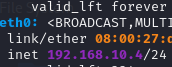
***Requirements before start to run the commands***

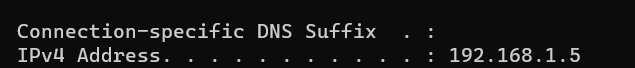
* Execute the command to open Wireshark and start capturing packets on a specific network interface.
* Apply a filter to capture only packets related to a given online IP address.
* Follow a TCP stream using Wireshark and reconstruct the data exchanged between two endpoints.
* Perform a basic Nmap scan on a provided online Demo IP address (demo.testfire.net).
* Analyze the scan results and identify open ports, services, and vulnerabilities.
* Visit A-Packets.com and upload a PCAP file for analysis.
* Extract transferred files and view details of IPv4, HTTP, Telnet, FTP, DNS, SSDP, and WPA2 protocols.

1. ***Take the screenshot of IP address of windows and Kali.***

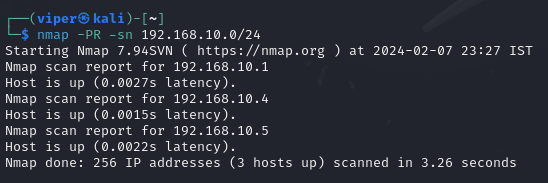
**Kali IP:**

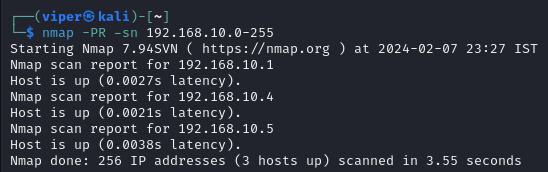
****

**Windows IP:**

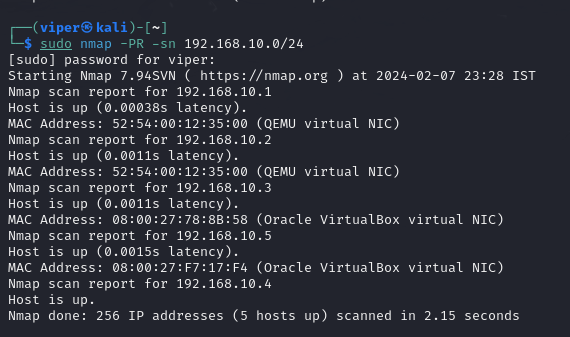
****

1. ***Execute the nmap command to perform a layer 2 host discovery on a specific IP address range.***

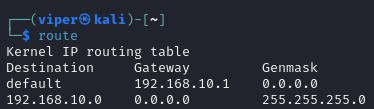
******

******

1. ***Use the sudo nmap command for layer 2 host discovery on a specified network.***

******

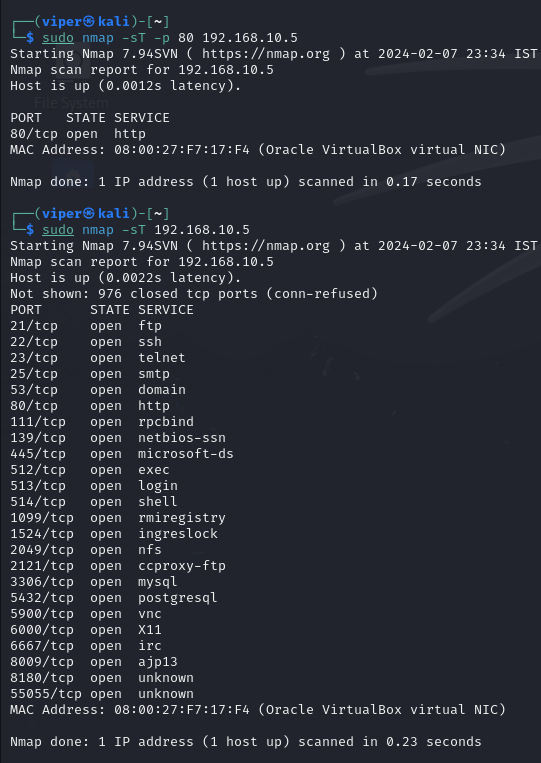
1. ***Execute the 'route' command to display routing information.***

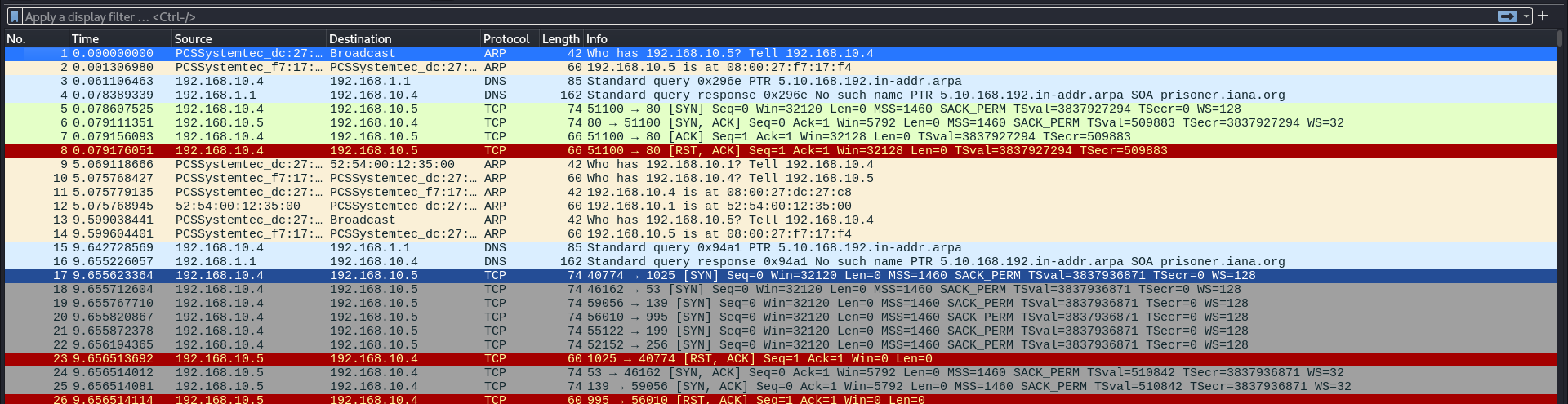
******

1. ***Use the 'ifconfig' command to view network interface configuration details.***

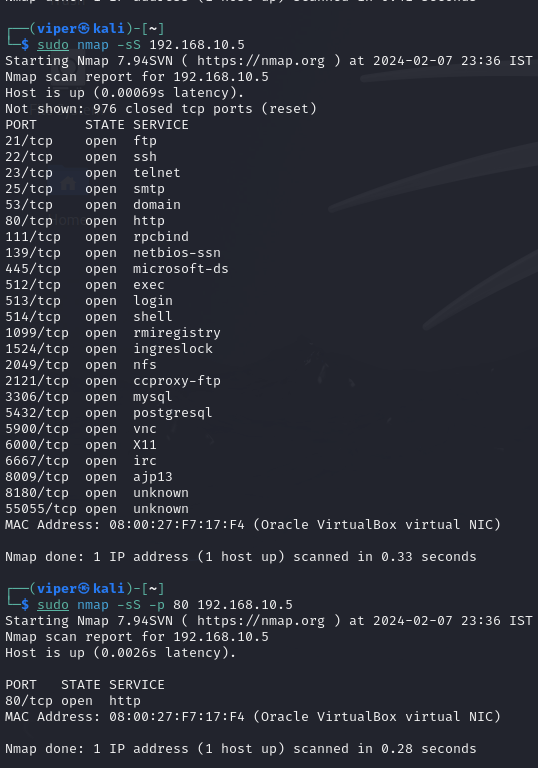
******

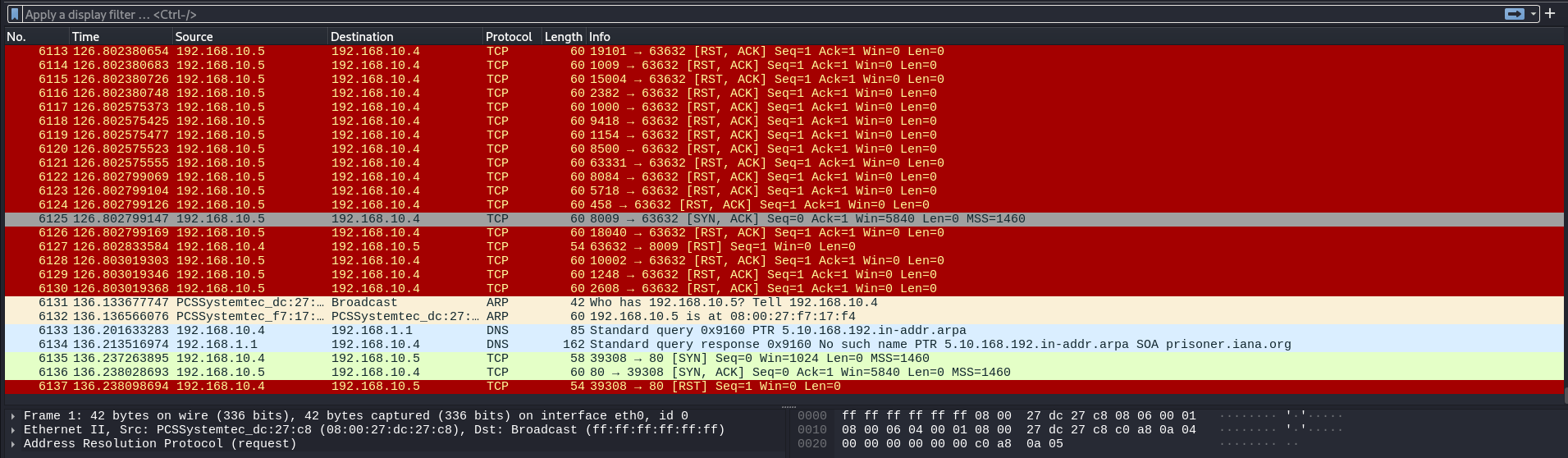
1. ***Capture packets using Wireshark while performing a TCP Connect Scan (-sT) with Nmap.***

******

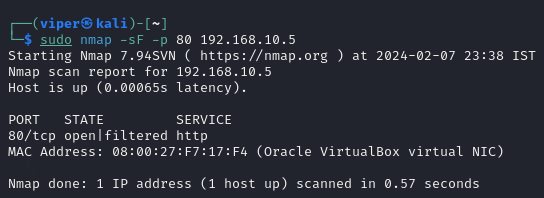
******

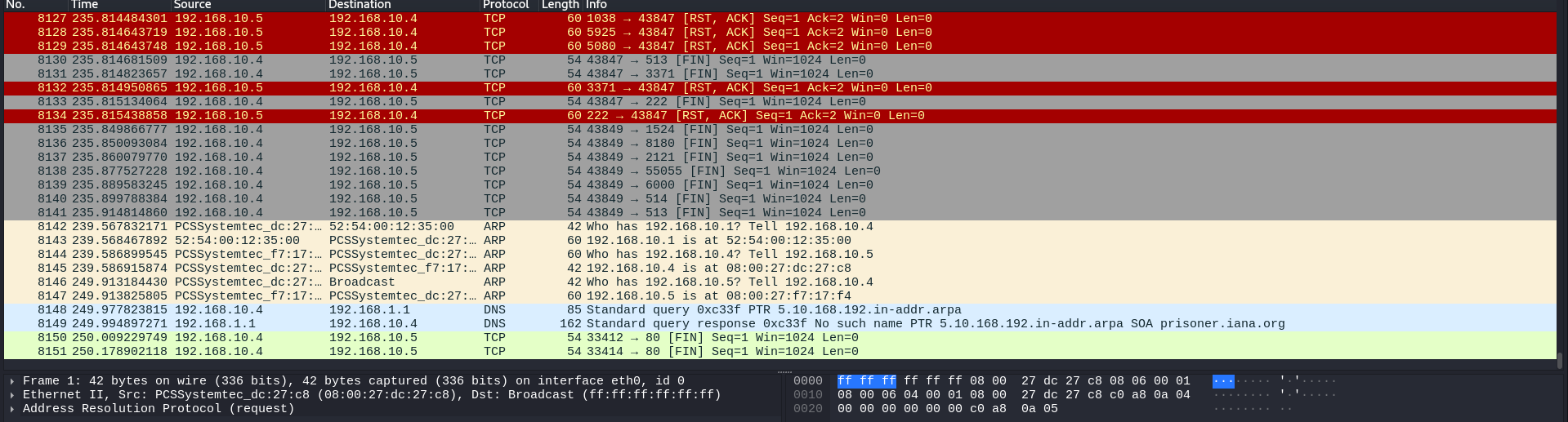
1. ***Analyze Wireshark results for a TCP SYN (Stealth) Scan (-sS) conducted by Nmap.***

******

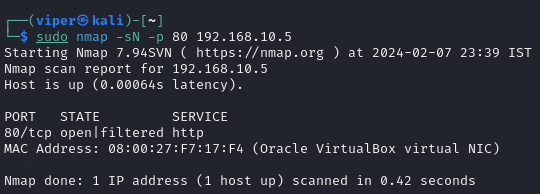
******

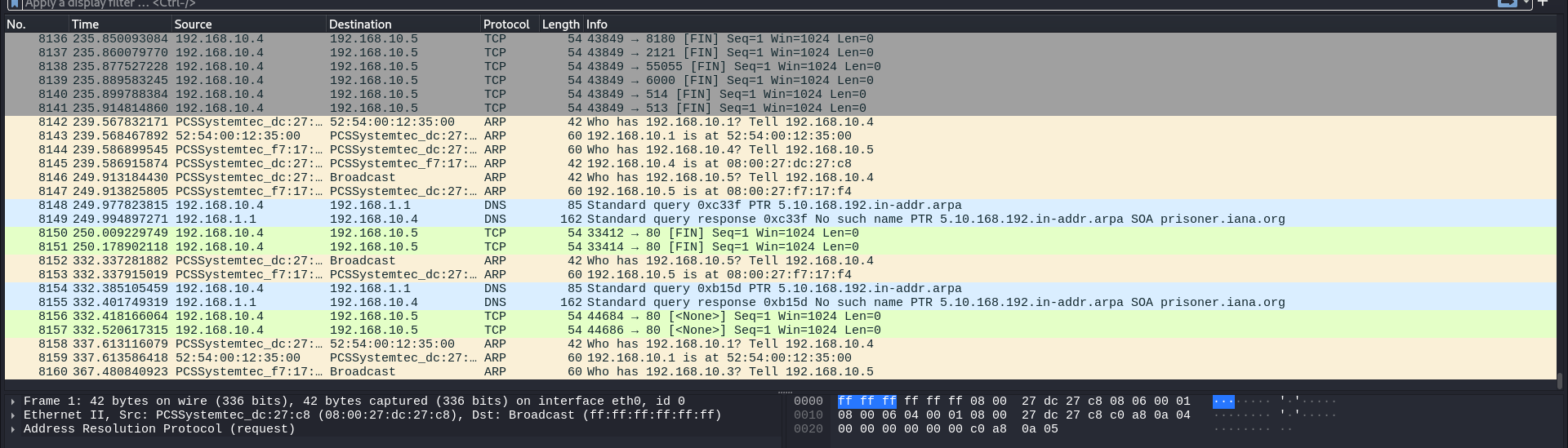
1. ***Perform a TCP FIN Scan (-sF) on a target IP address and analyze the captured packets in Wireshark.***

******

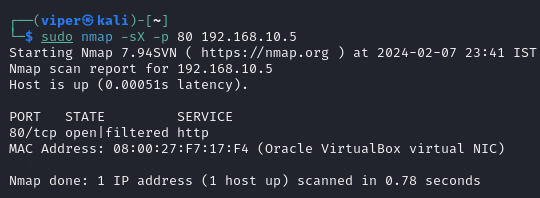
******

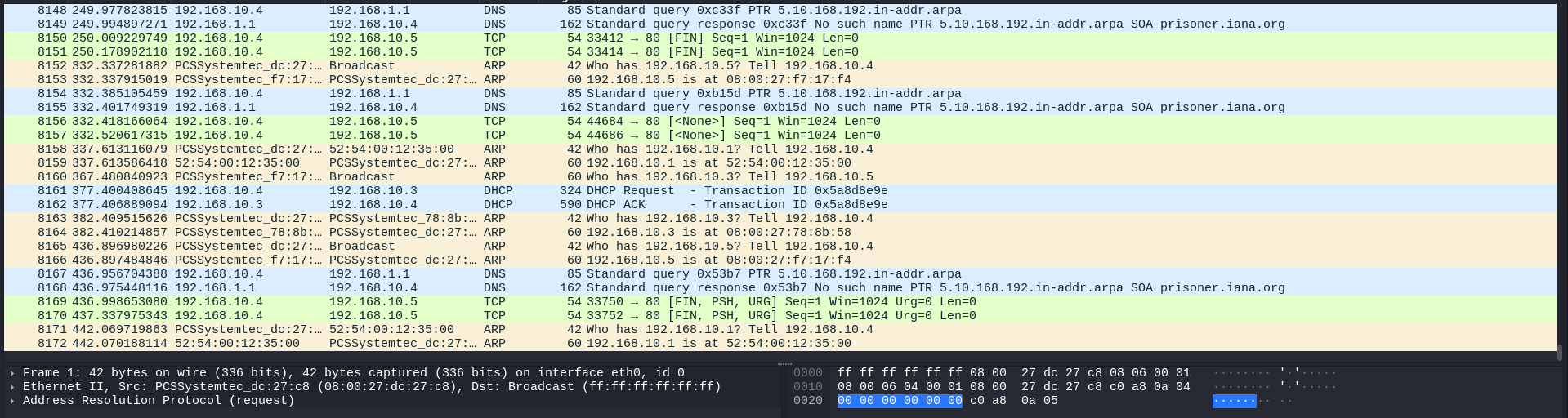
1. ***Execute a TCP Null Scan (-sN) using Nmap and observe the Wireshark analysis.***

******

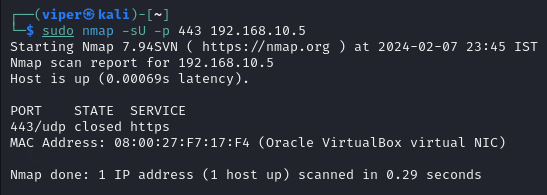
******

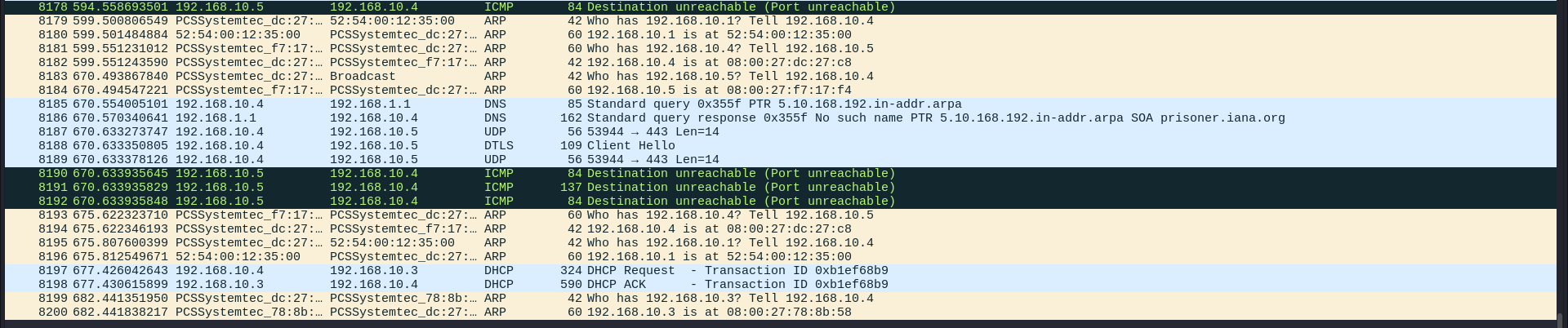
1. ***Conduct a TCP XMAS Scan (-sX) with Nmap and inspect the corresponding Wireshark data.***

******

******

1. ***Perform a UDP Scan (-sU) on a specified port of a target IP address using Nmap.***

******

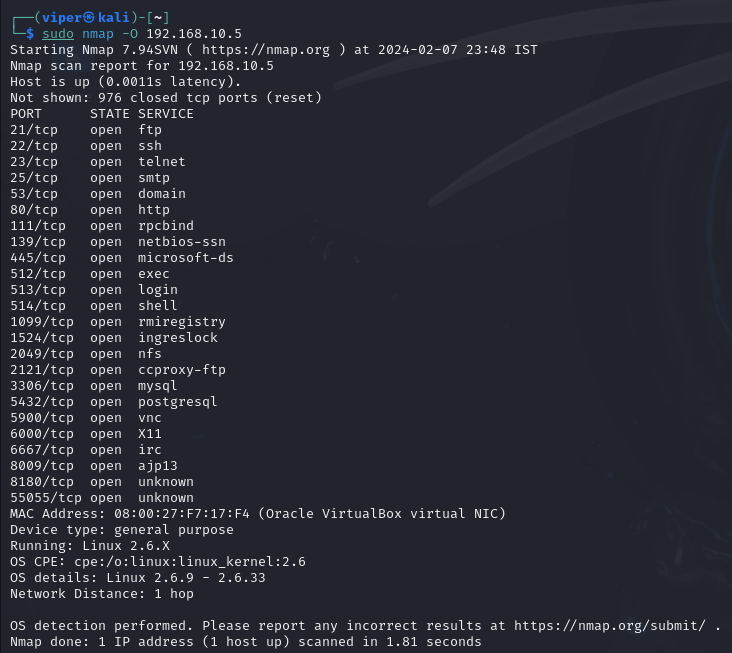
******

1. ***Examine the Wireshark capture to identify UDP scan results.***

**Destination Unreachable**

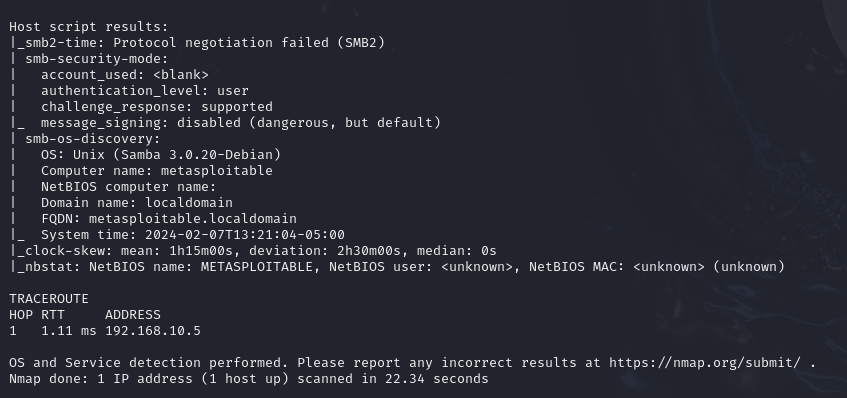
**Port 443 closed**

1. ***Use Nmap to perform operating system detection on a given target.***

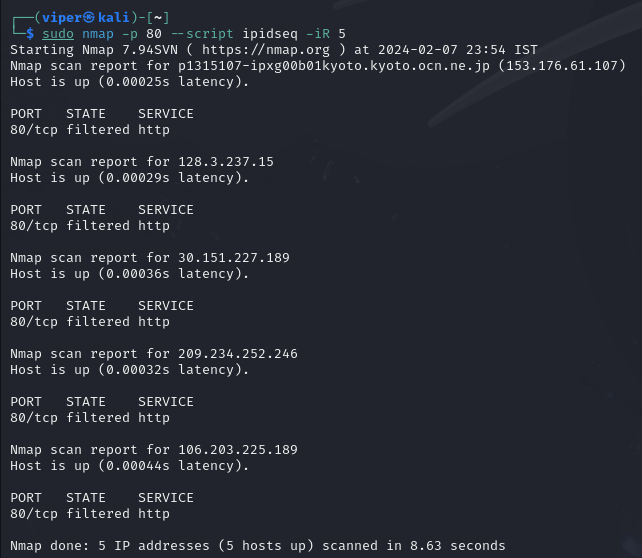
******

1. ***Execute an aggressive scan (nmap -A) with Nmap, including OS detection.***

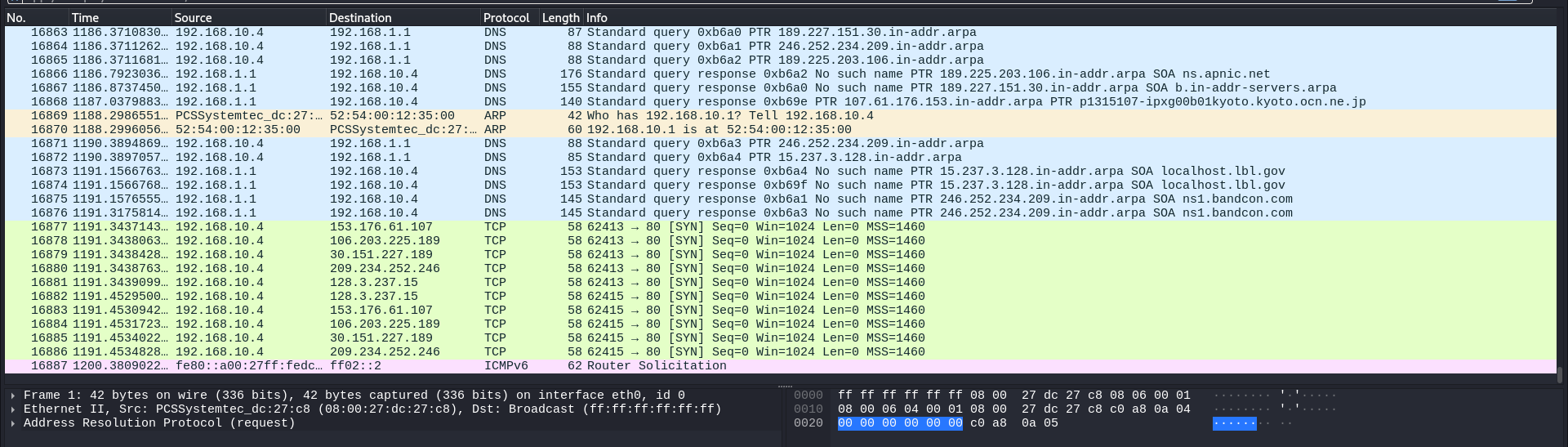
******

******

1. ***Discover a zombie or idle machine for use in an idle scan.***

******

1. ***Perform an idle scan using Nmap and interpret the results.***

******

Analyzing online IP addresses using Wireshark and Nmap, with a specific mention of A-Packets.com. Below is a general outline of steps you can take for this lab objective. Please note that you should have the necessary **permission to perform network scanning and analysis,** and it's crucial to comply with ethical and legal considerations.

**Introduction**

**1. Wireshark Analysis**

Wireshark is a network protocol analyzer that allows you to capture and inspect the data traveling back and forth on a network in real-time. In this case, you can use Wireshark to capture packets related to the online IP address you are investigating.

* **Capture Packets:** Open Wireshark and start capturing packets on the network interface through which the traffic passes. You may want to use filters to narrow down the captured packets to those related to the specific IP address.
* **Analyze Packets:** Look for interesting patterns, protocols, or any suspicious activities in the captured packets. You can filter the packets based on source or destination IP address to focus on the communication involving the online IP address.
* **Follow TCP Streams:** Wireshark allows you to follow TCP streams to reconstruct the data exchanged between two endpoints. This can be useful in understanding the content of the communication.

**2. Nmap Analysis**

Nmap is a powerful open-source network scanning tool that can be used to discover hosts and services on a computer network, thus creating a "map" of the network.

* **Scan the Online IP Address:** Use Nmap to perform a scan on the online IP address. The specific command might look like: nmap [target IP]
* **Analyze Scan Results:** Review the Nmap scan results to identify open ports, services running, and other relevant information about the target system. Pay attention to any vulnerabilities that may be reported.

**3. A-Packets.com**

* Effortless PCAP File Analysis in Your Browser. Read and view PCAP files online. Discover the details of IPv4/IPv6, HTTP, Telnet, FTP, DNS, SSDP, and WPA2 protocols effortlessly. Build an interactive map of your network structure and visualize node communications. Sniff and analyze network traffic and other PCAP data with ease.
* Analyze PCAP files to gain insights into HTTP headers, request and response data. Effortlessly extract transferred files, office documents, and images. Find passwords for various protocols.

**Important Considerations**

* Always ensure you have the proper authorization to perform network scanning and analysis, especially on systems you don't own.
* Be aware of the legal and ethical implications of your actions. Unauthorized scanning or monitoring can lead to serious consequences.
* Respect the privacy and security of others during your analysis.

|  |
| --- |
| 1. Layer 2 Host Discovery Commands  - nmap -PR -sn <ip address>  - nmap -PR -sn 191.168.10.0/24  - nmap -PR -sn 191.168.10.0-255  - sudo nmap -PR -sn 191.168.10.0-255  - sudo nmap -PR -sn 191.168.10.0/24  2. Network Verification Commands  - route  - ifconfig  3. Wireshark Analysis of Various Nmap Scans    - TCP Connect Scan (-sT)  - nmap -sT -p <port number> <destination IP>  - TCP SYN (Stealth) Scan (-sS)  - nmap -sS -p <port number> <destination IP>    - TCP FIN Scan (-sF)  - nmap -sF -p <port number> <destination IP>  - TCP Null Scan (-sN)  - nmap -sN -p <port number> <destination IP>    - TCP XMAS Scan (-sX)  - nmap -sX -p <port number> <destination IP>    - UDP Scan (-sU)  - nmap -sU -p <port number> <destination IP>  4. Operating System Detection  - nmap -O <target>  - nmap --osscan-guess <target>  - nmap -A <target> (Aggressive scan including OS detection)  5. Idle Scan / Zombie Scan Commands  - Finding Zombie/Idle Machine  - nmap -p<port scan> --script ipidseq -iR <range>  Example: `nmap -p80 --script ipidseq -iR 10 |
|  |