## INTERNSHIP REPORT

A report submitted to in partial fulfillment of the requirements for the award of the degree of

## BACHELOR OF TECHNOLOGY

**in**

**ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING**

**Submitted by**

**B SUBHASH (22R91A7320)**

**Under the Guidance**

**Of**

**Mr. Sandip Gavit**

## TechnoHacks Solutions Pvt.Ltd.

**Nasik, Maharashtra**

**(Duration: 30TH May, 2024 to 30th June, 2024)**



## Department of Artificial Intelligence and Machine Learning

## TEEGALA KRISHNA REDDY ENGINEERING COLLEGE

**(An Autonomous Institution)**

**Medbowli, Meerpet, Saroornagar, Hyderabad – 500097**

**(Affiliated to JNTUH, Approved by AICTE, Accredited by NBA & NAAC ‘A’) (2024-2025)**

**TEEGALA KRISHNA REDDY ENGINEERING COLLEGE**

**(Sponsored by TKR Educational Society)**

**Approved by AICTE, Affiliated by JNTUH, Accredited by NBA & NAAC-A)**

Medbowli, Meerpet, Saroornagar, Hyderabad – 500 097.

Phone: 040-24092838 Fax: +91-040-24092555

E-mail: [tkrec@rediffmail.com](mailto:tkrec@rediffmail.com) Website: [www.tkrec.ac.in](http://www.tkrec.ac.in)

**Department of Artificial Intelligence And Machine Learning**

# 

# College code: R9

# CERTIFICATE

This is to certify that the Internship report titled “**CYBERSECURITY & ETHICAL HACKING**” is being submitted by **BUREDI SUBHASH** (22R91A7320) is work done by him/her and submitted during 2024-2025 academic year, in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Artificial Intelligence and Machine Learning, at **Teegala Krishna Reddy Engineering College**, Hyderabad.

Internship Coordinator Head of the Department

Sangeeta Jawar

**TABLE OF CONTENTS**

TITLE PAGE NO

1. **Abstract 1**
2. **Introduction 2**
3. **Requirements 3**

3.1 Hardware Requirements

3.2 Software Requirements

3.3 Network Setup

3.4 Other Requirements

1. **Code Explaination 4-6**

4.1 Rock Paper Scissors Game

4.2 Kali Linux Setup in VirtualBox

4.3 Burp uite tool

1. **Significance in Python Development 7**
2. **Conclusion 8**
3. **References 9**

**Cybersecurity and Ethical Hacking**

**ABSTRACT**

Cybersecurity & Ethical Hacking often uses key tools for network and web security testing. It consists of projects like Sniffing Attack using Wireshark to capture and analyze network traffic, set up Kali Linux in a VirtualBox environment for penetration testing, and used Burp Suite to assess web application vulnerabilities. These tasks enhanced my understanding of ethical hacking methodologies and provided hands-on exposure to important security tools.

**2. INTRODUCTION**

Overview of Cybersecurity & Ethical Hacking:

Cybersecurity is a field dedicated to protecting systems, networks, and data from unauthorized access, attacks, and damage. Ethical Hacking involves legally testing and probing systems for vulnerabilities to help organizations enhance security. As digital systems become more interconnected, the need for cybersecurity professionals to prevent and mitigate potential threats is critical.

Importance of the Internship:

The internship provided hands-on experience and knowledge in the field of Cybersecurity & Ethical Hacking. Gained exposure to industry-standard tools like Wireshark, Kali Linux, and Burp Suite for network analysis, penetration testing, and web application security.

Tasks Completed:

* Sniffing Attack using Wireshark: Captured and analyzed network traffic to understand how data can be intercepted.
* Kali Linux Setup in VirtualBox: Installed Kali Linux for penetration testing and ethical hacking activities.
* Burp Suite Tool: Utilized Burp Suite to identify and test vulnerabilities in web applications.

Objective of the Report:

This report aims to document the tasks completed during the internship, the tools used, and the key skills learned. The report will detail the methodologies and techniques applied in each task, providing insights into the practical applications of ethical hacking and security analysis.

**3. REQUIREMENTS**

**3.1 Hardware Requirements:**

* Computer System: A PC or laptop with sufficient processing power, memory, and storage.
* Processor: A modern processor (e.g., Intel i5 or higher).
* RAM: At least 8GB (preferably 16GB for smooth operation, especially when using virtual machines).
* Storage: Sufficient disk space to install the necessary software

**3.2 Software Requirements:**

* Operating System: Windows, Linux, or macOS.
* VirtualBox: Needed for setting up Kali Linux in a virtualized environment.
* Web Browser: A modern browser like Google Chrome or Firefox to interact with tools like Burp Suite and access web applications for testing.
* Wireshark: For packet capture and network traffic analysis.
* Kali Linux: A Linux distribution specifically designed for penetration testing and ethical hacking.
* Burp Suite: A security testing tool for web applications, which helps in identifying vulnerabilities.

**3.3 Network Setup:**

* Local Network or Isolated Environment
* Access to Test Systems

**3.4 Other Requirements:**

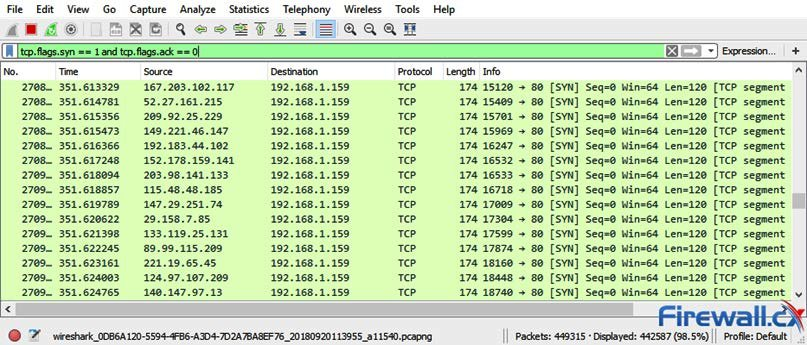
* Administrator Access
* Internet Access
* Technical Knowledge

**4. CODE EXPLAINATION**

**4.1 Sniffing Attack using Wireshark**

In this task, Wireshark was utilized to capture and monitor real-time network traffic. The objective was to understand how sensitive information, like usernames and passwords, can be exposed over unsecured networks.

The process involved selecting a network interface, applying filters to isolate specific protocols (such as HTTP, FTP), and analyzing packet data for vulnerabilities. This practical exposure demonstrated the risks of unencrypted communication and highlighted the importance of secure protocols like HTTPS in preventing data breaches.

****

**4.2 Kali Linux Setup in VirtualBox**

The goal here was to create a penetration testing environment without affecting the host system. Kali Linux, a Linux distribution packed with cybersecurity tools, was installed on VirtualBox.

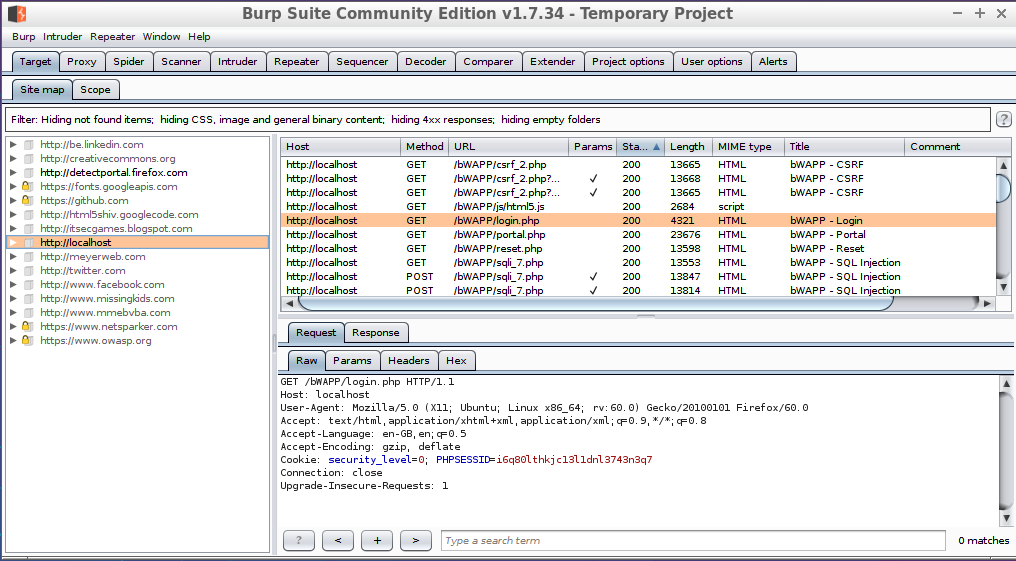
The setup process included configuring virtual hardware (CPU, RAM, network adapters), importing the Kali ISO image, and ensuring internet access within the VM. Post-installation, common tools like Nmap, Metasploit, and Wireshark were verified. This task emphasized the need for isolated, flexible environments for safely conducting ethical hacking and security assessments.

****

**4.3 Burp Suite Tool**

Burp Suite was used to perform web application vulnerability assessments. After setting up a browser proxy to route traffic through Burp Suite, the tool intercepted HTTP requests and responses.

The testing workflow involved using features like Intruder (for automated attack testing), Repeater (for manual testing), and Scanner (to detect vulnerabilities such as SQL Injection, Cross-Site Scripting). Through this project, a detailed understanding of how attackers find and exploit web app vulnerabilities was developed, along with methods for securing applications.



**5. Significance in Cybersecurity**

The internship tasks provided a foundational understanding of practical cybersecurity concepts critical in today’s digital landscape. Through Wireshark, real-world sniffing attacks were simulated, showcasing how attackers can intercept unprotected data on a network, emphasizing the need for encryption and secure communication protocols like HTTPS, VPNs, and SSL/TLS.

Setting up Kali Linux in VirtualBox demonstrated the importance of isolated environments for penetration testing, ensuring that security tests do not interfere with production systems. This approach reflects how cybersecurity professionals operate safely and ethically while discovering system vulnerabilities.

By working with Burp Suite, the internship highlighted the growing risk to web applications, one of the most targeted assets today. Skills in intercepting, modifying, and analyzing web traffic reinforced knowledge about common attack vectors such as SQL Injection, Cross-Site Scripting (XSS), and insecure session management. This experience stressed the importance of secure coding practices and regular vulnerability assessments in web development.

**6. Conclusion**

The internship at TechnoHacks Edutech offered valuable practical experience in cybersecurity fundamentals. By working on tasks like network sniffing with Wireshark, virtual environment setup with Kali Linux, and web vulnerability testing using Burp Suite, I developed strong technical and analytical skills. These activities provided insight into real-world security challenges, the importance of proactive defense strategies, and ethical considerations in cybersecurity. Overall, the internship enhanced both my theoretical knowledge and hands-on abilities, preparing me for advanced roles in the cybersecurity domain. Additionally, the projects helped in building a problem-solving approach and familiarized me with industry-standard tools and methodologies. This experience laid a strong foundation for further specialization in ethical hacking and network security fields.

**7. References**

* Official Wireshark Documentation

Provided in-depth understanding of packet capturing, network traffic analysis, and interpreting various protocol layers. Helped in learning how sniffing attacks are performed and how data can be protected.

Link: https://www.wireshark.org/docs/

* Kali Linux Documentation and Guides

Served as the primary source for installing and configuring Kali Linux in a virtualized environment. It guided the usage of ethical hacking tools and best practices for setting up a secure and efficient penetration testing environment.

Link: https://www.kali.org/docs/

* Burp Suite User Guide

Helped in mastering the features of Burp Suite for web application security testing, including techniques for intercepting traffic, scanning for vulnerabilities, and exploiting weaknesses for ethical hacking purposes.

Link: https://portswigger.net/burp/documentation

* TechnoHacks Edutech Internship Material and Training Resources

Internship-provided study material, practical tasks, and guidance notes formed the base for executing and understanding real-world cybersecurity scenarios effectively.

Link: https://technohacks.co.in/

