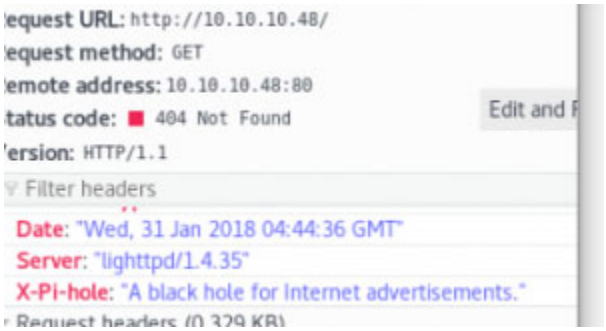
SWRhapsody

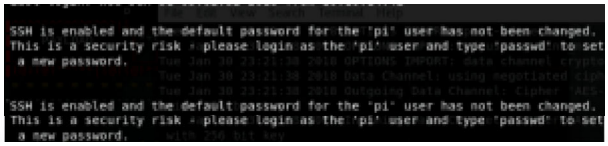
作为Hack The Box网站练习writeup的第一篇先记录点基础的东西。
要链接到网站提供的靶机需要使用openvpn链接到特定网络，在网站上登录后在Access中下载openvpn的配置文件然后链接即可。 每个靶机有user和root两个级别的挑战，如果找不到思路可以去官方的论坛寻找提示，论坛中提供了retired的靶机的writeup。

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。

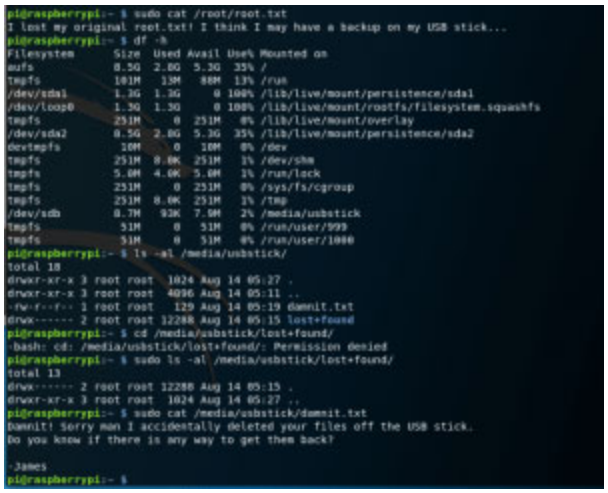


SWRhapsody

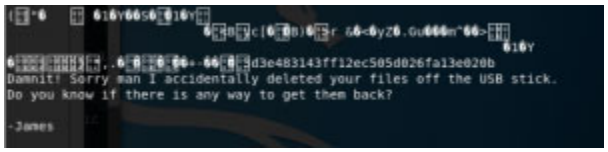
这里小计下一开始在桌面上什么都没看到然后ssh突然断了，看了下是有人reset靶机，等靶机重新启动后hash就在桌面上。

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。



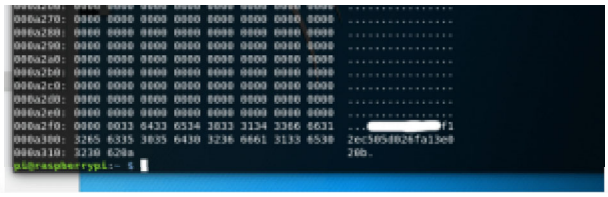
估计这里设备没有被写零，不然应该时恢复不了的，由于靶场没有联网靶机不能安装其他软件，先尝试使用debugfs恢复结果一个Inode没有看到，无奈只能再去论坛查看提示。看到很多讨论提到用基本文件命令就可以恢复，同时提示linux下所有东西都是文件。直接使用cat读取usb设备(不是mount之后的文件夹)可以看到一段hash



使用命令

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

可以得到完整的hash



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

近期评论

文章归档

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…

SWRhapsody