Lab - 1

Venkata Diwakar Reddy Kashireddy

***Abstract*—This report explains how to set up and work with the basic elements of the environments required for the course Cyber Defence Competitions.**

I. Introduction

In the lab we performed 6 tasks. We also performed an additional bonus task. We installed a standalone WebGoat application on our Ubuntu VM. WebGoat is an intentionally insecure web application maintained by OWASP that is intended to teach web application security lessons.

II. Tools

• KVM (Kernel-based Virtual Machine): It is a full virtualization solution for Linux [1].
• WebGoat: A deliberately insecure web application maintained by OWASP designed for teaching web application security concepts. [2].
• WebWolf: – It is a part of WebGoat 8, but it is a separate web application that simulates an attacker's machine [2].
• Overleaf: - It is a collaborative cloud-based LaTeX editor that helps to create documents easily by providing standard formats [3].
• GitHub: – GitHub is an Internet hosting service for software development and version control using Git [4].
• Red: – IU Research Desktop (RED) is a virtual desktop service for users with accounts on the Carbonate research supercomputer at IU. [5]
• Defend the Web: It is an interactive security platform used for learning and skill development. [6]

III. VIRTUAL MACHINE

A new VM was used to set up the environment. The new VM was created using ISO image of Ubuntu 20.04.4 LTS and allocated 4096 Mb RAM, 2 CPU, 50 Gb disk. NAT was chosen for the network type. Install Ubuntu on the VM.

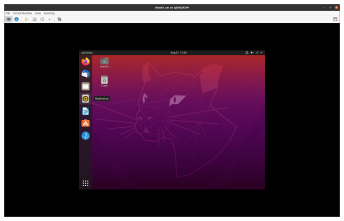

Fig. 1: Ubuntu VM Interface

IV. OWASP WEBGOAT

WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security lessons. Standalone WebGoat application was installed on the VM. Java was installed by executing apt commands in the terminal.

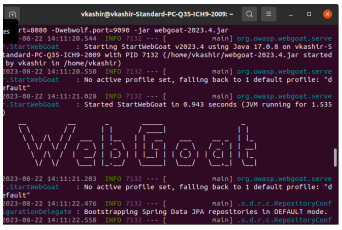

Fig. 2: WebGoat Installation

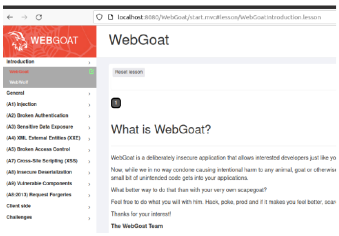

Fig. 3: WebGoat Interface

V. OWASP WEBWOLF

WebWolf is a separate web application that simulates an attacker's machine. The tool is very useful to make a clear distinction between what takes place on the attacked site and what you need to do from your end. It supports multiple functionalities like files, mailbox, and incoming requests. Files functionality can be used to lure the victim to download the file, the mailbox can be used for phishing, and incoming requests can be redirected to pages where a victim could provide private/sensitive data.

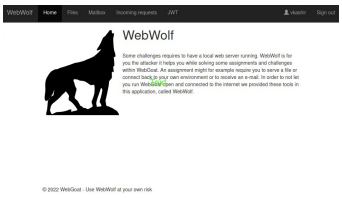

Fig. 4: WebWolf

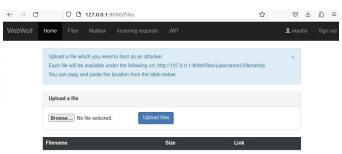

Fig. 5: WebWolf Files

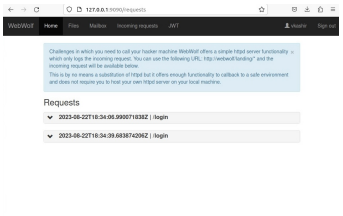

Fig. 6: WebWolf Incoming Requests

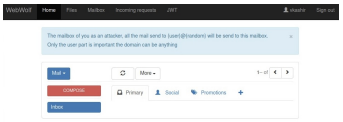

Fig. 7: WebWolf Mailbox

VI. OVERLEAF

Overleaf is an open-source online real-time collaborative LaTeX editor. The tool was used for lab write-ups. The report was created with the help of the Template from the LNT Seminar Report.

VII. GITHUB

Created a GitHub repository with the name ”IU_B649_I590_CyberDefense_vkashir” to save the write-ups. The instructor and AI were added as collaborators for this repository.

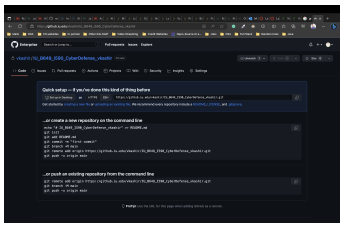

Fig. 8: GitHub Repository

VIII. IU RESEARCH DESKTOP (RED)

IU RESEARCH DESKTOP is a web-based Linux desktop. It allows you to ssh into the system in the labs in order to use virtual manager. I created an account at Carbonate to login into RED and use the machines in the lab.

IX. DEFEND THE WEB

Defend the Web is an interactive security platform used for learning and skill development. I have completed the challenge intro 3 in the playground.

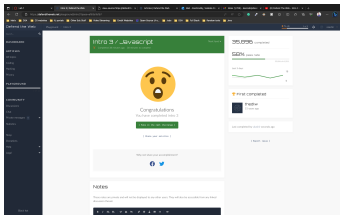

Fig. 9: DefendTheWeb Intro 3

X. CONCLUSION

We learned to configure virtual machines using the KVM interface. We set up the environment to install and run Webwolf. The GitHub and Overleaf accounts helped us create and share reports seamlessly.

REFERENCES

[1] KVM
https://www.linux-kvm.org/page/MainPage..
[2] WebGoat
https://owasp.org/www-project-webgoat/..
[3] OverLeaf
https://www.overleaf.com/.
[4] Github
https://en.wikipedia.org/wiki/GitHub.
[5] RED
https://kb.iu.edu/d/apum.
[6] Defend The Web
https://defendtheweb.net/