Lab 1: Setup Lab Environments

Shivali Mate

I. Introduction

THE objective of this lab was to build a secure and controlled environment to learn cybersecurity concepts. This involved setting up a Virtual Machine with Ubuntu 20.04 LTS, installing and running WebGoat along with WebWolf, and exploring their functionalities. These tools provided a practical introduction to common vulnerabilities in web applications, how attackers exploit them, and how defenders can analyze and mitigate such risks.

II. Lab Setup Overview

The setup process for this lab involved configuring a Virtual Machine with Ubuntu, installing WebGoat and WebWolf, and enabling remote access through IU's Research Desktop (RED). These steps established the environment needed to safely explore web application vulnerabilities and attacker techniques.

A Virtual Machine was created using Ubuntu 20.04 LTS [1] as the operating system, configured with 4 GB RAM, 2 CPUs, and 50 GB storage. The VM creation process is illustrated in Fig. 1, and the resulting Ubuntu instance running inside Virtual Machine Manager is displayed in Fig. 2. Virtualization provides isolation and flexibility, making it a common practice in both academic and industry research environments.

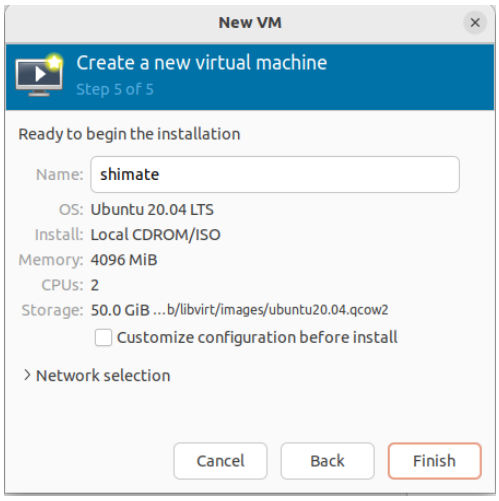

Fig. 1. VM creation in Virtual Machine Manager

WebGoat version 2023.8 was then installed in standalone mode after setting up Java 17. WebGoat is a deliberately insecure application maintained by OWASP (as discussed in [2], [3], [4]), which is widely used for teaching and testing common vulnerabilities. Once launched, the login page was successfully accessed through the browser, as shown in Fig. 3. WebWolf was also enabled to complement WebGoat by simulating attacker infrastructure, providing features such as file hosting, phishing mailboxes, and request capture.

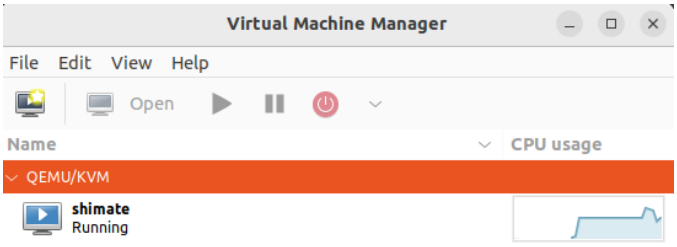

Fig. 2. Running Ubuntu instance in VM Manager

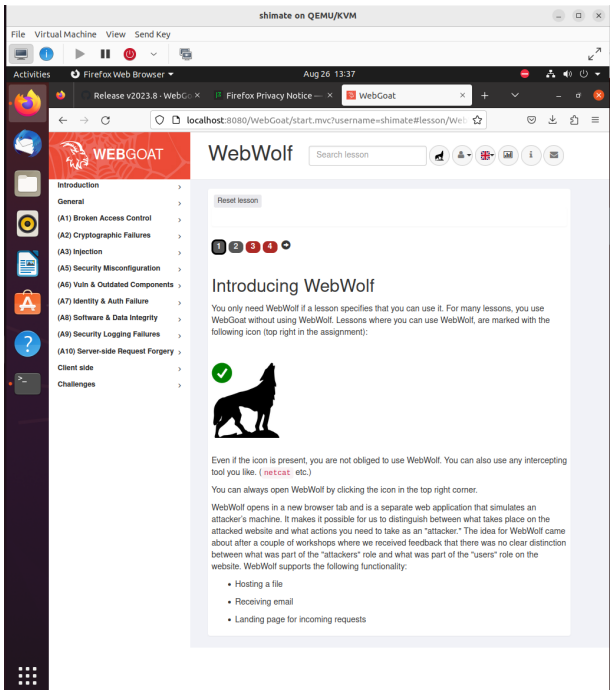

Fig. 3. Running Ubuntu instance and Webwolf localhost in VM Manager

To support remote access, IU's Research Desktop (RED) was configured [9]. RED provides a browser-based Linux desktop that allows students to securely log in with their IU accounts and connect to lab machines through SSH. This enables continued work outside the classroom while still managing virtual machines seamlessly. A sample RED session is displayed in Fig. 4.

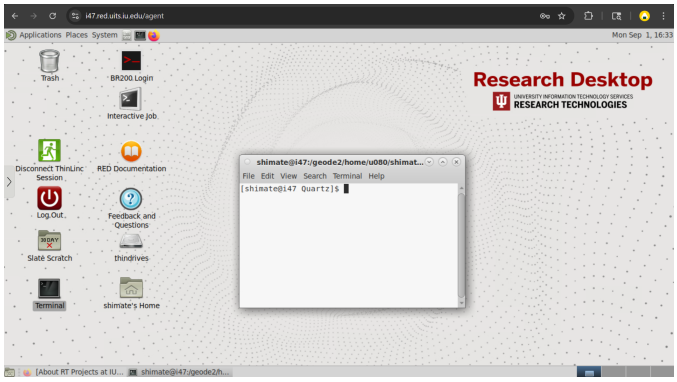

Fig. 4. Remote desktop session using IU RED

In addition, Overleaf (Open Web Application Security Project) [5] and GitHub [6], [7], [8] were set up to manage lab reports and maintain version control of submissions. While these tools primarily support documentation and collaboration, the main technical focus of this lab remained on working with WebGoat and WebWolf for security practice.

III. Tools Learned and Their Purpose

As part of this lab, several tools were introduced that form the foundation for practicing cybersecurity in a safe and controlled environment. Each tool serves a distinct purpose, from providing isolation to simulating real-world attack scenarios.

- **Virtual Machine Manager / Ubuntu VM:** Provided an isolated and safe environment to install and run tools without impacting the host machine, simulating a real-world test environment.
- **WebGoat (OWASP):** A deliberately insecure web application designed to demonstrate common vulnerabilities such as SQL injection, XSS, and weak authentication. It is used by security professionals and students to practice penetration testing and improve secure coding skills.
- **WebWolf:** Works alongside WebGoat to simulate the attacker-controlled infrastructure. It gives a realistic environment to practice how attackers use external systems during attacks.

IV. WebWolf Functionalities

WebWolf extends WebGoat by providing attacker-like services. In real-world scenarios, attackers rarely operate solely within a target system, they rely on external infrastructure to store stolen data, host malicious files, or interact with compromised applications. WebWolf replicates this environment with three main features:

- **Files:** This functionality allows upload and download of files, simulating how attackers might host malicious payloads or exfiltrate sensitive data from a compromised system.
- **Mailbox:** Provides an email inbox where phishing messages or fake emails can be sent and received. This demonstrates how attackers trick users into clicking links, downloading attachments, or revealing credentials.
- **Incoming Requests:** Captures and displays HTTP requests, mimicking the way attackers set up servers to receive callbacks from vulnerable applications. This is commonly used in command-and-control communication or data collection after exploitation.

Together, these features illustrate how attackers coordinate between a vulnerable target and their own infrastructure, giving students hands-on practice in recognizing and defending against these strategies.

V. Knowledge and Improvements

This lab helped me understand how insecure coding leads to vulnerabilities like SQL injection and session hijacking. WebGoat made these issues practical, while WebWolf showed how attackers can use external systems to steal data, send phishing emails, or capture requests. I also learned more about HTTP, cookies, and sessions, and how they can be exploited if not secured properly. These lessons are directly useful in both academic research and industry security practices. At the same time, I saw that the exercises are simplified compared to real-world attacks, where tools like OWASP ZAP or Burp Suite are often needed for deeper analysis.

VI. Conclusion

This lab successfully provided hands-on experience with virtualization and web application security. The key outcome was learning how WebGoat and WebWolf simulate real vulnerabilities and attacker infrastructure, offering a safe space to understand and practice offensive and defensive security. These tools will be central to the upcoming labs and are directly relevant to modern cybersecurity practices in both industry and academia.

References

[1] https://ftp.ussg.iu.edu/linux/ubuntu-releases/focal/ubuntu-20.04.6-desktop-amd64.iso
[2] https://github.com/WebGoat/WebGoat/wiki
[3] https://github.com/WebGoat/WebGoat/releases/tag/v2023.8
[4] https://owasp.org
[5] https://www.overleaf.com/
[6] https://guides.github.com/activities/hello-world/
[7] https://help.github.com/articles/fetching-a-remote/
[8] https://help.github.com/articles/caching-your-github-password-in-git/platform-linux
[9] https://red.uits.iu.edu/