
VULNERABILITY
SCANNER

Fullstack Academy

Hacking Mr. Robot Virtual Machine

Ivan Arias

Contents

Fullstack Academy

Step 1: Set Up Environment

- **Prepare the Kali Linux VM and the Mr. Robot Vulnhub VM:** Ensure your Kali Linux environment is ready by installing essential tools such as Nmap, Gobuster, Hydra, and Metasploit.

Step 2: Network Scanning

- **Objective:** Identify the target's open ports and services.
- **Tools: Nmap:** Utilize Nmap to scan the target for open ports and services.

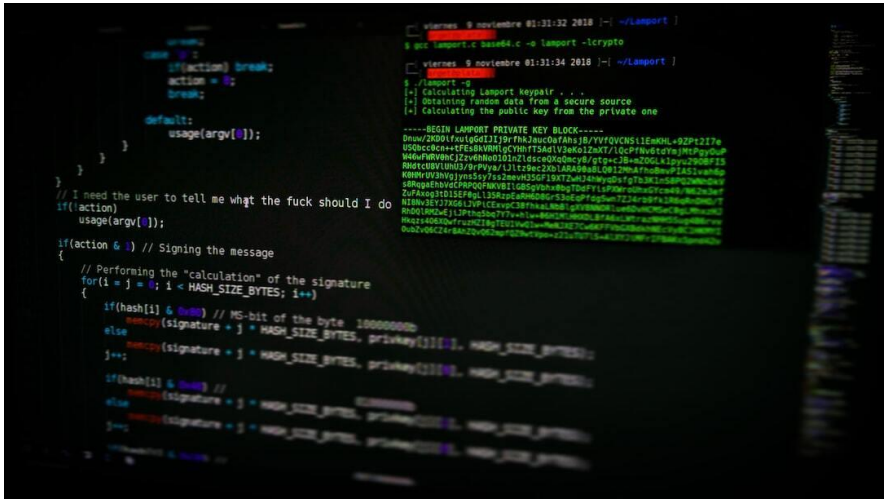

Photo by Arget on Unsplash

Step 3: Enumeration

Fullstack Academy

- **Objective:** Gather detailed information about the target's web applications and technologies.

- **Tools: Gobuster, Wappalyzer:** Utilize Gobuster and Wappalyzer for directory enumeration and identifying web technologies.

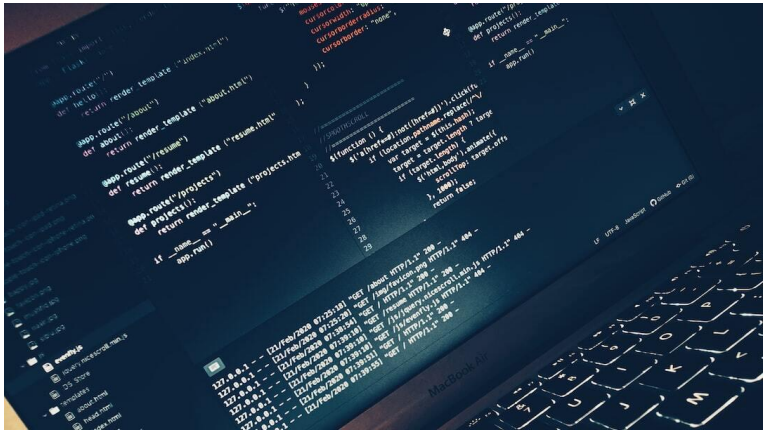

Photo by Muhammed suhail ek on Unsplash

Step 4: Vulnerabilities

- **Objective:** Identify vulnerabilities in the target's web applications and services.
- **Tools: Nmap, Nikto:** Utilize Nmap and Nikto for vulnerability scanning.

Photo by Mar Linares on Unsplash

Step 5: Brute-force

- **Objective:** Gain access to the target by brute-forcing login credentials.
- **Tools: Hydra:** Utilize Hydra for brute-force attacks.

Photo by Markus Spiske on Unsplash

Step 6: Reverse Shell

- **Objective:** Gain remote access to the target system.
- **Tools: PHP Reverse Shell, Metasploit:** Utilize a crafted PHP reverse shell and Metasploit to exploit vulnerabilities and gain access.

Photo by Markus Spiske on Unsplash

Findings

Fullstack Academy

Finding	CVSS Score	Severity	Finding Name	Description	Recommendation
1	9	High	HTTP (80/tcp) - Apache HTTPD	Open ports 80 and 443 running Apache HTTPD, potential entry points	Ensure Apache is up-to-date and configure security headers
2	8	High	SSL Info	Missing security headers and outdated SSL configurations	Update SSL/TLS settings and add security headers
3	6	Medium	WordPress Plugins	Various plugins, including outdated versions	Regularly update all plugins and monitor for vulnerabilities
4	5	Medium	WordPress Themes	Multiple themes, including outdated versions	Update themes and remove unused ones
5	8	High	Configuration Issues	Missing security headers and outdated PHP version	Update server configurations and PHP version
6	9	Critical	Credentials Found	Username and password retrieved (elliot/ER28-0652)	Change all passwords and review user access controls
7	5	Low	Directories/Files	Various sensitive directories and files exposed	Restrict access to sensitive directories and files

Recommendations

Fullstack Academy

- ✓ Update and Patch Management
- ✓ Implement Security Headers and Update SSL/TLS Configurations
- ✓ Regular Security Audits and Monitoring
- ✓ Strengthen Authentication Mechanisms
- ✓ Restrict Access to Sensitive Directories and Files
- ✓ Enhance Configuration Management