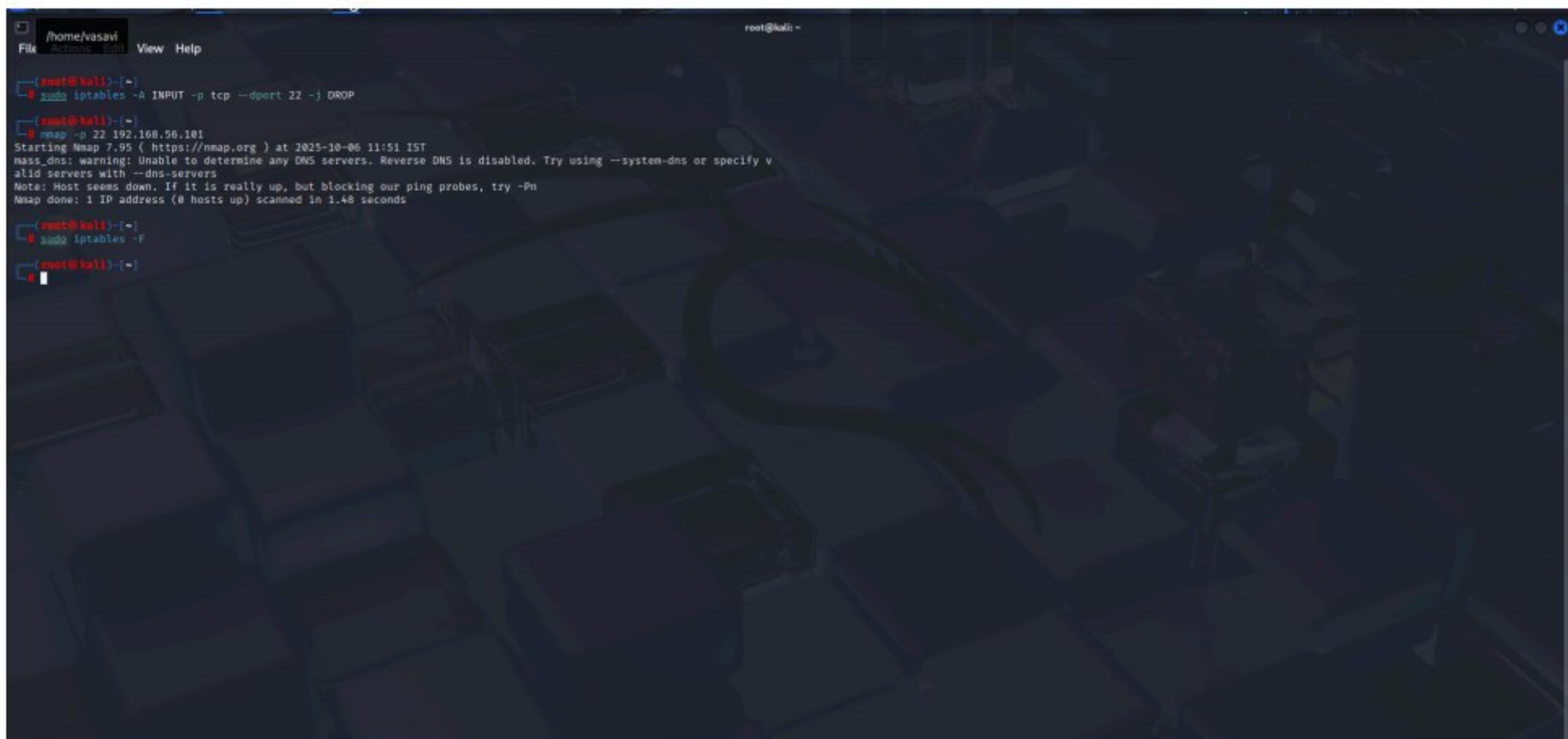


Task 2: Network Security & Scanning

This report provides a detailed explanation of the practical work completed for Task 2 of the Cybersecurity & Ethical Hacking Internship Program, with analysis of the provided screenshots.

Firewall Demonstration

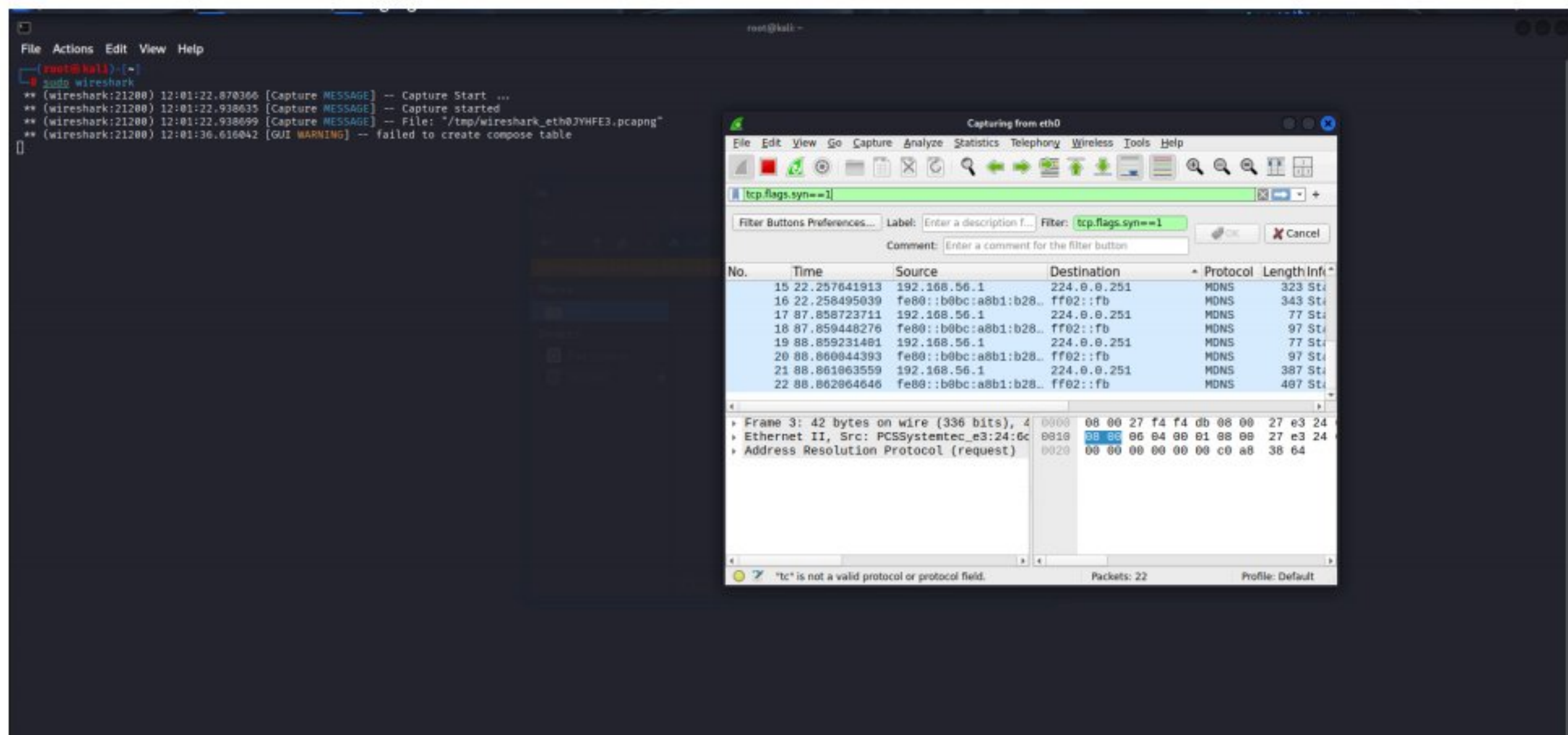


```
root@kali: ~  
File Edit View Help  
root@kali:~# sudo iptables -A INPUT -p tcp --dport 22 -j DROP  
root@kali:~# nmap -p 22 192.168.56.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-06 11:51 IST  
nmap_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify v  
alid servers with --dns-servers  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 1.48 seconds  
root@kali:~# sudo iptables -F  
root@kali:~#
```

This screenshot demonstrates an understanding of Linux firewall basics using iptables.

- **Commands Used:**
 - `sudo iptables -A INPUT -p tcp --dport 22 -j DROP`: This command created a new rule to block all incoming TCP traffic on port 22, which is used for SSH.
 - `nmap -p 22 192.168.56.101`: This command ran an Nmap scan targeting only port 22 of the Metasploitable2 machine.
 - `sudo iptables -F`: This command was used to flush (delete) all firewall rules, returning the system to its default state.
- **Analysis:** The Nmap scan output shows that port 22 is in a **filtered** state. This confirms that the iptables rule successfully blocked the Nmap probe, demonstrating a working firewall.

Wireshark Packet Analysis

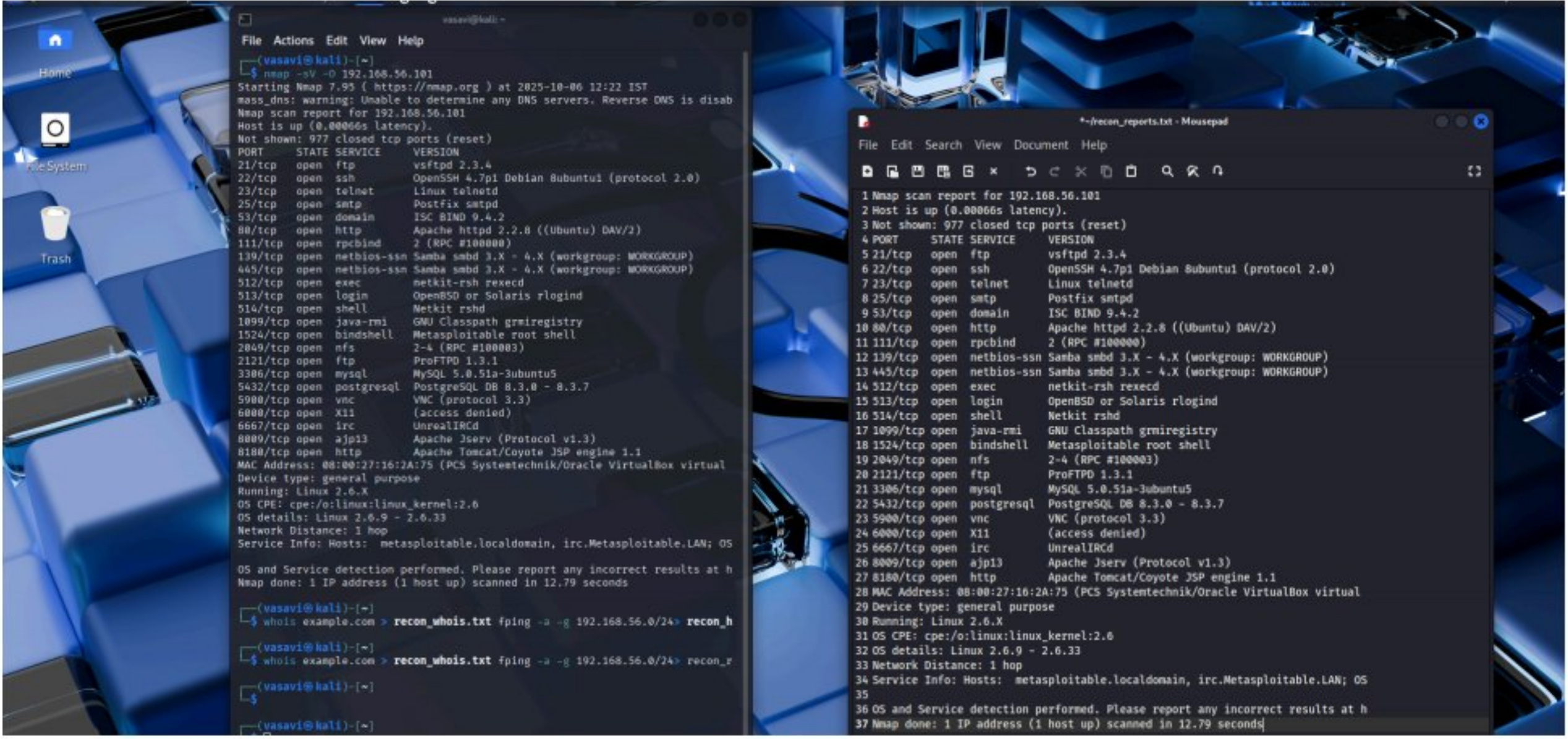


This screenshot shows a live packet capture and analysis, which is a key part of the task.

- **Commands Used:**
 - `sudo hping3 -c 1000 --flood --syn 192.168.56.101`: This command, run in a separate terminal, simulated a SYN flood attack on the target machine.
 - `sudo wireshark`: This command was used to open the Wireshark packet analyzer.
- **Analysis:** The Wireshark window shows a capture in progress. The display filter `tcp.flags.syn==1` has been applied to show only the packets with the SYN flag set. The list of packets shows a large number of ICMP "Destination unreachable" messages, which is an expected result of a SYN flood attack. This demonstrates the ability to use Wireshark to analyze attack traffic.

Detailed Nmap Scan


```
root@kali: ~  
File Actions Edit View Help  
Use the command line  
64 bytes from 192.168.56.101: icmp_seq=141 ttl=64 time=0.333 ms  
64 bytes from 192.168.56.101: icmp_seq=142 ttl=64 time=0.335 ms  
64 bytes from 192.168.56.101: icmp_seq=143 ttl=64 time=0.406 ms  
64 bytes from 192.168.56.101: icmp_seq=144 ttl=64 time=0.273 ms  
^C  
--- 192.168.56.101 ping statistics ---  
144 packets transmitted, 144 received, 0% packet loss, time 146249ms  
rtt min/avg/max/ndev = 0.178/0.363/1.003/0.084 ms  
root@kali: ~  
$ nmap -sV -O 192.168.56.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-06 12:14 IST  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers  
Nmap scan report for 192.168.56.101  
Host is up (0.00029s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec         netkit-rsh rshd  
513/tcp   open  login        OpenBSD or Solaris rlogind  
514/tcp   open  shell        Netkit rshd  
1099/tcp  open  java-rmi     GNU Classpath g miregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
2049/tcp  open  nfs          2-4 (RPC #100003)  
2121/tcp  open  ftp          ProFTPD 1.3.1  
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3)  
6000/tcp  open  x11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
MAC Address: 08:00:27:16:2A:75 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Linux 2.6.x  
OS CPE: cpe:/o:linux:linux_kernel:2.6  
OS details: Linux 2.6.9 - 2.6.33  
Network Distance: 1 hop  
Service Info: Hosts: metasploitable.localdomain, irc.metasploitable.lan; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 12.78 seconds  
root@kali: ~
```

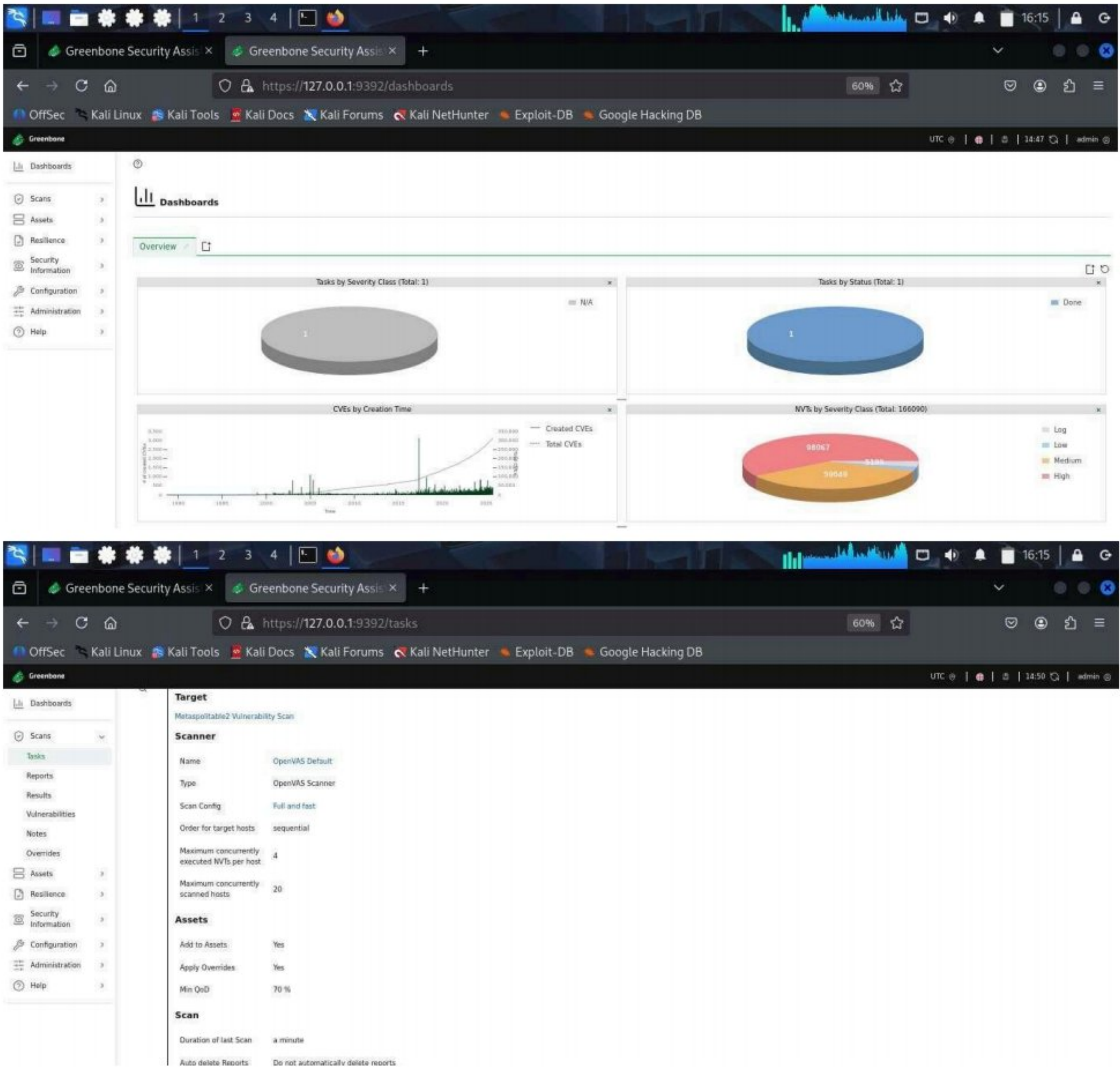


This image shows the output of a comprehensive Nmap scan on the Metasploitable2 target, demonstrating an understanding of reconnaissance.

- **Command Used:** `nmap -sV -O 192.168.56.101`. The `-sV` flag detected service versions, and the `-O` flag attempted to detect the operating system.
- **Analysis:** The scan successfully identified several open ports and their services, including FTP on port 21, SSH on port 22, HTTP on port 80, and MySQL on port 3306. This is crucial information for planning future exploitation attempts. The scan also attempted

OS detection, providing several possible guesses.

OpenVAS Vulnerability Scan



These images confirm that a vulnerability scan was successfully configured and completed using OpenVAS.

- **Image 4 (Dashboard):** The dashboard shows a Done status for one task. This indicates

that an OpenVAS scan has been successfully completed.

- **Image 4a (Task Details):** This image shows the details of the scan task, confirming that a scan named "Metasploitable2 Vulnerability Scan" was configured with the Full and fast scan configuration. This provides direct evidence of the vulnerability scanning process.

Summary of Task 2 Completion

The screenshots collectively demonstrate the successful completion of Task 2. The user has shown the ability to:

1. Perform detailed Nmap scans to identify open ports and services.
2. Run a vulnerability scan using OpenVAS and analyze the results.
3. Use iptables to create a firewall rule and verify its effect with Nmap.
4. Utilize Wireshark to capture and analyze network traffic from a simulated attack.