Title: Sniffing in a Controlled Environment: By Rohinish Sharma

Objective

The goal of this demonstration is to show how **unencrypted credentials** (like usernames and passwords) can be intercepted using **packet sniffing techniques** in a controlled lab setup. This helps organizations understand the importance of **encrypting network traffic** and the **risks of insecure protocols** like HTTP and FTP.

Key Concepts

What is Packet Sniffing?

Packet sniffing is the process of **monitoring and capturing data packets** as they travel over a network. Tools like **Wireshark** or **tcpdump** can be used to **analyze this traffic**, making it possible to extract sensitive information — if the data is not encrypted.

What is Network Traffic Analysis?

This refers to examining packets flowing through a network to:

- Identify communication patterns
- Monitor protocol use
- Detect suspicious activity or sensitive data leaks

Risks of Unencrypted Data Transmission

When data (especially **credentials**) is transmitted without encryption:

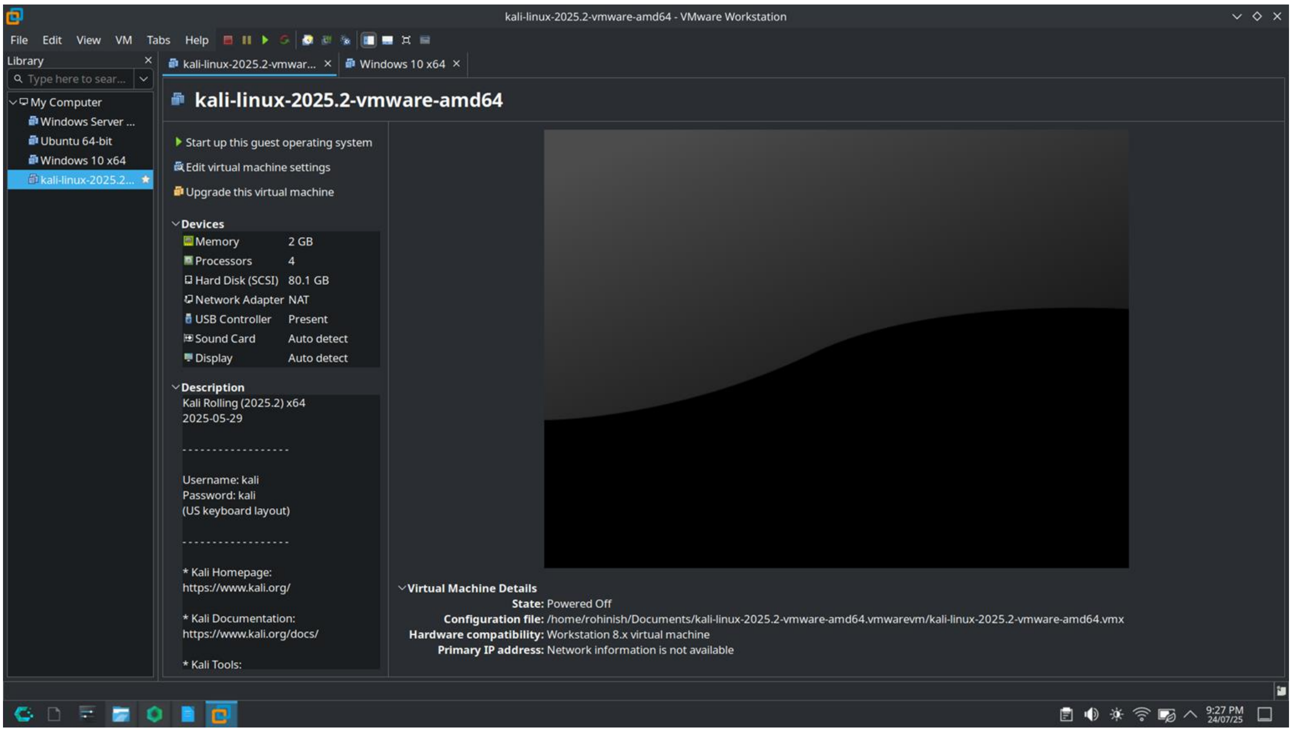
- Anyone on the same network can **intercept** it
- Tools like Wireshark can easily **read login forms, FTP credentials, emails, etc.**
- Attackers can use this to **impersonate users**, **access systems**, or **steal data**

Step 1: Setting Up the Lab Environment

Objective: Create a safe and isolated network to simulate real-world attacks without any legal or ethical risks.

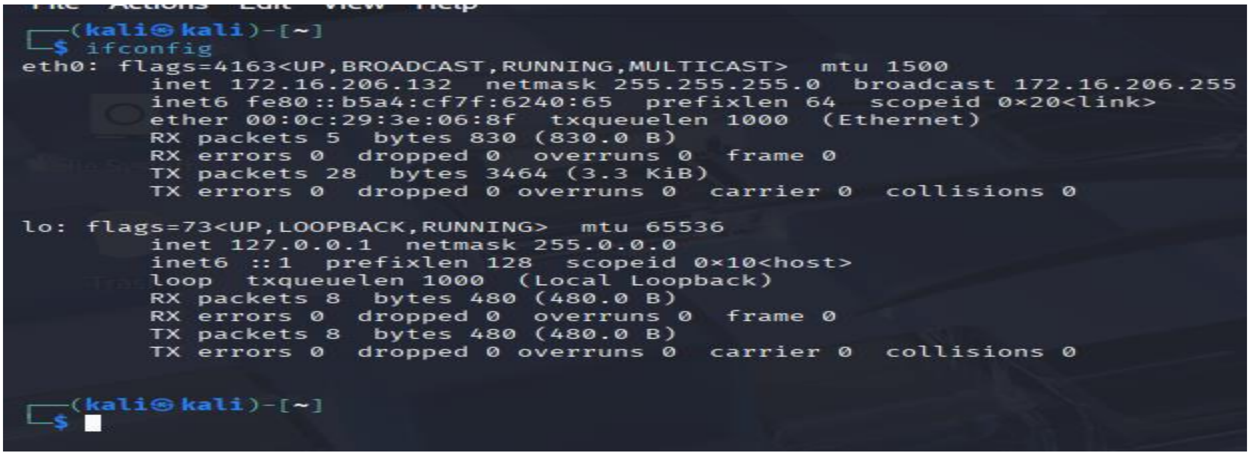
Actions:

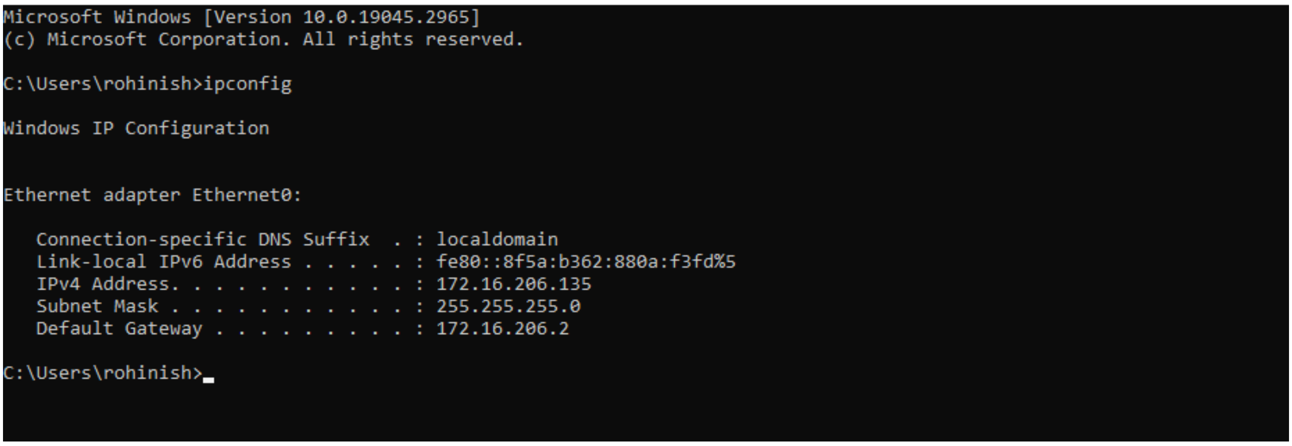
- Launch two Virtual Machines (VMs) in VMware:
  - **Kali Linux** (Attacker)
  - **Windows** (Victim)
- Set both VMs to use the **Host-Only Network** adapter.

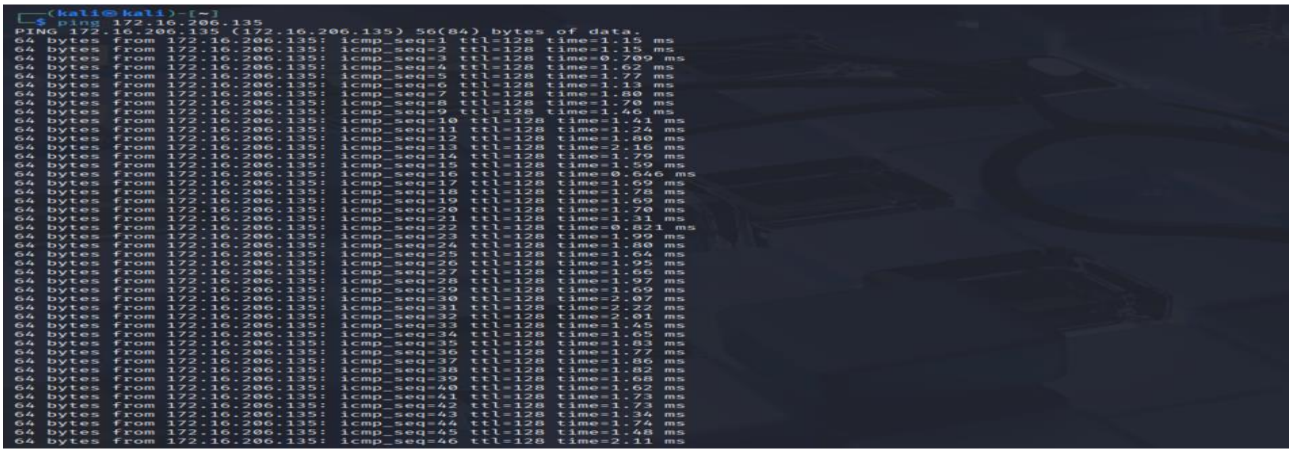


Host-Only networking ensures both machines are on the **same private subnet**, allowing direct communication while keeping them **isolated from the internet**. This simulates a **local corporate LAN** scenario for penetration testing.

Step 2: Identifying IP Addresses & Verifying Connectivity





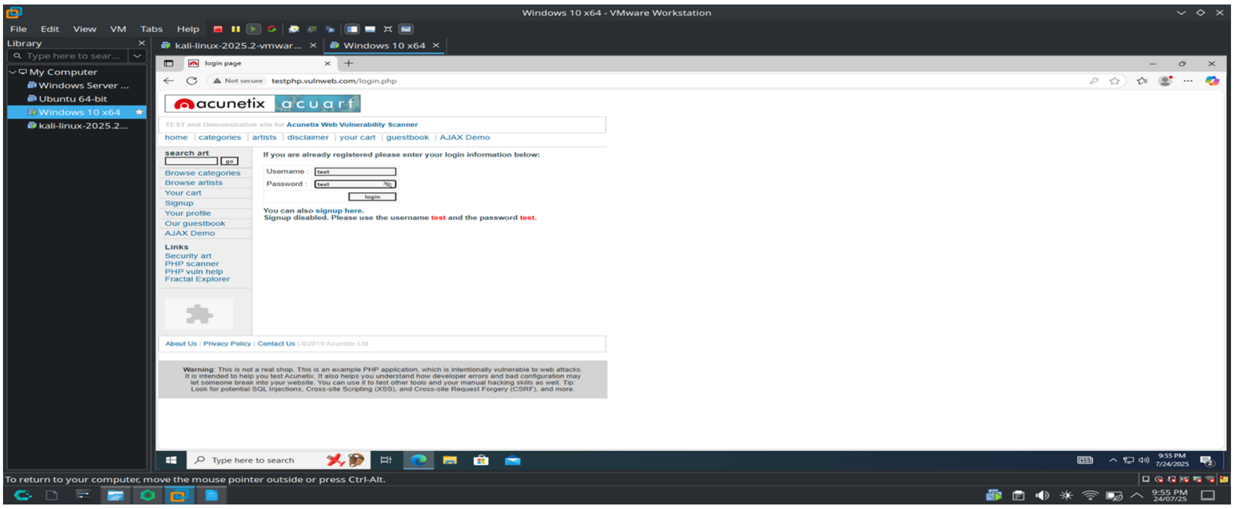


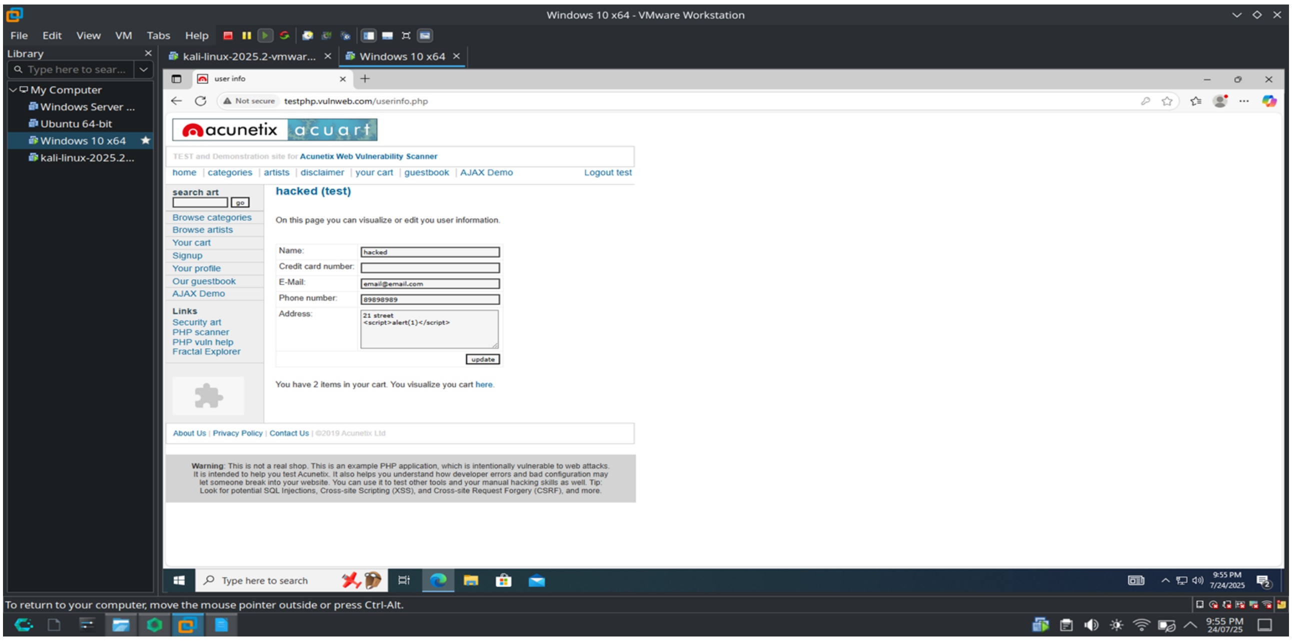
Step 3: Accessing the Site from Windows VM

Actions:

➓ Open browser in Windows VM.

- Fill the form with credentials (`admin / password`) and submit.



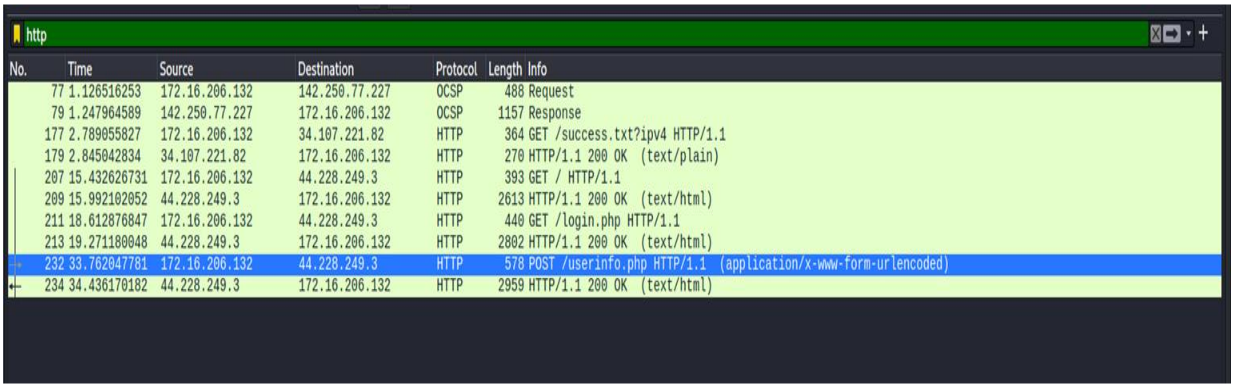


Step 4: Starting Wireshark on Kali Linux

Actions:

- Launch Wireshark:
- Select the active network interface (e.g., `eth0`, `ens33`)
- Apply filter:

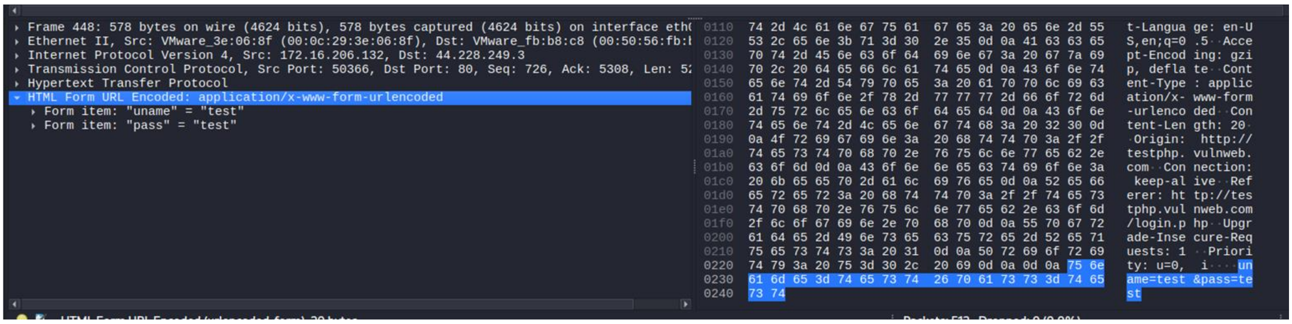
http



Step 5: Capturing and Analyzing HTTP Credentials

Actions:

1. In Wireshark, locate packet with `POST /login HTTP/1.1`
2. Right-click → Follow → **HTTP Stream**
3. Extract:



Conclusion

This project shows that:

- **Unencrypted traffic is easily intercepted**
- **Sensitive data must be protected using encryption**
- Organizations must move away from insecure legacy protocols

Recommendations

- Enforce use of **HTTPS**, **SFTP**, **SSH**
- Deploy **TLS/SSL certificates** across all web services
- Monitor and audit network activity regularly
- Educate users about secure communication