UC-263 Cybersecurity Capstone

INTRO/ABSTRACT

In this capstone project, our team was assigned a virtual machine with a small business website. We were to analyze the server, fix vulnerabilities, and implement measures to harden its security. During the attack phase, we were to attempt to take down the server of an opposing team while protecting our own.

METHODS

Our team used a wide variety of tools for vulnerability and penetration testing. We updated our server, WordPress, and fixed vulnerabilities. In addition, we hardened the security of the server, enabled two-factor authorization, and installed a self-signed SSL certificate.

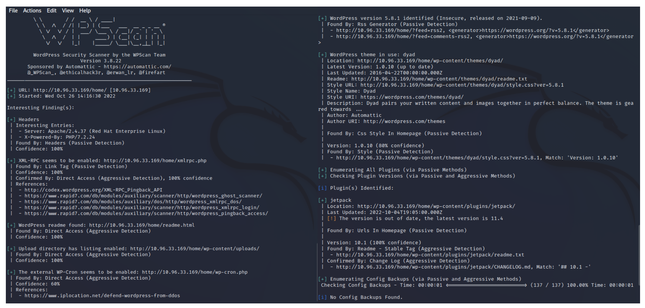

Fig. 1 One of our frequently used tools in action, WPScan.

RESULTS

During the attack phase, we discovered that our target never changed any of their passwords. Within 30 minutes of getting their IP, we breached their website and brought it down by the end of the first day. Our target remained offline for the entirety of the attack phase, while our website remained online.

This project was a fantastic way to learn how to maintain a Linux Red Hat server and properly secure and work on a WordPress website. It has given us experience with different tools while working in a cybersecurity environment.

We updated our server, fixed vulnerabilities, and implemented security measures to protect it from attack. We took down our target with their own passwords while our server remained online.

Scan the QR code to visit our project website.

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

Author(s): Jordan White, Hector Gomez, Jenny Owens, Aaron Scott, Caleb Woodman
Advisor: Donald Privitera