UC-401 Website Hardening and Ethical Hacking

Abstract

This project is to showcase a real-life scenario of securing a theoretical business website on Red Hat Linux, Apache, MariaDB, and PHP hosted in a virtual machine. The project objective is for a team to research ways to secure the theoretical business website, develop and implement security policies, and perform a red/blue team exercise. This project is a way for a team to exercise ethical hacking in a closed environment to obtain experience.

Introduction

The website Hardening and Ethical Hacking Project aims to enhance the security posture and of our organization's website. Breaking down into three phases, it includes identifying vulnerabilities, implementing security measures and conducting ethical hacking testing to ensure the website against potential cyber threats.

Fig 1 – Akwaaba's WordPress Webpage

Research Question(s)

- **How can we protect this vulnerable website from attackers?**
- **How can we exploit the other team's vulnerabilities to gain access to their environment?**
- **How do we identify vulnerabilities in our infrastructure?**

Tools and Methods

Tools Used for red and Blue team Phase

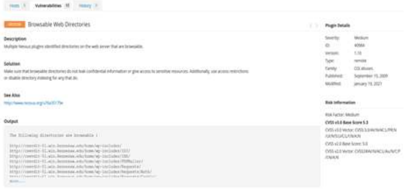
- Nessus
- Skipfish
- Nmap
- Redirection
- Limit Login Attempts
- John the Ripper
- Hydra
- Slowloris

Results

Highlights

Phase 1- Our team worked to identify vulnerabilities and implement security measures. We also did vulnerability testing and found open ports and user information. Our team created security policies for Akwaaba business website and performed a risk assessment.

Phase 2 – We used Nessus and Skipfish tools to test the server for vulnerabilities and we found that the Red Hat Security patches are not up-to date, HSTS not present in the HTTPS server, HTTP Trace/Track is allowed within the server, SSL certificate is untrusted., SSH CBC mode ciphers enabled and has weak key Exchange.We also implemented Cockpit – web-based server monitoring tool, Limit Login Attempts Reloaded Plugin, Redirection Plugin.


Vulnerabilities

Browsable Web Directories

Description

Solution

See Also

Output

Plugin Details

Severity: Medium

Risk Information

Risk Factor: Medium

Fig 2- Example of Vulnerability Found using Nessus

Phase 3 –This Red and Blue Team phase went smoothly. We managed find a few vulnerabilities in the target IP. On the defense side we did find attempts of break-in but due to our quick response to the attempts, there was no intrusion from the other team. Further more, we managed to keep the server up the entire 3rd phase.

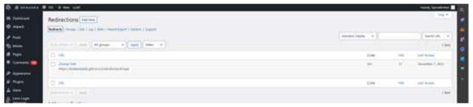

Redirections

Fig 3- Redirection plugin in action

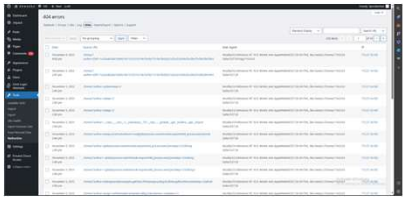

404 errors

Fig 4- Attempts of accessing content resulting in 404s

Experience

During this project, we were able to gain some hands-on experience that will translate over to the industry such as honing our cybersecurity skills with vulnerability testing and hardening our website. We also gained some experience in ethical hacking during the Red vs Blue phase.

Future Career Plans

Our future plans is to continue what we have learn during the project in our future jobs. To continue using our tools in our future IT journey. To use our people skills what we learned as working as a team..

Team Members

- Alex Liu – wrote security policies, managed weekly reports, vulnerability testing, researched network defense techniques, planned network defense, and created project showcase website
- Kenny Frontin – vulnerability testing, monitored the environment, carried out threat analysis, researched risk assessment on import assets
- Kenndy Sanchez- Researched the vulnerabilities and did the PowerPoints.
- Komlan Wogomebu- contributed to the enhancement of the security policies, contributed on the technical project planning (Work Breakdown Structure), hardened RedHat Linux security.
- Samrat Pandya- conducted server security vulnerability tests, project management, risk assessment, helped secure the website, conducted both the attack and defense strategies, edited the videos and showcase website.

Conclusions

The website hardening and ethical hacking project concluded without any problems. Our team was able to secure the business website and network infrastructure. The team managed to finish all phases of this project without delay and disorganization. All deliverables were completed on time. Overall, the project was a success without many difficulties.

Acknowledgments

Professor Donald Privitera IT4983 Capstone W01

Contact Information

Alex Liu – aliu4@students.kennesaw.edu
Kenny Frontin – kfrontin@students.kennesaw.edu
Kennedy Sanchez-ksanch21@students.kennesaws.edu
Komlan Wogomebu
Samrat Pandya – Spandya1@students.Kennesaw.edu

References

Provide references here.
You can use the departmental logo instead of the college logo. The official logo policy is available at http://styleguide.kennesaw.edu/logo-policy/unacceptable-variations.php

Chinthaguntla, K. (2023, August 9). Setting up multi-factor authentication on Linux systems. Enable Sysadmin. https://www.redhat.com/sysadmin/mfa-linux

CrowdStrike. (2023, April 20). *What is Remote Code Execution (RCE)? - CrowdStrike*. crowdstrike.com. Retrieved November 9, 2023, from https://www.crowdstrike.com/cybersecurity-101/remote-code-execution-rce/

Understanding Denial-of-Service Attacks | CISA. (2021, February 1). Cybersecurity and Infrastructure Security Agency CISA. Retrieved November 9, 2023, from https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

Authors: Alex Liu, Kenny Frontin, Kennedy Sanchez, Komlan Wogomebu, Samrat Pandya
Advisors: Professor Donald Privitera