Packet Sniffing and Network Traffic Analysis  
 By Maryam Sulaiman  
 Date: 09-june-2025

Introduction  
 This project is about capturing and analyzing network traffic to understand how information like usernames, passwords, and communication between computers can be seen if the data is not encrypted. I used two virtual machines: Kali Linux as the attacker machine and Metasploitable 2 as the target. The goal was to study how different network protocols behave and what risks they carry.

Objective  
 To simulate different types of network traffic, capture them using tcpdump and Wireshark, and analyze them to identify possible security weaknesses.

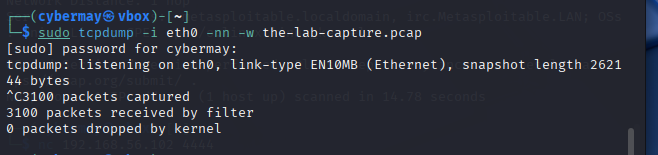
Tools Used

* Kali Linux
* Metasploitable 2
* Tcpdump
* Wireshark
* Netcat
* Nmap
* VirtualBox

Setup  
 Both Kali Linux and Metasploitable 2 were installed on VirtualBox. I set them to use the same network . I made sure both machines could ping each other. On Metasploitable, I made sure Apache (for HTTP), FTP, and Netcat were working.

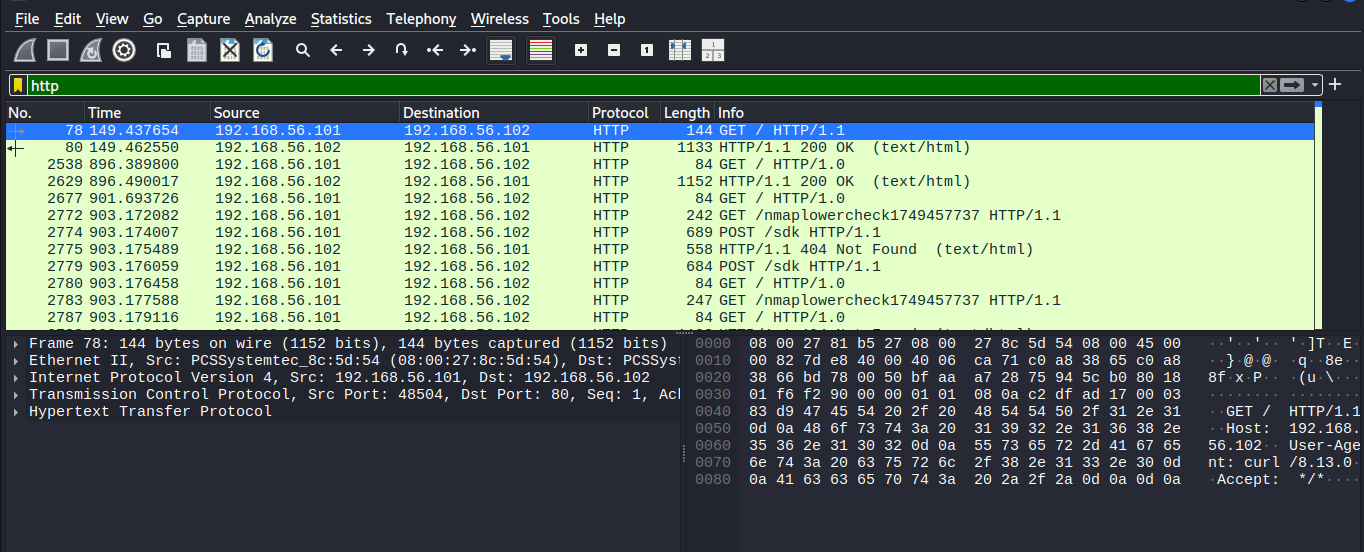
Step 1: Capturing Traffic with Tcpdump  
 On the Kali machine, I ran tcpdump to capture traffic:

To capture all traffic:  
 sudo tcpdump -i eth0 -nn -w the-lab-capture.pcap

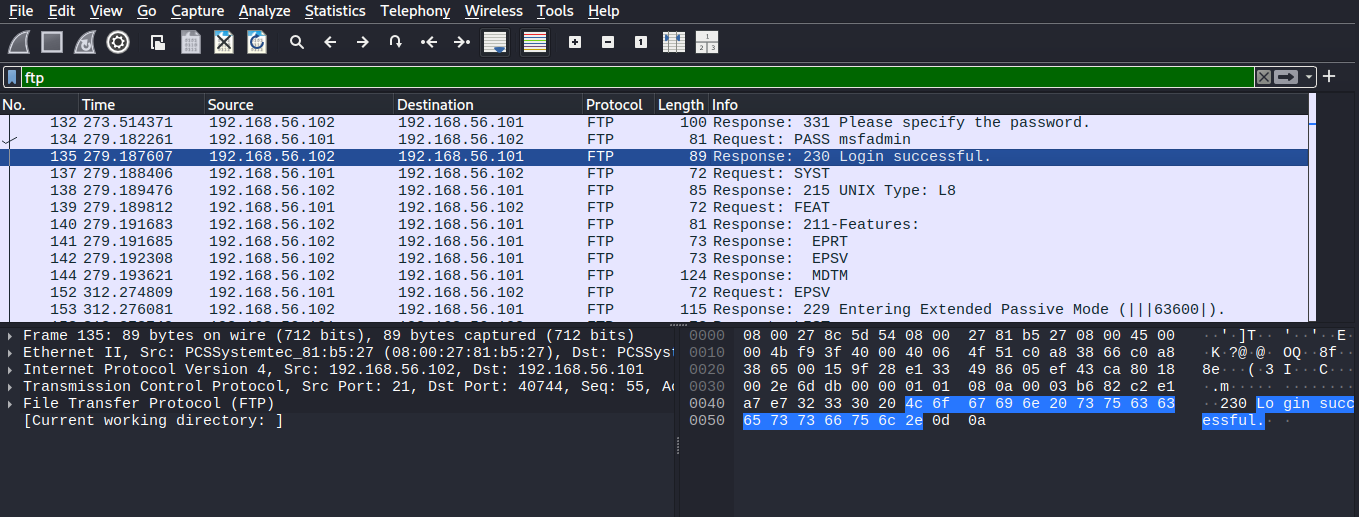


The captured file was later opened in Wireshark for easier analysis.

Step 2: HTTP Traffic Analysis  
 I visited the Metasploitable web server from Kali using its IP address. Wireshark showed the details of the HTTP requests. I could see what pages were requested and in some cases, login information if sent through a form. Everything was in plain text.

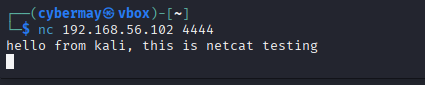


Step 3: FTP Traffic Analysis  
 I connected to the FTP server on Metasploitable using this command:  
 ftp [target IP]  
 I logged in using msfadmin as the username and password.  
 In Wireshark, I could see the username and password clearly in the captured packets. FTP does not use encryption.

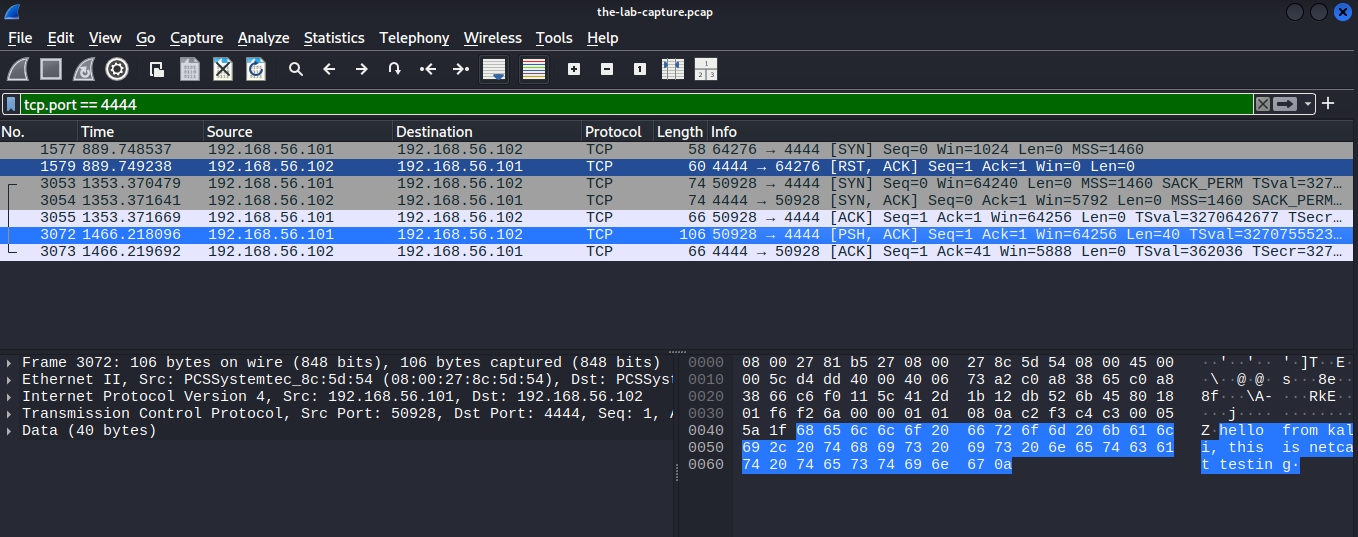


Step 4: Netcat Communication  
 I started a Netcat listener on Metasploitable:  
 nc -lvp 4444

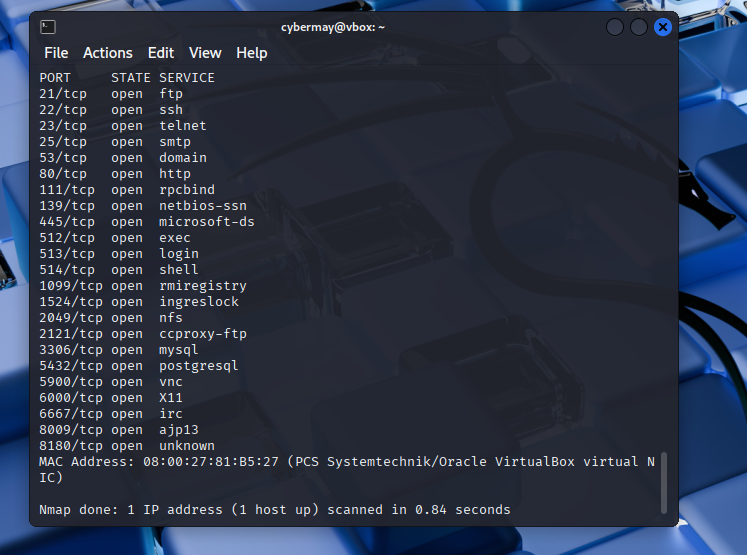
Then on Kali I ran:  
 nc [target IP] 4444

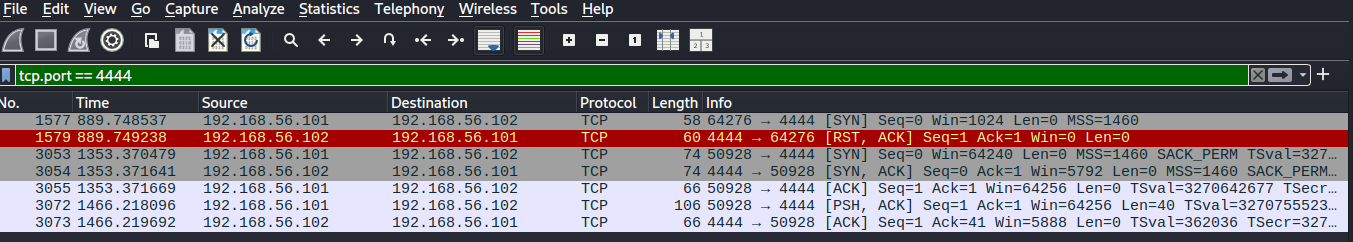


I typed a message, and both the message and response were captured in Wireshark. The communication was visible in plain text.



Step 5: Nmap Scan Detection  
 From Kali, I scanned Metasploitable using:  
 nmap -sS [target IP]

  
 In Wireshark, I saw SYN packets being sent, and responses from Metasploitable indicating open or closed ports. This shows how scanning can be detected by a network monitor.



Summary of Results

* HTTP traffic was readable and showed requests and login details.
* FTP traffic exposed usernames and passwords.
* Netcat messages were clearly visible.
* Nmap scanning behavior was easy to detect in the packet data.

Recommendations

* Use secure versions of protocols, like HTTPS and SFTP.
* Disable unused services on servers.
* Monitor network traffic for suspicious activity.
* Educate users about the risks of unencrypted communication.
* Use firewalls and intrusion detection systems.

Conclusion  
 This project shows how easy it is to intercept sensitive data on a network when no encryption is used. Packet sniffing is a powerful tool for attackers, but also for cybersecurity analysts who want to detect vulnerabilities. Encrypting data and monitoring traffic are essential parts of network security.