Wireshark & Firewall Scan Analysis

Target System: Metasploitable2

Tools Used: Wireshark, hping3, iptables.

Wireshark Packet Analysis:

Objective:

To capture and analyze network traffic for signs of insecure communication and simulated attacks.

Traffic Captured:

- FTP credentials transmitted in plaintext

- HTTP requests and DNS queries

- SYN flood attack simulated using hping3

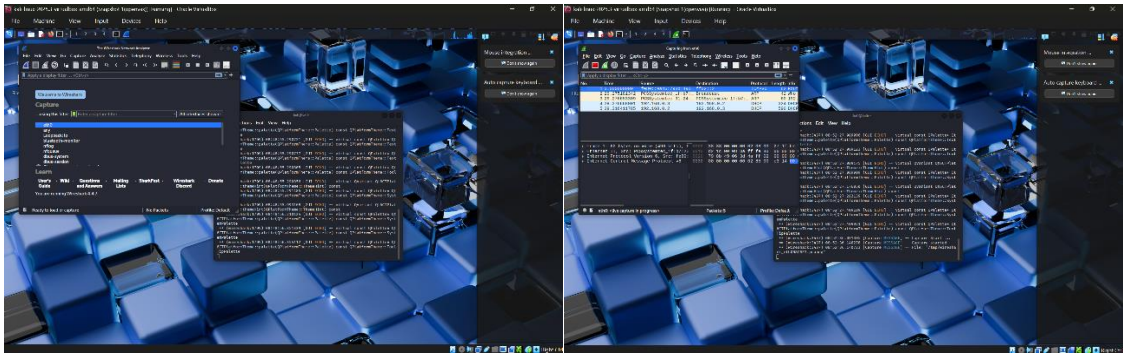
Filters Used:

- ftp – to capture login credentials

- http – to inspect web traffic

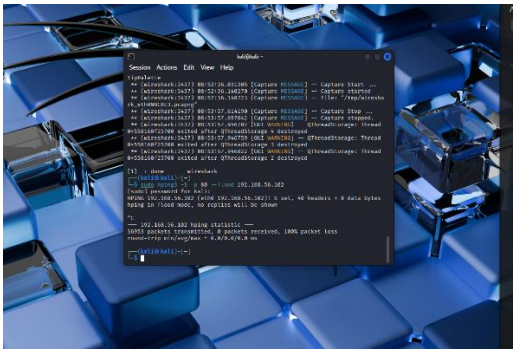
- dns – to monitor domain resolution

- tcp.flags.syn == 1 && tcp.flags.ack == 0 – to detect SYN flood packets



SYN Flood Simulation Command:

sudo hping3 -S -p 80 --flood 192.168.56.101



Observations:

- Wireshark captured high-volume SYN traffic
- FTP credentials were visible in plaintext
- DNS queries revealed potential exposure to suspicious domains

Firewall Rule Demonstration:

Objective:

To block insecure services and prevent port scan attempts.

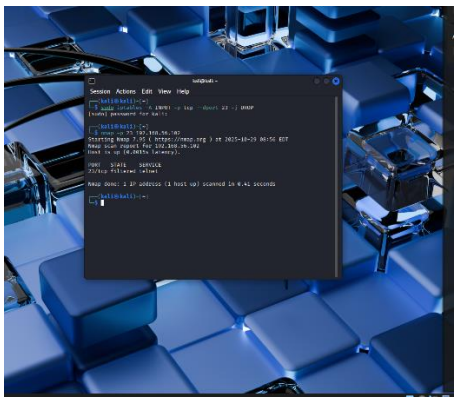
Rule Applied (Blocking Telnet):

sudo iptables -A INPUT -p tcp --dport 23 -j DROP

Verification:

nmap -p 23 192.168.56.101

- Result: Port 23 was no longer accessible
- Demonstrated successful blocking of Telnet service



Optional Additional Rules:

Block FTP

sudo iptables -A INPUT -p tcp --dport 21 -j DROP

Allow SSH

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

Recommendations:

- Disable insecure protocols like FTP and Telnet.
- Use encrypted alternatives such as SFTP and SSH.
- Apply firewall rules to reduce attack surface.
- Monitor traffic regularly for anomalies.
- Simulate attacks only in isolated lab environments.