

Mr. Robot CTF – TryHackMe Walkthrough

Author: Fidha Thasni N

Date: July 2025

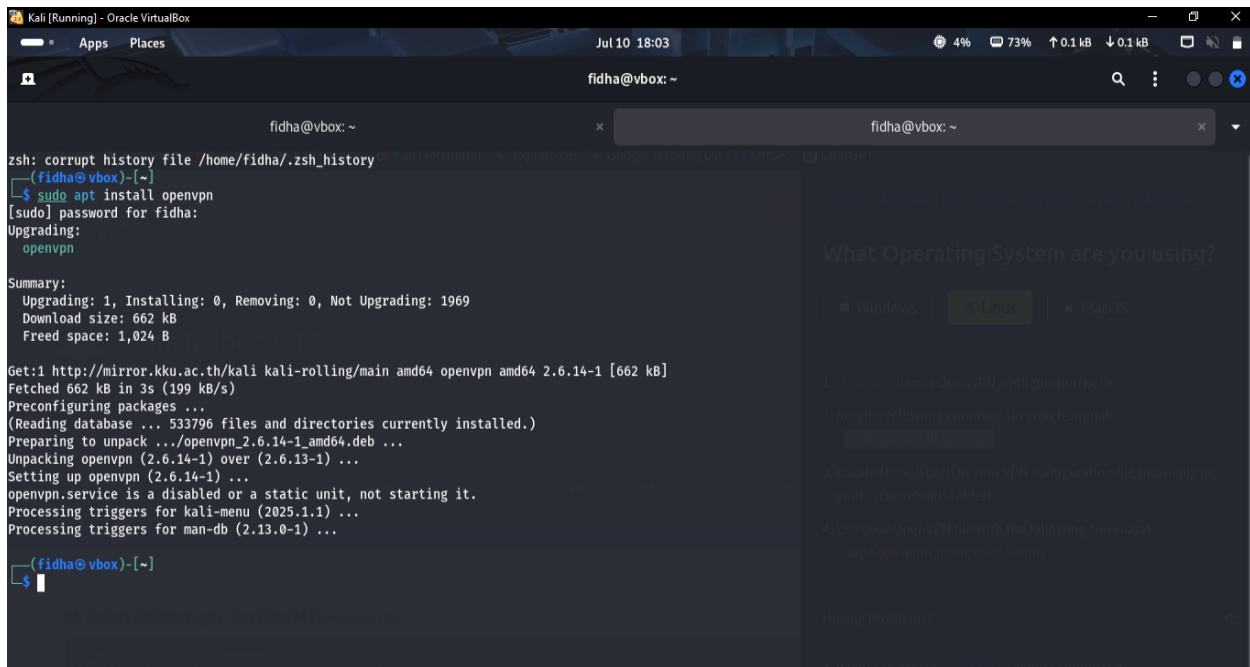
Room Link: <https://tryhackme.com/room/mrrobot>

VPN Setup

Installed OpenVPN and connected using the provided .ovpn file.

```
sudo apt install openvpn
```

```
sudo openvpn fidhasthasni.ovpn
```



```
Kali [Running] - Oracle VM VirtualBox
Jul 10 18:03
fidha@vbox: ~

fidha@vbox: ~
zsh: corrupt history file /home/fidha/.zsh_history
(fidha@vbox)-[~]
$ sudo apt install openvpn
[sudo] password for fidha:
Upgrading:
  openvpn

Summary:
  Upgrading: 1, Installing: 0, Removing: 0, Not Upgrading: 1969
  Download size: 662 kB
  Freed space: 1,024 B

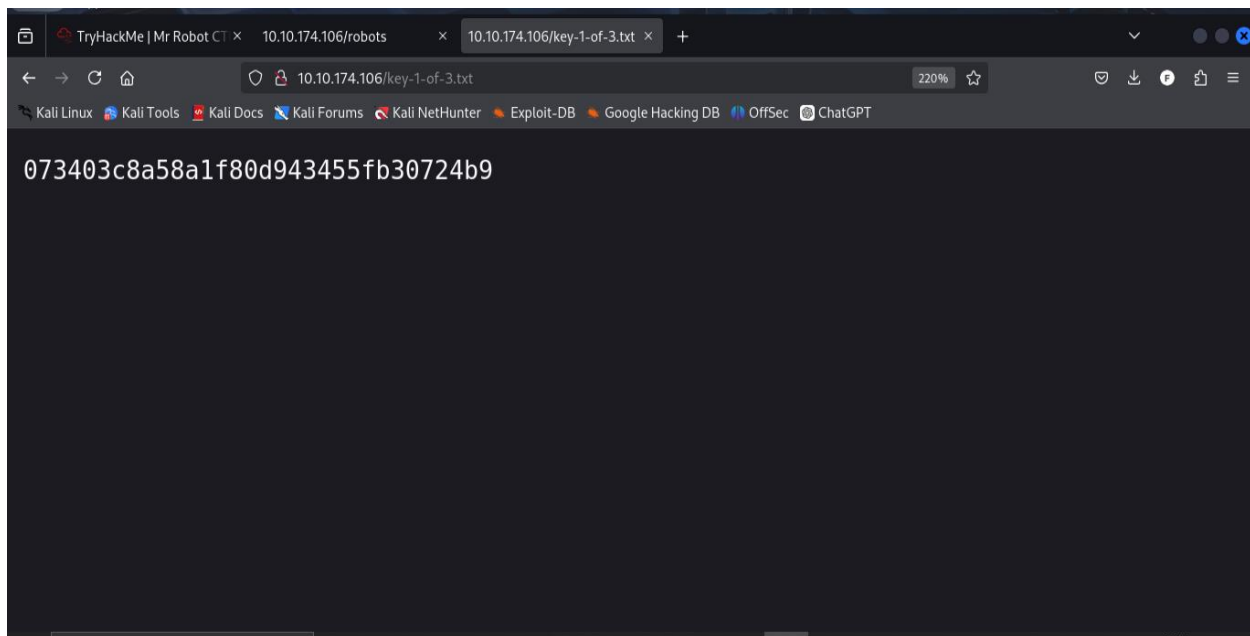
Get:1 http://mirror.kku.ac.th/kali kali-rolling/main amd64 openvpn amd64 2.6.14-1 [662 kB]
Fetched 662 kB in 3s (199 kB/s)
Preconfiguring packages ...
(Reading database ... 533796 files and directories currently installed.)
Preparing to unpack .../openvpn_2.6.14-1_amd64.deb ...
Unpacking openvpn (2.6.14-1) over (2.6.13-1) ...
Setting up openvpn (2.6.14-1) ...
openvpn.service is a disabled or a static unit, not starting it.
Processing triggers for kali-menu (2025.1.1) ...
Processing triggers for man-db (2.13.0-1) ...

(fidha@vbox)-[~]
$
```

Enumeration

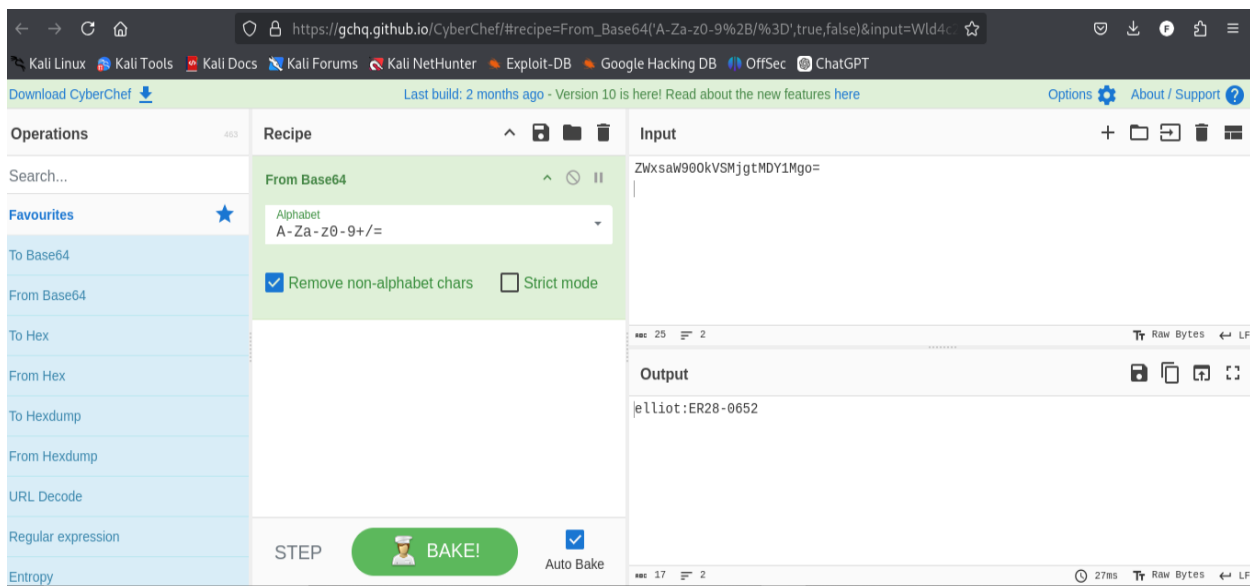
Used `nmap` and `gobuster` to identify available services and directories.

- Open ports: 80 (HTTP), 443 (HTTPS)
- `/robots.txt` exposed `fsociety.dic` and the first flag



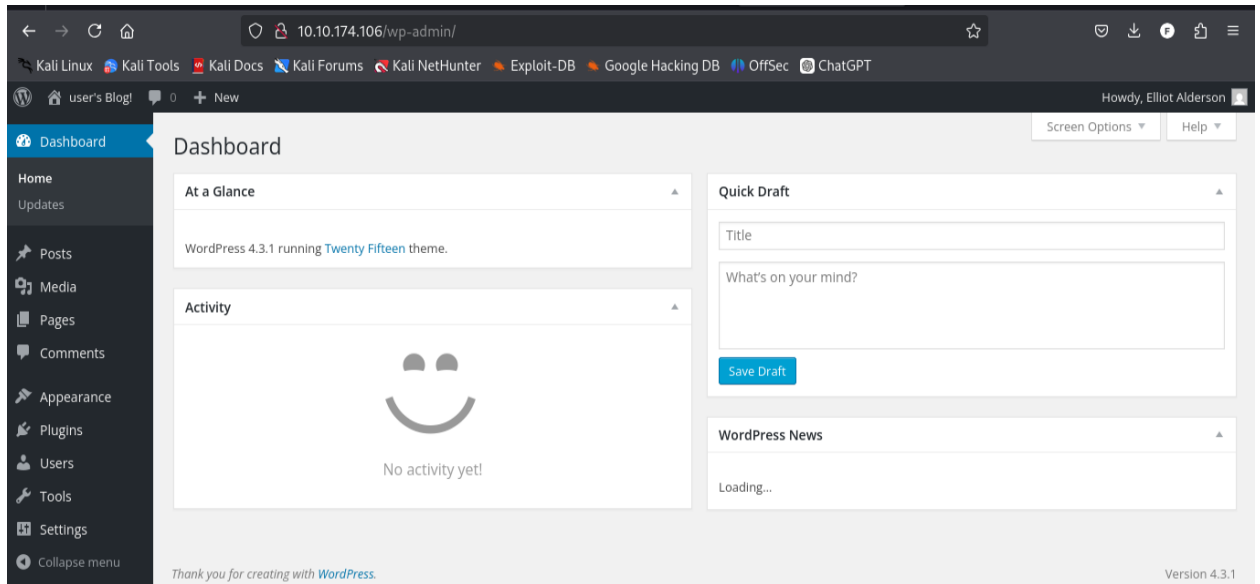
Credential Discovery

- Decoded base64 string using CyberChef → `elliott:ER28-0652`



WordPress Login & Reverse Shell

- Logged into WordPress as `elliott`
- Injected a reverse shell into `404.php`
- Gained initial foothold via netcat listener



User Escalation

- Found password hash in `/home/robot/`
- Cracked with John the Ripper
- Switched to `robot` user

Privilege Escalation

- Found SUID binary `nmap`
- Used `nmap --interactive` shell escape
- Got root shell

