UC-161

Cybersecurity Capstone

INTRO/ABSTRACT

The purpose of this capstone was to form a cyber security team to help a small business, a restaurant, and secure their server. As a team, we had to research any risks and generate a plan based on the information we found. We researched the best tools to use and configured them on to our server. In order to identify how secure our server was, a team was responsible to try to exploit the URL. It was our job to monitor the server for any potential threats/vulnerabilities.

METHODS

Faraday was used to unite the results of multiple tools that are used in the process of recon of potential issues with the server and WordPress instance. Everything used in open-sourced and freely available.

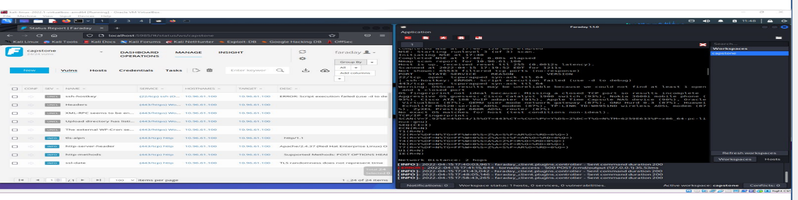

Fig.1 Faraday scan output and Faraday dashboard. This demonstrates how a scan executed in Faraday will coincide with the Faraday dashboard.

RESULTS

We successfully identified the dangers of phishing as well as outdated software and the vulnerabilities that are tied with the outdated system.

Resources:

-, R., By, -, & Ranjith. (2020, May 30). *Faraday: Collaborative penetration test & vulnerability management*. Kali Linux Tutorials. Retrieved March 25,2022,from https://kalilinuxtutorials.com/faraday/?msclkid=291a8880aca511ec8b9364a06f07c929

As a team, we updated the server and protected it from any possible vulnerabilities. Furthermore, the team successfully monitored the server, keeping it fully available, while pen testing an opposing team's server.

Please scan the QR code for more information about the team and about the project.

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

Author(s) Evelyn Cronnon, Magan Silwal, Ihab Eid, Scott Weaver
Advisors(s)Donald Privitera, Lei Li