Lab 1: Setup Lab Environments

B649 Cyber Defense

***Abstract*—This lab introduced key tools and workflows used throughout the semester in cyber defense competitions. The main objectives were to set up a virtual machine running Ubuntu, install and configure WebGoat and WebWolf to explore common web vulnerabilities, and establish collaborative workflows using Overleaf and GitHub. Additionally, I configured IU Research Desktop (RED) for remote access. During the process, I faced challenges with Quartz account activation and transferring images from the VM, which helped me develop persistence and practical troubleshooting skills.**

I. Introduction

Cybersecurity requires both safe environments to practice attacks and defenses as well as professional workflows to document and share results. This lab laid the groundwork for both. By building an Ubuntu virtual machine, I created an isolated environment to test tools like WebGoat. Using Overleaf and GitHub, I adopted academic and industry-standard methods for documentation and collaboration. Finally, IU's RED platform ensured that I could continue my lab work remotely. While the technical tasks were central, the experience also emphasized the importance of adaptability—resolving issues such as delayed Quartz account activation and difficulties transferring screenshots from the VM tested my patience and improved my problem-solving skills.

II. Tools Used

Virtual Machine Setup

I installed Ubuntu 20.04.6 LTS on a virtual machine using Virtual Machine Manager with specifications of 4 GB RAM, 2 CPUs, and 50 GB storage. NAT networking was configured to allow the VM to access the internet safely while being isolated from the host system [Fig.1] This gave me firsthand experience with virtualization, a critical skill for creating controlled environments in cybersecurity.

Installing Webgoat

WebGoat, developed by OWASP, is deliberately insecure web application designed for practicing web application security. I installed WebGoat (v2023.8) in standalone mode after setting up Java 17. Once launched, I accessed the WebGoat login page via http://localhost:8080/WebGoat. [1] [Fig.2] As I read further on WebGoat it revealed topics on vulnerabilities like SQL injection, cross-site scripting (XSS), authentication flaws, and insecure deserialization. This taught me how insecure code can be exploited, and why secure coding practices are vital. Alongside WebGoat, I also ran WebWolf, which simulates attacker infrastructure. Its features included:

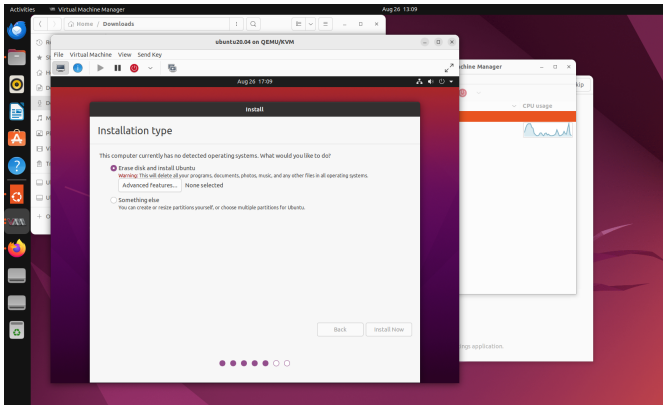

Fig. 1: Virtual Machine Installation

- **Files** – used for hosting or exfiltrating files, as an attacker might.
- **Mailbox** – used in simulating phishing emails and user deception.
- **Incoming** – requests used in mimicking callback traffic from compromised systems.

Together, WebGoat and WebWolf provided me with insight into both the attacker's toolkit and the defender's perspective in analyzing these malicious behaviors.

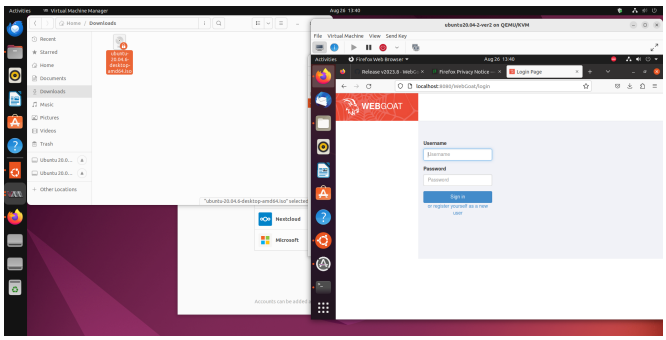

Fig. 2: Webgoat Login Page

Overleaf

I created an Overleaf account and used the provided LaTeX template to draft lab reports. This taught me how to structure professional technical documents with automatic formatting. Compared to traditional word processors, Overleaf enforces consistency and readability—skills valuable in both academia and industry.[2]

GitHub

I created a private repository on github.iu.edu using the naming convention IU_B649_I590_CyberDefense_shasbi. I

added collaborators [Fig.3] and pushed my first PDF report generated from Overleaf. This taught me how to manage version control workflows, track changes, and share academic work securely. While I was familiar with GitHub conceptually, this exercise gave me real confidence in committing, pushing, and organizing content.[3][4]

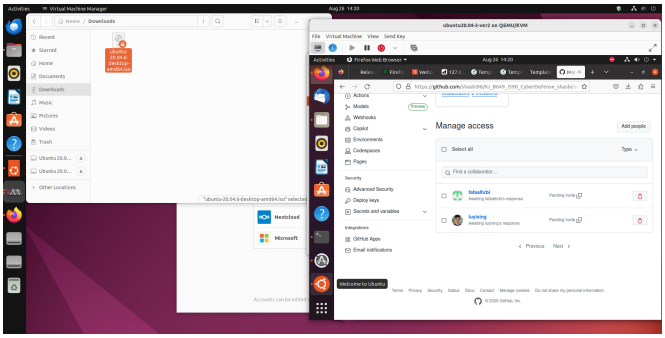

Fig. 3: GitHub collaborators added

IU RED AND QUARTZ ACCOUNT

Setting up remote access involved creating a Quartz account and logging into IU RED [Fig.4]. I initially struggled because my Quartz account did not activate right away. Later, I learned that activation only occurs after a confirmation email is received. Once connected, I used SSH to access the lab host and resume my VM.[5]

Another challenge was handling screenshots: although I could generate them in the VM and locate them via terminal (/Pictures/Screenshots), I couldn't easily access them in the RED file manager. This made it difficult to transfer them to my local computer. This experience emphasized the differences between GUI and CLI environments, and the importance of mastering terminal-based navigation for precise file management.[7][6]

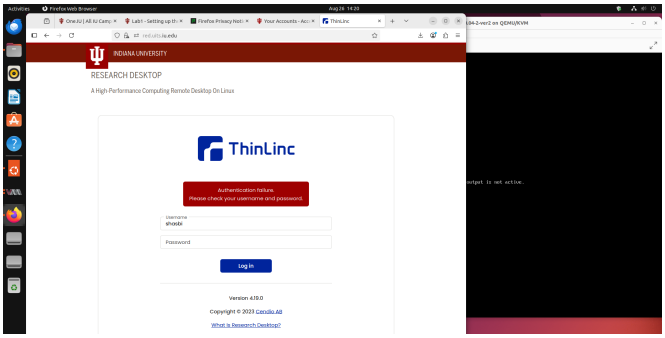

Fig. 4: Webgoat Login Page

III. CONCLUSION

This lab gave me hands-on practice with essential cybersecurity tools and workflows. I set up an isolated VM for experimentation, installed WebGoat and WebWolf to study common web vulnerabilities, and adopted Overleaf and GitHub for academic documentation and collaboration. I also configured remote access using IU RED.

Beyond the technical setup, I faced challenges—waiting for Quartz account activation, and struggling to extract screenshots from the VM onto my local system. These difficulties reinforced the importance of patience, problem-solving, and comfort with the command line in real-world cybersecurity work.

Most importantly, I learned how to push code and reports to GitHub and prepare academic documents with Overleaf, giving me a workflow that is both professional and reproducible. This lab not only provided me with the necessary environment for future exercises but also gave me practical exposure to the kinds of problems and solutions that cybersecurity professionals deal with every day.

REFERENCES

[1] https://owasp.org/www-project-webgoat/
[2] https://www.overleaf.com/
[3] https://help.github.com/articles/fetching-a-remote/
[4] https://help.github.com/articles/caching-your-github-password-in-git/#platform-linux
[5] https://uisapp2.iu.edu/confluence-prd/x/UoK3E.
[6] https://i45.red.uits.iu.edu/agent
[7] https://stackoverflow.com/questions/19945881/copy-file-folder-using-scp-command