



Florida International University

Fall 2024 Senior Design Project

Vulnerability Scanner

Students: Jean Bagnis

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

PROBLEM

- Overwhelming amount of potential cybersecurity vulnerabilities for any system or network.
- Default vulnerability scanners often miss specific configurations or custom scenarios.
- Need for tailored templates to target unique vulnerabilities.

INTRODUCTION

- Nuclei: An open-source tool designed for customizable vulnerability scanning.
- Metasploitable: A deliberately vulnerable machine used for testing security tools and learning exploitation techniques.
- Focus: Write custom Nuclei templates to detect vulnerabilities inherent in Metasploitable, showcasing adaptability and precision.

REQUIREMENTS

- Software & Tools:
 - Kali Linux with Nuclei installed for scanning.
 - Metasploitable VM as the target vulnerable machine.
 - VirtualBox or VMware for hosting both VMs.
- Networking Setup:
 - Configured a NAT network to enable secure and isolated communication between the machines.
 - Verified connectivity using basic network tools like ping.
- Knowledge Base:
 - Understanding YAML for template creation. Familiarity with common vulnerabilities, including services like FTP, SSH, and web servers.

RESEARCH

- Nuclei Functionality: Studied how Nuclei identifies vulnerabilities using template-based scans. Explored syntax and best practices for writing effective templates.
- Metasploitable Vulnerabilities: Focused on key services, such as outdated software versions, default credentials, open ports, and misconfigured applications.
- Network Configuration and Setup: Learned how to have both virtual machines connected via the same NAT network to ensure communication
- Testing: Analyzed existing Nuclei templates to understand formatting, input parameters, and payload usage.

IMPLEMENTATION

- Network Setup:
 - Created a NAT network within VirtualBox to link the Kali Linux and Metasploitable machines.
 - Validated connectivity through tools like ping.
- Template Development:
 - Wrote custom YAML templates targeting known Metasploitable vulnerabilities, specifically I focused on an unintentional remote backdoor from a C compiler.
 - Integrated payloads for testing specific exploit paths.
- Scanning Process:
 - Ran Nuclei scans using the newly created templates.
 - Logged and analyzed the scan results to ensure accuracy and completeness.

CHALLENGES

- Adapting to Nuclei’s specific syntax and ensuring proper formatting was challenging.
- Debugging templates to make sure Nuclei can find and run them in the first place was challenging enough, let alone making sure these templates find the desired vulnerability within the system.
- Learning Nuclei’s command codes to navigate the software and execute tasks like debugging and targeted scans. (No GUI, just commands)

VERIFICATION

- Ran scans with custom templates and cross-checked results against Metasploitable’s exploitability guide.
- Improved templates through iterative adjustments to ensure accurate detection.
- Ensured templates found accurate results regardless of assigned IP address.

CONCLUSION

- Successfully developed and deployed custom Nuclei templates to scan and identify vulnerabilities in Metasploitable, which could also be used when targeting other environments
- Highlighted the importance of creating custom solutions to address specific vulnerabilities that default scanners may overlook.
- Project provides a framework for using Nuclei in other penetration testing scenarios with tailored requirements.

REFERENCES

Metasploitable 2 Exploitability Guide | Metasploit Documentation. (n.d.). <https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/>

Projectdiscovery. (n.d.). GitHub - projectdiscovery/nuclei: Nuclei Scanner. GitHub. <https://github.com/projectdiscovery/nuclei>



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.