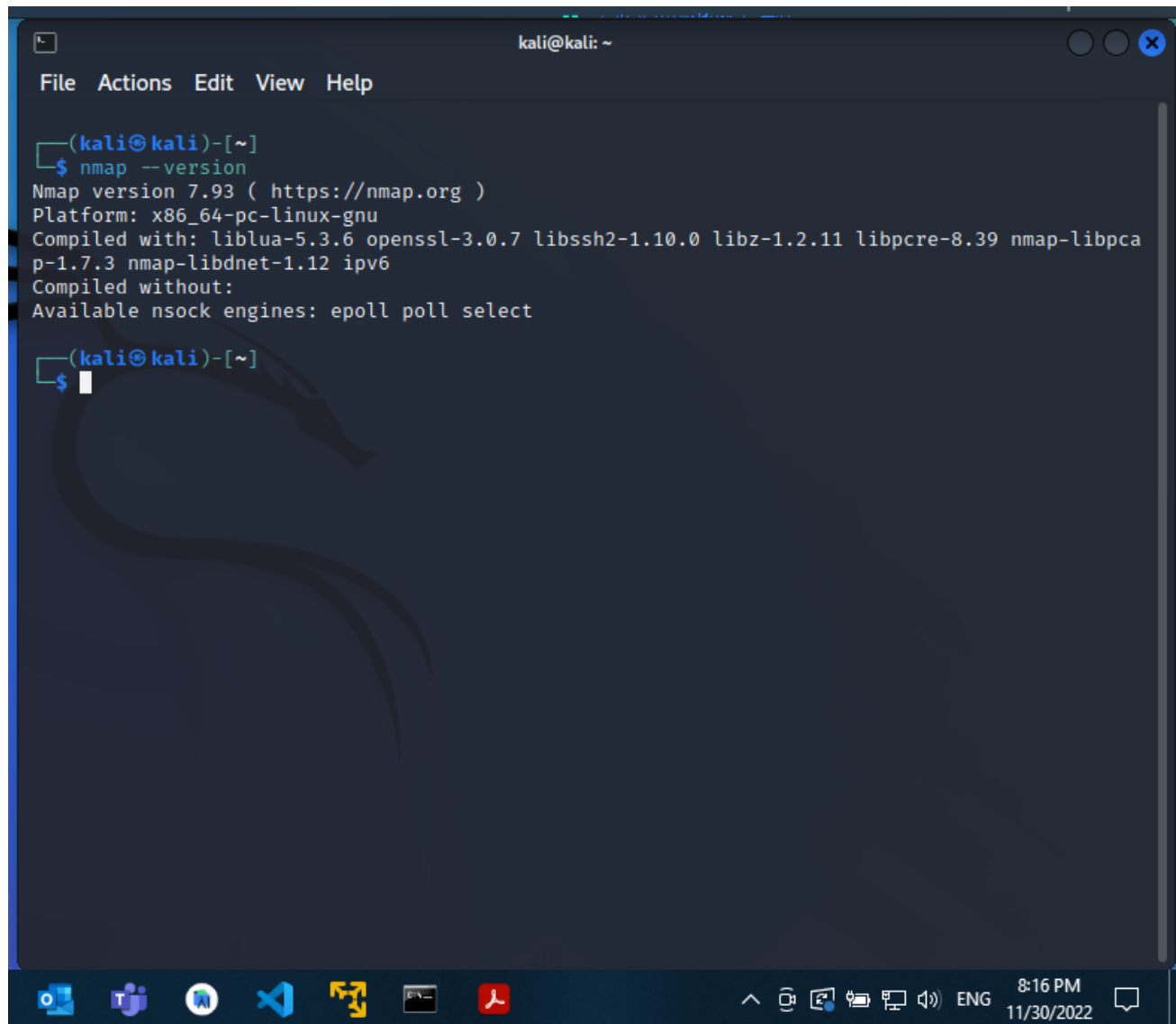
2. How to use nmap to detect remote OS?

Sudo nmap -O 192.168.11.135 (Windows server 2016 IP)



```
kali@kali: ~  
File Actions Edit View Help  
QUITTING!  
  
(kali@kali)-[~]  
$ nmap -O 192.168.11.135  
TCP/IP fingerprinting (for OS scan) requires root privileges.  
QUITTING!  
  
(kali@kali)-[~]  
$ nmap -O 192.168.11.134  
TCP/IP fingerprinting (for OS scan) requires root privileges.  
QUITTING!  
  
(kali@kali)-[~]  
$ sudo nmap -O 192.168.11.135  
[sudo] password for kali:  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-30 13:11 EST  
Nmap scan report for 192.168.11.135  
Host is up (0.00030s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
MAC Address: 00:0C:29:2D:71:17 (VMware)  
Device type: general purpose  
Running: Microsoft Windows 2016  
OS CPE: cpe:/o:microsoft:windows_server_2016  
OS details: Microsoft Windows Server 2016 build 10586 - 14393  
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 16.32 seconds  
  
(kali@kali)-[~]  
$
```

3. How to check whether NMAP already installed or not?

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~'. The menu bar shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal output shows the command 'nmap --version' being executed, followed by the Nmap version 7.93 details, including the platform (x86_64-pc-linux-gnu), compiled libraries (liblua-5.3.6, openssl-3.0.7, libssh2-1.10.0, libz-1.2.11, libpcre-8.39, nmap-libpcap-1.7.3, nmap-libdnet-1.12, ipv6), and available nsock engines (epoll, poll, select). The prompt '(kali@kali)-[~]' is shown twice, indicating the command was entered and the prompt returned.

```
(kali@kali)-[~]  
$ nmap --version  
Nmap version 7.93 ( https://nmap.org )  
Platform: x86_64-pc-linux-gnu  
Compiled with: liblua-5.3.6 openssl-3.0.7 libssh2-1.10.0 libz-1.2.11 libpcre-8.39 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6  
Compiled without:  
Available nsock engines: epoll poll select  
  
(kali@kali)-[~]  
$
```

4. what are the phases of NMAP scanning?

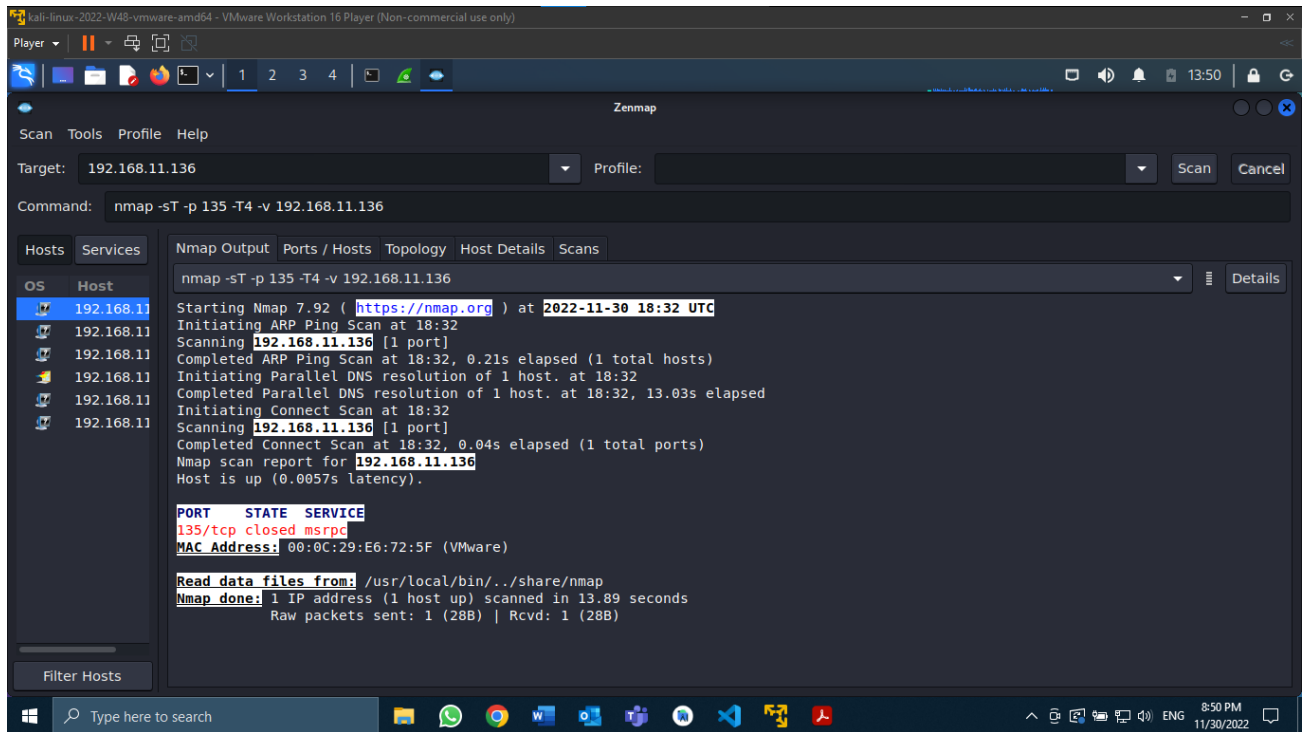
- Script pre-scanning
- Target enumeration
- Host discovery (ping scanning)
- Reverse-DNS resolution
- Port Scanning
- Version Detection

- OS Detection
- Traceroute
- Script Scanning
- Output
- Script post-scanning

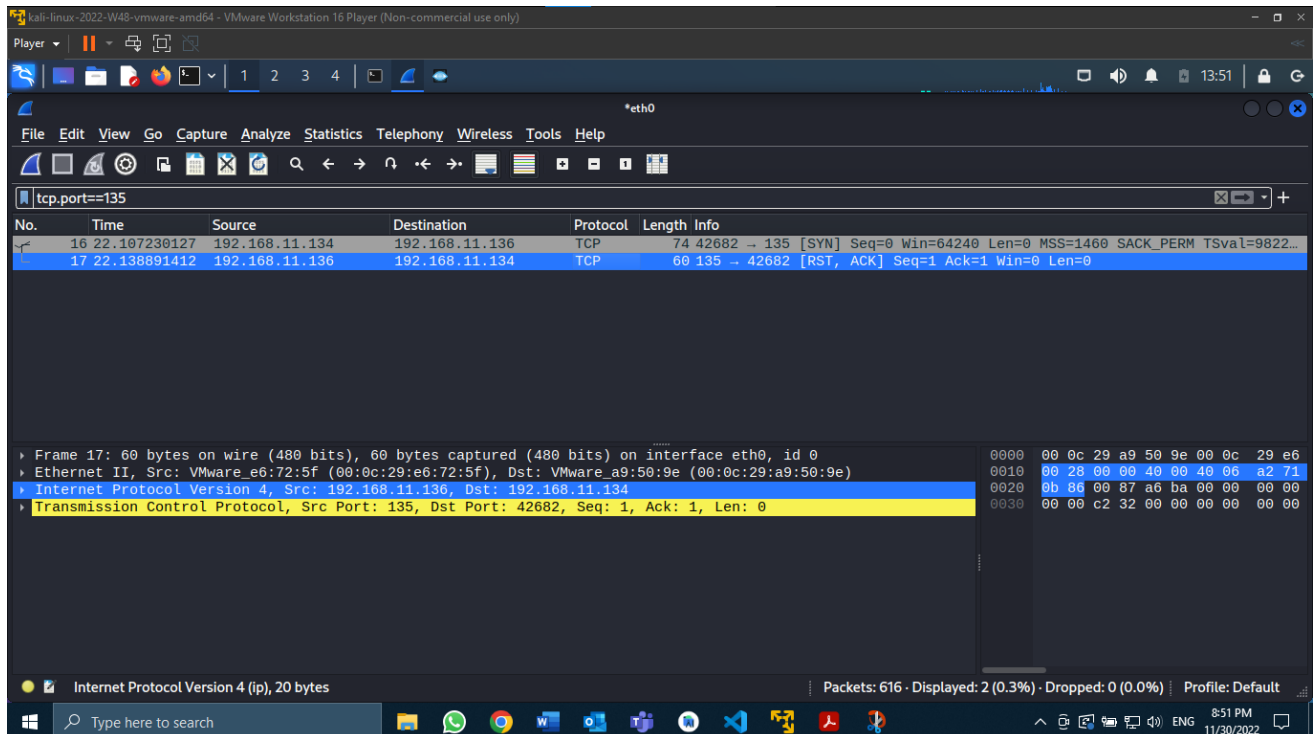
5. Describe the technique behind nmap work principles.

Nmap functions with checking a network for hosts and services. When its found, the software sends this information to the hosts and services and then they respond. Nmap now is going to read and interfere with the response and uses the collected information to make a map for the network. This map has specific information on what each port is doing and who exactly is using it, how are the hosts connecting, which is making it through the firewall, and which is not, and also identifying potential security problems that can be present.

6. TCP scan for the metasploitable Linux machine



Screen shot of the Wireshark program



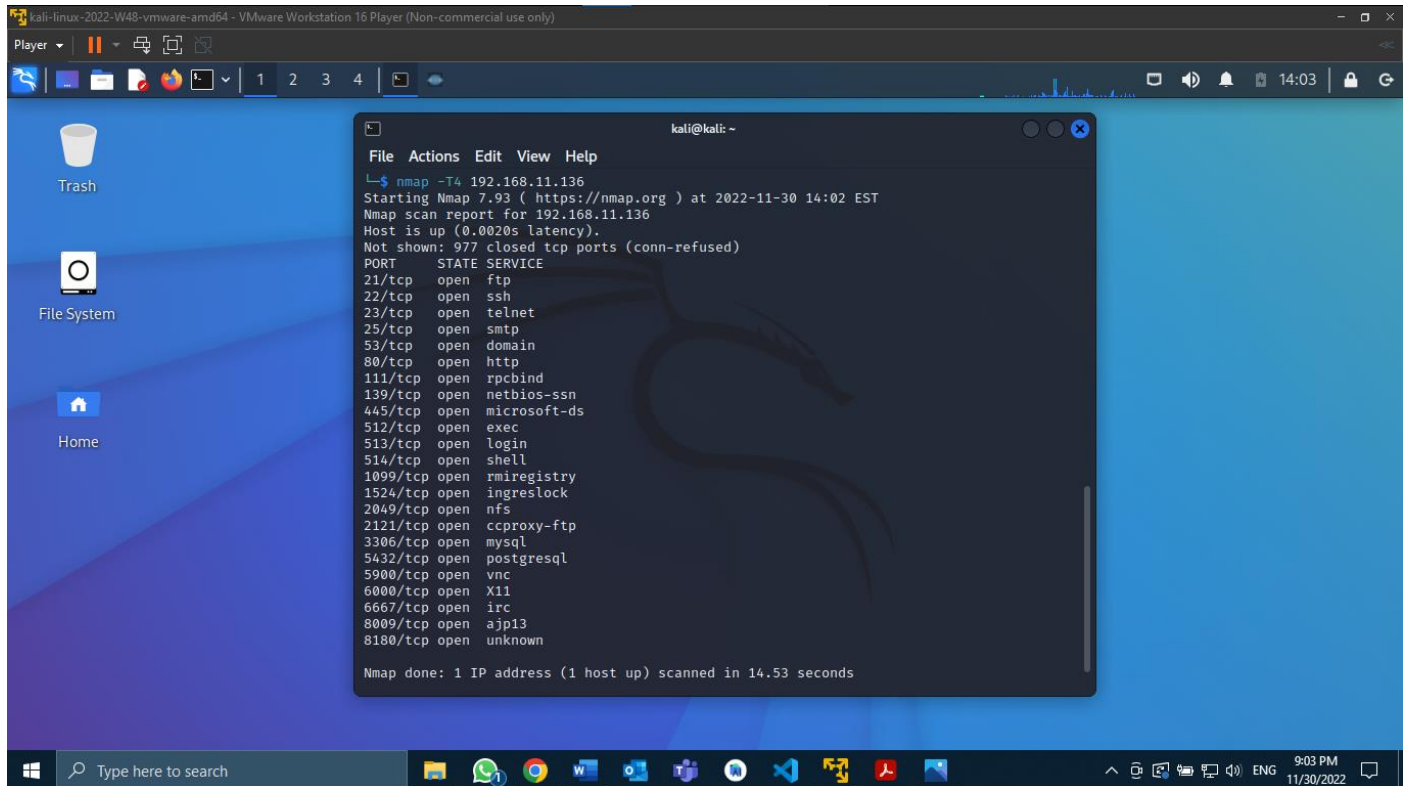
Drive Link to .pcap file of wireshark:

https://drive.google.com/drive/folders/1HwpDgfk6yzN8BaKLiHsznncWj5BVTbuy?usp=share_link

7. Screen shots

Machine	IP
Linux Kali	192.168.11.134
Windows Server 2016	192.168.11.135
Linux Metasploit	192.168.11.136

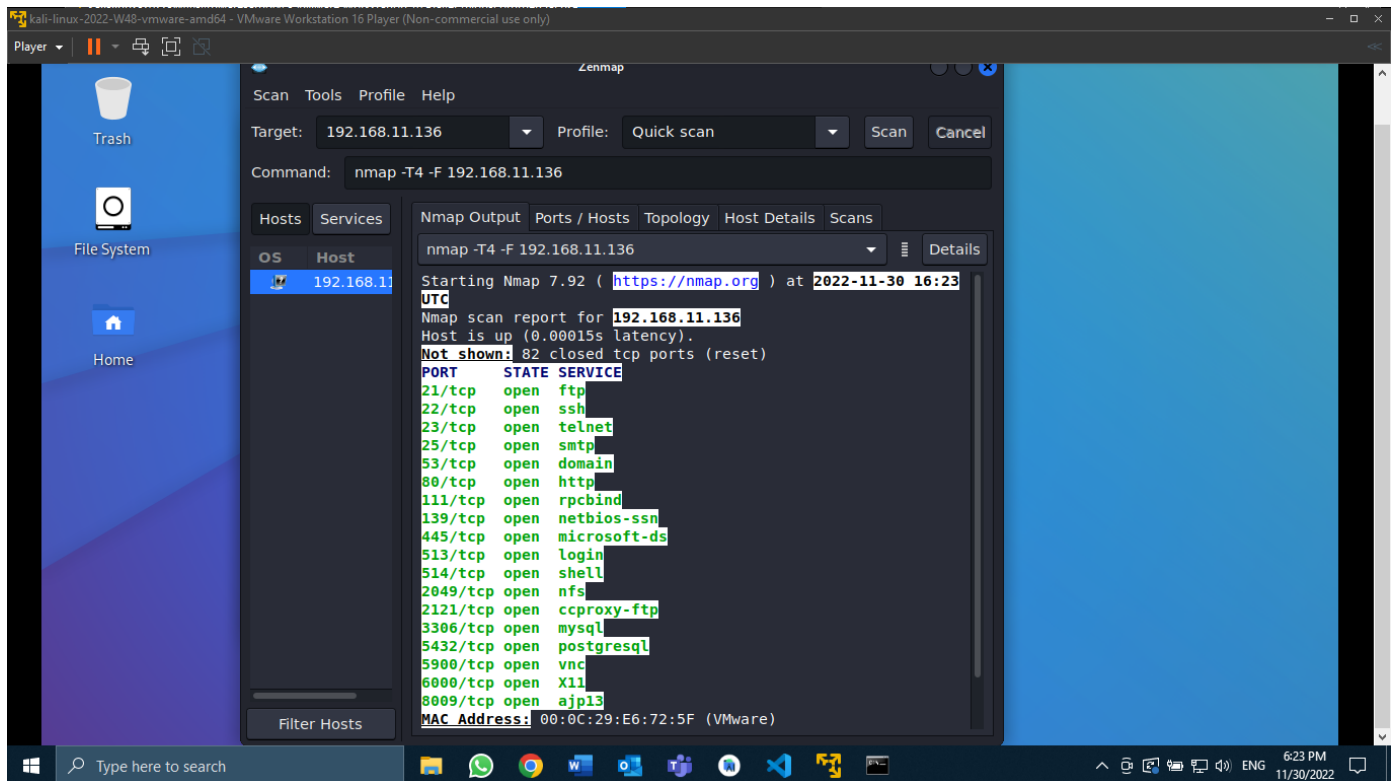
Scanning the Target Using nmap (Metasploit)



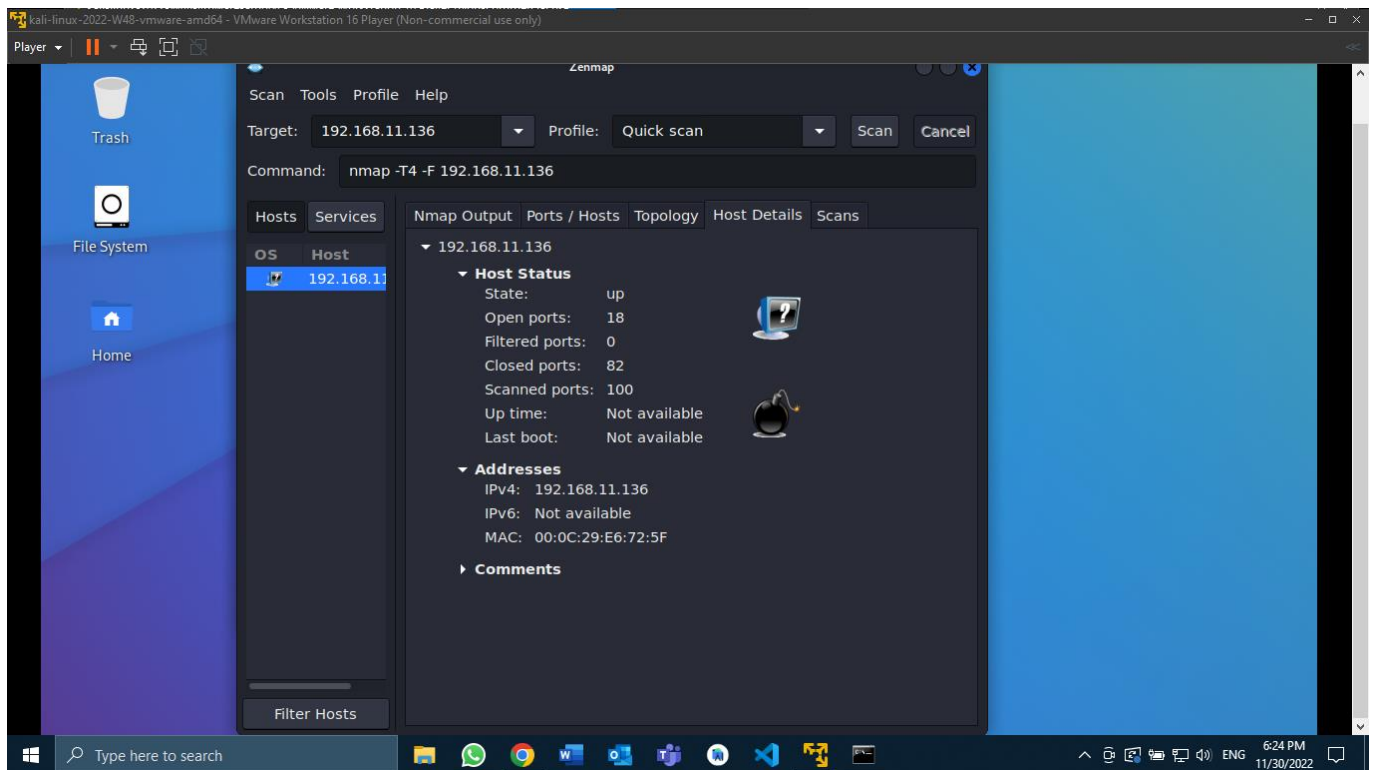
The screenshot shows a Kali Linux desktop environment within a VMware Workstation 15 Player. The desktop has a blue background with icons for Trash, File System, and Home. A terminal window titled 'kali@kali: ~' is open, displaying the output of an nmap scan. The scan was performed on 192.168.11.136 using the -T4 flag. The output shows that the host is up and lists 21 open ports with their corresponding services. The scan was completed in 14.53 seconds.

```
kali@kali: ~  
File Actions Edit View Help  
└─$ nmap -T4 192.168.11.136  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-30 14:02 EST  
Nmap scan report for 192.168.11.136  
Host is up (0.0020s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
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  
2040/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  
  
Nmap done: 1 IP address (1 host up) scanned in 14.53 seconds
```

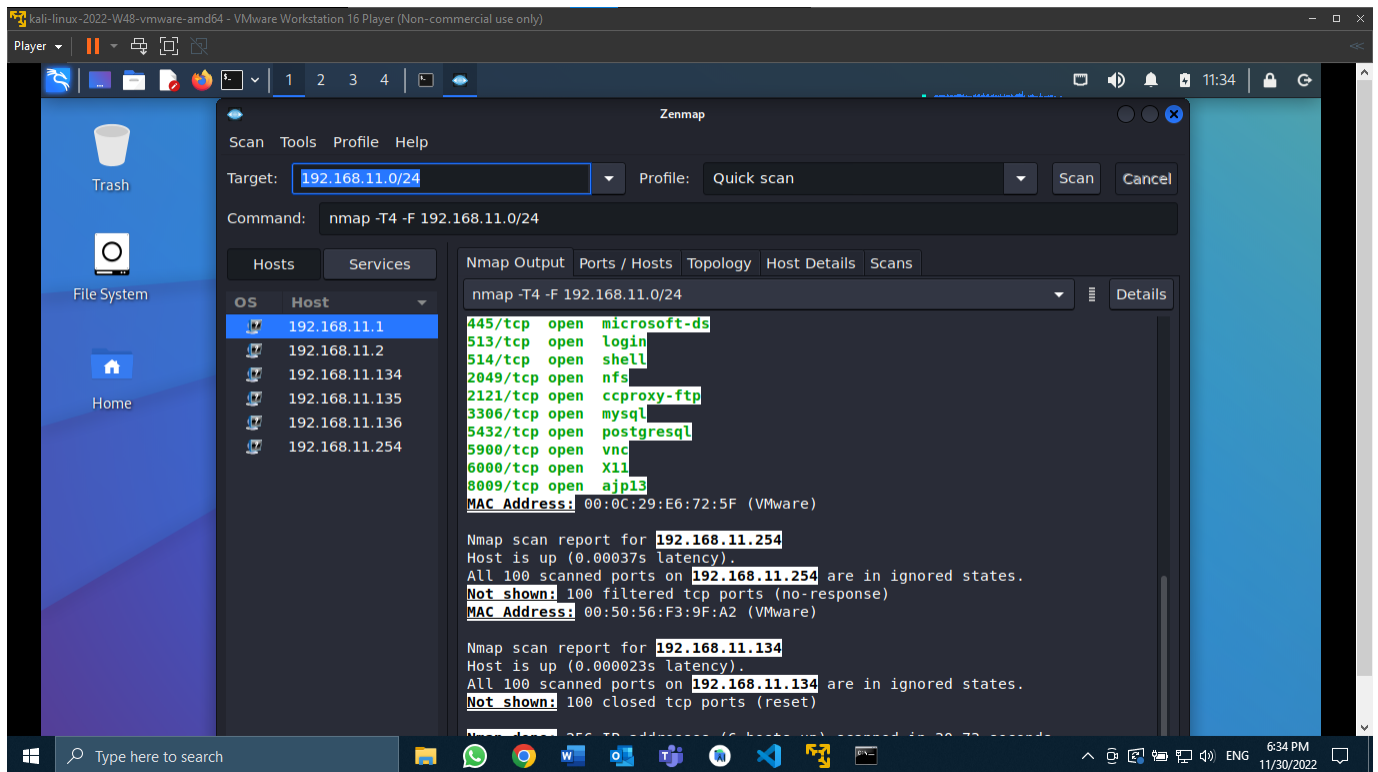

Same command but in “Zenmap”



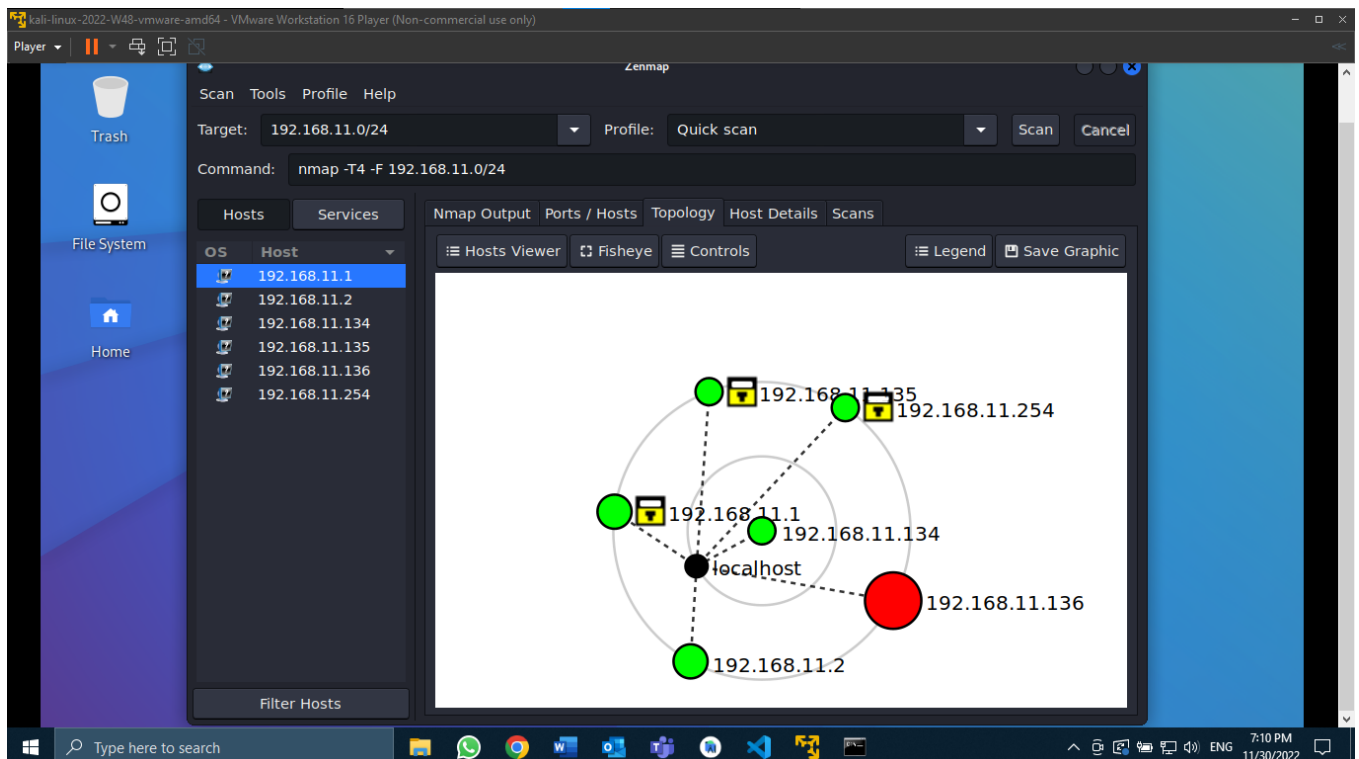
Host Details



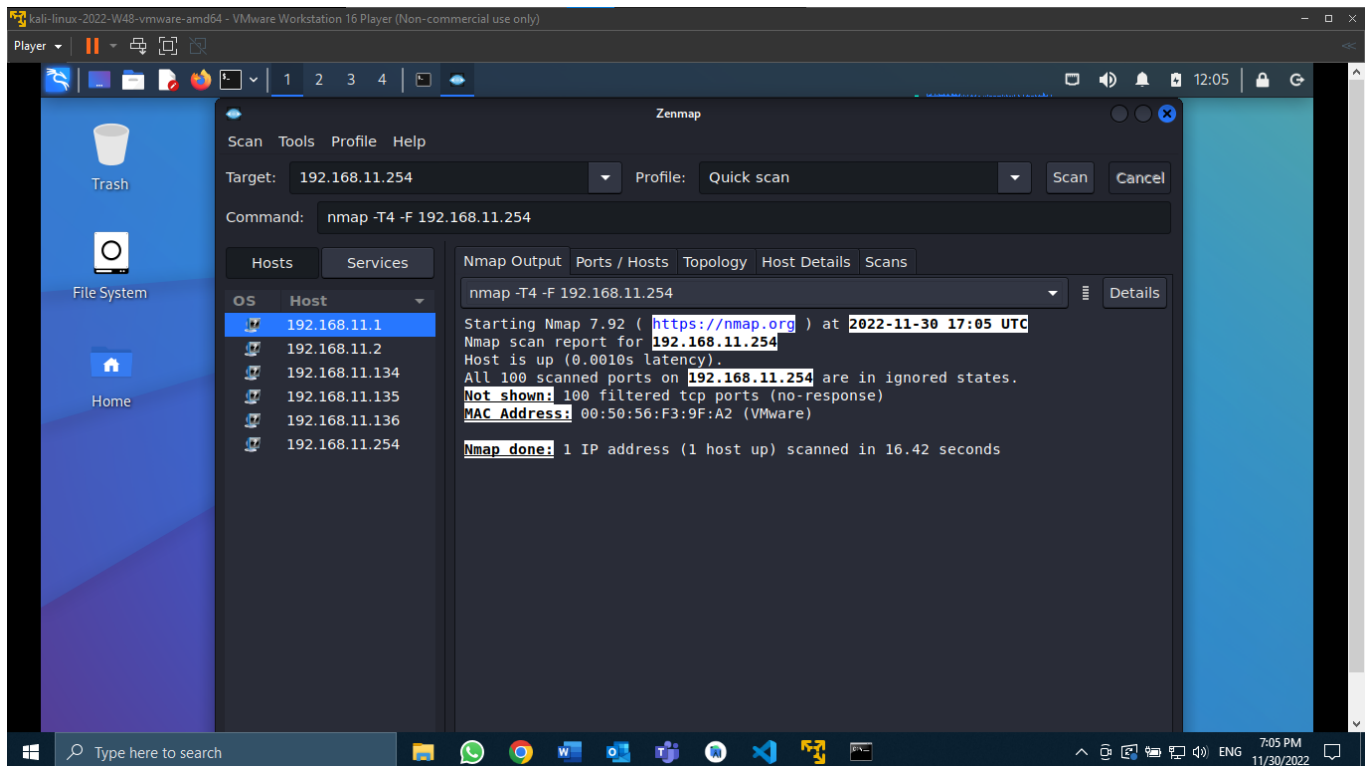
Scanning the network for computers and host (Using slash notation and 6 machines are discovered)



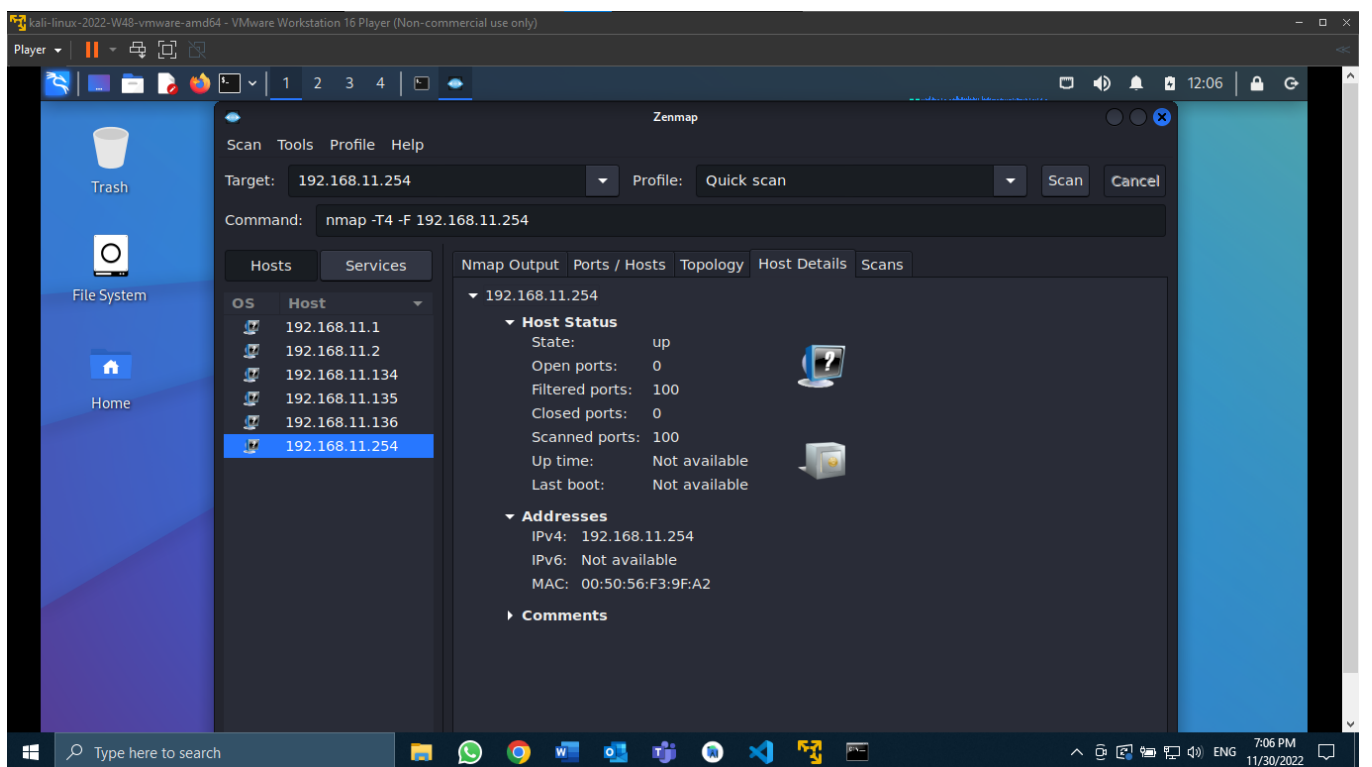
Topology



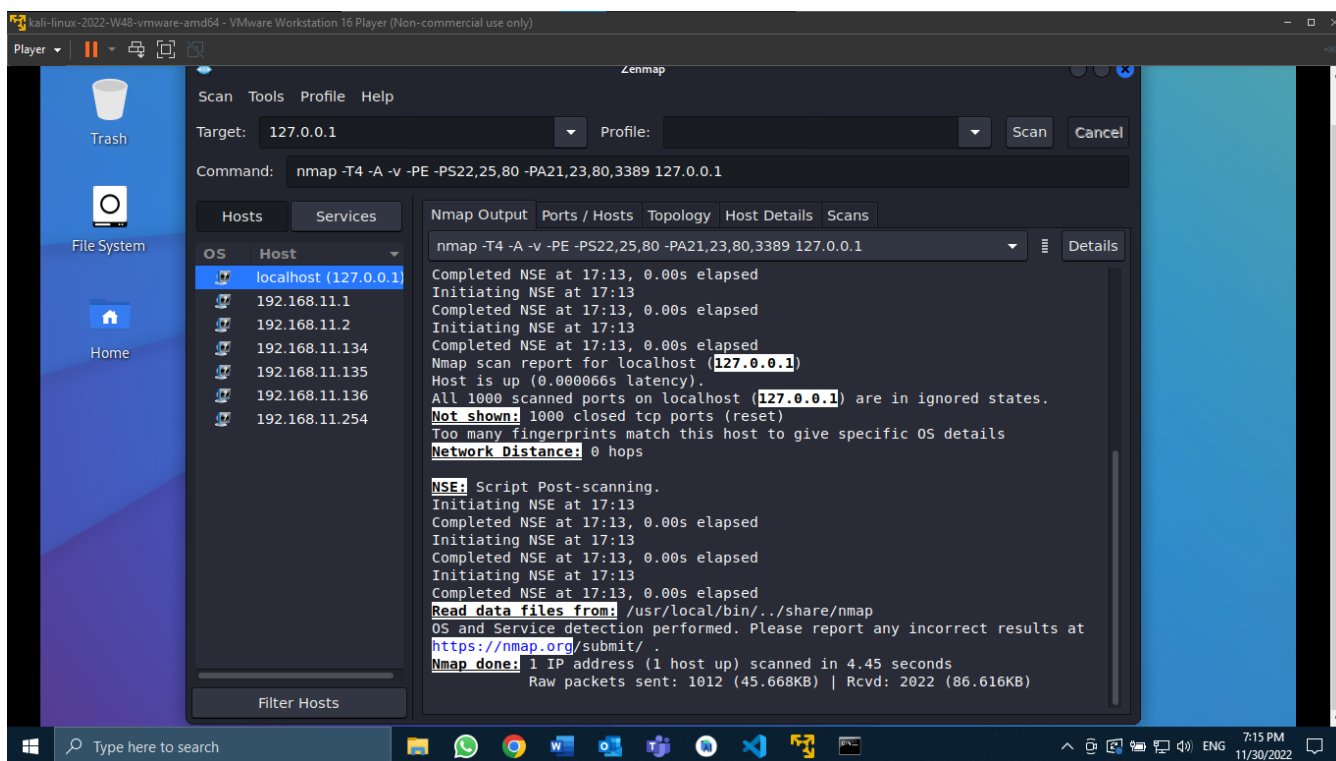
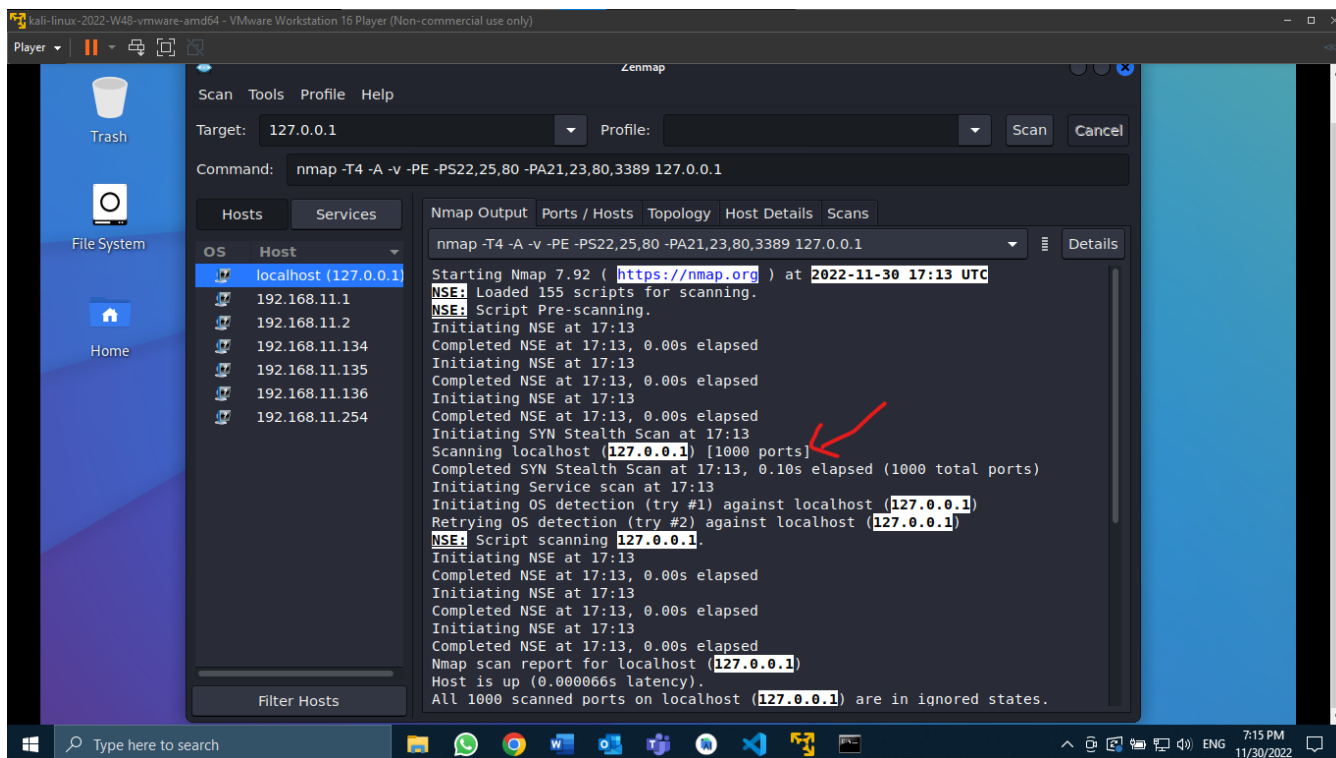
Finding about last one 192.168.11.254



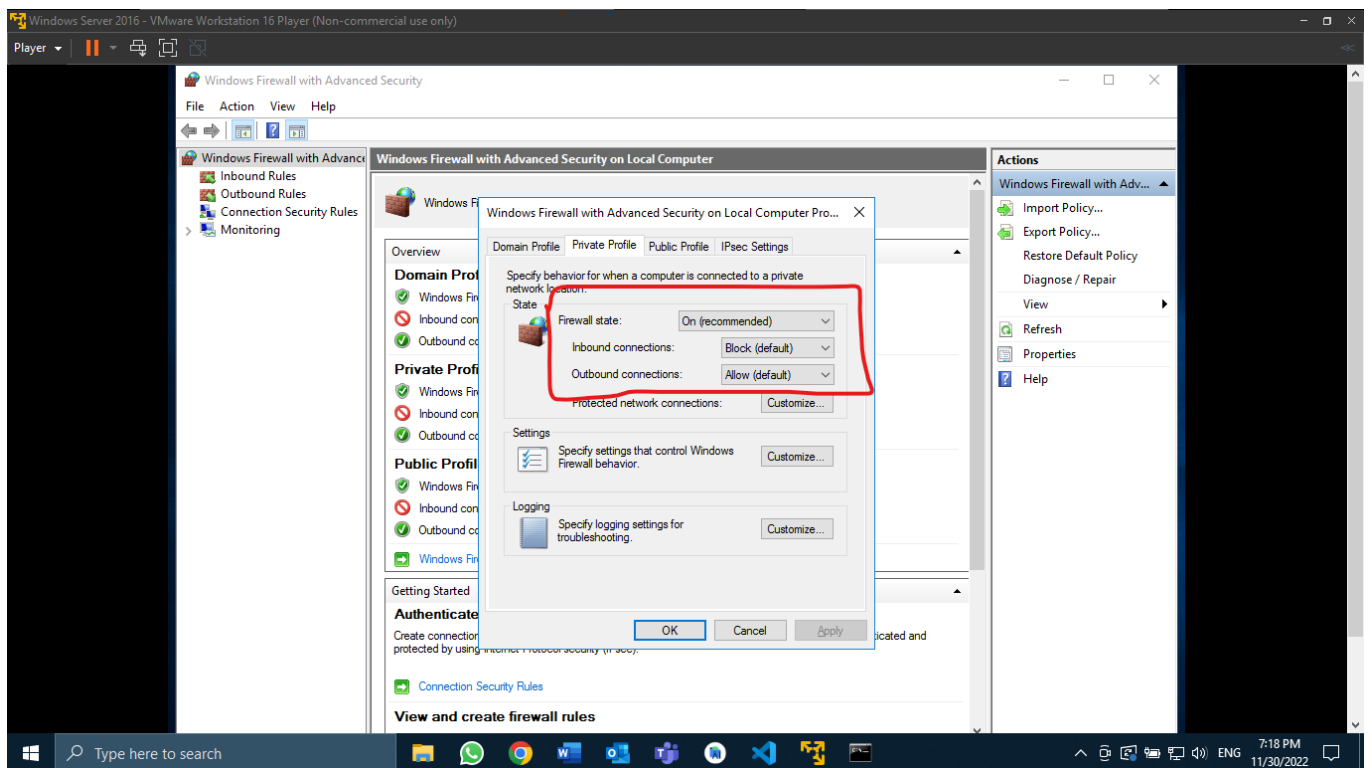
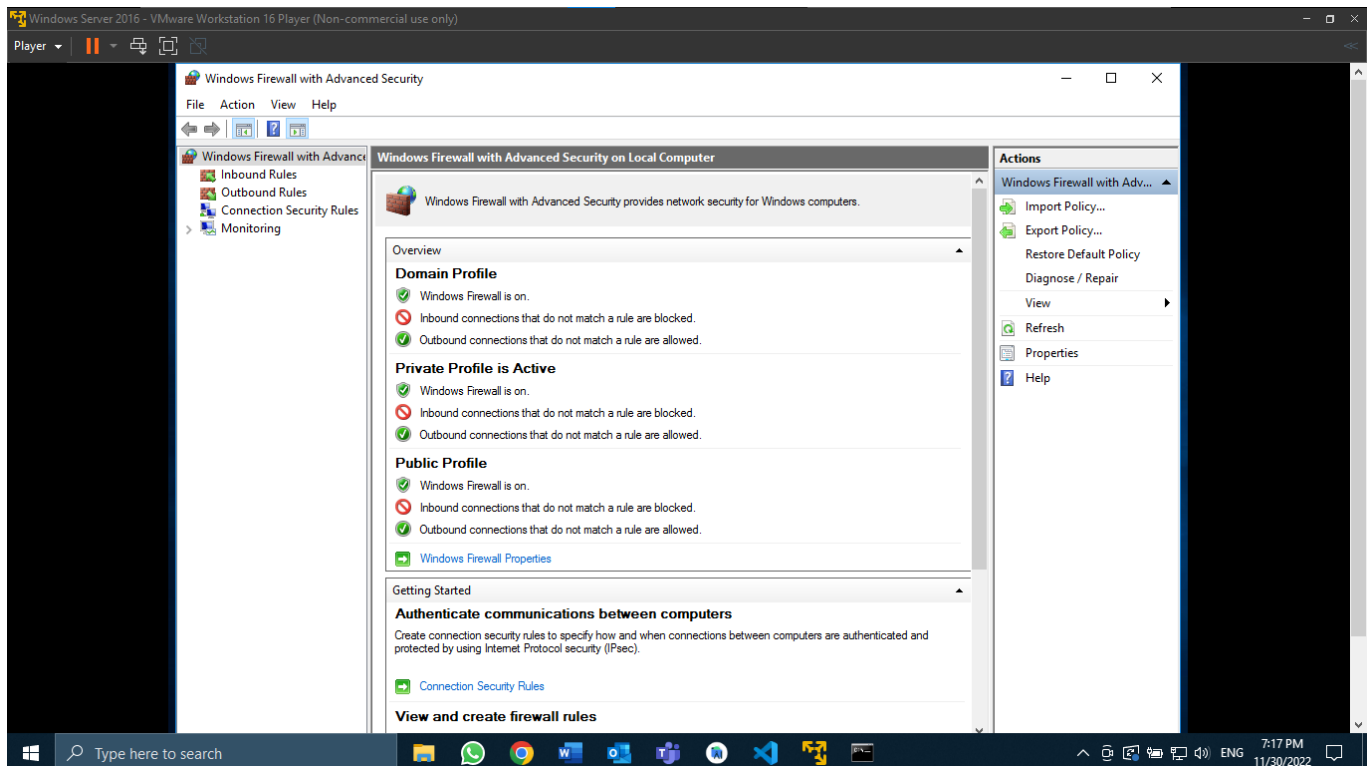
Its Host Details

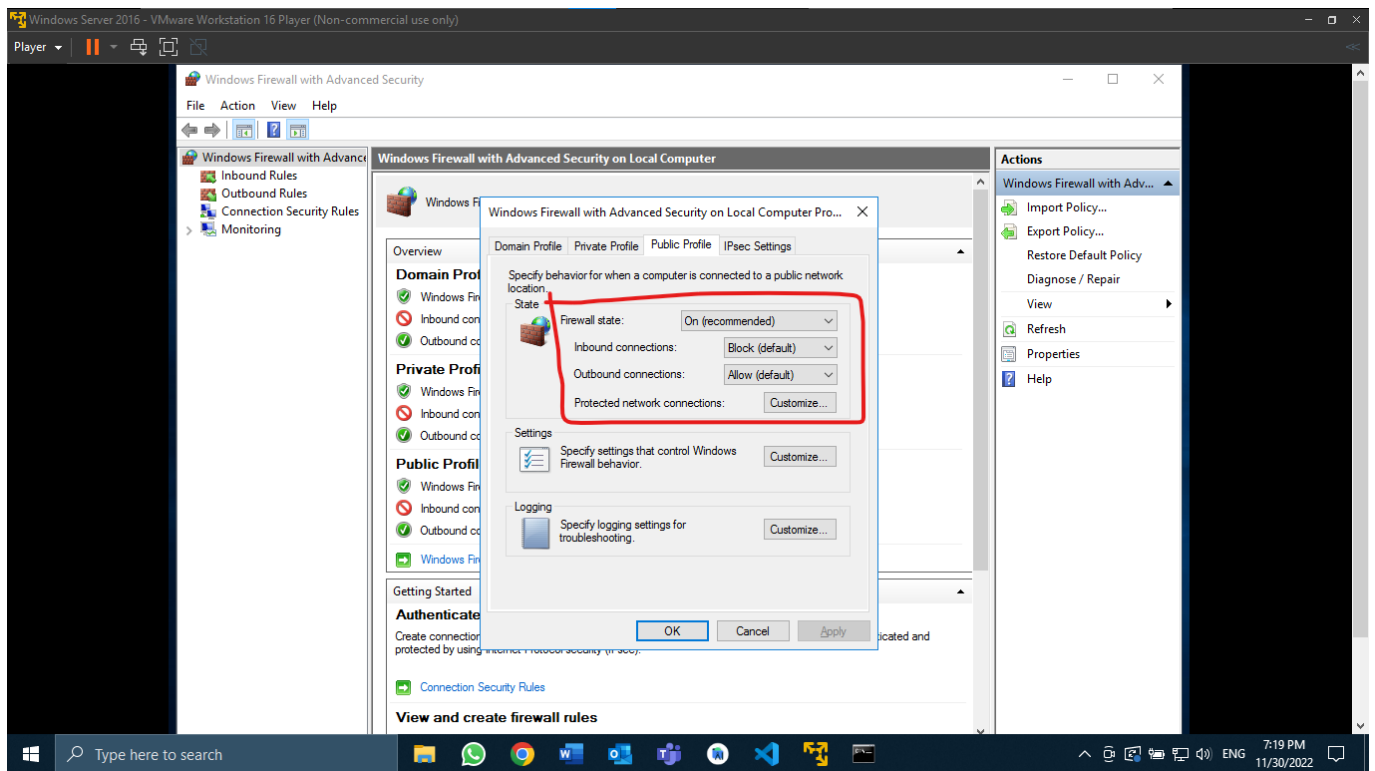


Intense scan of your Kali machine

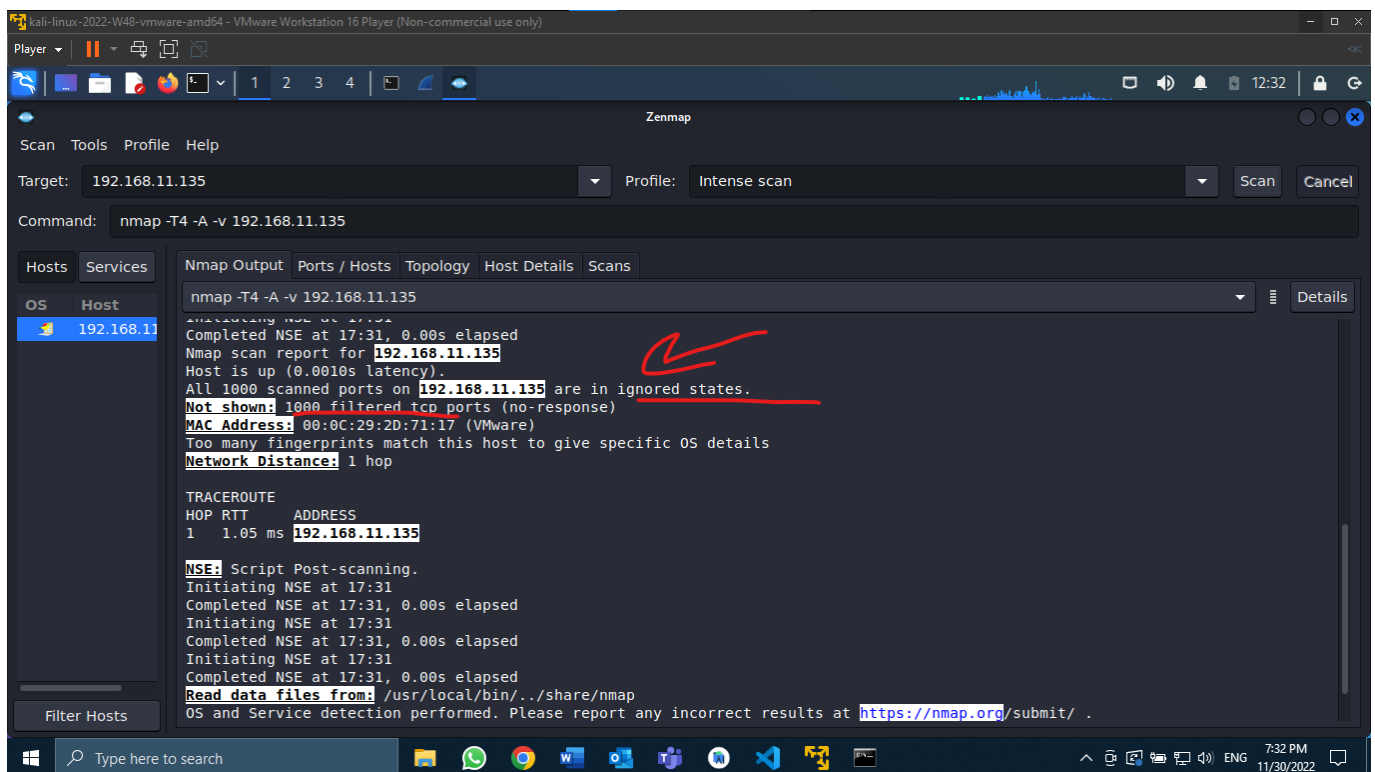


Difference between a protected target and none protected target

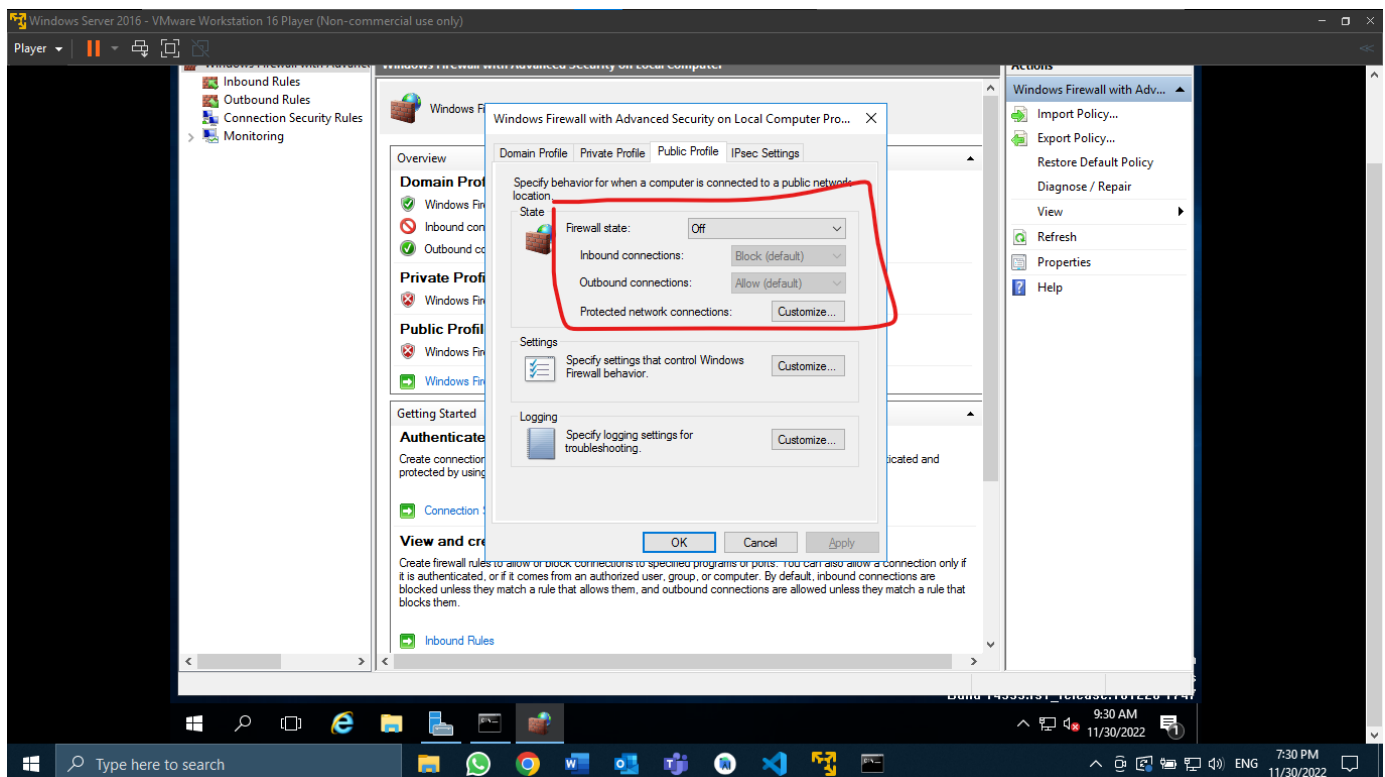
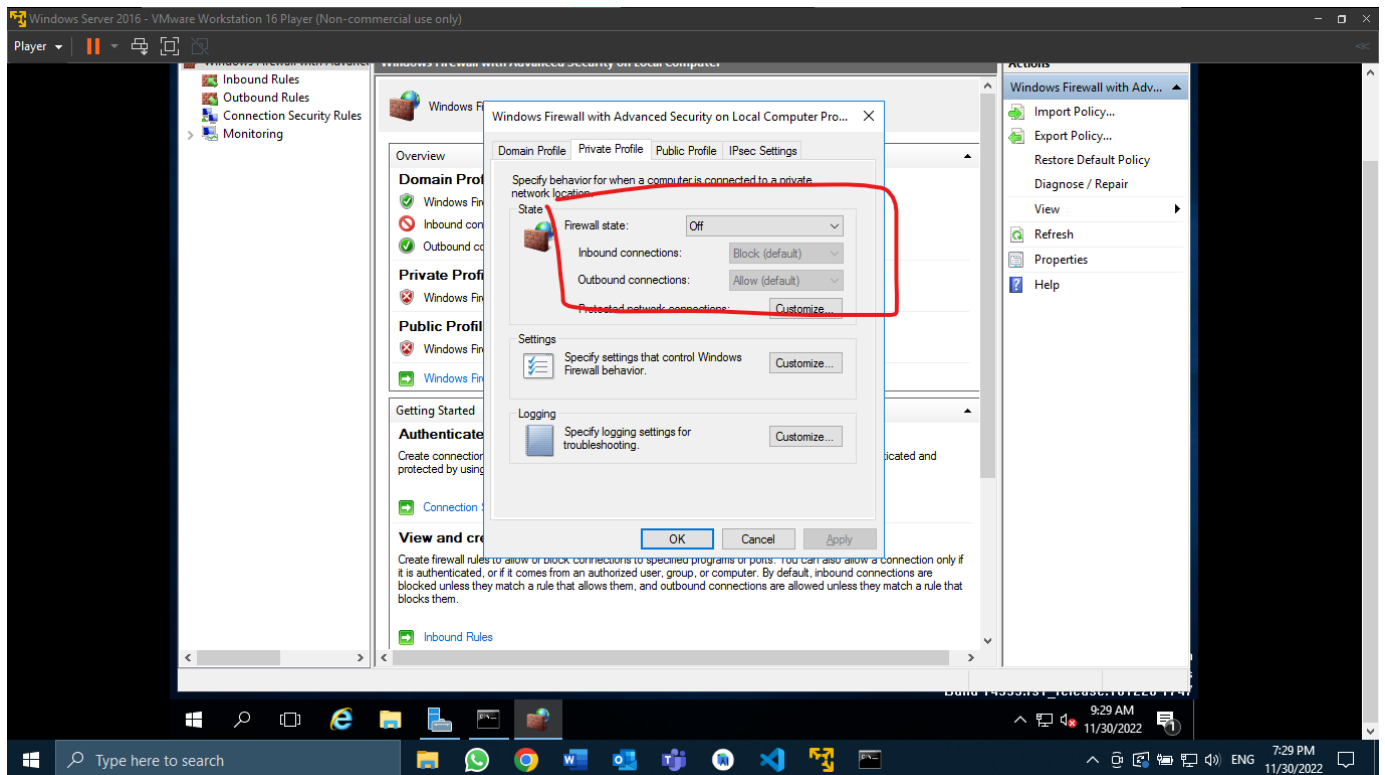




Scanning Your Windows Machine with Incoming Connections Blocked



Scanning My Windows Machine with firewall off



kali-linux-2022-W48-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)

Player

1 2 3 4

Zenmap

Scan Tools Profile Help

Target: 192.168.11.135 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.11.135

Hosts Services

OS Host

192.168.11.135

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 192.168.11.135

Completed NSE at 17:28, 0.01s elapsed

Nmap scan report for 192.168.11.135

Host is up (0.0014s latency).

Not shown: 997 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

MAC Address: 00:0C:29:2D:71:17 (VMware)

Device type: general purpose

Running: Microsoft Windows 2016

OS CPE: cpe:/o:microsoft:windows_server_2016

OS details: Microsoft Windows Server 2016 build 10586 - 14393

Uptime guess: 0.045 days (since Wed Nov 30 16:23:01 2022)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=262 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

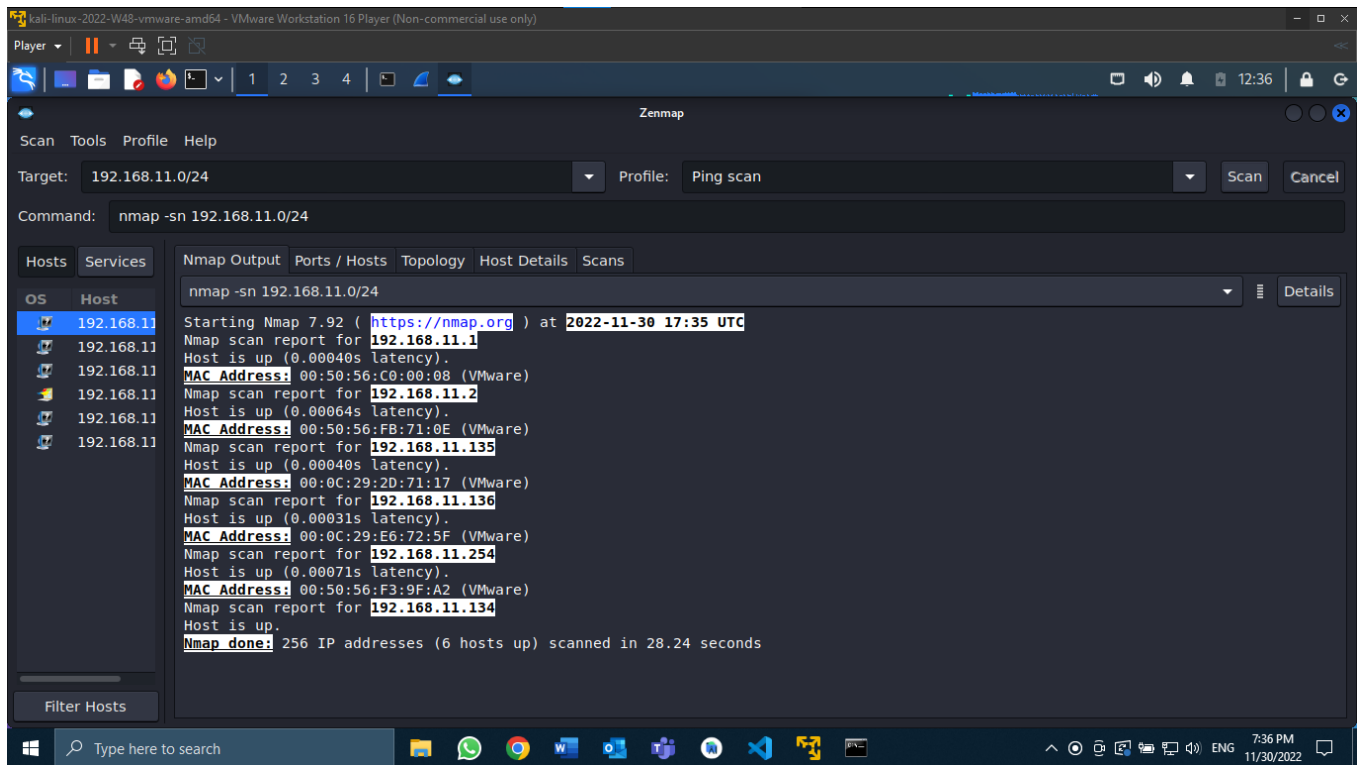
Host script results:

```
| nbstat: NetBIOS name: WIN-HGV07Q68M3M, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:2d:71:17 (VMware)
| Names:
| WTN-HGV07Q68M3M<00> Flags: <unique><active>
```

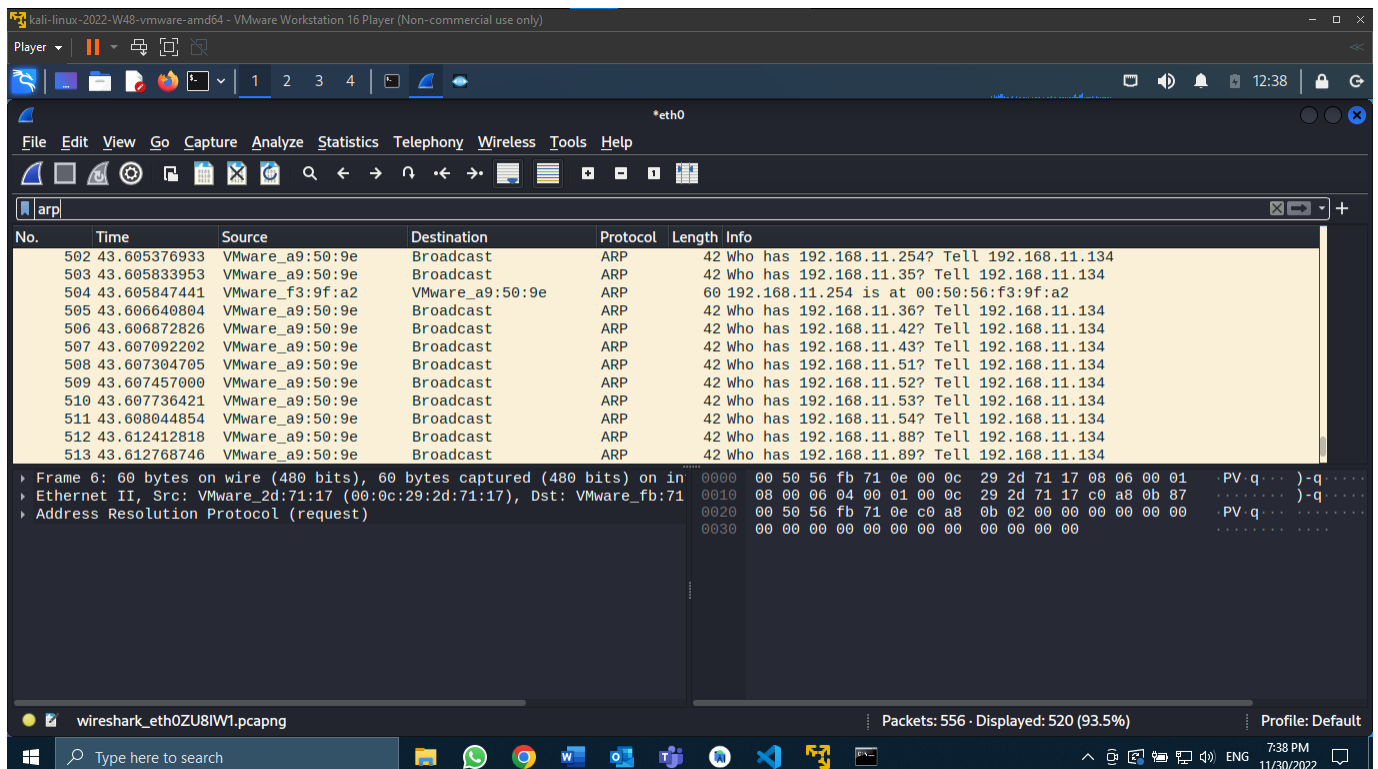
7:28 PM 11/30/2022

Analyzing a Port Scan

Performing a Ping Sweep of your Network

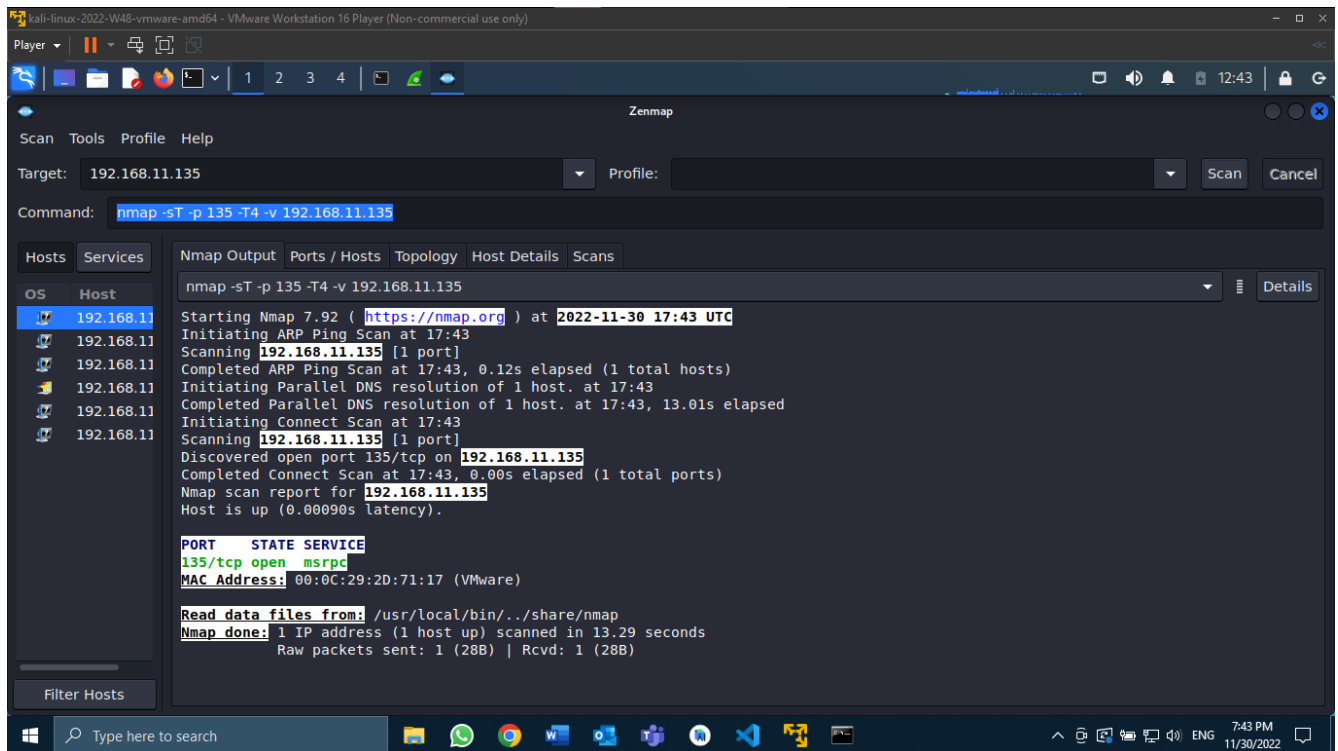


Using Wireshark to Analyze the Ping Sweep



Targeting a specific machine and port

Performing a Connect Scan of Port 135 only



Using Wireshark to Analyze the Connect Scan

