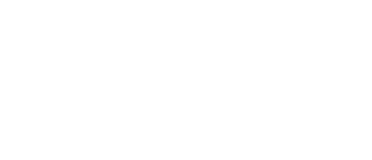


# Packet Sniffing: Risks and Mitigation

By Dhanni Koul, Arya Sharma , Aaditya Pratap Singh.

Roll No: 2023A1R005

Branch: CSE A3



5

Key Takeaways & Mitigation

Protecting your network.

# Agenda

3

Lab Setup & Tools

Hands-on demonstration with Wireshark.

1

Understanding Packet Sniffing

What it is and why it's used.

2

Unencrypted Data Risks

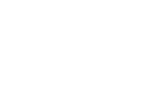
Exposure of sensitive information.

4

Simulating Credential Exposure

Real-world scenario replication.

What is Packet Sniffing?



### Definition

Packet sniffing is the act of capturing and analysing data packets as they travel across a computer network. It's like eavesdropping on network conversations.

### Purpose

Used for network monitoring, diagnostics, and security analysis. Malicious actors use it to intercept sensitive data.

# The Risk: Unencrypted Data Transmission

## preencoded.png Credential Exposure

Usernames and passwords sent in plain text are easily intercepted and stolen.

## preencoded.png Session Hijacking

Attackers can steal session cookies, gaining unauthorised access to user accounts.

## preencoded.pngData Leakage



Sensitive business documents, personal information, and financial data can be compromised.

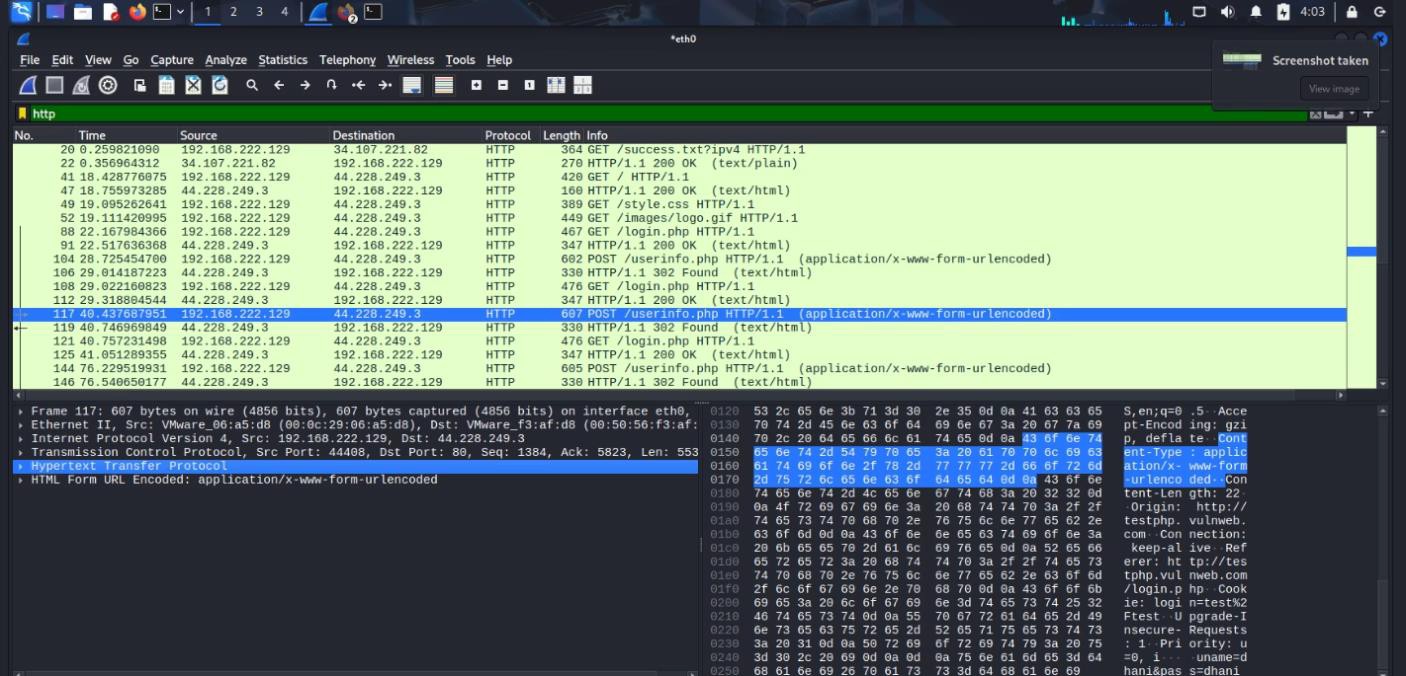
## Compliance Violations

Failure to encrypt data can lead to regulatory fines and legal consequences.

Lab Simulation: Sniffing Credentials

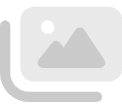


#### Lab Setup

* Virtual Machines: Kali Linux (attacker) and Windows (victim).
* Network Configuration: Both VMs on the same virtual network.

#### Tools Used

* Wireshark on Kali Linux: For packet capture and analysis.
* Test Website/FTP: A non-HTTPS platform for credential transmission.



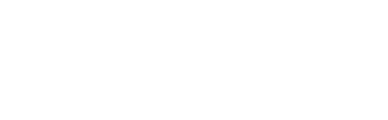
# Mitigation Strategies and Best Practices

## Always Use Encryption

Implement HTTPS/SSL/TLS for all web traffic and SFTP/SCP for file transfers.

## Network Segmentation

Divide your network into isolated segments to limit attacker movement.



## Strong Authentication

Enforce multi-factor authentication (MFA) and strong

password policies.

## Regular Audits

Conduct frequent penetration testing and security audits to

identify vulnerabilities.



Thank You!