Lab Report 4

CSE451, Computer and Networks Security

Name: Ahmed Khaled Saad Ali Mekheimer ID: 1809799

Lab No: (4) Experiment Title: Discovering the Network, Scan and Reconnaissance

Date: 30 / 11 /2022

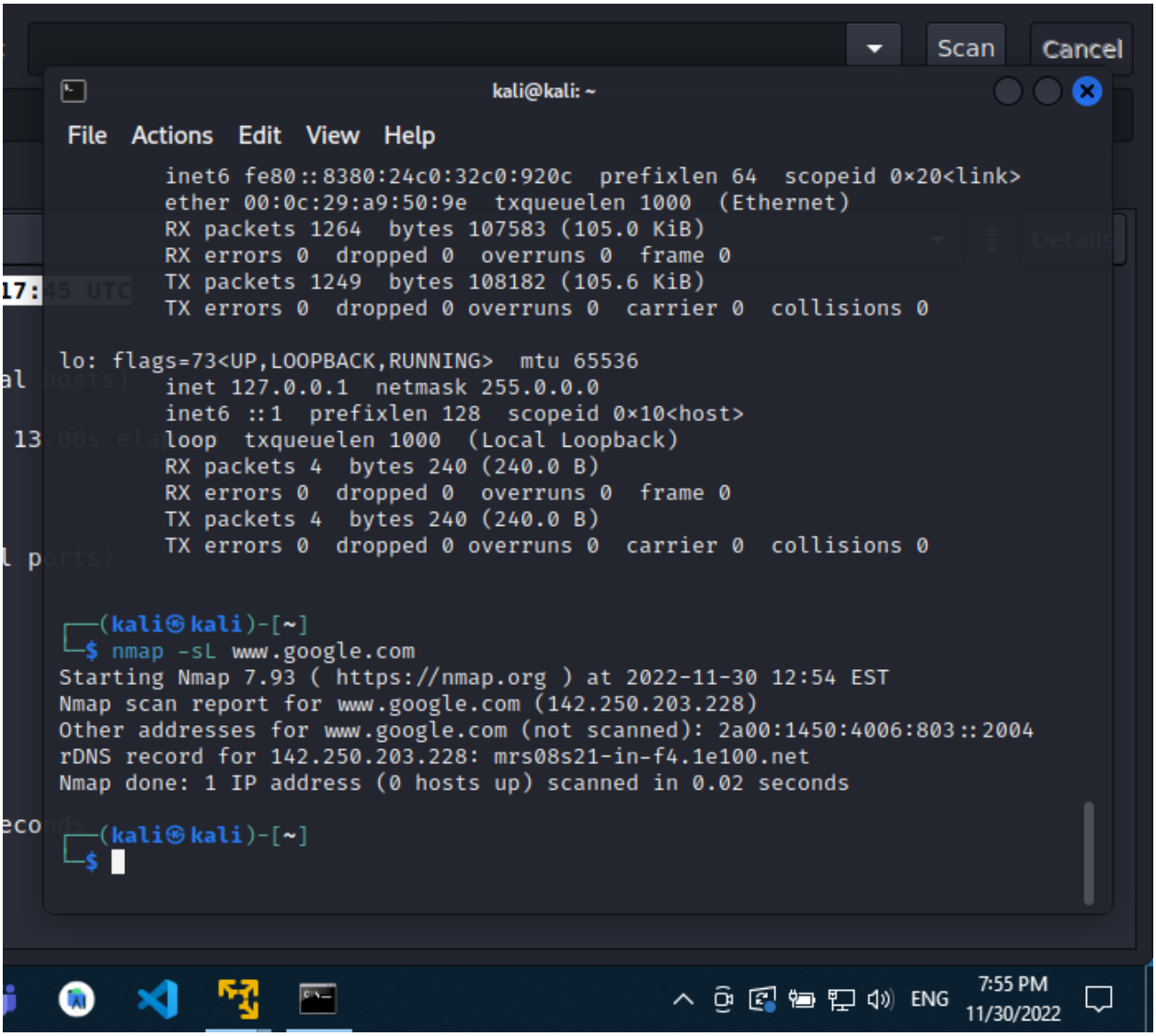
Questions and Discussion:

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.



- 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

┌──(kali㉿kali)-[~]
└─$
```

ENG 7:56 PM 11/30/2022

- 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

┌──(kali㉿kali)-[~]
└─$
```

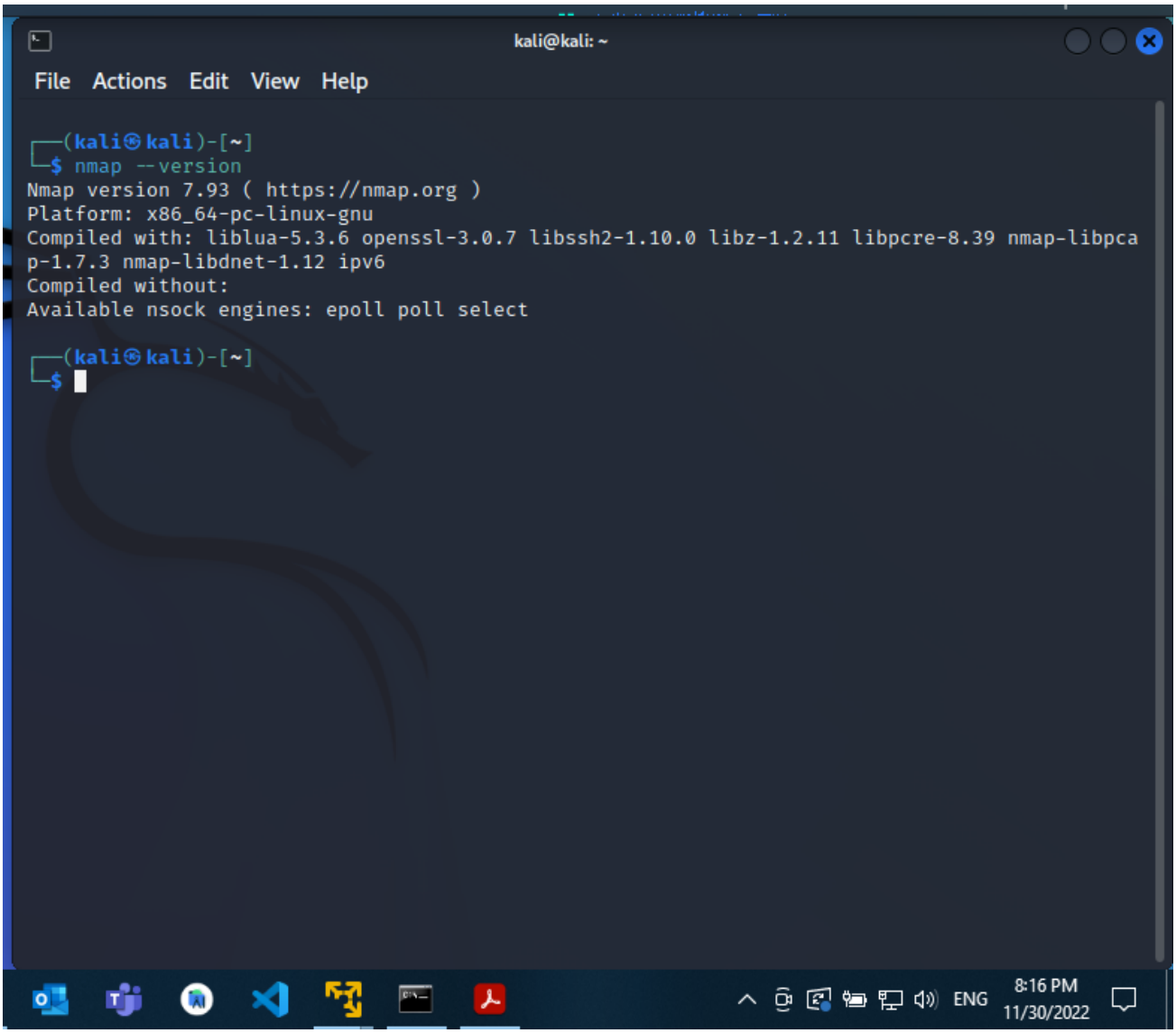
ENG 7:58 PM 11/30/2022

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?



4. what are the phases of NMAP scanning?

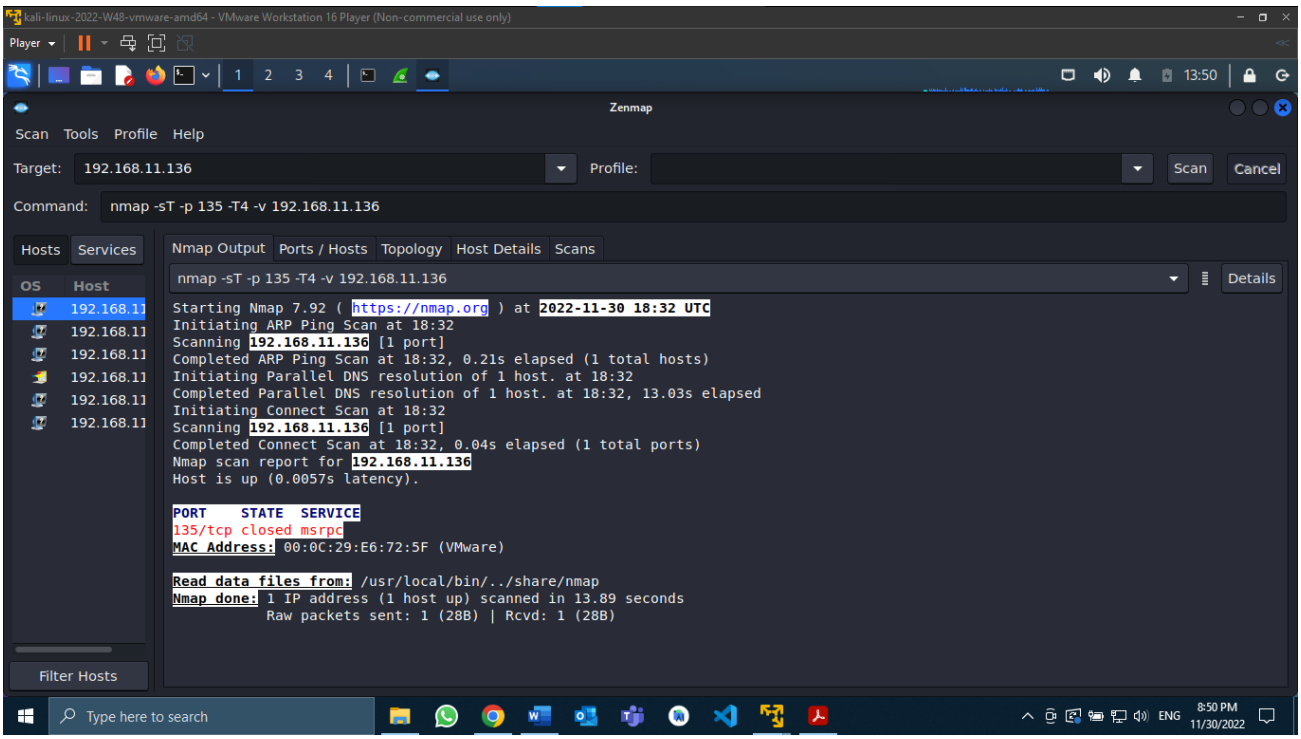
- Script pre-scanning
- Target enumeration
- Host discovery (ping scanning)
- Reverse-DNS resolution
- Port Scanning
- Version Detection

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

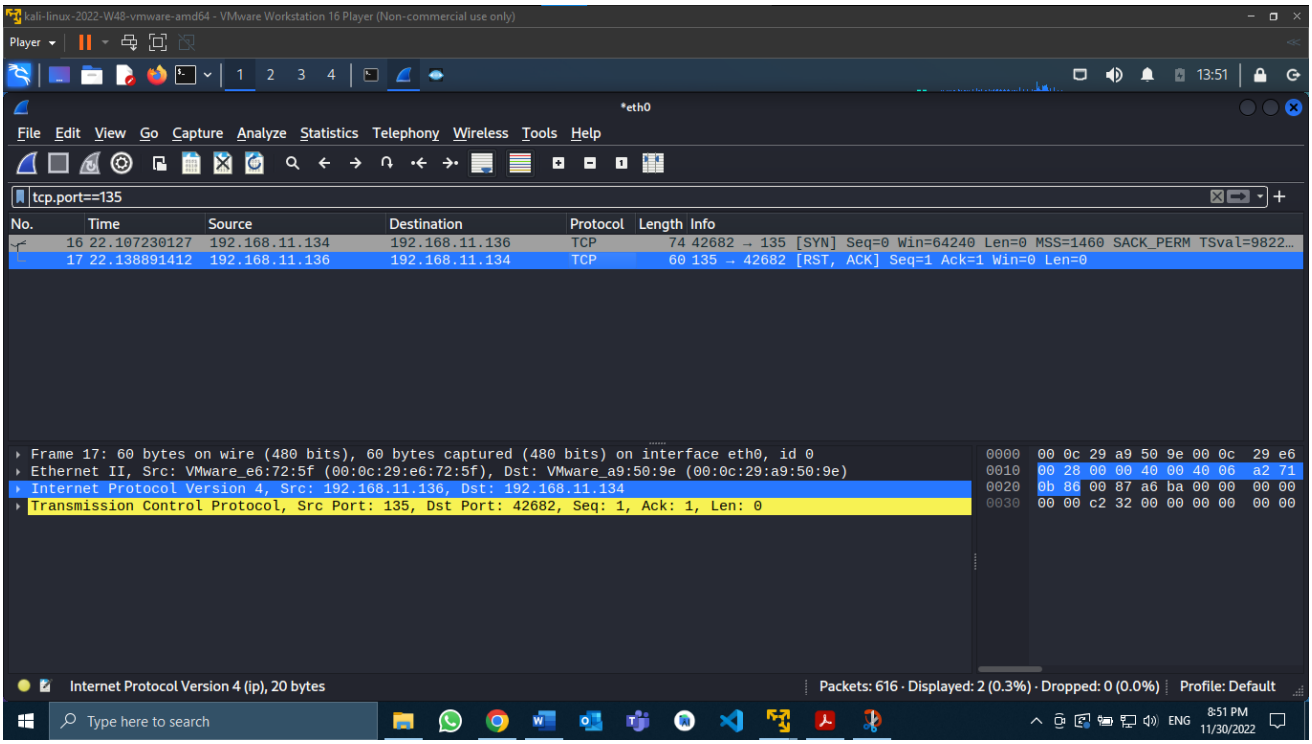
5. Describe the technique behind nmap work principles.

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



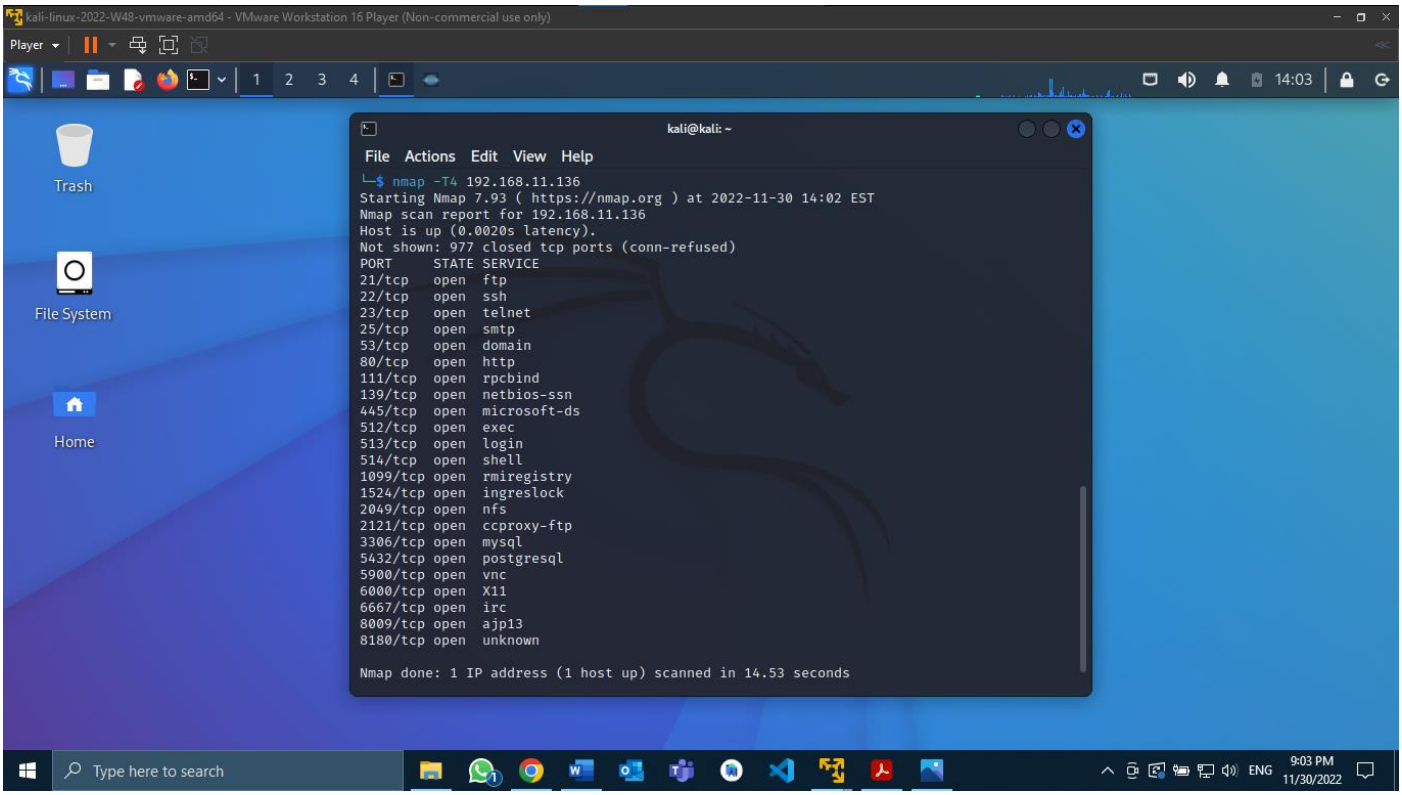
Drive Link to .pcap file of wireshark:

https://drive.google.com/drive/folders/1HwpDgfk6yzN8BaKLiHszzncWj5BVTbuy?usp=share_link

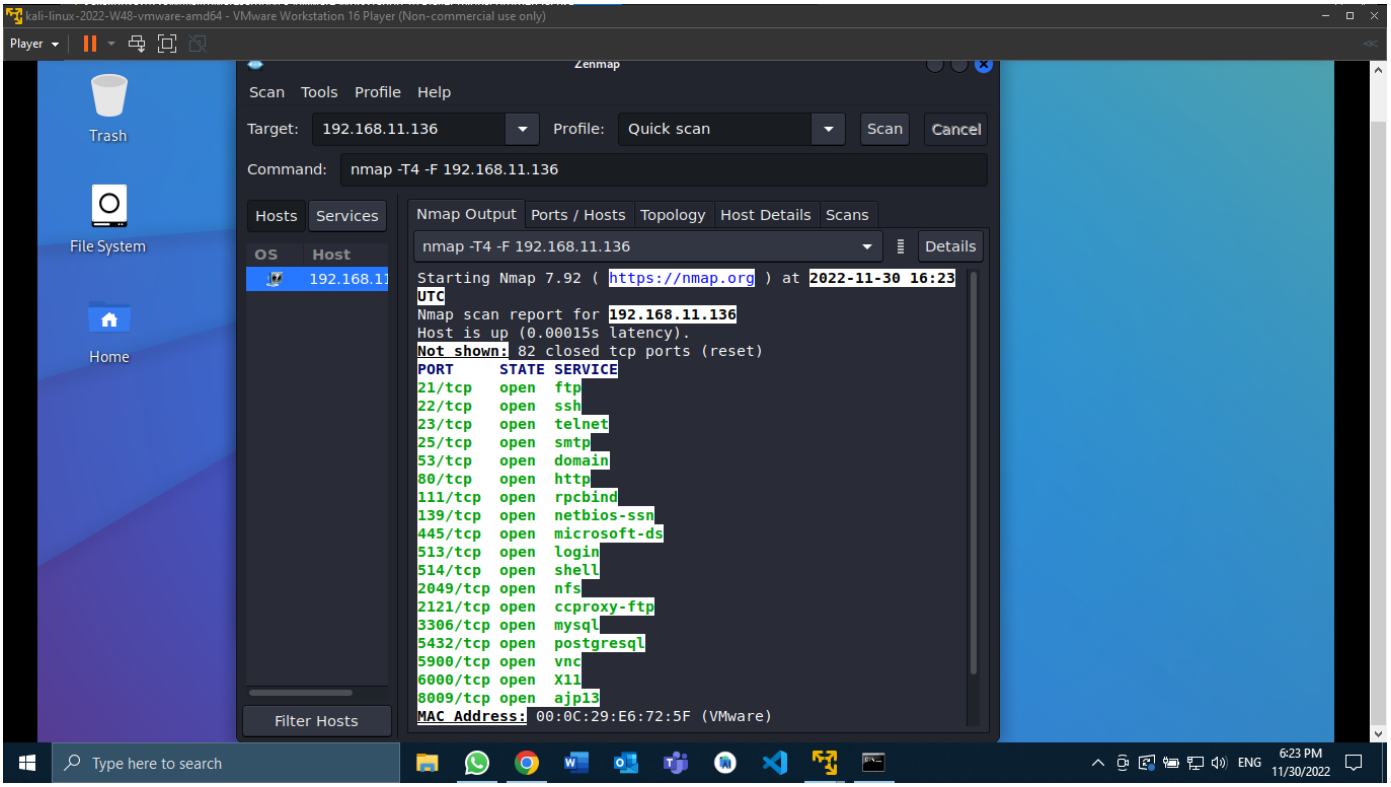
7. Screen shots

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

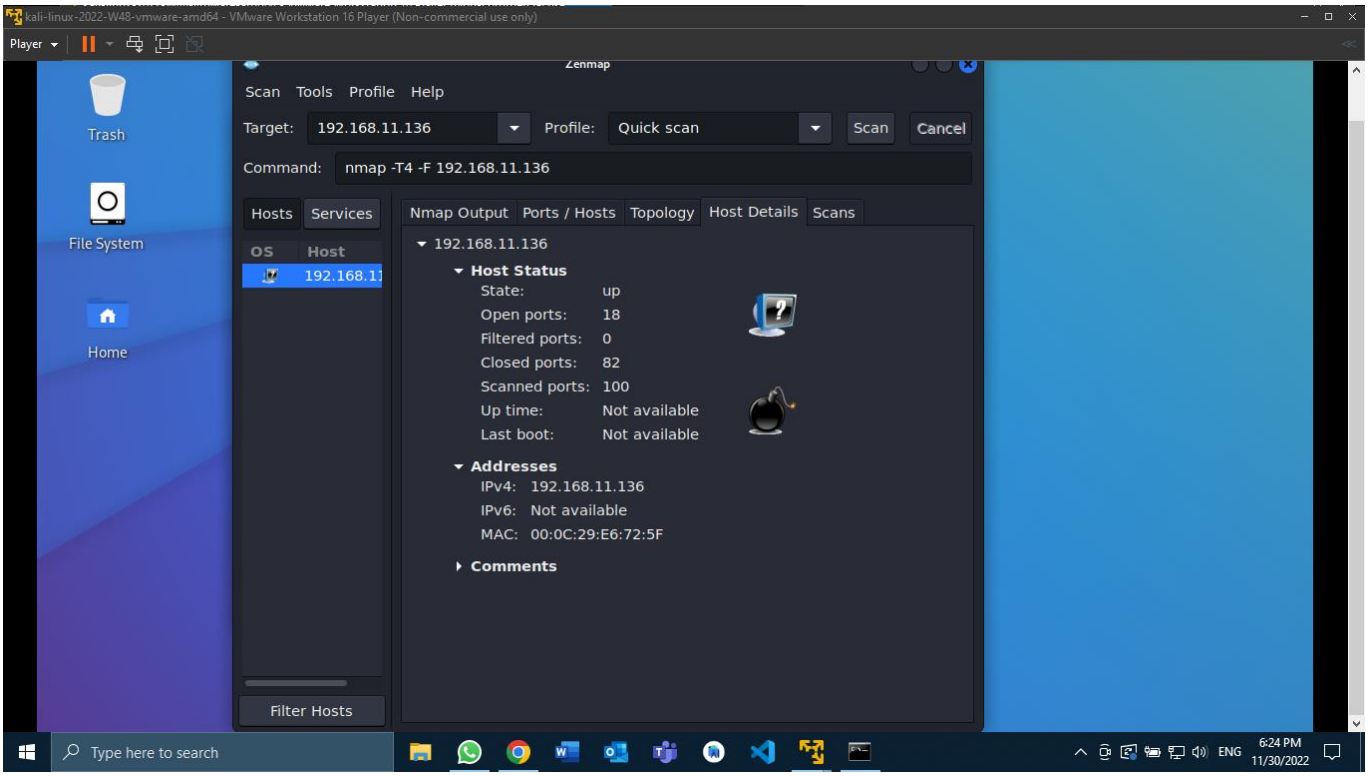
Scanning the Target Using nmap (Metasploit)



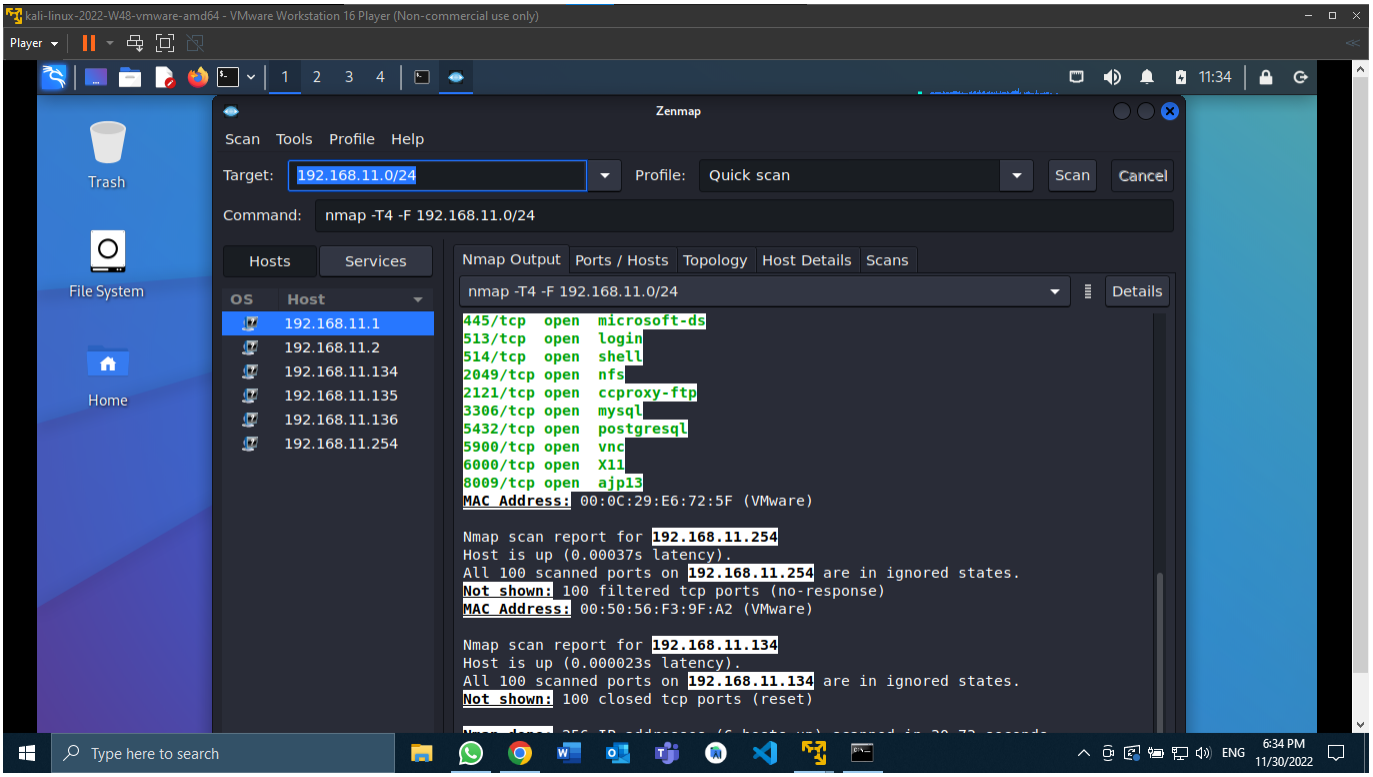
Same command but in “Zenmap”



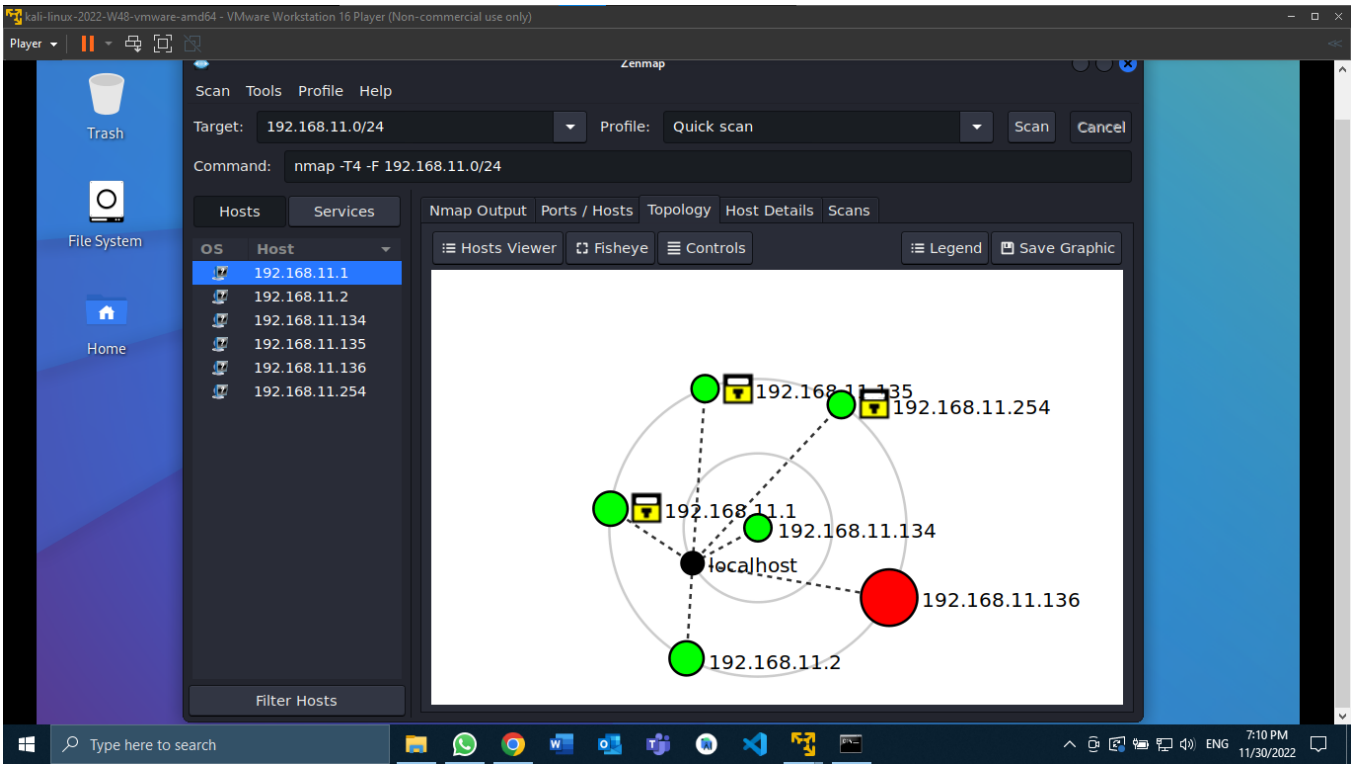
Host Details



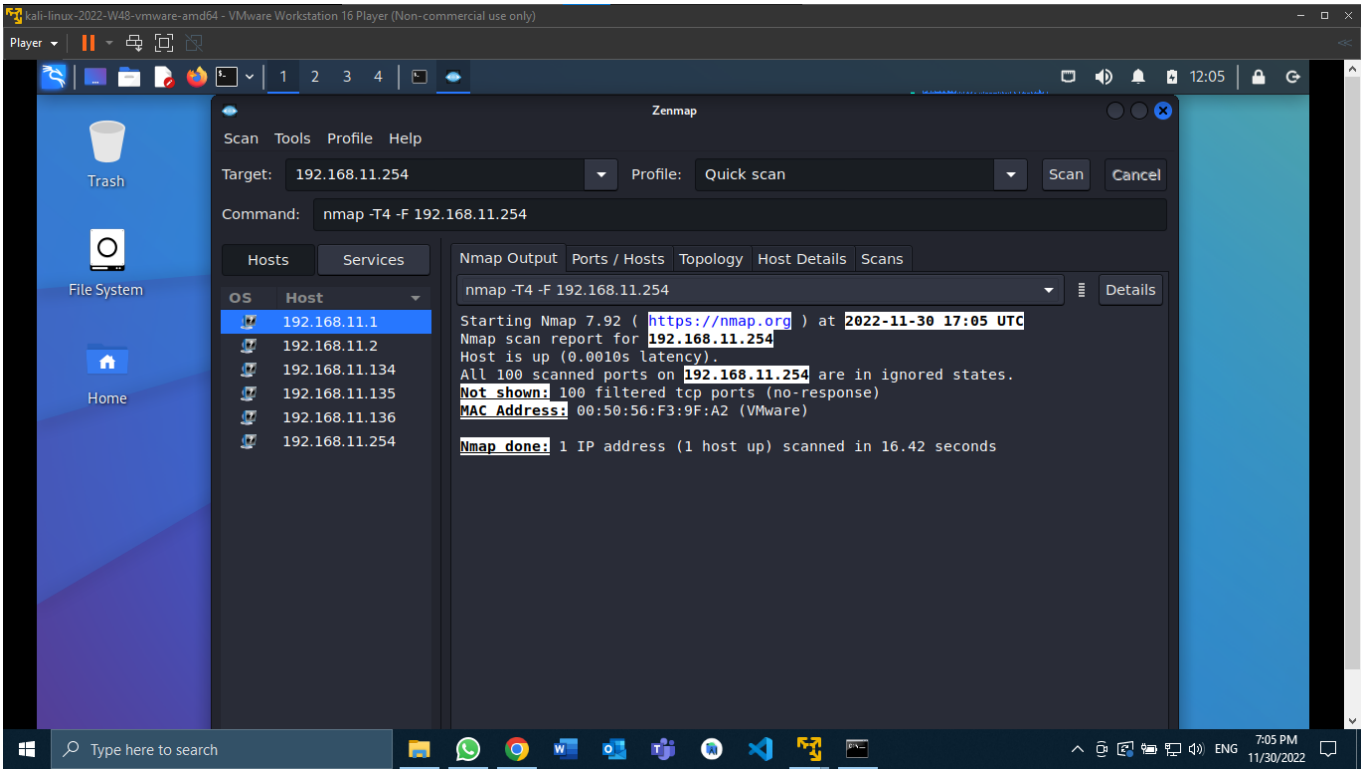
Scanning the network for computers and host (Using slash notation and 6 machines are discovered)



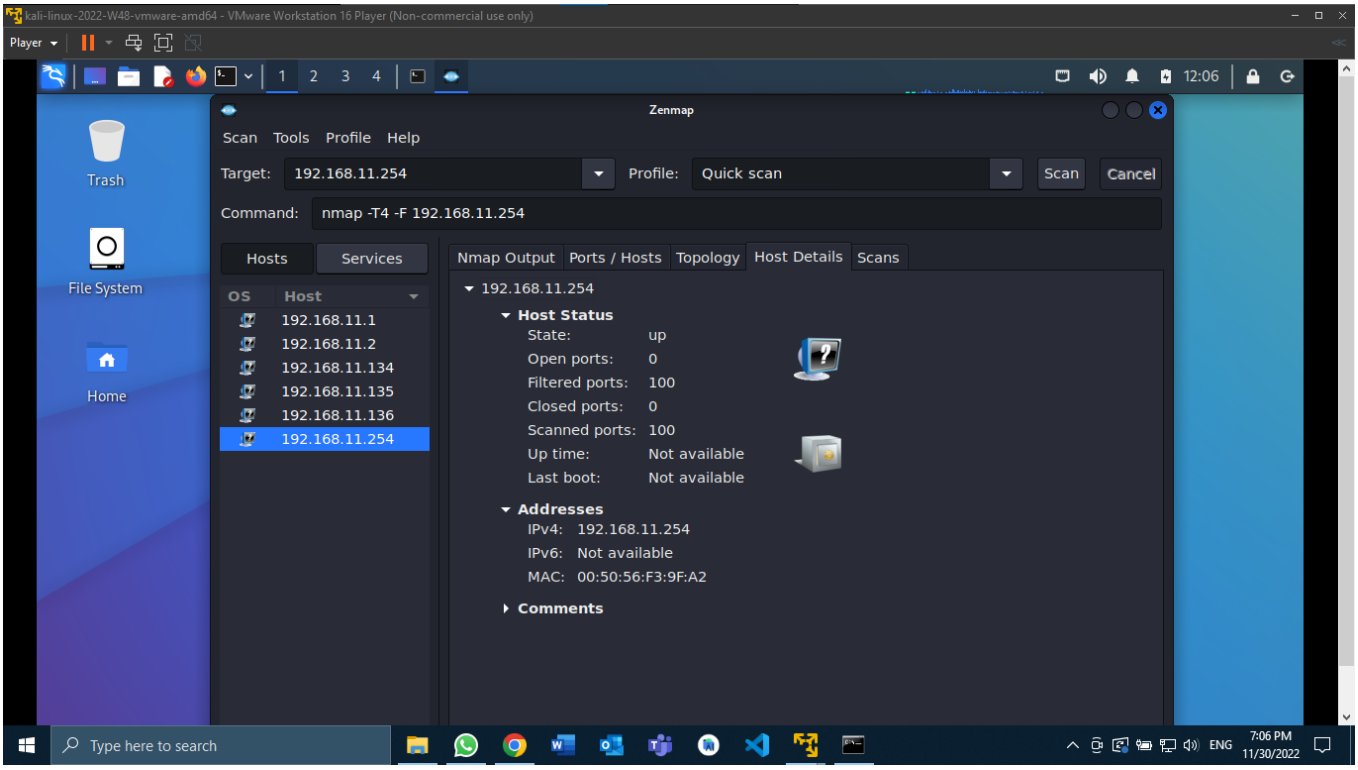
Topology



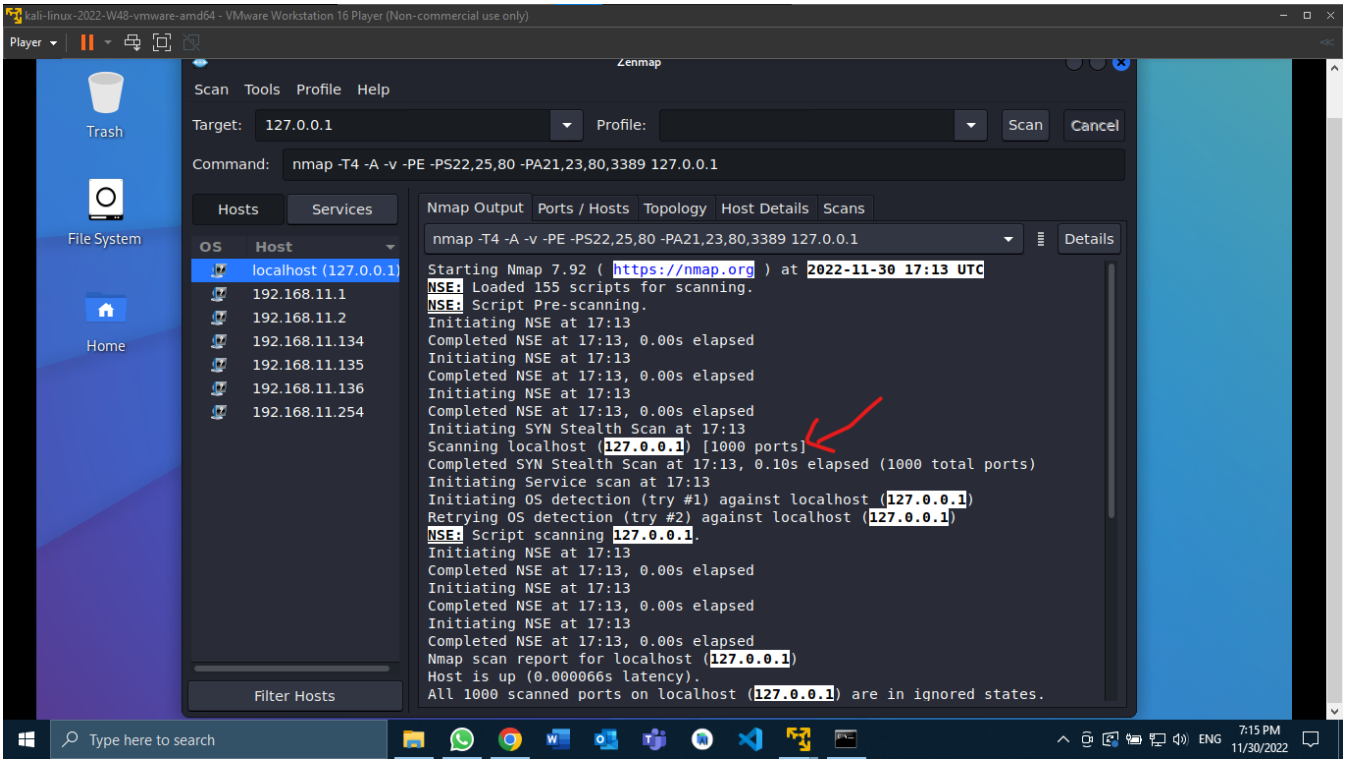
Finding about last one 192.168.11.254

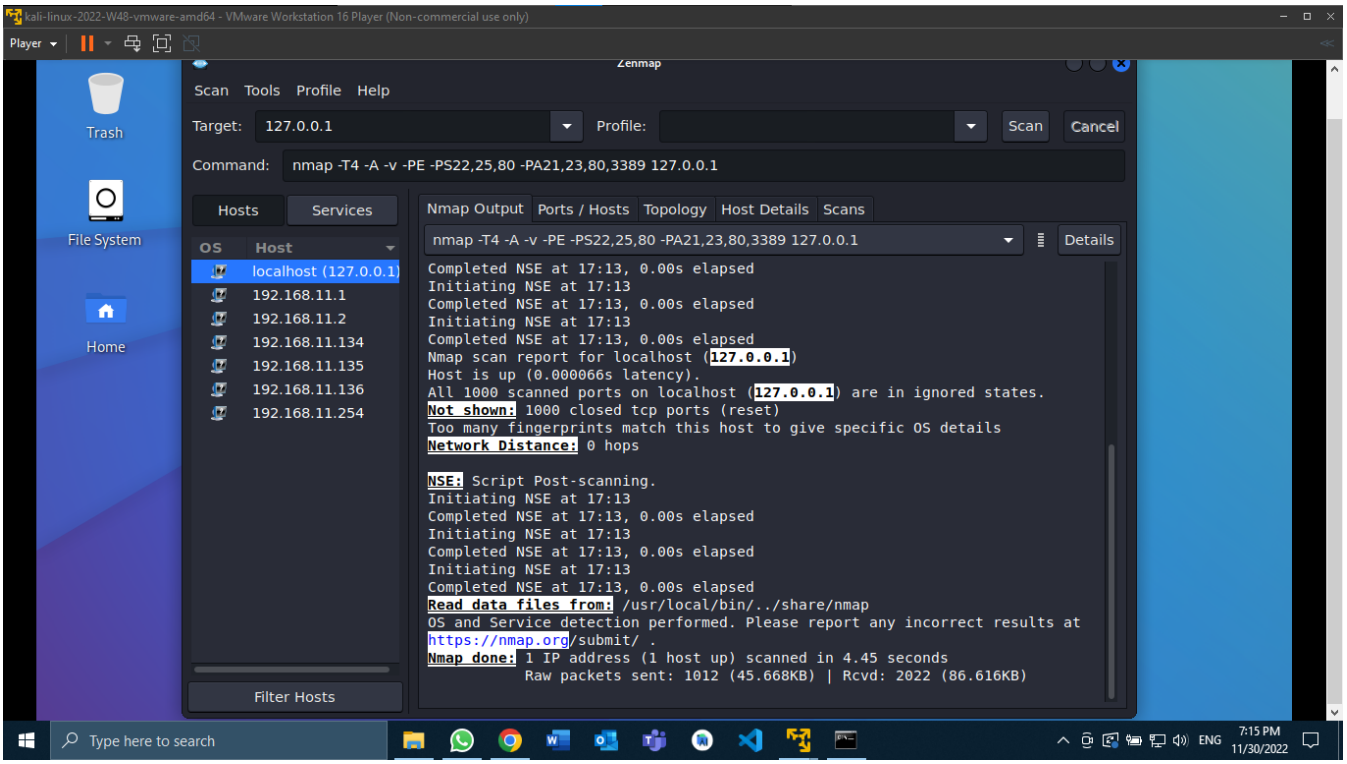


Its Host Details

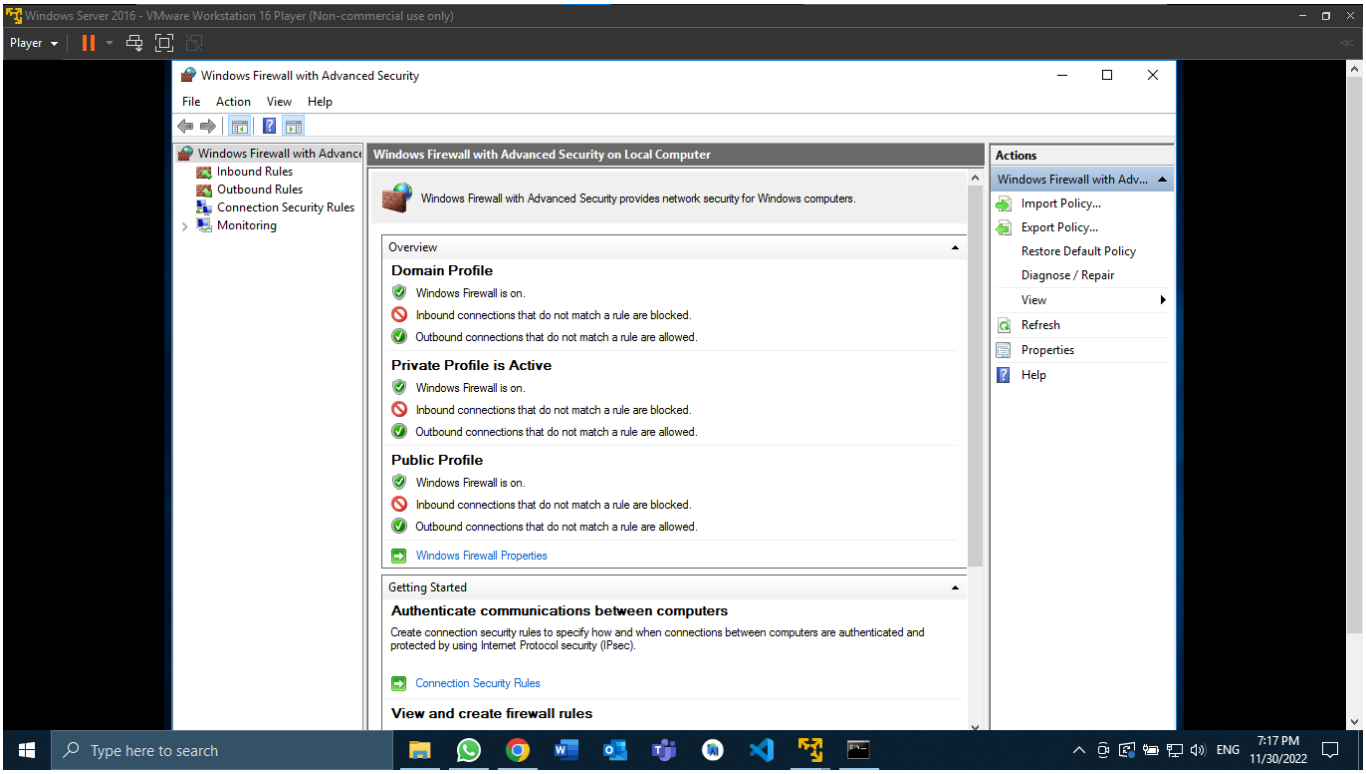


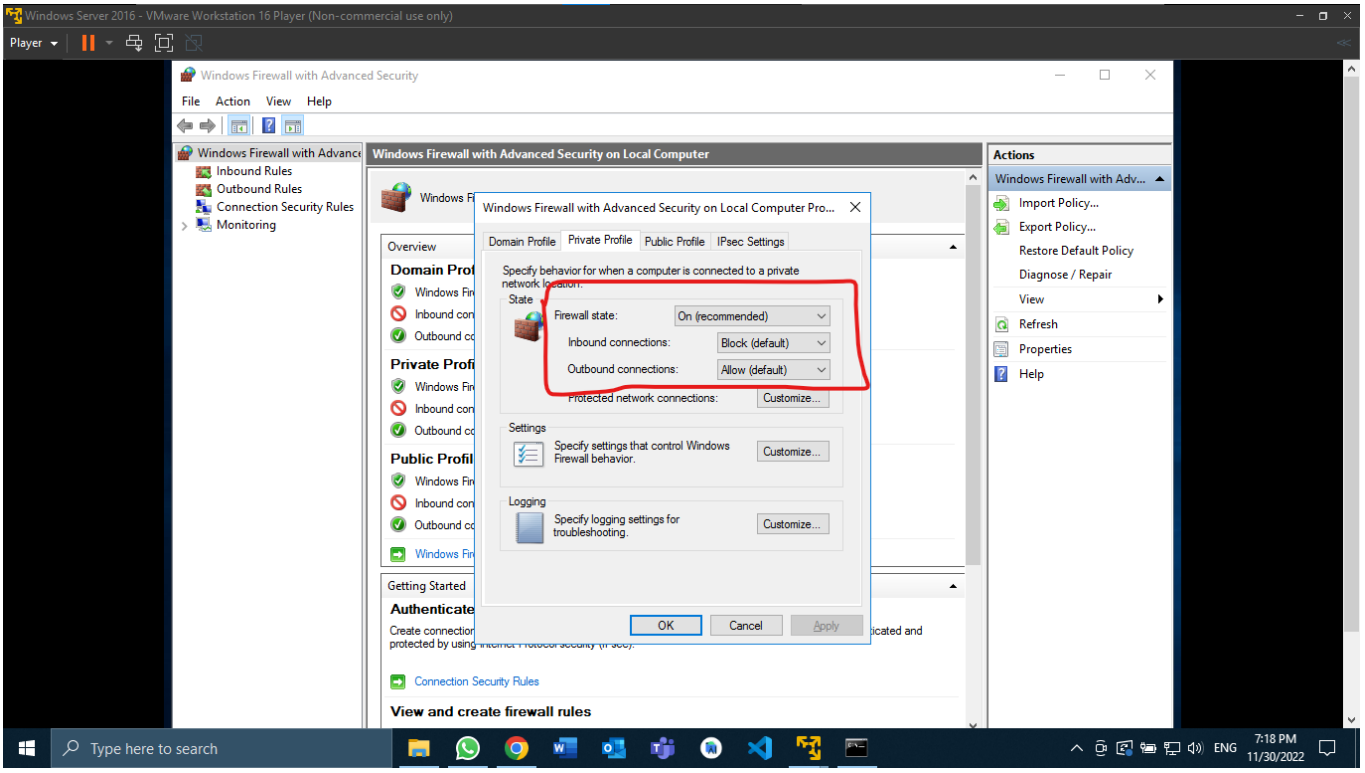
Intense scan of your Kali machine

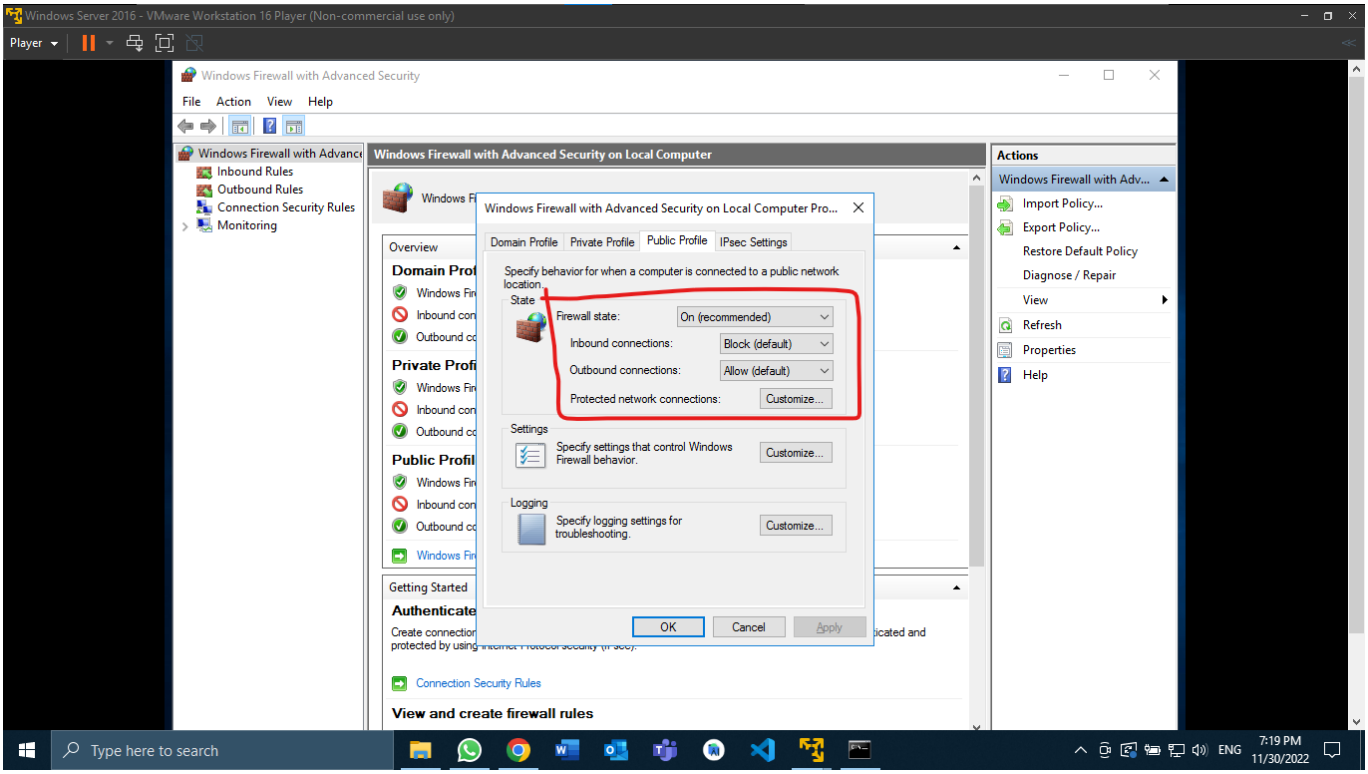




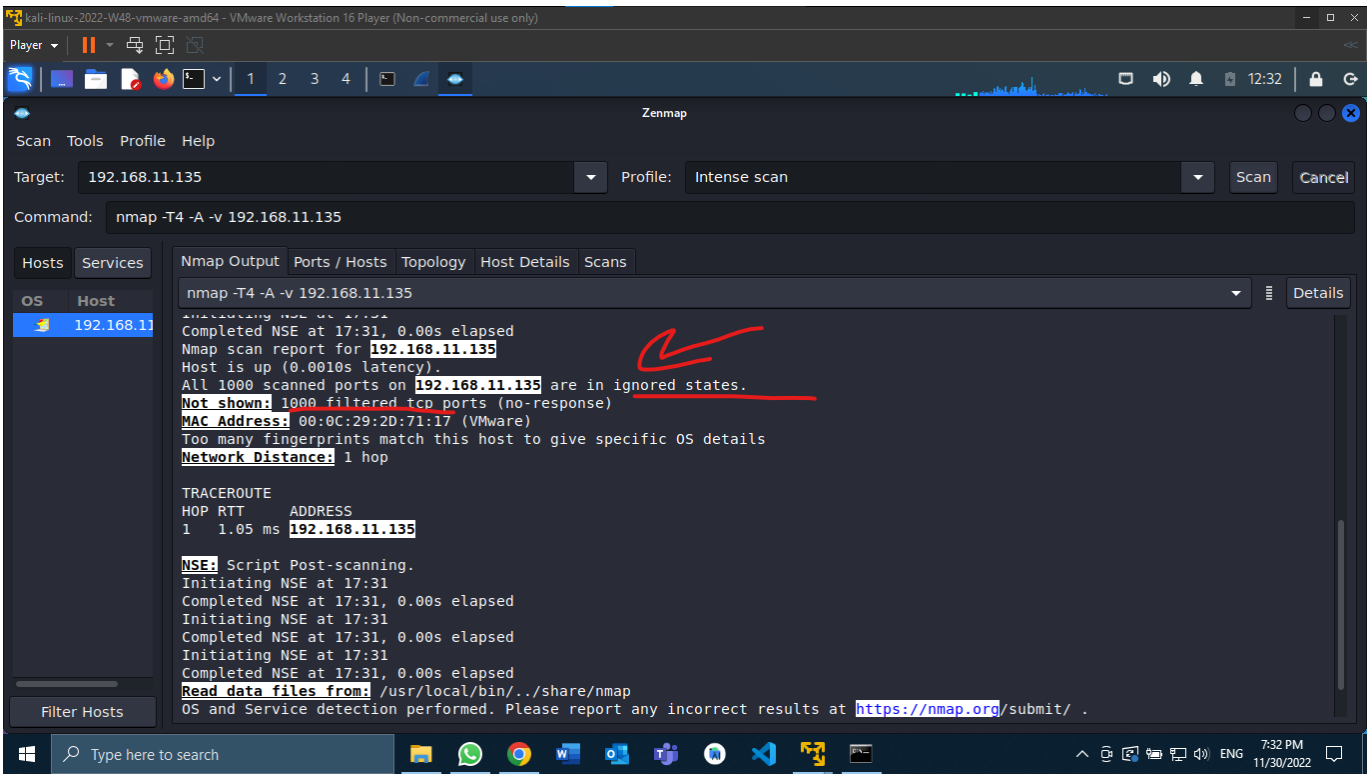
Difference between a protected target and none protected target



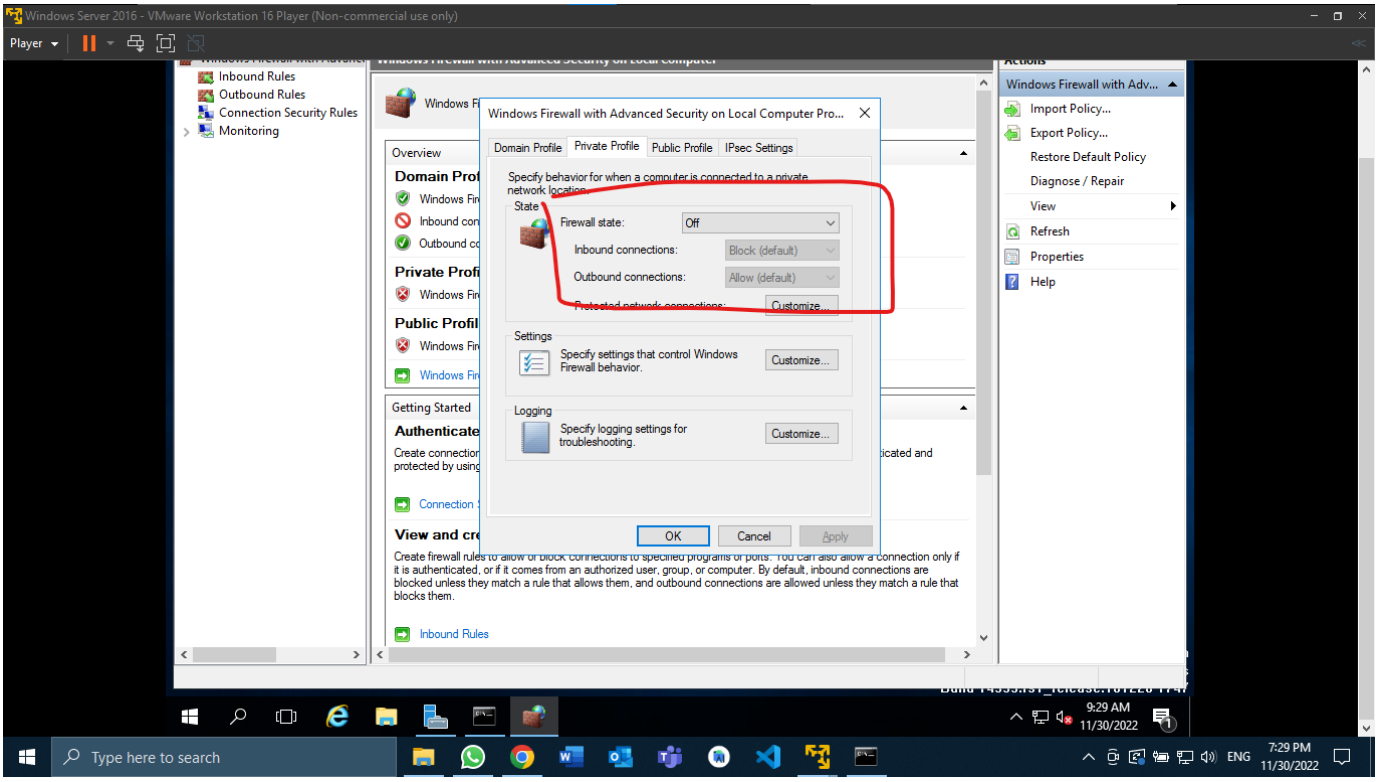


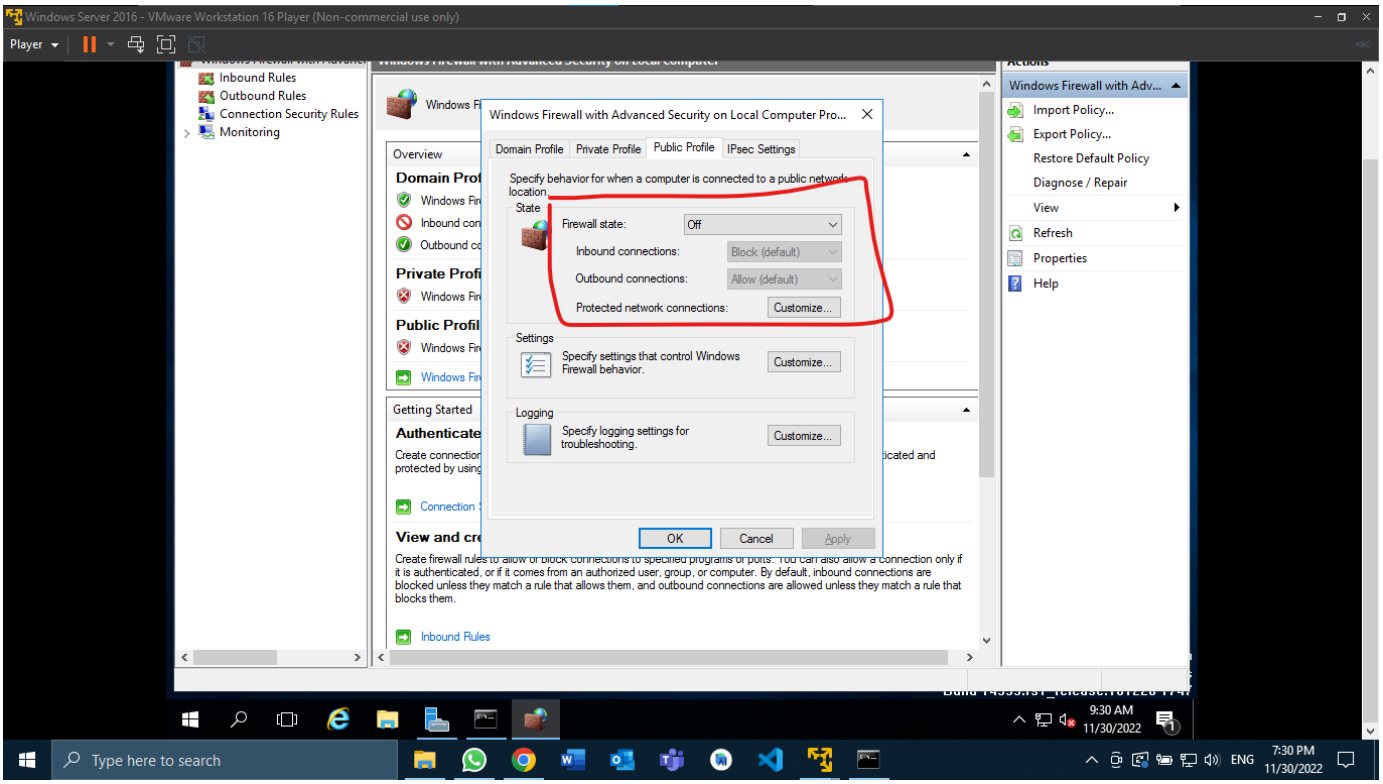


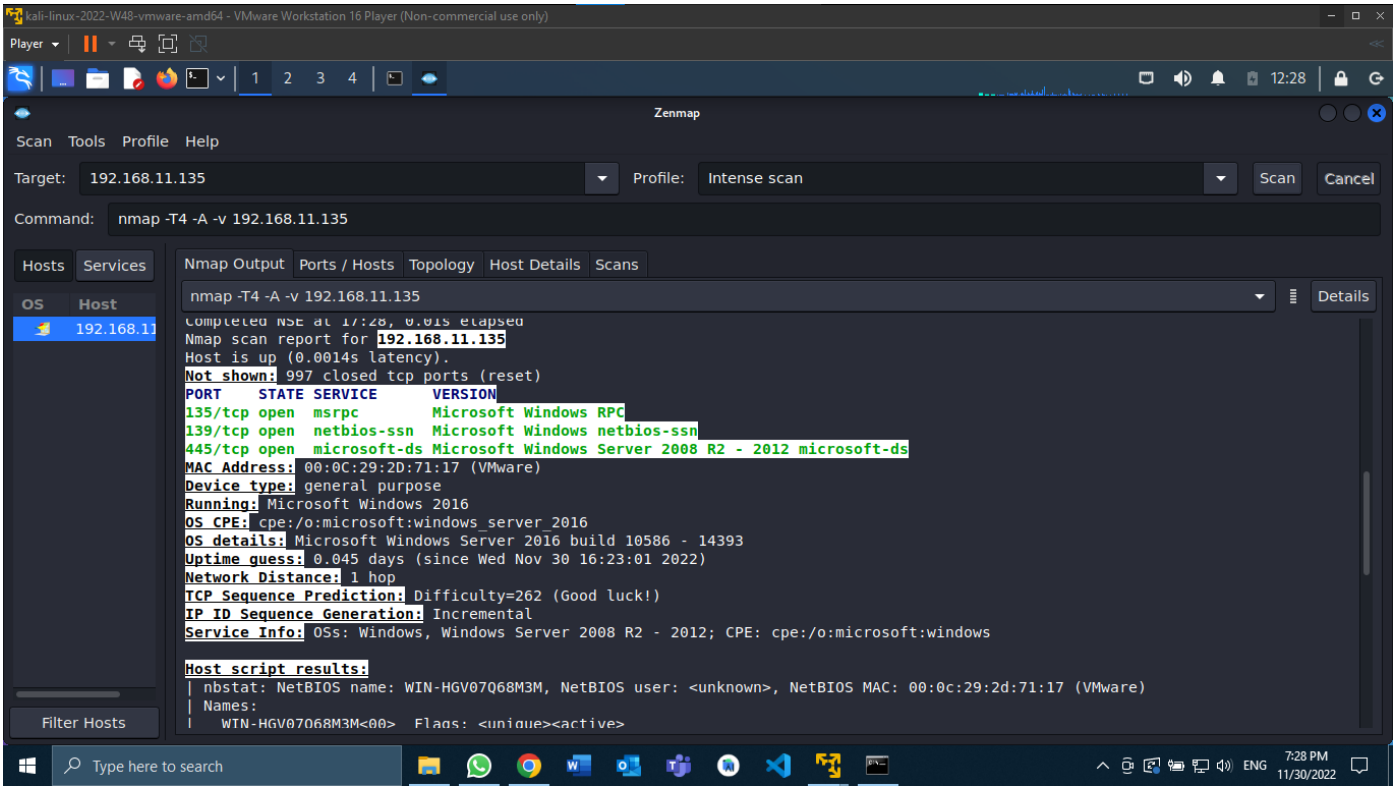
Scanning Your Windows Machine with Incoming Connections Blocked



Scanning My Windows Machine with firewall off

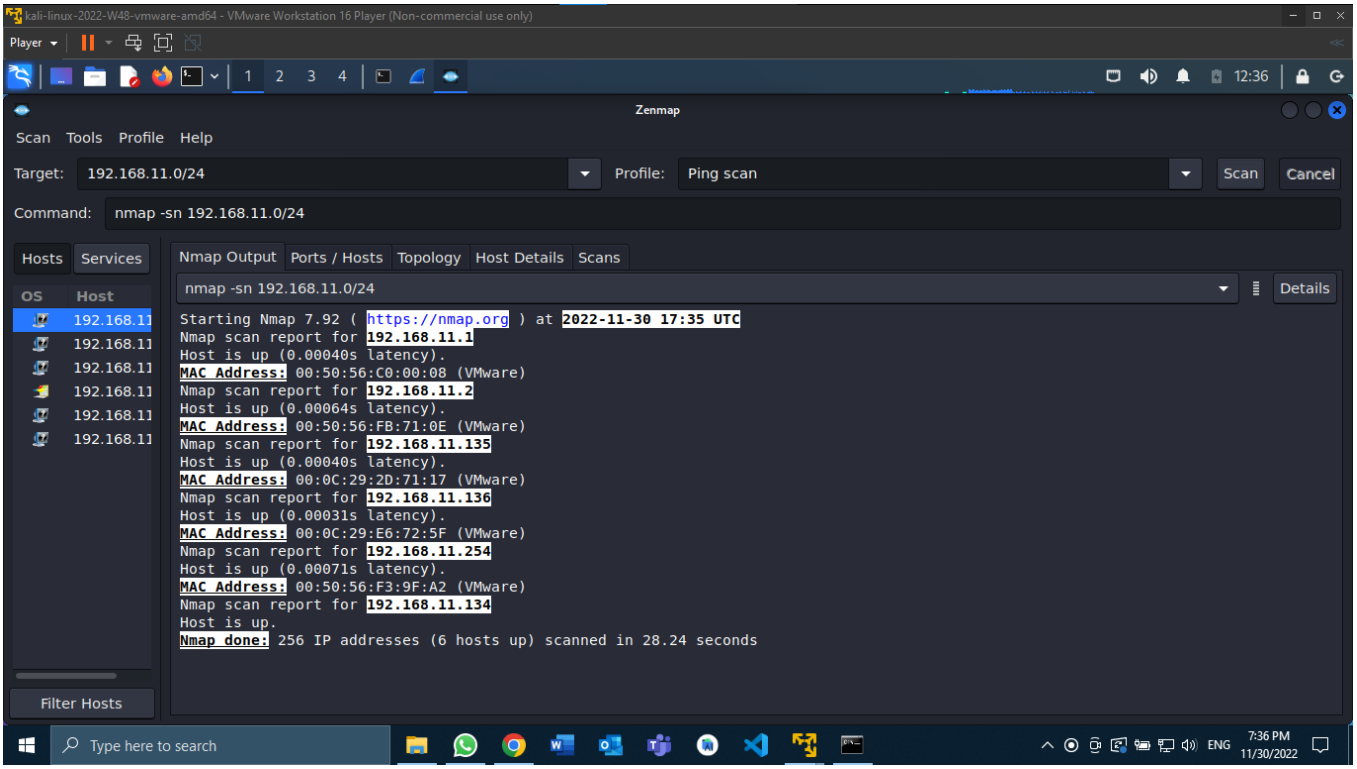




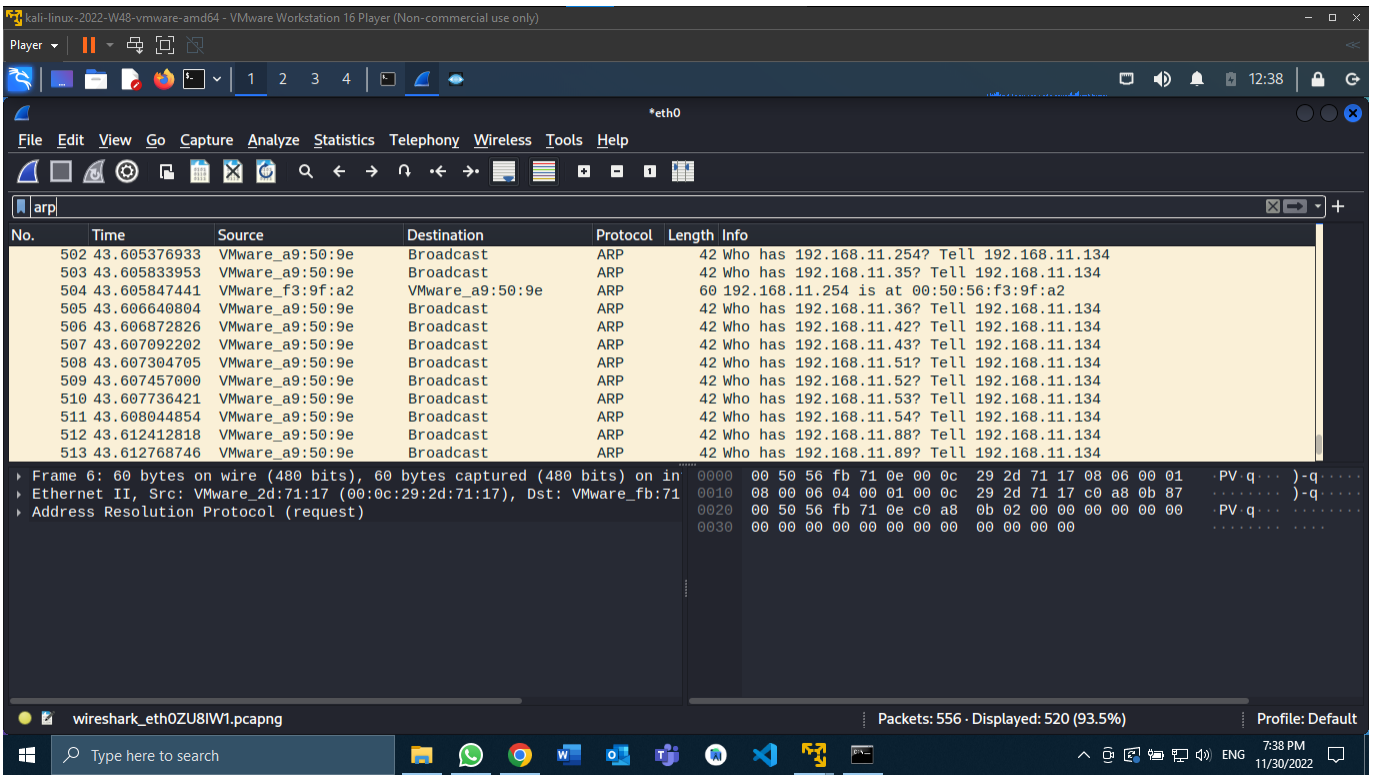

kali-linux-2022-W48-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Zenmap
Scan Tools Profile Help
Target: 192.168.11.135
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.11.135
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
192.168.11
Details
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:
| WIN-HGV07Q68M3M<00> Flags: <unique><active>
Filter Hosts
Type here to search
ENG
7:28 PM
11/30/2022

Analyzing a Port Scan

Performing a Ping Sweep of your Network

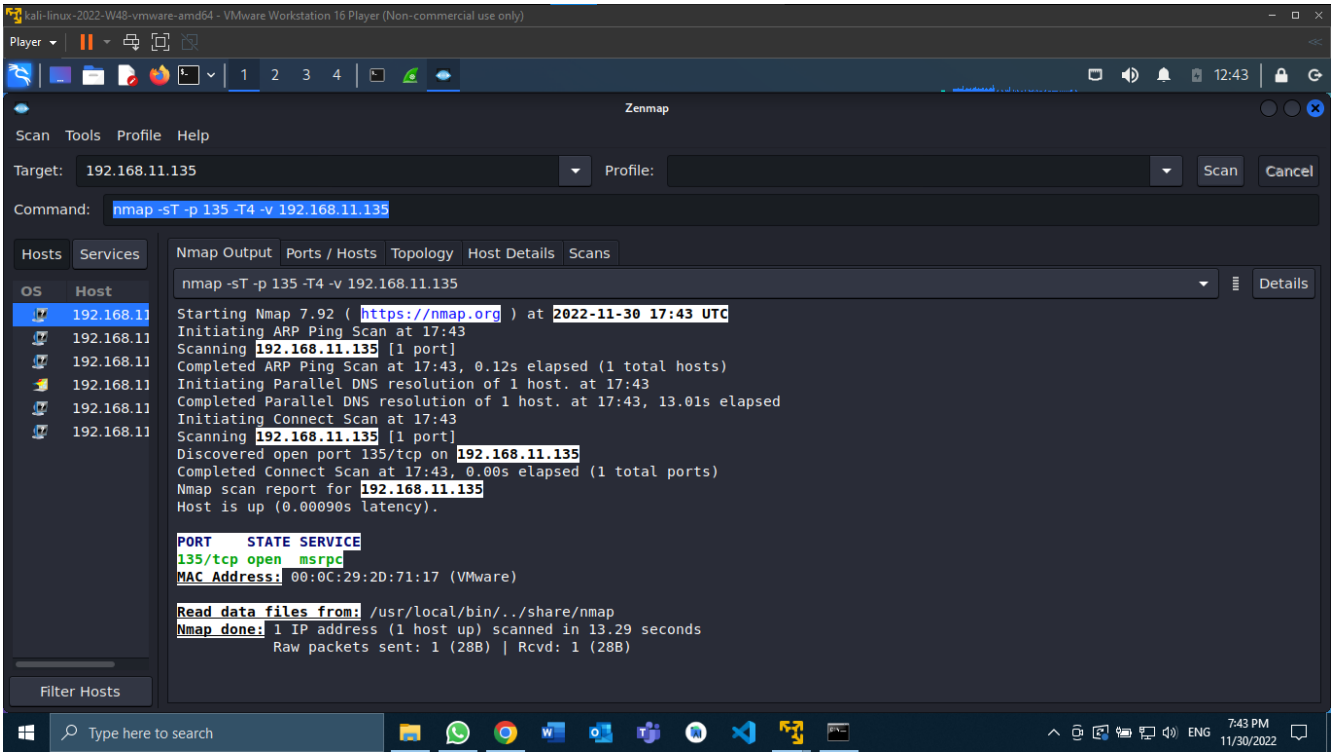


Using Wireshark to Analyze the Ping Sweep



Targeting a specific machine and port

Performing a Connect Scan of Port 135 only



Using Wireshark to Analyze the Connect Scan