

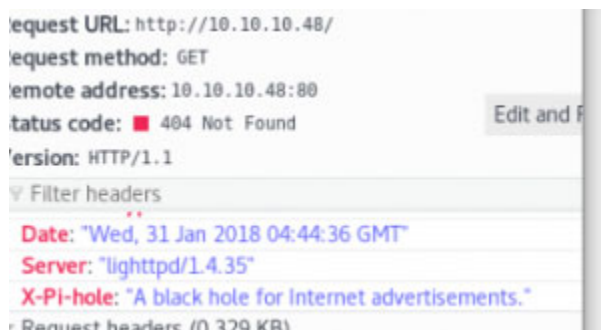
## SWRhapsody

作为Hack The Box网站练习writeup的第一篇先记录点基础的东西。

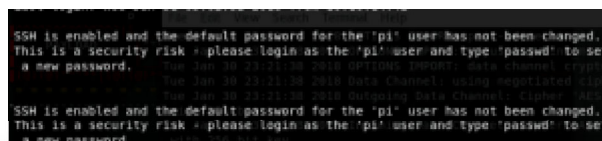
要链接到网站提供的靶机需要使用openvpn链接到特定网络，在网站上登录后在Access中下载openvpn的配置文件然后链接即可。每个靶机有user和root两个级别的挑战，如果找不到思路可以去官方的论坛寻找提示，论坛中提供了retired的靶机的writeup。

### user

从列表中看到机子的ip后用nmap扫描，发现靶机开放了ssh和http的端口但没有识别出OS，估计需要爆破不过不清楚字典范围，论坛中有人提示靶机的名字是关键要素，Google发现Mirai是个通过尝试默认用户密码名感染IOT设备的僵尸病毒。从github上可以找到病毒的源码，但尝试使用源码中的字典爆破失败。于是转头查看http端口，浏览器访问靶机发现直接给了个404，查看http响应看到有个“X-Pi-hole”字段。



搜索这个字段找到可以知道靶机使用Pi-hole，但尝试搜了Pi-hole的默认密码没有找到，论坛中有人提示要找到OS的版本，但搜索Pi-hole适用的系统得知其基本支持所有Linux发行版本，这时想到Mirai是感染IOT设备，搜索发现Pi-hole支持树莓派，尝试树莓派默认密码登陆ssh成功，去桌面可以拿到hash。



## SWRhapsody

这里小计下一开始在桌面上什么都没看到然后ssh突然断了，看了下是有人reset靶机，等靶机重新启动后hash就在桌面上。

### root

root的密码放在/root目录下直接su失败，使用sudo成功，但它告诉你hash丢了但usb里还有一份备份，查看usb内文件结果告诉你文件被删了，也不在lost+found里，看来要恢复被删除的文件。

```
pi@raspberrypi:~$ sudo cat /root/root.txt
I lost my original root.txt! I think I may have a backup on my USB stick...
pi@raspberrypi:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
aufs            8.5G  2.0G  5.3G  33% /
tmpfs           181M  13M   80M  13% /run
/dev/sda1       1.3G  1.3G   0 100% /lib/live/mount/persistence/sda1
/dev/loop0      1.3G  1.3G   0 100% /lib/live/mount/rootfs/filesystem.squashfs
tmpfs           251M   0 251M   0% /lib/live/mount/overlay
/dev/sda2       8.5G  2.0G  5.3G  35% /lib/live/mount/persistence/sda2
devtmpfs        10M   0  10M   0% /dev
tmpfs           251M  8.0K  251M   1% /dev/shm
tmpfs           5.0M  4.0K  5.0M   1% /run/lock
tmpfs           251M   0 251M   0% /sys/fs/cgroup
tmpfs           251M  8.0K  251M   1% /tmp
/dev/sdb        8.7M  92K  7.5M   2% /media/usbstick
tmpfs           51M   0  51M   0% /run/user/999
tmpfs           51M   0  51M   0% /run/user/1000
pi@raspberrypi:~$ ls -al /media/usbstick/
total 18
drwxr-xr-x 3 root root 1024 Aug 14 05:27 .
drwxr-xr-x 3 root root 4096 Aug 14 05:11 ..
-rw-r--r-- 1 root root 129 Aug 14 05:19 damnit.txt
drwx----- 2 root root 12288 Aug 14 05:15 lost+found
pi@raspberrypi:~$ cd /media/usbstick/lost+found/
bash: cd: /media/usbstick/lost+found/: Permission denied
pi@raspberrypi:~$ sudo ls -al /media/usbstick/lost+found/
total 13
drwx----- 2 root root 12288 Aug 14 05:15 .
drwxr-xr-x 3 root root 1024 Aug 14 05:27 ..
pi@raspberrypi:~$ sudo cat /media/usbstick/damn.txt
Damnit! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?
-James
pi@raspberrypi:~$
```

估计这里设备没有被写零，不然应该时恢复不了的，由于靶场没有联网靶机不能安装其他软件，先尝试使用debugfs恢复结果一个Inode没有看到，无奈只能再去论坛查看提示。看到很多讨论提到用基本文件命令就可以恢复，同时提示linux下所有东西都是文件。直接使用cat读取usb设备(不是mount之后的文件夹)可以看到一段hash

```
00000000: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000008: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000010: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000018: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000020: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000028: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000030: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000038: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000040: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000048: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000050: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000058: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000060: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000068: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000070: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000078: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000080: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000088: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000090: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000098: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000a8: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000b0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000b8: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000c8: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000d8: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000e0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000e8: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000f0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
000000f8: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00000100: 3265 6335 3035 6430 3236 6461 3133 6530 2ec505026fa13e0
00000110: 3230 620a                                     20b.
pi@raspberrypi:~$
```

### 使用命令

```
1 grep -a 'hash segment' /dev/sdb | xxd
```

可以得到完整的hash

```
0000270: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0000280: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0000290: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00002a0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00002b0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00002c0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00002d0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00002e0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
00002f0: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0000300: 3265 6335 3035 6430 3236 6461 3133 6530 2ec505026fa13e0
0000310: 3230 620a                                     20b.
pi@raspberrypi:~$
```

## SWRhapsody

---



0 条评论

发表评论

名称 \*

电子邮件 \*

网站

在想些什么?

发表评论

### 近期文章

携程Apollo YAML 反序列化

CVE-2020-5410

# SWRhapsody

---

[CodeQL 部分使用记录](#)

[近期评论](#)

[文章归档](#)

[2020年8月](#)

[2020年6月](#)

[2020年5月](#)

[2020年3月](#)

[2020年1月](#)

[2019年12月](#)

[2019年11月](#)

[2019年8月](#)

[2019年7月](#)

[2019年5月](#)

[2019年4月](#)

[2019年1月](#)

[2018年11月](#)

[2018年10月](#)

[2018年9月](#)

[2018年4月](#)

[2018年3月](#)

[2018年2月](#)

[2018年1月](#)

## SWRhapsody

---

[Article Collection](#)

[Cheat Sheet](#)

[cryptography](#)

[Exercise](#)

[Exploit](#)

[HackTheBox](#)

[Penetration Test](#)

[Uncategorized](#)

## 相关文章

HACKTHEBOX

### Bashed writeup

user nmap扫描结果显示只开放了80端口(如果看到开放其他端口应 [阅读更多...](#)

ABOUT

Hestia | 由Themeisle开发

## SWRhapsody

---