Task 2: Vulnerability Assessment and Scanning Report

Attacker Machine (Kali Linux): 192.168.56.3

Target Machine (Metasploitable 2): 192.168.56.4

# 1. Passive Reconnaissance

## WHOIS Lookup

Command:

whois apexplanet.in

Purpose: Retrieve domain ownership and registration details.

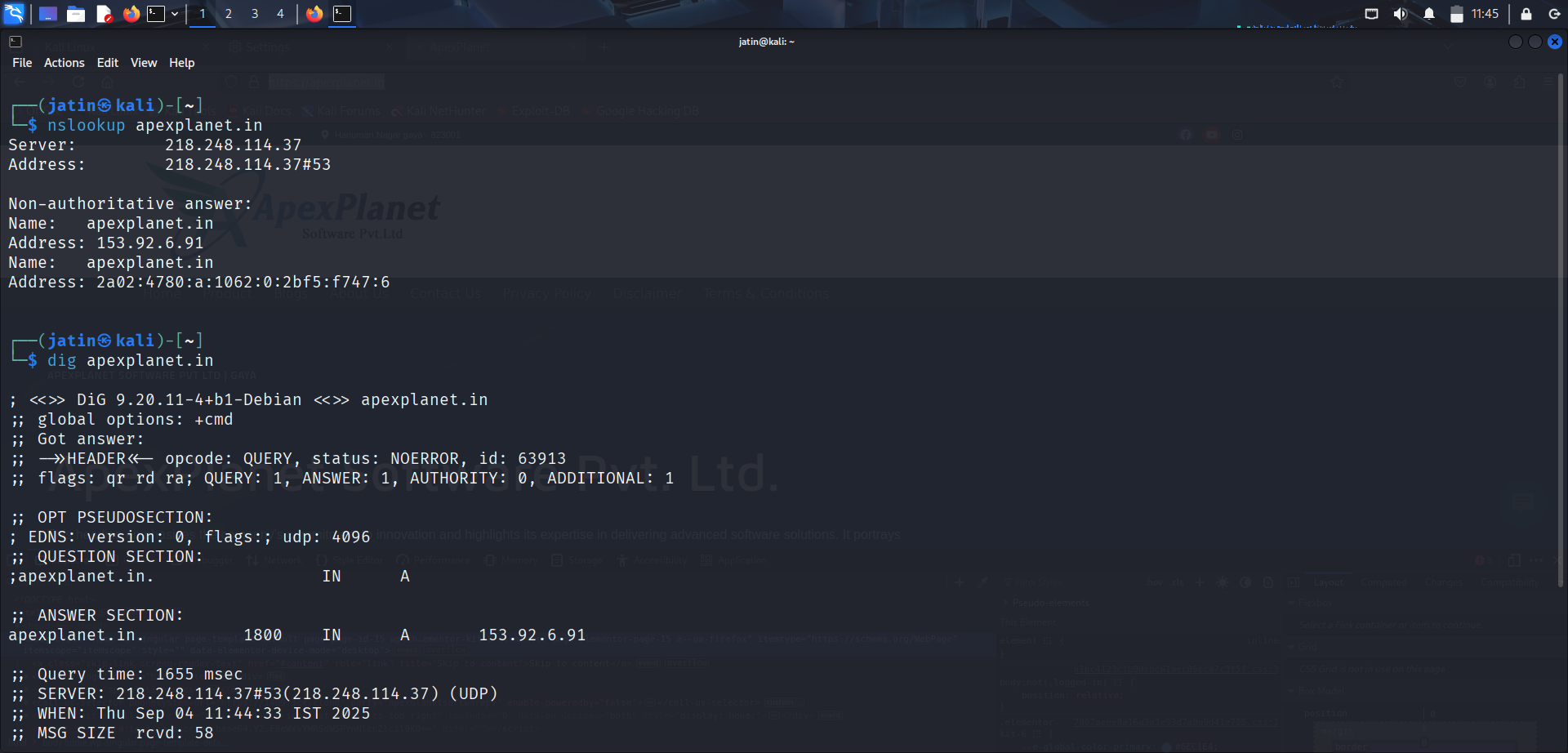


## nslookup

Command:

nslookup apexplanet.in

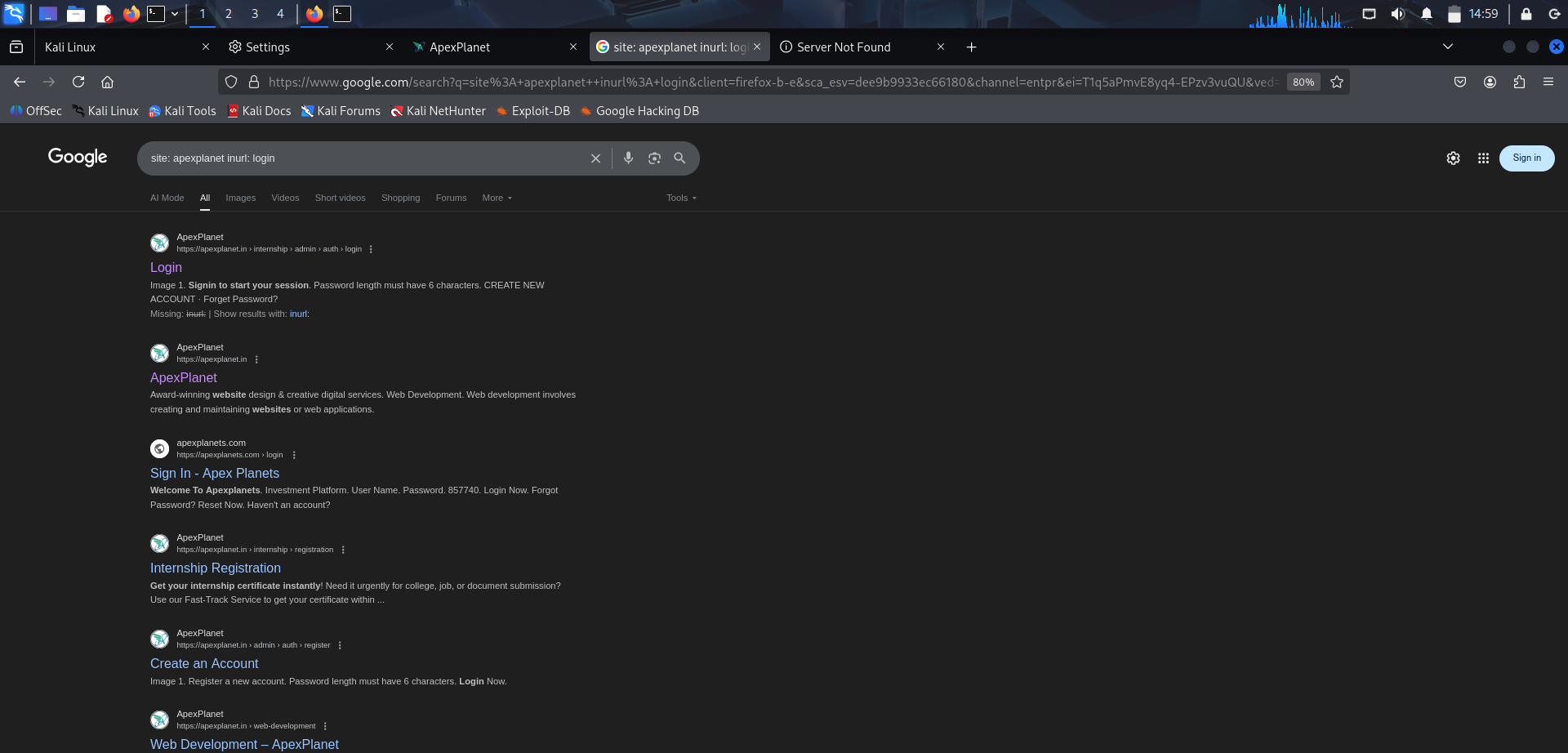
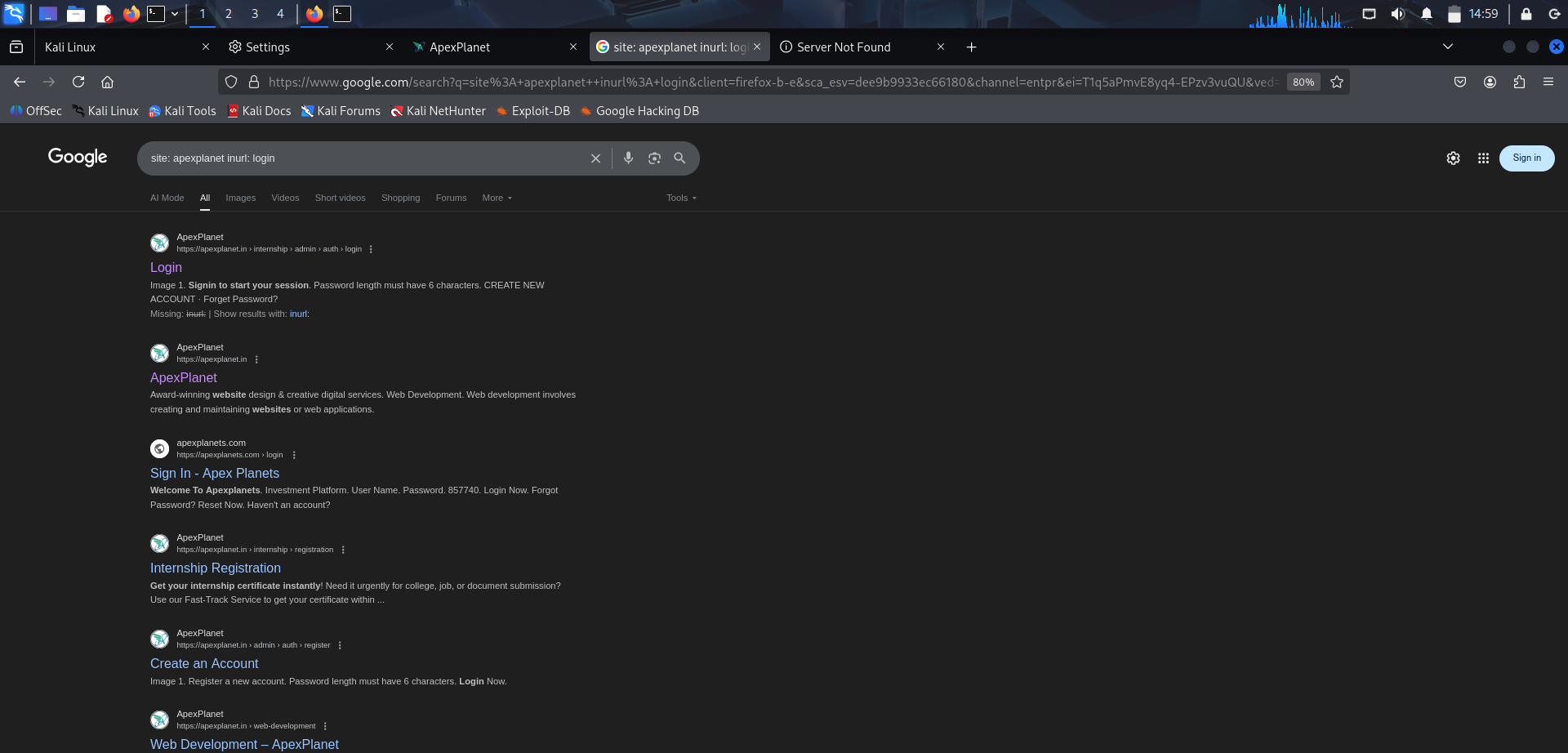
Purpose: Resolve domain names to IP addresses.



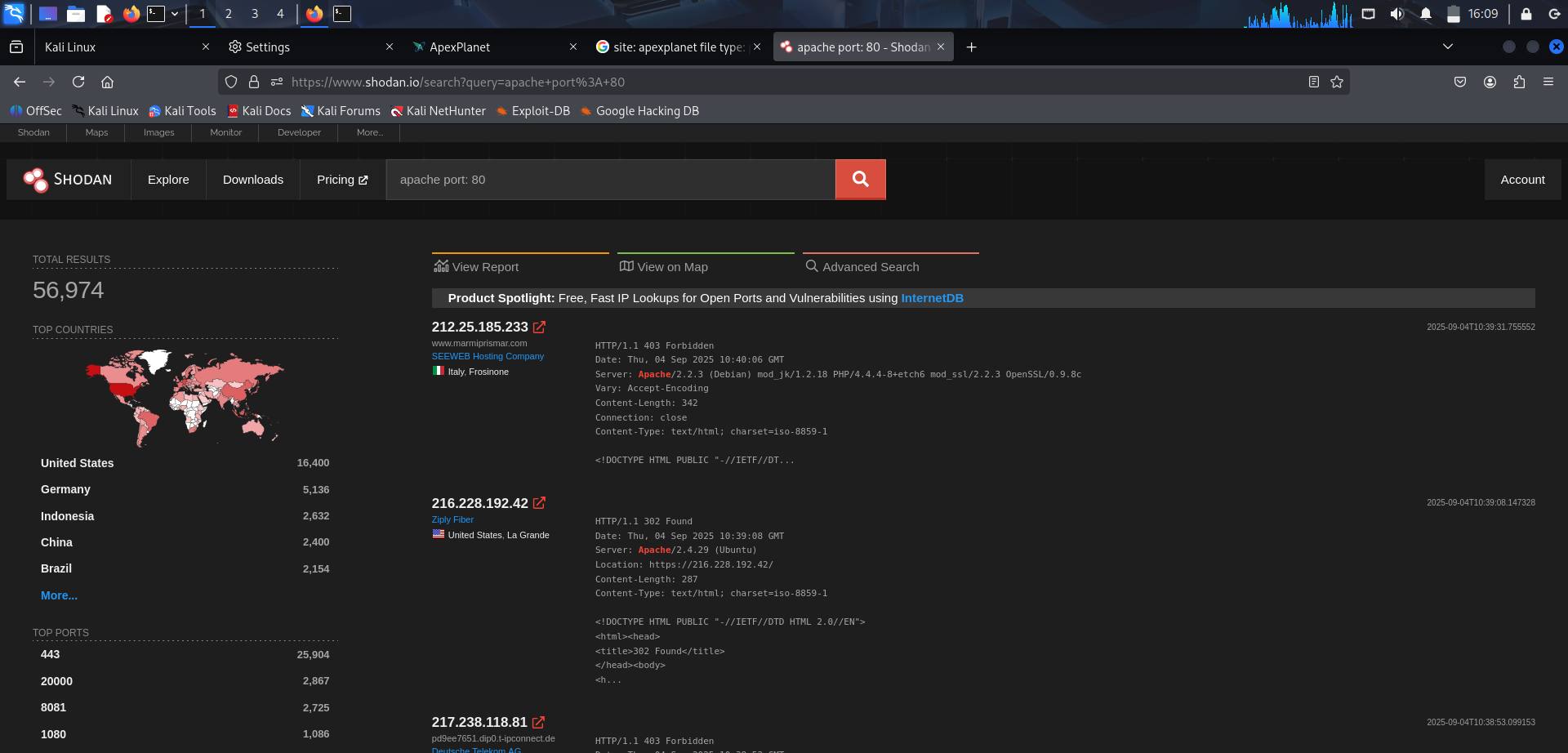
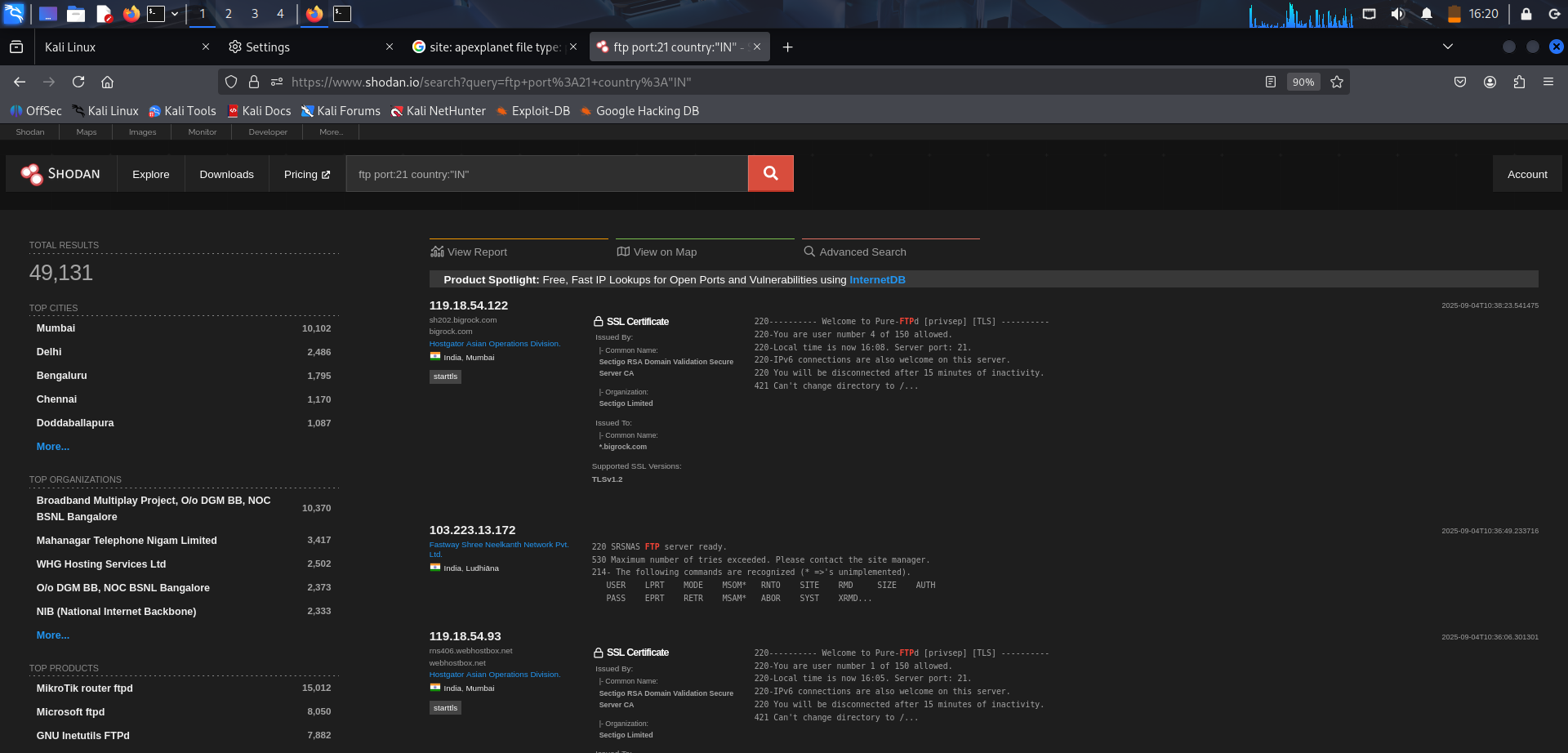
## Goggle Dorking

Command:

site: apexplanet.in inurl: login or site: apexplanet.in file type: pdf

  
  
Shodan

* **Command / Tool:** apache port: 80 & ftp port: 21 country “IN ”/ Shodan (online search engine)
* **Purpose:** Used for **passive reconnaissance** to find information about publicly exposed devices, services, and vulnerabilities on the internet without directly scanning the target.

# 2. Active Reconnaissance Ping Sweep

**Command:**

nmap -sn 192.168.56.0/24

Purpose: Identifies which hosts are up and reachable in the subnet by sending ICMP Echo requests (ping). This helps in mapping active machines before deep scanning.

# Banner Grabbing

Command:

# nc 192.168.56.4 21

Purpose: Connects to a service port and retrieves its banner (service name, version). This reveals useful info about running services (e.g., FTP server version).

# 

## Nmap TCP, Service & OS Detection

Command:

sudo nmap -sS -sV -O -192.168.56.5

Purpose: Detect open TCP ports using stealth scan and Identify running services and operating system.

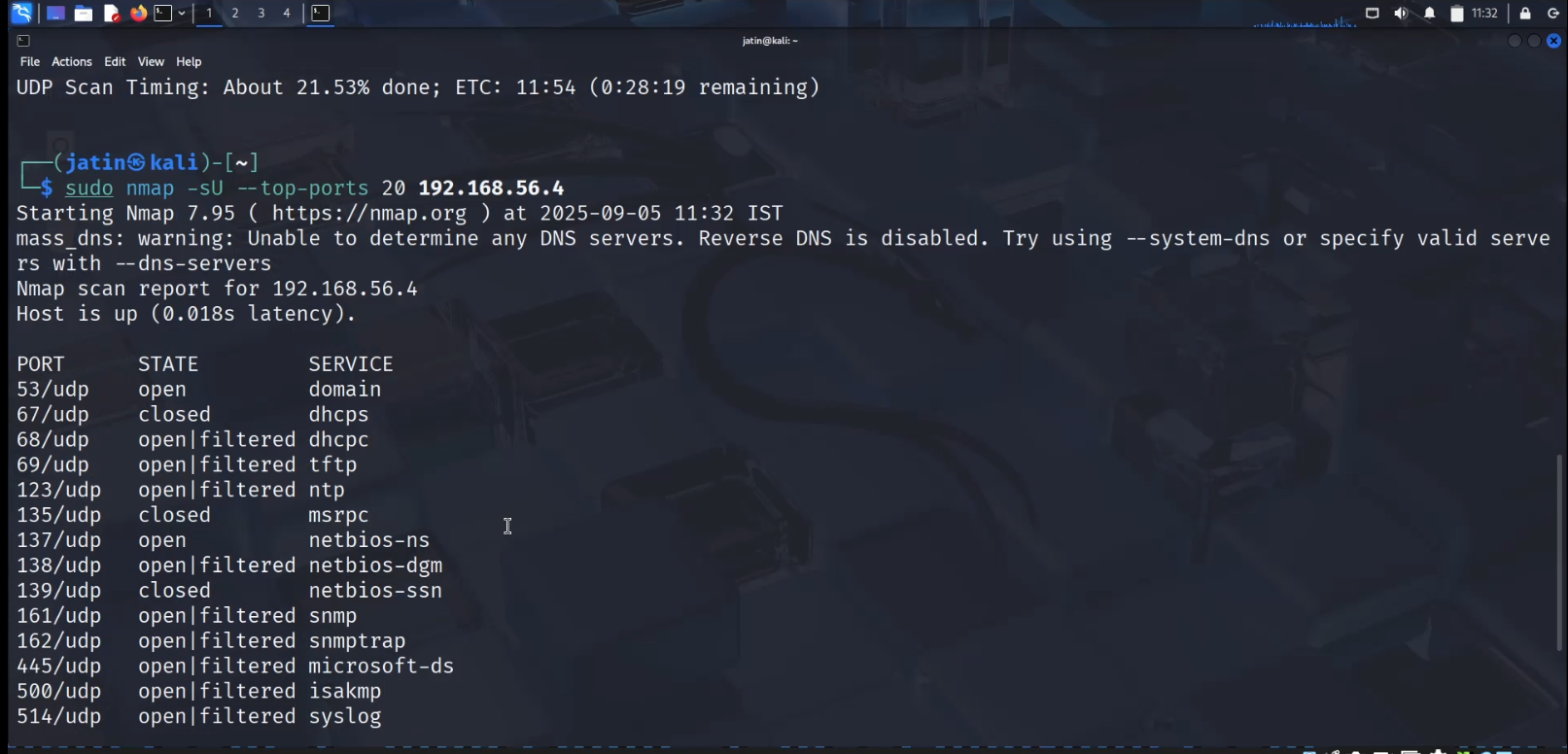


## Nmap UDP Scan

Command:

sudo nmap -sU –top-ports 20 192.168.56.4

Purpose: Identify open UDP ports.



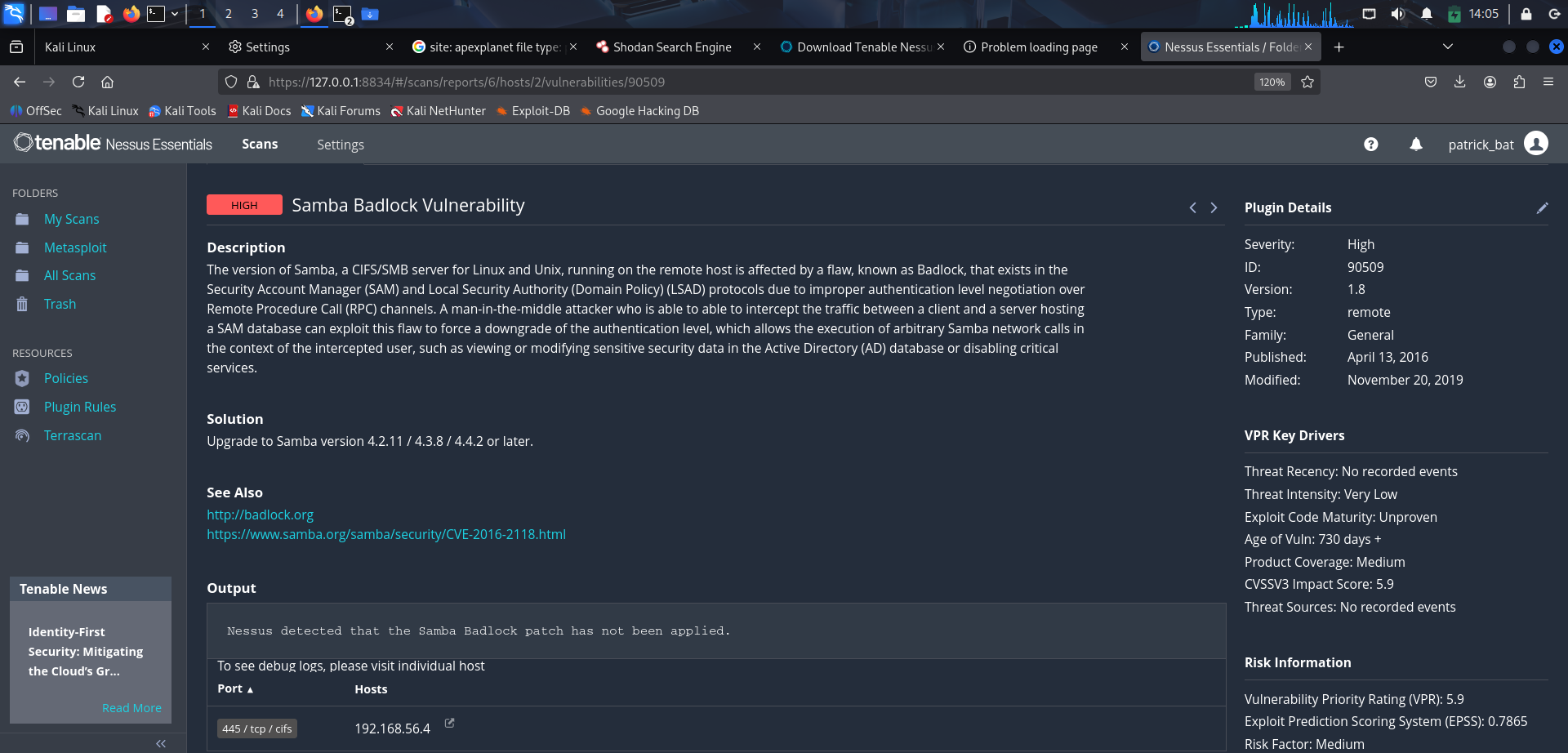
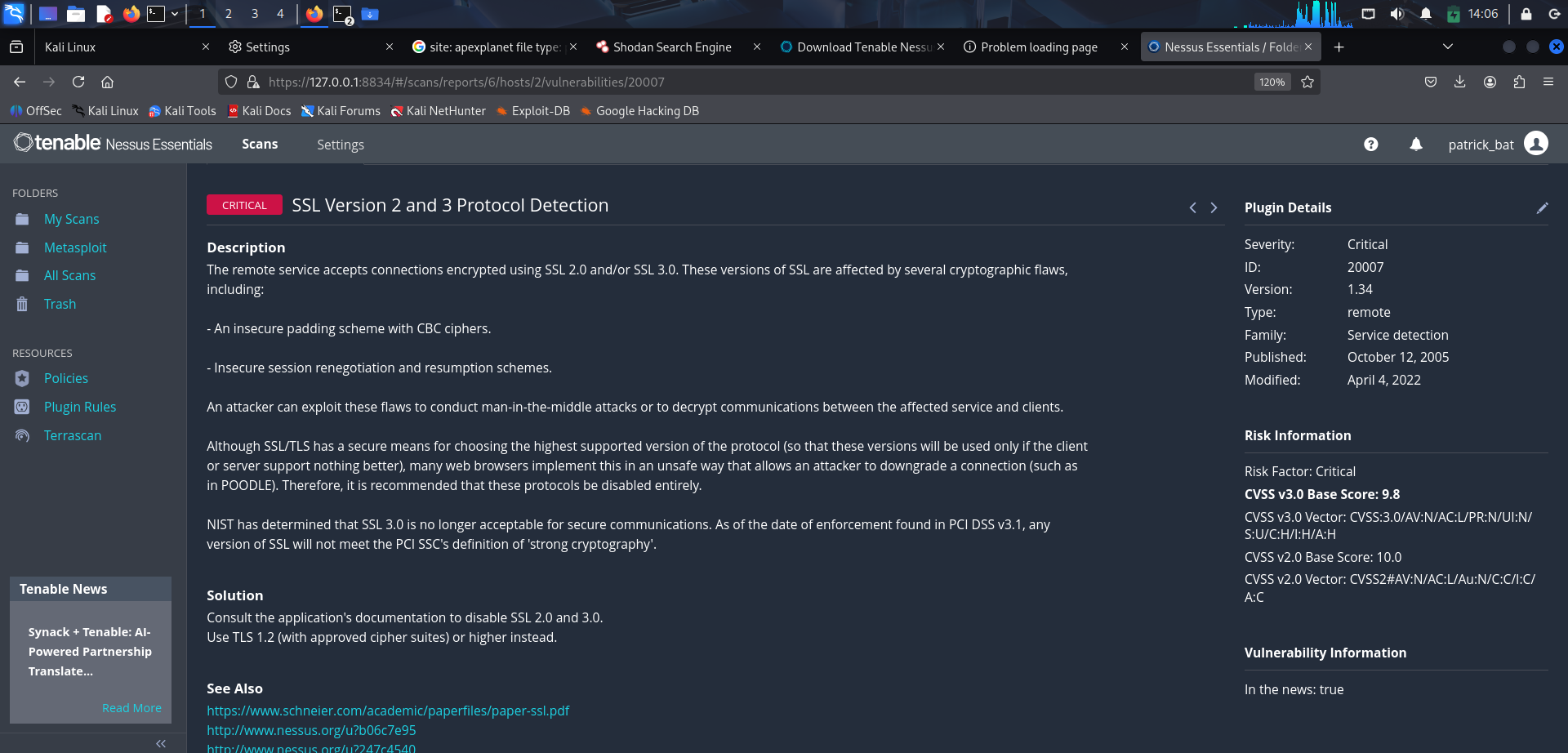
# 3. Vulnerability Scanning (Nessus)

## Nessus Setup

Command:

Access Nessus at https://127.0.0.1:8834/

Purpose: Perform automated vulnerability assessment on the target.

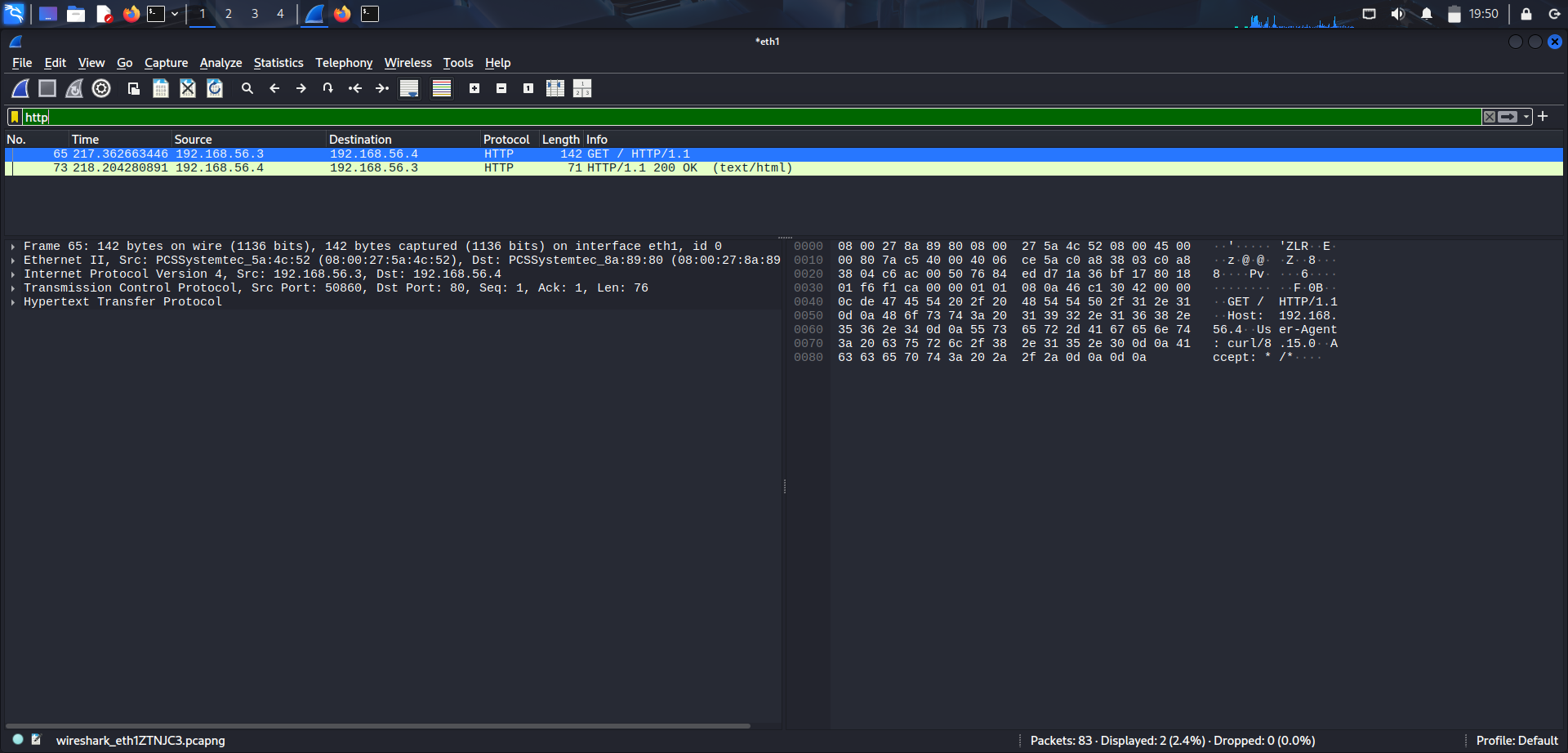
# 4. Packet Analysis with Wireshark

## HTTP/FTP/DNS Traffic Capture

Command:

Captured unencrypted protocols for analysis.

Purpose: Analyze raw traffic.

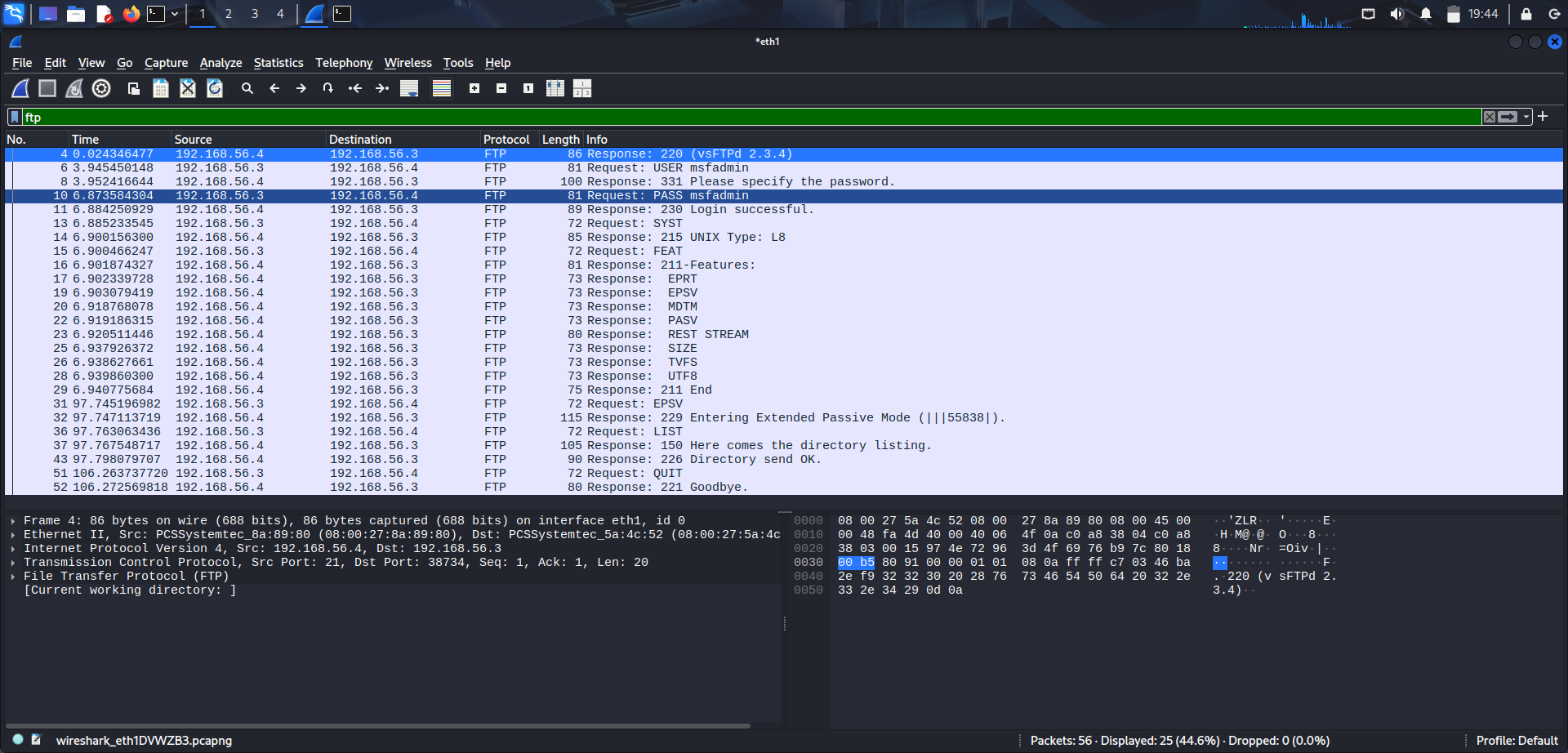


## Extracting FTP Credentials

Command:

Filter: ftp

Purpose: Observed clear-text username and password in FTP session.

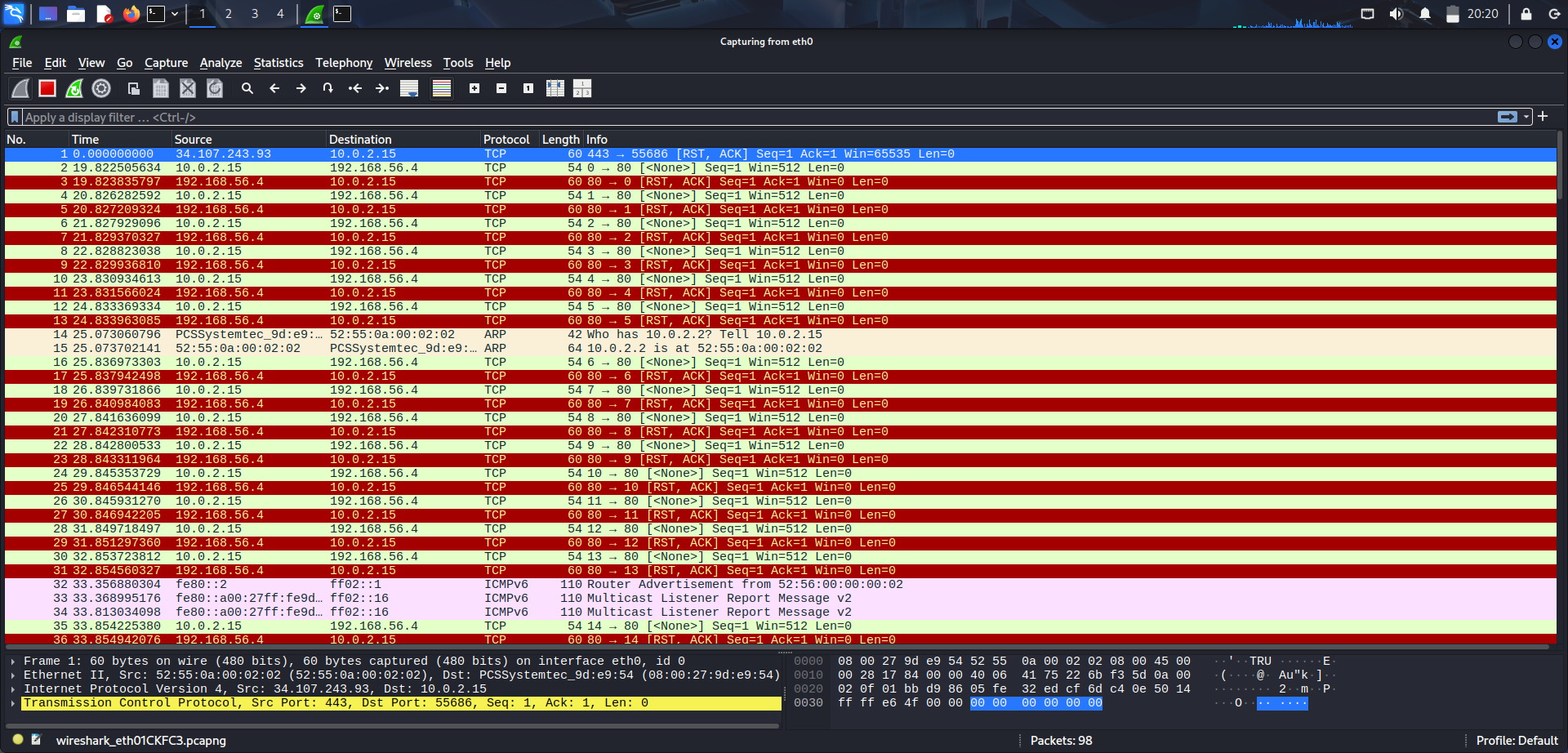


## SYN Flood Attack Simulation

Command:

sudo hping3 -S --flood -V -p 80 192.168.56.4

Purpose: Generate a SYN flood towards port 80 of target.  
Wireshark Filter: tcp.flags.syn == 1 && tcp.flags.ack == 0



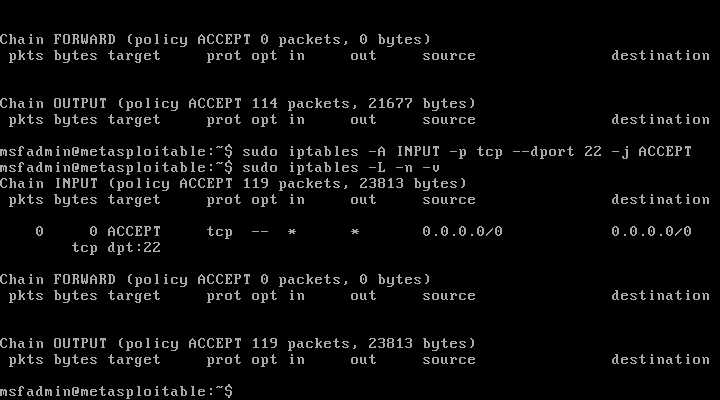
# 5. Firewall Basics (iptables)

## Block Telnet (Port 23)

Command:

sudo iptables -A INPUT -p tcp --dport 22 -j DROP

Purpose: Block access to Telnet service.



# Conclusion

- Passive Recon: WHOIS, nslookup, google dork, shodan gave us external info.  
- Active Recon: Ping sweep, banner graping and nmap revealed open services like FTP, SSH, HTTP, MySQL, VNC.  
- Vulnerability Scan: Nessus confirmed exploitable weaknesses on Metasploitable.  
- Packet Analysis: Wireshark captured HTTP, FTP, and simulated SYN flood traffic.  
- Firewall: iptables rules successfully demonstrated access restrictions.