#### Project report on

**Investigating Network Vulnerabilities Using Packet Sniffing**

**A Dissertation submitted in partial fulfillment of the Academic requirements for the award of the degree of**

**Bachelor of Technology**

## In

**Computer Science & Engineering (Cyber Security)**

**Submitted by**

S. Saiteja (22H51A6250)

V. Anjali (22H51A6260)

G. Sai Deepthi (23H55A6201)

**Under the esteemed Guidance of**

**Dr.R.Venkateswara Reddy (Associate Professor and HOD,CSC)**



**Department of Cyber Security**

#### CMR COLLEGE OF ENGINEERING & TECHNOLOGY

**(Autonomous)**

**(NAAC Accredited with ‘A+’ Grade & NBA Accredited) (Approved by AICTE, Permanently Affiliated to JNTU Hyderabad)**

**KANDLAKOYA, MEDCHAL ROAD, HYDERABAD-501401**

#### CMR COLLEGE OF ENGINEERING & TECHNOLOGY

**(Autonomous)**

**(NAAC Accredited with ‘A+’ Grade & NBA Accredited) (Approved by AICTE, Permanently Affiliated to JNTU Hyderabad)**

**KANDLAKOYA, MEDCHAL ROAD, HYDERABAD-501401**

**DEPARTMENT OF CYBER SECURITY**



#### CERTIFICATE

This is to certify that the Mini Project -1 report entitled “**Investigating Network Vulnerabilities Using Packet Sniffing”**  being submitted by **S Saiteja (22H51A6250), V Anjali (22H51A6260), G Sai Deepthi (23H55A6201)** in partial fulfillment for the award of **Bachelor of Technology in Computer Science and Engineering (Cyber Security)** is a record of bonafide work carried out his/her under my guidance and supervision .The results embodied in this project report have not been submitted to any other University or Institute for the award of any Degree.

K. Sujitha Dr. R. Venkateswara Reddy

Assistant Professor Associate Professor & HOD

Dept. of CSC Dept. of CSC

#### ACKNOWLEDGEMENT

With great pleasure I want to take this opportunity to express my heartfelt gratitude to all the people

`who helped in making this project a grand success.

I am grateful to **K. Sujitha**, Assistant Professor, Dept. of Computer Science and Engineering for her valuable suggestions and guidance during the execution of this project.

I would like to thank **Dr. R. Venkateswara Reddy**, Head of the Department of Computer Science and Engineering, for his moral support throughout the period of my study in CMRCET.

I am highly indebted to **Major Dr. V.A. NARAYANA**, Principal CMRCET, for giving permission to carry out this project in a successful and fruitful way.

I would like to thank the Teaching & Non- teaching staff of the Department of Computer Science and Engineering for their co-operation.

Finally, I express my sincere thanks to **Mr. CH. GOPAL REDDY**, Secretary, CMR Group of Institutions, for his continuous care. I sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project work.

S Saiteja

(22H51A6250)

V Anjali

(22H51A6260)

G Sai deepthi (23H55A6201)

#### ABSTRACT

* A packet sniffing attack, or simply a sniffing attack, is a cyber-attack that involves intercepting

and misusing content (like reading sensitive data) passing through a network in the form of

packets. Unencrypted email communications, login passwords, and financial information are

common targets for a packet sniffing attack.

* Besides this, an attacker may also use sniffing tools to hijack packets by injecting malicious code into the packet itself, which executes once it reaches the target device. Security specialists in the industry frequently employ this technique to keep tabs on how data is transmitted across their network.
* Typically, a packet comprises the information or data that is to be transported between two network sit from the sender to the intended recipient.
* Additionally, we can set up a system to trace any unauthorized access to critical information or ensure that the network infrastructure surrounding this packet transmission is protected from external incursions.

**Table Of Content**

|  |  |  |
| --- | --- | --- |
| **CHAPTERS** | **DESCRIPTION** | **PAGE NUMBERS** |
| 1 | INTRODUCTION | 2 |
| 1.1 | AIM | 3 |
| 1.2 | SCOPE | 4 |
| 2 | LITERATURE REVIEW | 6 |
| 3 | EXISTING SOLUTIONS | 8 |
| 4 | PROPOSED SYSTEM | 11 |
| 4.1 | REQUIREMENT ANALYSIS | 12 |
| 4.1.1 | HARDWARE REQUIREMENTS | 12 |
| 4.1.2 | SOFTWARE REQUIREMENTS | 12 |
| 4.2 | MERITS AND DEMERITS | 13 |
| 5 | DESIGN DESCRIPTION | 15 |
| 5.1 | CONCEPTUAL DESIGN | 15 |
| 6 | IMPLEMENTATION AND DISCUSSION | 16 |
| 6.1 | IMPLEMENTATION | 17 |
| 7 | RESULT | 20 |
| 8 | CONCLUSION AND FUTURE ENHANCEMENT | 21 |
| 8.1 | CONCLUSION | 21 |
| 8.2 | ENHANCEMENT | 21 |
| 8.3 | REFERENCES | 24 |

# CHAPTER 1

1

#### INTRODUCTION

* In cyberspace, the systems are vulnerable which makes easier to gain an unauthorized access to sensitive data .
* Identification and prevention of vulnerability plays a key role in solving the issues related to unauthorized access.
* Vulnerability analysis, is a thorough security testing process that helps identify and fix weaknesses in computer systems, networks, and applications.
* It generates a report summarizing key findings and recommended actions, providing stakeholders with a clear overview of the security status.
* Moreover, our open-source platform enables easy access and sharing of these vital reports via our website.

#### AIM

* + The aim of our project is to investigate network vulnerabilities using packet sniffing exploiting a windows machine.
  + We can analyze the traffic through the network, so that we can gain access to user names and passwords while logging in to a website.
  + Security weaknesses represent vulnerabilities or gaps in a system's defenses that, if exploited, can compromise the confidentiality, integrity, or availability of sensitive information and expose an organization to potential cyber threats.

#### SCOPE

* + Simulate real-world cyber attacks on the Windows machine to exploit identified vulnerabilities and assess the effectiveness of existing security measures.
  + Enhances user awareness of emerging threats and vulnerabilities.
  + Tool is open source to encourage collaboration, community contributions, and continuous improvement.
  + Foster a community of security professionals and developers to enhance the platform's capabilities.
  + Simulating real-world cyberattacks to assess the effectiveness of existing security controls and to identify any potential security gaps.

# CHAPTER 2

#### LITERATURE REVIEW

###### 

**Early Reviews**

In the early days of networking, packet sniffing was primarily discussed in the context of network troubleshooting and protocol analysis. Early reviews, such as those by McCanne and Jacobson (1993), focused on the development and application of tools like tcpdump. These reviews provided foundational knowledge on how packet sniffing could be used to understand network behavior and diagnose issues.

**The Rise of Network Security**

As cybersecurity became a more prominent concern, reviews in the late 1990s and early 2000s, such as those by Paxon (1999), began to emphasize the role of packet sniffing in detecting and preventing security breaches.

**Educational Uses**

Kurose and Ross (2010) discussed the pedagogical applications of packet sniffing, particularly with Wireshark. Their review emphasized how packet sniffing could be used to teach networking concepts and protocols in academic settings, providing practical, hands-on experience to students.

# CHAPTER 3

#### EXISTING SOLUTION

###### Nessus:

A widely used vulnerability scanner that identifies vulnerabilities, configuration issues, and malware in various environments.



**Fig 1:** Nessus

###### Metasploit:

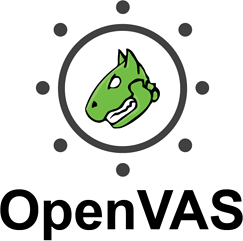
An advanced penetration testing tool that helps test security vulnerabilities, perform security assessments, and manage security assessments.



**Fig 2:** Metasploit

###### OpenVAS:

An open-source vulnerability scanner that detects issues in systems and networks, providing a comprehensive view of potential vulnerabilities.



**Fig 3:** OpenVas

###### Nmap:

A powerful network scanning tool that can be used for both security and network exploration, helping to discover hosts and services on a computer network.



###### Burp Suite:

**Fig 4:** NMAP

A comprehensive platform for web application security, offering a range of tools for performing security testing of web applications.

**Fig 5:** Burpsuit

# CHAPTER 4

#### PROPOSED SYSTEM

The proposed system is a simple process that helps find vulnerabilities in a network. In this project we will be using Wireshark for packet sniffing. First we need to capture the packets and then analyze. In this page the user will find the unencrypted data passing through a network.

For this purpose we need kali Linux in which we use a tool called Wireshark, by scanning the network.

Let us see some pictures of tool and how it works and captures the packets.

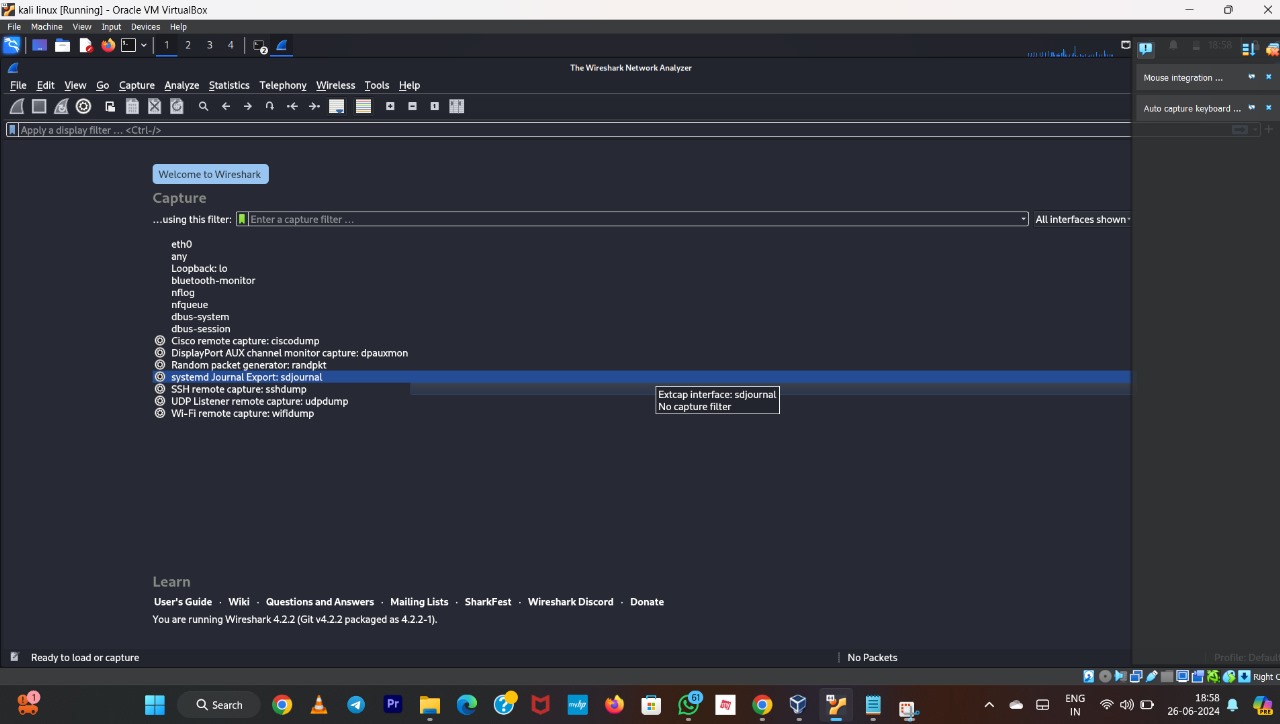


Fig 6

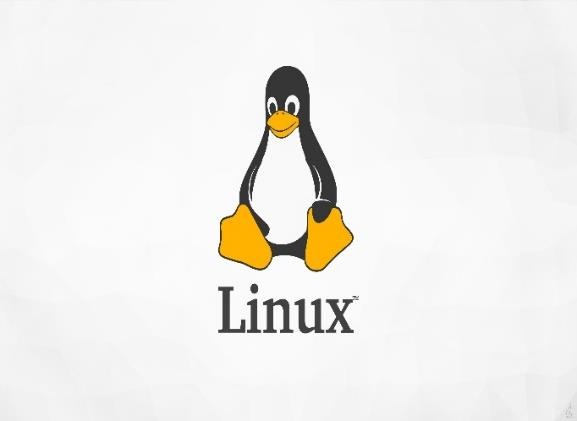
#### REQUIREMENT ANALYSIS

###### Software Requirements

* + - * Windows 7 or later, Linux, or macOS
      * Web application framework
      * Scanning Tools

###### Hardware Requirements

* + - * System 32 or 64 bit with 4 GB or 8 GB RAM
      * Network Security Devices
      * CPU
      * RAM



##### MERITS AND DEMERITS

###### Merits:

* Proactive Risk Management
* Centralized Reporting
* User-Friendly Interface
* Scalability
* Community Collaboration

###### Demerits:

* Security Concerns (if Not Properly Secured)
* Reliance on third-party tools introduces a dependency on their accuracy and effectiveness, and vulnerabilities in these tools could pose risks.

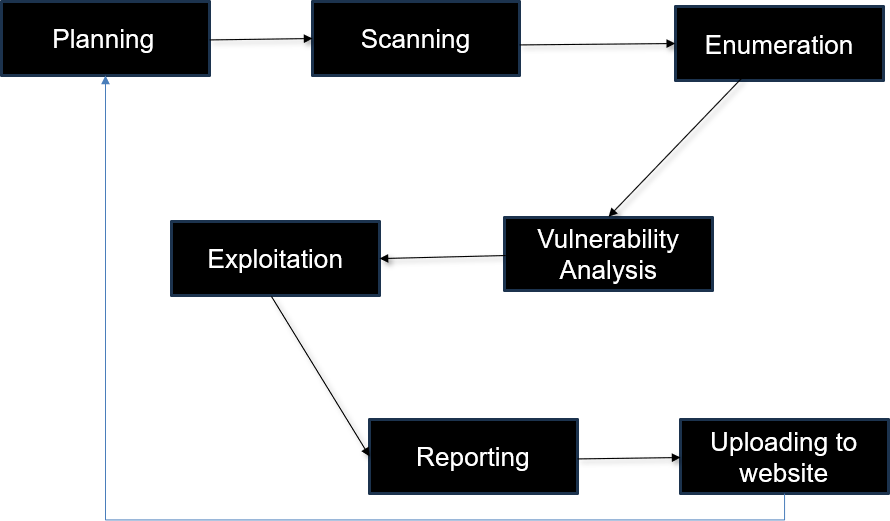
# CHAPTER 5

14

#### DESIGN DESCRIPTION

##### 5.1 CONCEPTUAL DESIGN

The diagram shows the steps involved in investigating network vulnerabilities using packet sniffing



**Fig 7:** Steps for scanning a network

# CHAPTER 6

* 1. **IMPLEMENTATION AND DISCUSSION**
     1. **IMPLEMENTATION**

## Capture Traffic:

It is the first stage in sniffing the network traffic. we need to select the interface capture filter in wireshark whether it is eth0,any or Bluetooth etc. Here we will be using eth0 interface.

### COMMAND: sudo wireshark -i eth0 -k

**Fig 8:** selecting interface

## Scanning:

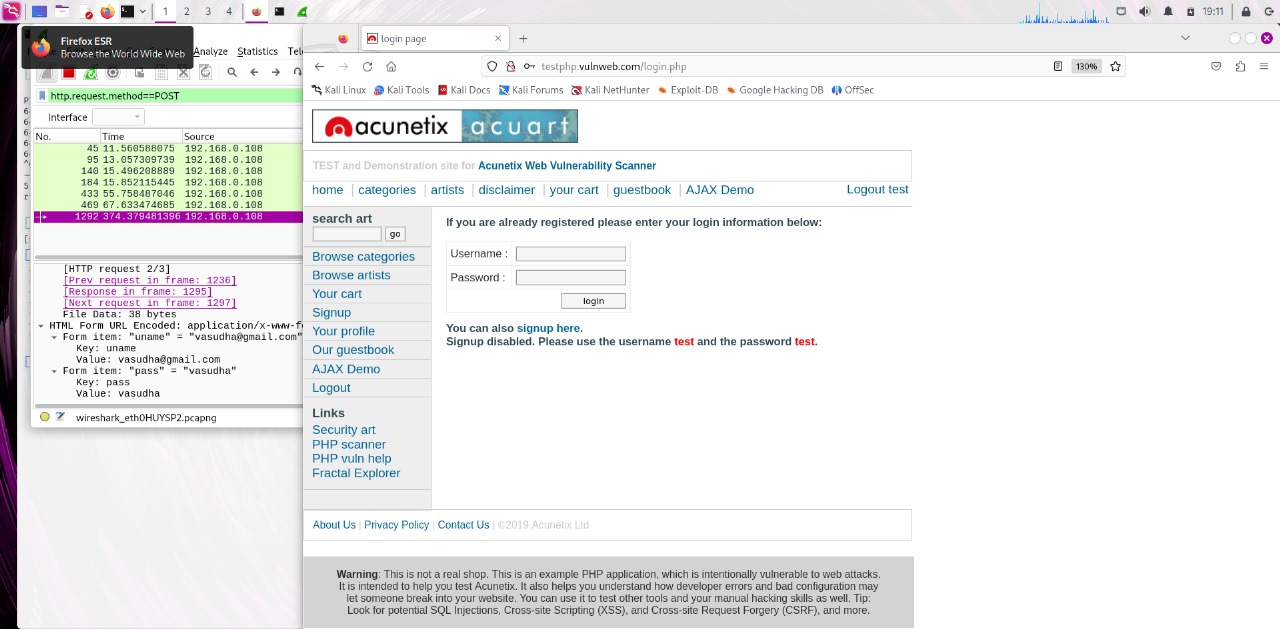
It is the methodical process of inspecting systems, applications, and networks to find any potential flaws, incorrect setups, or vulnerabilities.

### COMMAND: sudo wireshark -i eth0 -k

**Fig 9:**Scanning

## Gaining access:

It is the phase where an attacker obtains control over the target. Be it a network or a web application, “Gaining Access” is only the beginning.

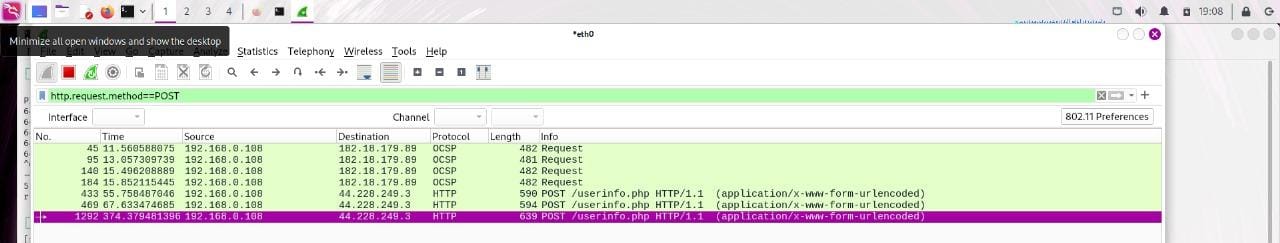


**Fig 10**

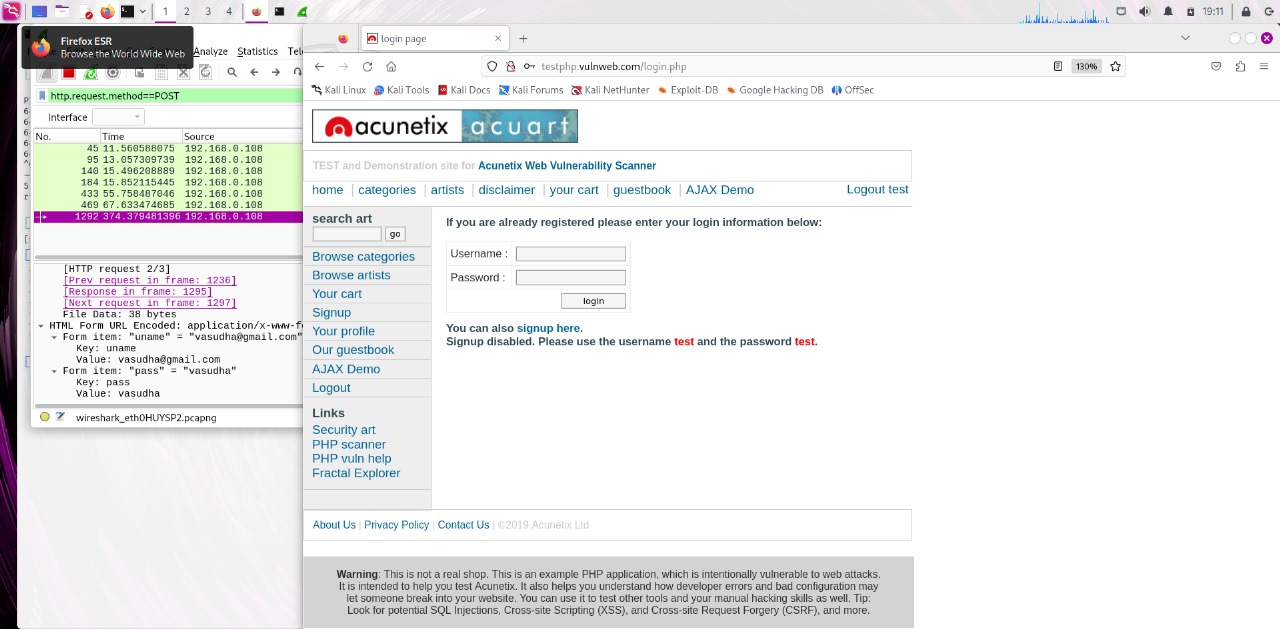
# CHAPTER 7

#### RESULT

we have successfully gained the access to the vulnerable system .Now we can take control of system



**Fig 11**



**Fig 12**

# CHAPTER 8

#### CONCLUSION AND FUTURE ENHANCEMEMT

##### CONCLUSION

* + - In conclusion, Critical vulnerabilities have been identified and addressed through robust measures.
    - Prioritizing security has equipped us to protect our data and operations
    - This project serves as a foundation for continuous improvement and commitment to security.
    - User credentials like username and password are captured.
    - Thanks to the team members and stakeholders for their dedicated efforts.

##### 8.2 FUTURE ENHANCEMENTS

* **Enhanced Support for Encrypted Traffic Analysis**

As the use of encryption grows to protect data privacy and integrity, the ability to analyze encrypted traffic becomes increasingly important for network monitoring and security.

* **Integration with Machine Learning and AI**

The integration of machine learning (ML) and artificial intelligence (AI) can automate the detection of patterns, anomalies, and potential security threats in vast amounts of network data.

* Implement a notification system to alert users about new vulnerabilities, updates, and critical security

#### 8.3 REFERENCES

* Al-Shaer, E., Al-Haj, S., & Hariri, S. (2014). Network Security: A Beginner's Guide. McGraw-Hill Education.
* Cascarilla, J., Zhou, H., & Chen, Z. (2018). Network Security Monitoring Using Wireshark. Journal of Network and Computer Applications, 111, 95-104.
* Comer, D. (2018). Internetworking with TCP/IP Volume One (6th ed.). Pearson.
* Dilley, J., Dean, J., Barroso, L., & Jeffery, C. (2017). Network Performance Analysis and Optimization. Communications of the ACM, 60(4), 45-53.
* Kurose, J. F., & Ross, K. W. (2010). Computer Networking: A Top-Down Approach (6th ed.). Pearson.
* McCanne, S., & Jacobson, V. (1993). The BSD Packet Filter: A New Architecture for User-level Packet Capture. Proceedings of the USENIX Winter Conference.
* Orebaugh, A., Ramirez, G., & Beale, J. (2006). Wireshark & Ethereal Network Protocol Analyzer Toolkit. Syngress.
* Paxon, V. (1999). Bro: A System for Detecting Network Intruders in Real-Time. Computer Networks, 31(23-24), 2435-2463.
* Sanders, C. (2011). Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems. No Starch Press.
* Zekri, M., El Kafhali, S., Aboutabit, N., & Saadi, Y. (2020). Anomaly Detection Using Machine Learning Techniques in Wireshark Network Traffic. International Journal of Advanced Computer Science and Applications, 11(5), 24-31.