***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. ***What does DVWA stand for?***

**Damn Vulnerable Web Application**

1. ***Take the screenshot of IP address of window, Metasploit2 and Kali.***

**Windows IP:**

******

**Kali IP:**

******

**Metasploitable IP:**

******

1. ***What is the purpose of DVWA?***

**The main purpose of this pentesting playground is to help penetration testers and security professionals to test their skills and tools.**

1. ***Why is DVWA used in the field of cybersecurity?***

**It is widely recommended for practicing web application security testing. It is designed to provide a safe and legal environment where we can learn and enhance our skills in identifying and exploiting vulnerabilities commonly found in web applications.**

1. ***How do you install DVWA on a local server for testing purposes?***

* **Install LAMP Stack**
* **Install PHP and PHP Modules**
* **Configure MySQL**
* **Download DVWA**
* **Configure DVWA**
* **Set Permissions**
* **Set Up Apache**
* **Access DVWA**

**OR**

**You can simply install metasploitable 2 which is a setup using virtual box and access through kali browser.**

1. ***What are the prerequisites for setting up DVWA?***

* **Kali Linux**
* **LAMP Stack:**
* **Apache**
* **MySQL**
* **PHP**
* **Network Configuration**
* **Permissions**
* **Browser**

**OR**

* **Kali Linux**
* **Metasploitable 2**
* **Browser**

1. ***Can you briefly describe the configuration steps needed after installing DVWA?***

**Kali Linux: Ensure you have Kali Linux installed on your system. DVWA can be installed on Kali Linux for testing and practicing web application security.**

**LAMP Stack:**

**Apache: Kali Linux usually comes with Apache pre-installed. If not, you can install it using sudo apt install apache2.**

**MySQL: Install MySQL server using sudo apt install mysql-server.**

**PHP: Install PHP and required PHP modules using sudo apt install php libapache2**

**mod-php php-mysql.**

**Database Configuration: Set up a MySQL database for DVWA. Create a database,**

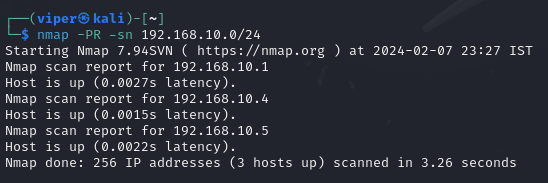
**user, and grant privileges to the user within MySQL.**

**Network Configuration: Configure your network settings to allow access to DVWA from other devices on the network if needed.**

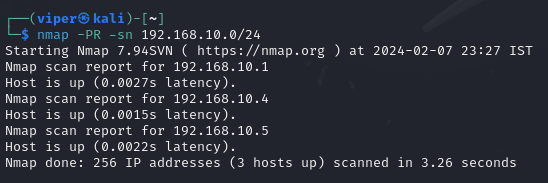
**Permissions: Ensure that the web server has the necessary permissions to access and write to the DVWA directory and its files. You may need to adjust permissions using chown and chmod commands.**

**Browser: You'll need a web browser to access the DVWA web interface for setup and testing. Any modern web browser should work fine.**

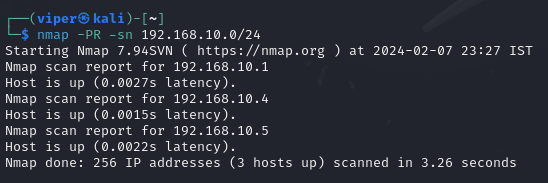
1. ***Use the appropriate nmap command to perform a Layer 2 Host Discovery on the given IP address (replace `<ip address>` with an actual IP).***

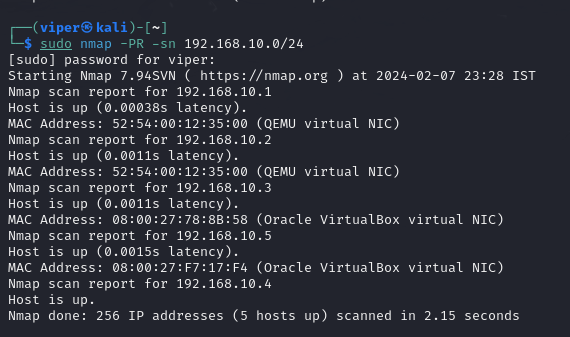
******

1. ***Execute the nmap command to perform Layer 2 Host Discovery on the entire subnet `191.168.10.0/24`.***

******

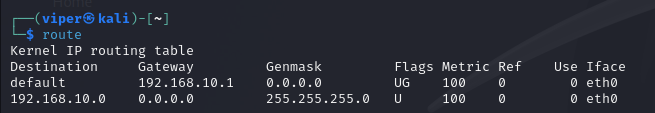
1. ***Try different nmap commands for Layer 2 Host Discovery, including both sudo and non-sudo variations. Observe and note any differences in the results.***

******

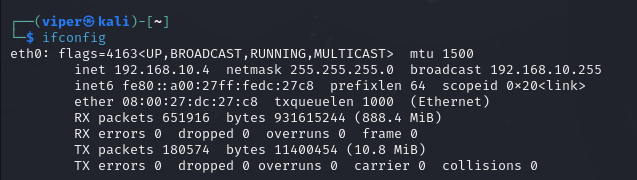
******

**It shows the MAC Address also and machine on which it is running**

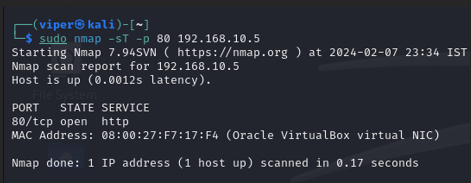
1. ***Utilize the 'route' command to display the routing table. Note down the information related to network routes.***

******

1. ***Use the 'ifconfig' command to retrieve information about network interfaces. Identify the IP address, MAC address, and other relevant details.***

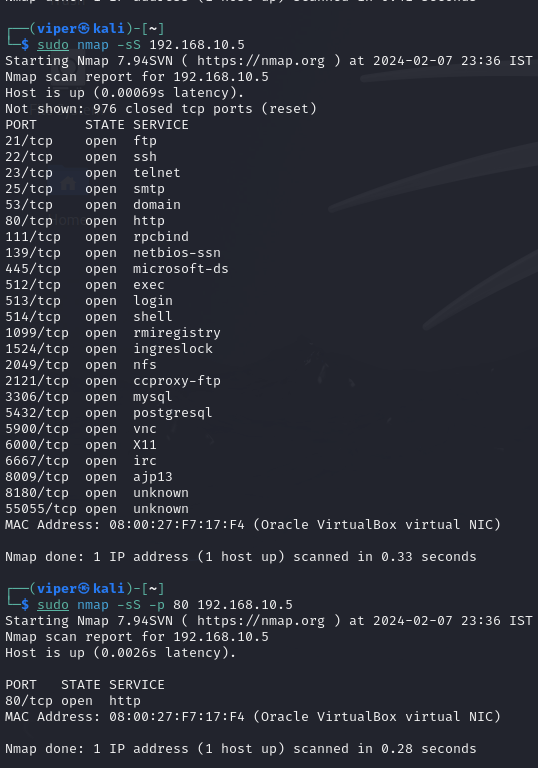
******

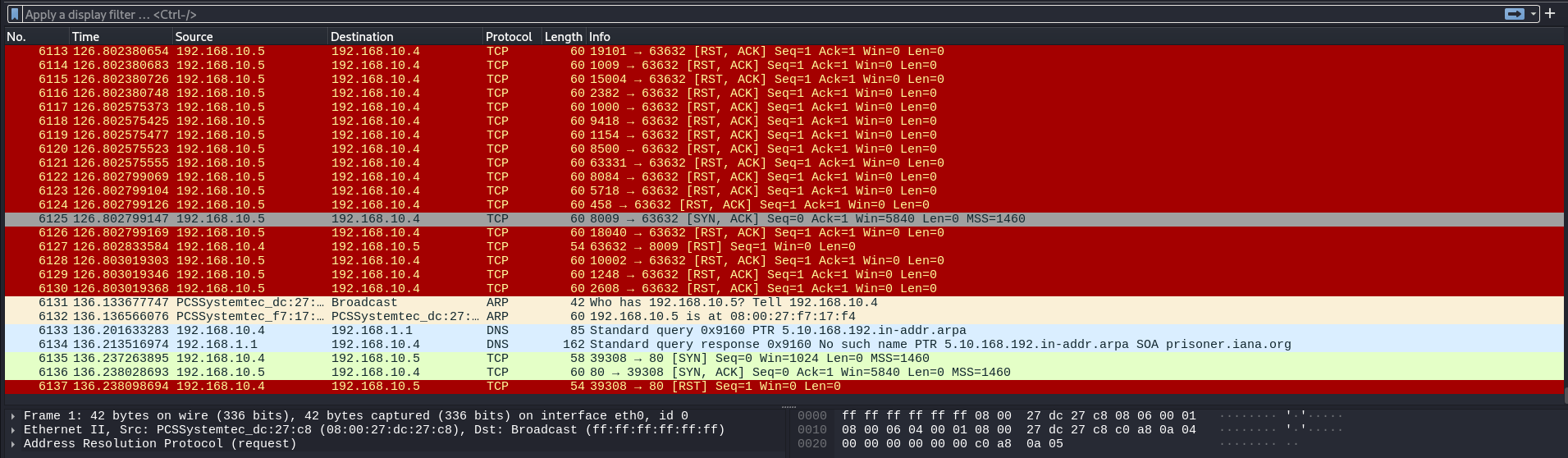
1. ***Perform a TCP Connect Scan (-sT) on a specified port and IP address using the provided nmap command.***

******

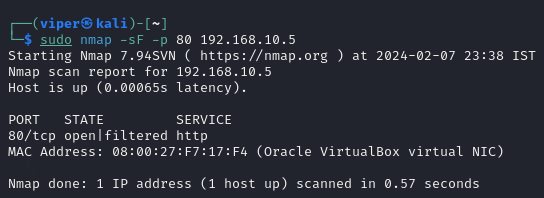
1. ***Repeat the process for TCP SYN (Stealth) Scan (-sS), TCP FIN Scan (-sF), TCP Null Scan (-sN), TCP XMAS Scan (-sX), and UDP Scan (-sU). Document any differences in the packet structure and behavior.***

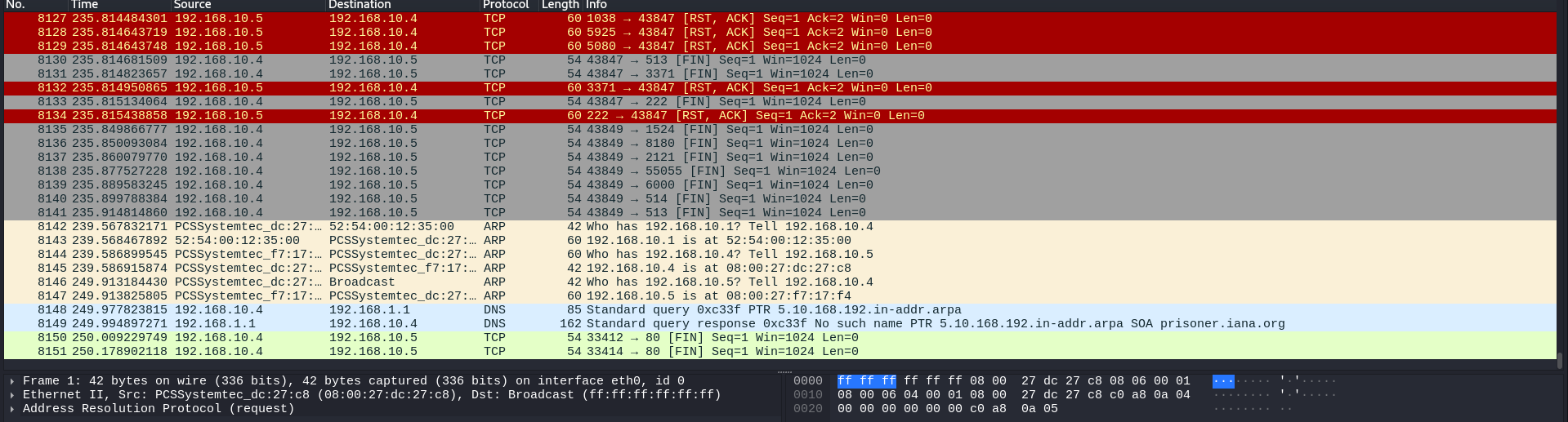
* **The SYN scan sends a TCP packet with the SYN flag set and no further flags. It's called a "stealth" scan because it tries to avoid detection by not completing the full TCP handshake.**

******

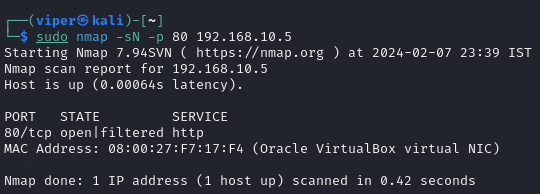
******

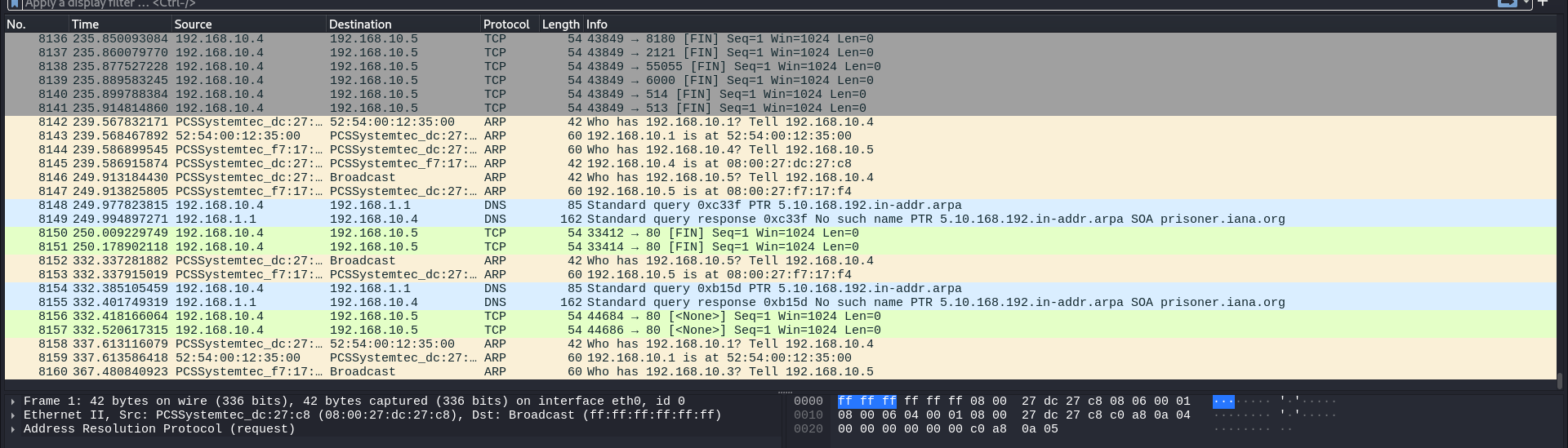
* **This scan sends a TCP packet with only the FIN flag set.It's used to determine whether ports are closed or filtered (firewalled). If a port is open, it should ignore the FIN packet and not respond. If it's closed, it should respond with a RST packet.**

******

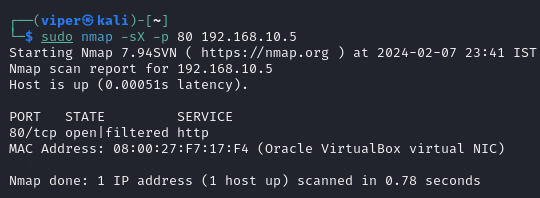
******

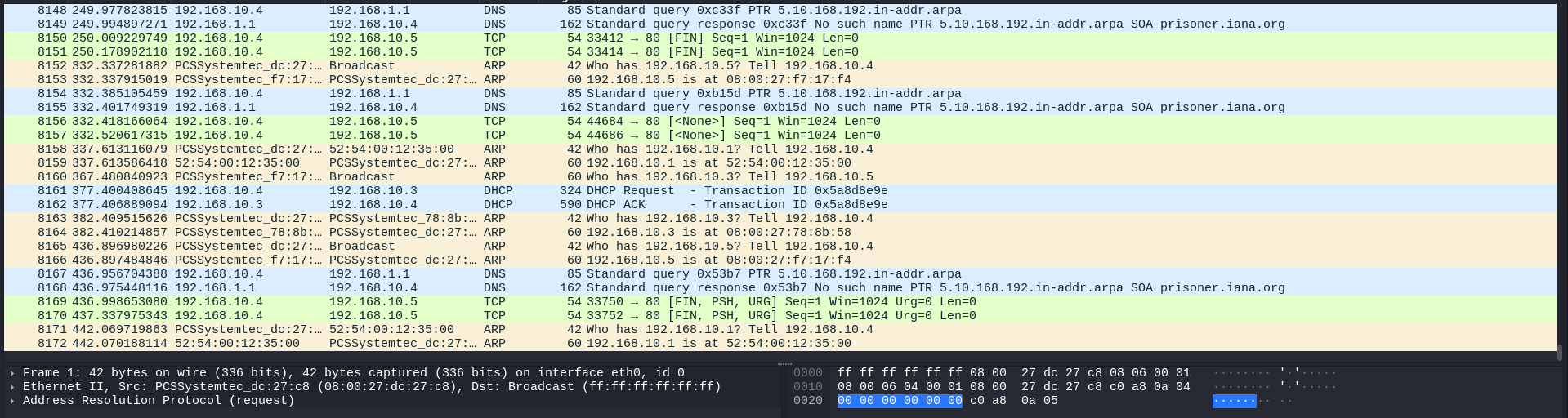
* **Similar to the FIN scan, it sends a TCP packet with no flags set.** **It relies on the behavior of some systems that respond to a TCP packet with no flags set. If a port is open, it typically doesn't respond. If it's closed, it usually responds with a RST packet.**

******

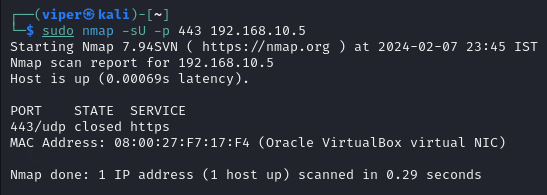
******

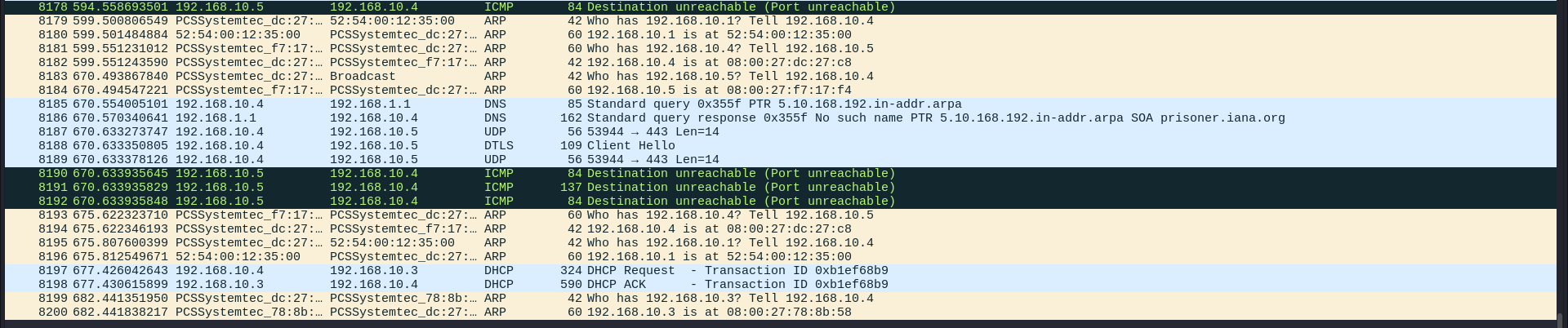
* **This scan sets the FIN, URG, and PSH flags in the TCP packet.It's similar to the FIN scan but may behave differently on certain systems. If a port is open, it might not respond. If it's closed, it may respond with a RST packet.**

******

******

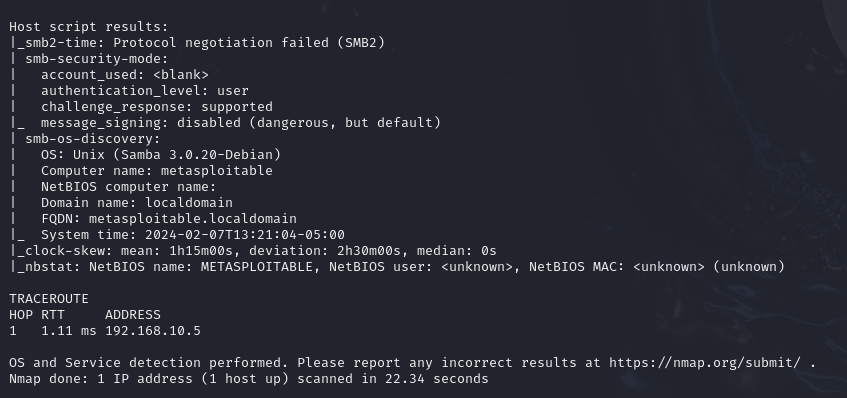
* **UDP scans send UDP packets to various ports.Unlike TCP scans, UDP is a connectionless protocol, so there's no handshake. This makes UDP scans less reliable. If a port is open, it might respond with a UDP packet. If it's closed, it may respond with an ICMP port unreachable message.**

******

******

1. ***Analyze the output for detailed OS information.***

******

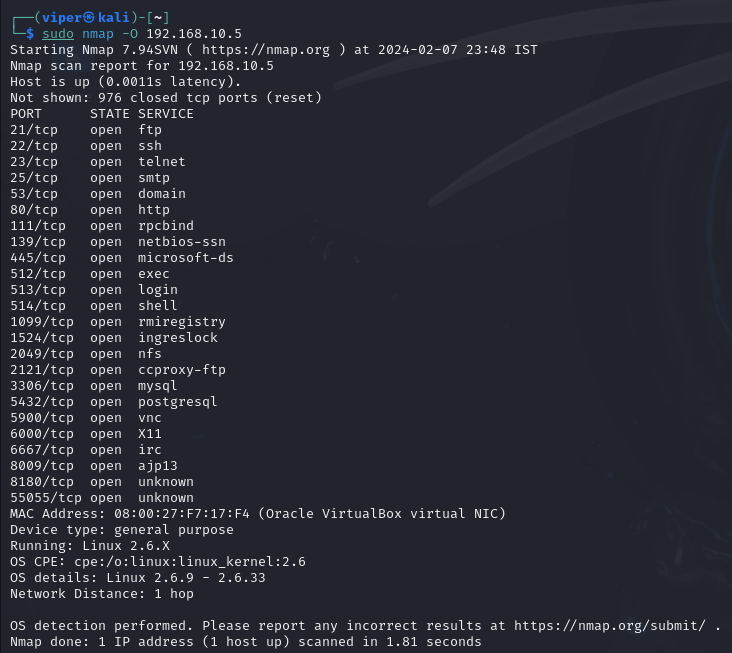
******

**Open ports, services running on that port, version**

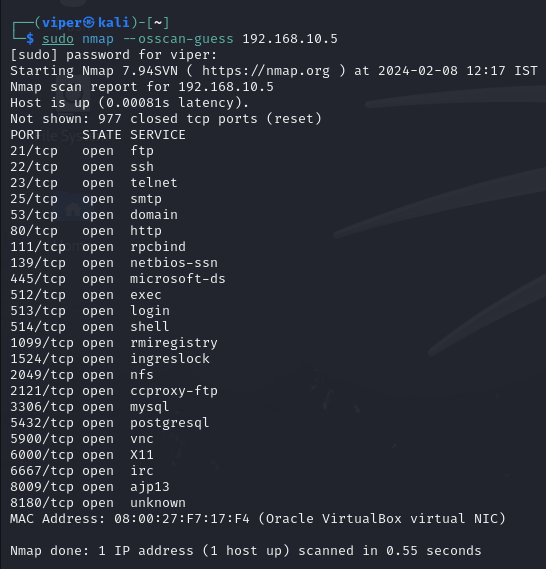
**OS discovery i.e. Unix(Samba 3.0.20-Debian)**

**Computer name - Metasploitable**

1. ***Execute the nmap command to perform basic Operating System Detection on a target machine.***

******

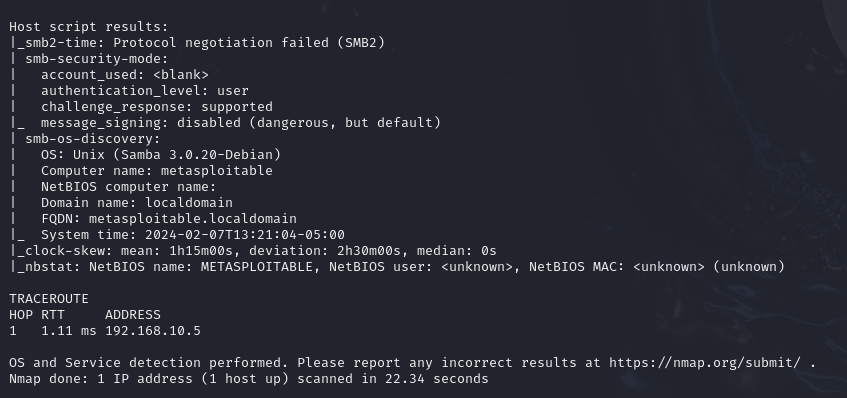
1. ***Use the `--osscan-guess` option with nmap for another scan and compare the results with the basic OS detection.***

******

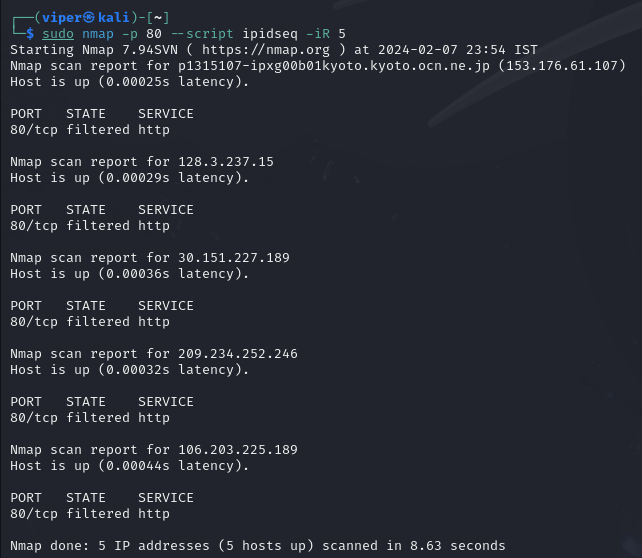
**The –osscan-guess command does not gives the OS details whereas the basic scan gives the OS details**

1. ***Perform an Aggressive Scan, including OS detection, using the command `nmap -A <target>`.***

******

******

1. ***Find a suitable Zombie or Idle machine using the provided nmap command. Document the process and results.***

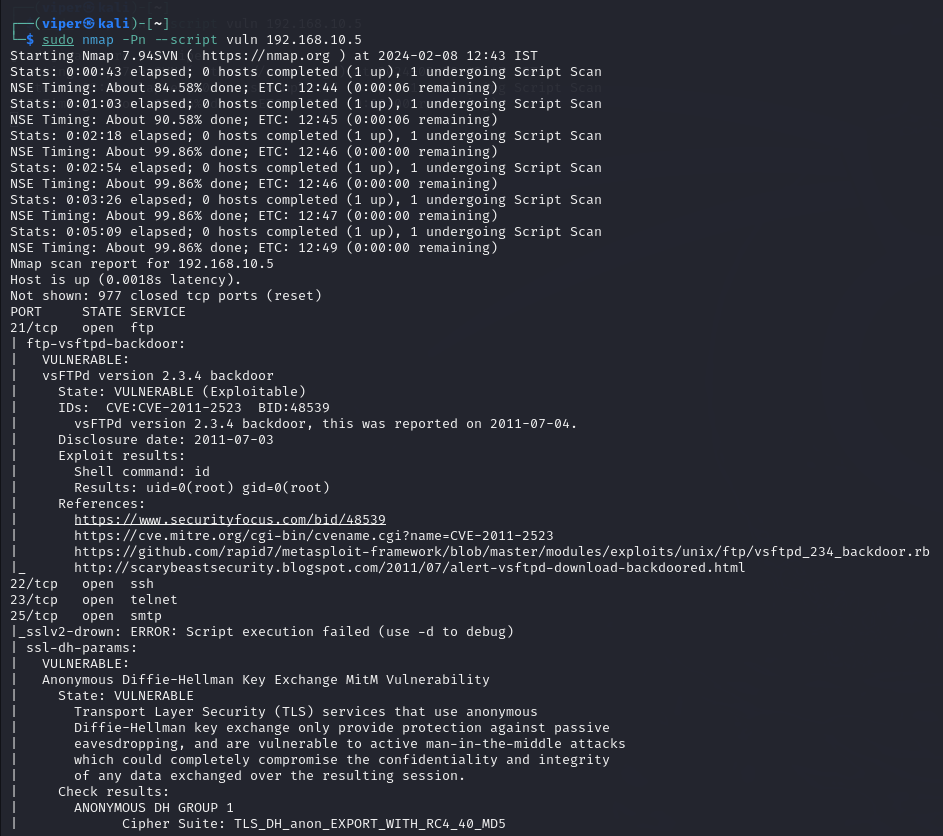
******

**Command – sudo nmap -p 80 –script ipidseq -iR 5**

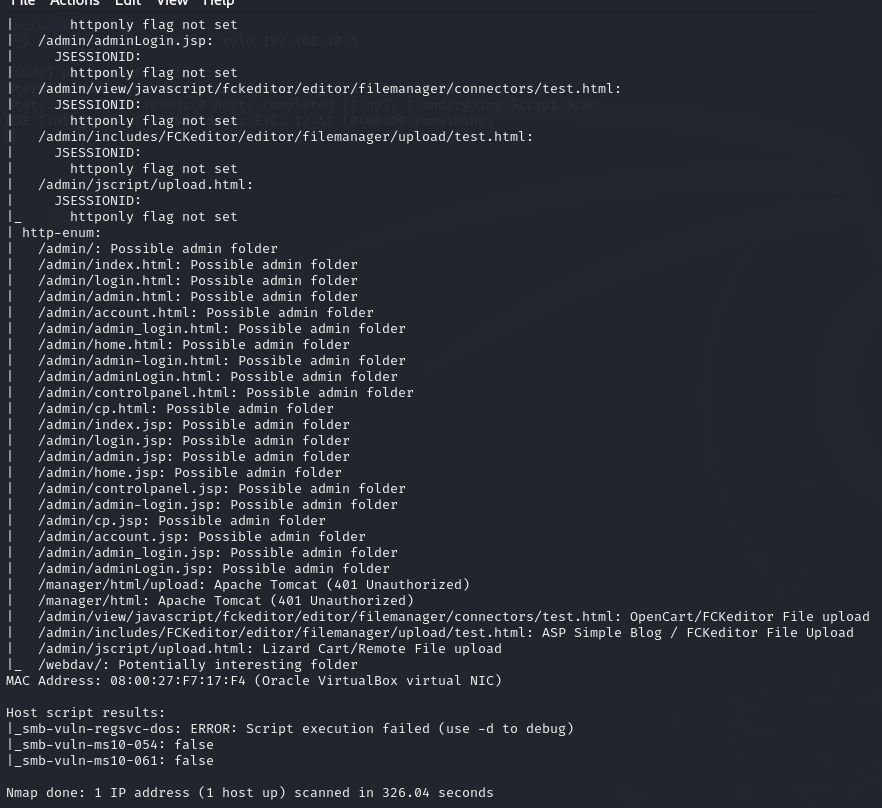
**Result – gives 5 ip address for specified port number and their running services.**

1. ***Execute nmap scripts for vulnerability scanning (nmap --script -Pn vuln <destination IP>), exploitation (nmap --script exploit <destination IP>), denial-of-service (nmap --script dos -Pn <destination IP>), and brute-force (nmap --script brute -Pn <destination IP>). Analyze the outcomes and identify any potential security risks.***

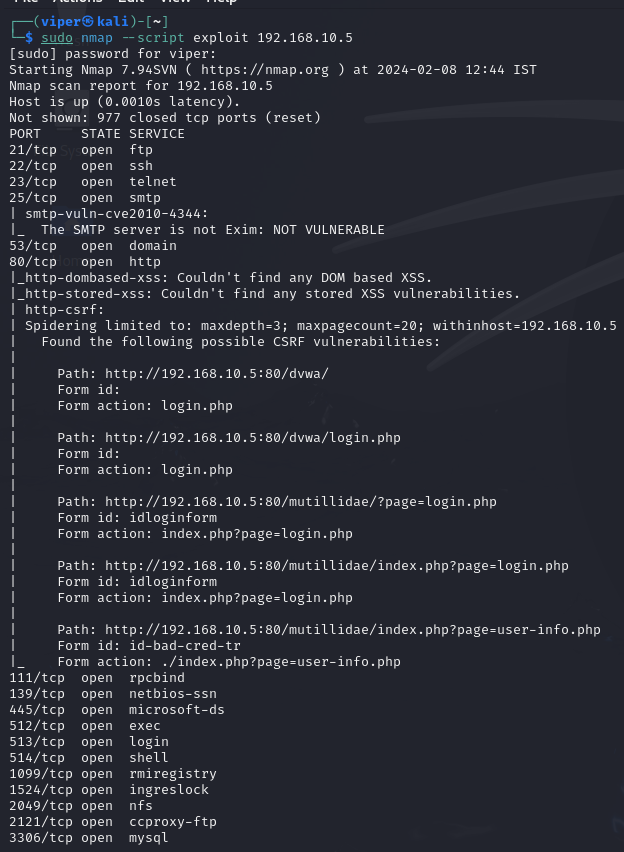
* **Sudo nmap -Pn –script vuln 193.168.10.5**

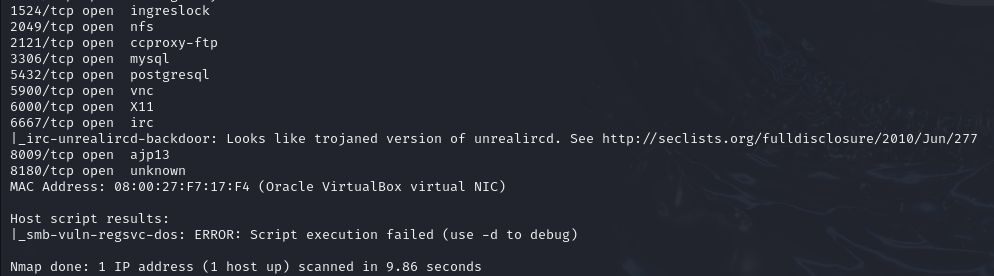
******

******

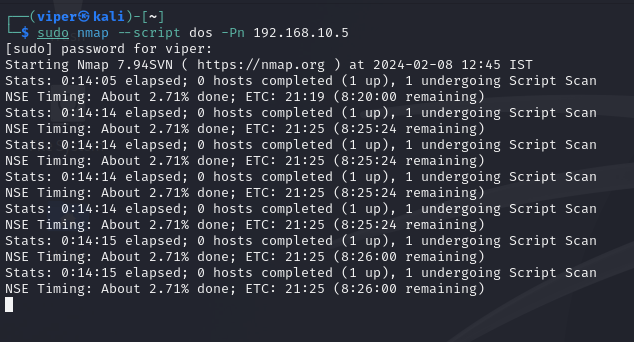
******

* **Sudo nmap –script exploit 192.168.10.5**

****

****

* **Sudo nmap –script dos -Pn 192.168.10.5**

****

* **Sudo nmap –script brute 192.168.10.5**

****

****

* **Sudo nmap -Pn –script vuln 193.168.10.5 command executes Nmap scripts specifically designed to detect known vulnerabilities in the target system. The risk associated with vulnerability scanning is that it can potentially identify weaknesses that could be exploited by attackers if not promptly addressed by system administrators.**
* **Sudo nmap –script exploit 192.168.10.5 command executes Nmap scripts that attempt to exploit known vulnerabilities in the target system. Exploiting vulnerabilities without permission is highly illegal and unethical and can lead to severe consequences, including legal action.**
* **Sudo nmap –script dos -Pn 192.168.10.5 command executes Nmap scripts designed to launch denial-of-service (DoS) attacks against the target system. DoS attacks can disrupt the availability of services, causing inconvenience or financial loss to the target organization.**
* **Sudo nmap –script brute 192.168.10.5 command executes Nmap scripts that attempt to guess credentials or crack passwords through brute-force methods. Brute-force attacks can compromise the security of accounts and systems by gaining unauthorized access.**

**Introduction**

Metasploit is an open-source penetration testing framework that provides tools for developing, testing, and executing exploit code against a remote target. It was originally created by H.D. Moore and has been maintained by Rapid7 since 2009. Metasploit is widely used by security professionals, ethical hackers, and penetration testers to identify and exploit vulnerabilities in computer systems for the purpose of improving security.

***Key features of Metasploit include:***

* **Exploitation Framework:** Metasploit provides a comprehensive set of tools for developing and executing exploit code against a target system. This allows security professionals to test and validate the effectiveness of security measures.
* **Payloads:** Metasploit supports a variety of payloads, which are pieces of code that can be delivered to a target system after successful exploitation. Payloads can range from simple commands to full-fledged remote access to the target.
* **Post-Exploitation Modules:** Once a system is compromised, Metasploit provides modules for gathering additional information, maintaining access, and performing various post-exploitation activities.
* **Auxiliary Modules:** These modules are used for tasks that support the exploitation process, such as information gathering, scanning, and fuzzing.
* **Meterpreter:** Meterpreter is an advanced payload that provides a powerful interactive shell on the target system. It allows the penetration tester to execute commands, manipulate the file system, capture screenshots, and perform various other tasks.
* **Integration with Other Tools:** Metasploit can be integrated with other security tools and frameworks, enhancing its capabilities and making it part of a broader security testing toolkit.
* **Community and Updates:** Metasploit has an active community of contributors, and updates are regularly released to address vulnerabilities, add new features, and improve existing ones.

***DVWA includes installation, security levels, common vulnerabilities, and specific attack scenarios:***

1. **Security Levels**
2. **Common Vulnerabilities**
3. **Cross-Site Scripting (XSS)**
4. **Cross-Site Request Forgery (CSRF)**
5. **File Inclusion and File Upload**
6. **Brute Force and Authentication**

|  |
| --- |
| ***Commands*** |
| 1. Layer 2 Host Discovery Commands:  - nmap -PR -sn <Metasploit2\_IP>  - 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 Nmap Scans  - TCP Connect Scan (-sT): nmap -sT -p <port number> <Metasploit2\_IP>  - TCP SYN (Stealth) Scan (-sS): nmap -sS -p <port number> <Metasploit2\_IP>  - TCP FIN Scan (-sF): nmap -sF -p <port number> <Metasploit2\_IP>  - TCP Null Scan (-sN): nmap -sN -p <port number> <Metasploit2\_IP>  - TCP XMAS Scan (-sX): nmap -sX -p <port number> <Metasploit2\_IP>  - UDP Scan (-sU): nmap -sU -p <port number> <Metasploit2\_IP>  4. Operating System Detection  - nmap -O <Metasploit2\_IP>  - nmap --osscan-guess <Metasploit2\_IP>  - nmap -A <Metasploit2\_IP> (Aggressive scan including OS detection)  5. Idle Scan / Zombie Scan Commands  - Finding Zombie/Idle Machine: nmap -p<port scan> --script ipidseq -iR <range>  - Vulnerability Scanning: nmap --script -Pn vuln <Metasploit2\_IP>  - Exploitation: nmap --script exploit <Metasploit2\_IP>  - DoS (Denial-of-Service): nmap --script dos -Pn <Metasploit2\_IP>  - Brute-Force: nmap --script brute -Pn <Metasploit2\_IP>  Replace <Metasploit2\_IP> and <port number> with the actual IP address of the Metasploit 2 target machine and a specific port number, respectively, as needed. Ensure that all commands are executed responsibly and in compliance with ethical guidelines. |