11-Mr-Robot1

##信息收集
开发端口以及目标服务和目标系统识别

```
nmap -A $IP -p`nmap -sS -sU -p- -PN $IP --min-rate 10000 | grep '/tcp\|/udp' | awk -F
'/' '{print $1}' | sort -u | tr '\n' ','`
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 02:13 GMT
Nmap scan report for 10.30.13.218
Host is up (0.00039s latency).

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
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
MAC Address: 08:00:27:B9:D0:F9 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.10 - 4.11 (98%), Linux 3.2 - 4.9 (94%), Linux 3.2 - 3.8
(93%), Linux 3.18 (93%), Linux 3.13 (92%), Linux 3.13 or 4.2 (92%), Linux 4.2 (92%),
Linux 4.4 (92%), Linux 3.16 - 4.6 (91%), Linux 2.6.26 - 2.6.35 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.39 ms 10.30.13.218

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 34.06 seconds
```

目录扫描

```
dirb http://www.example.com -w /usr/share/wordlists/seclists/Discovery/Web-
Content/directory-list-lowercase-2.3-medium.txt
```

wpscan

```
wpscan --url https://192.168.1.84:12380/blogblog/ --disable-tls-checks --api-token BZ95DkmRoUuUZZ4azwYn4cGZDkVOas8AvkoRUUas88Q
```

有用信息

```
WordPress 4.3.33
http://10.30.13.218/robots.txt
```

robots

```
http://10.30.13.218/fsocity.dic #类似id一样的文件
```

爆破获取可能的账号密码

用上面获取到id文件，在博客的找回密码处，该功能点输入网站存在用户就会发送找回密码邮件，不存在就会报错，利用这点枚举到3个用户

```
elliot
Elliot
ELLIOT
```

枚举密码

```
ER28-0652
```

##立足点

user

```
#user1
wordpress后台主题编辑处，有个错误模板404页面，当网站出错自动跳转到这，在此页面写入webshell，弹shell获取user

$ id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
$ whoami
daemon

#user2
查找历史遗留密码文件时，发现第二个用户
cat /home/robot/password.raw-md5
robot:abcdefghijklmnopqrstuvwxyz
shell稳定化后登录第二个user
robot@linux:/bin$ id
uid=1002(robot) gid=1002(robot) groups=1002(robot)
```

```
robot@linux:/bin$ whoami
robot
```

##system

提取

```
robot用户相同里，有个nmap 具有suid权限，使用此程序提升权限
# id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
# whoami
root
```