



Florida International University

Fall Semester – 2024 – Senior Design Project

Vulnerability Scanner

Students: Frederick Gonzalez

Instructor/Faculty: *Masoud Sadjadi*, Florida International University

Coming up with a Plan/Brainstorming

- Contributed significantly to brainstorming new ideas for our senior project after the team decided to shift from our original concept.
- Engaged actively in daily scrum meetings, helping to refine and discuss ideas, which ultimately led to the decision to build a vulnerability scanner

Researching and Set up

- Performed thorough research using articles and videos to explore how to implement the vulnerability scanner with Nuclei, Kali, and Metasploitable.
- Explored methods for integrating Nuclei (installed on Kali Linux) with Metasploitable, which was running as a standalone virtual machine.
- Configured the network setup to ensure smooth communication between the two virtual machines, sharing my findings with the team and supporting the implementation process.

Research and Learning

- Studied and familiarized myself with the YAML syntax needed to develop custom templates for Nuclei.
- Developed Custom templates specifically designed to target vulnerabilities in the Mutillidae, Twiki, phpMyAdmin, DVWA, and WebDAV web servers on Metasploitable.
- Addressed and resolved various challenges in debugging and refining my template, ensuring they accurately detected vulnerabilities.

How it works

- Request Structure: The template sends POST or authentication requests to the login pages of the web applications and services running on the target machine. These requests contain the default login credentials.
- Matchers: The matchers are used to look for specific words, status codes, or regex patterns that indicate a successful login or the presence of a vulnerability (like weak passwords). For example, the template looks for phrases like "Login successful" or "Welcome" in the response.
- Target IP: The template is designed to run against an IP address (in this case, 10.0.2.4), typically a Metasploitable machine, but can be easily adapted to scan other systems by changing the target IP.

Challenges and Adjustments

- Accuracy: One challenge was ensuring that the matchers worked across different web services, as the success message or behavior might vary between services. Some services might return subtle differences in HTTP responses (like status codes or specific text), requiring careful fine-tuning of matchers.
- Environment Specificity: While the template is built for Metasploitable, it could be adapted for other vulnerable machines or real-world systems by modifying the credentials and checking for different vulnerable services.

Summary and Impact

- The template checks for weak or default credentials across multiple services on Metasploitable, including web applications like TWiki, phpMyAdmin, Mutillidae, DVWA, and WebDAV, by sending POST requests with default login credentials and analyzing the responses for successful login indications. It also checks SSH login vulnerabilities by testing the default credentials root:toor and msfadmin:msfadmin, looking for a "Welcome" message in the response. For FTP, it tests anonymous:anonymous and ftp:ftp credentials, using regex to detect a "Login successful" message. Finally, it tests MySQL login vulnerabilities using default credentials like root:root and msfadmin:msfadmin, checking for a "MySQL welcome" message in the response.
- This template can be used in vulnerability assessments to quickly identify weak or default credentials across commonly used services. By automating the detection of such weaknesses, it reduces the time spent on manual penetration testing and provides an easy way to identify potential security gaps in a target system.



ACKNOWLEDGEMENT

The material presented in this poster is based upon the work supported by XXXXX (*name of the project sponsor: federal, state or local government, or corporate partners, where applicable*). We/I thank XXXX for his/her/their assistance and mentorship that I/we received throughout the senior design project.