目录

前言

2024.1.13 沙青图书馆
甚至一开始打成了2023年。各位新年快乐。有时间会写下2023的年度总结。不过在此要提前开一个博客，记录一下接下来学习Iot安全的记录了。实在是再不学就要被学弟学妹追上了啊！此时此刻我却还要复习公钥和马原还有python，啊！感叹。

想从黑自己的小米手环开始，不过好像没啥资料捏。仔细想想还是先做别的吧，确实没啥参考。

参考记录

https://github.com/H4lo/IOT_Articles_Collection/blob/master/env_building.md （已经停止更新）
https://github.com/H4lo/awesome-IoT-security-article （上面的更新版本应该是）
https://mp.weixin.qq.com/s/7tvj_9LyNy0DGIJgFwsGJA （小米手环，不过太老了。）
https://zlibrary-redirect.se/book/11642985/b7f20c/? (nep师傅推荐的书)

> @.N1nEmAn 可以看下这两个
> https://h4lo.github.io/2020/02/24/iot_collection/
> https://delikely.eu.org/2099/01/01/IOT-Vulns/

后来还看了异步图书的物联网漏洞挖掘实战。

挖掘工具

https://blog.csdn.net/weixin_49393427/article/details/117625901#t10

https://www.douban.com/note/851702722/?_i=8948667QpmY7XQ

https://blog.csdn.net/weixin_43695001/article/details/123486237

https://mp.weixin.qq.com/s/-s5GGA70vcHAVfyz1QeBtQ

我是pwn手，为啥想着用肉眼挖漏洞啊！人都傻了。

最后败给了现实，工具都是基于ubuntu的。老老实实用ubuntu挖再用arch打吧！ubuntu还能存快照，挺好。

目前可用的：

attifyos：https://github.com/AttifyOS/AttifyOS

firmAE:https://github.com/pr0v3rbs/FirmAE

emba:https://github.com/N1nEmAn/emba.git

```
git clone https://github.com/e-m-b-a/embark.git; cd embark; sudo ./installer.sh -d
```

自己fork了怕没了。

简单记录一下。工具都是在attifyos4.0安装跑的。

embark

直接运行：

```
git clone https://github.com/e-m-b-a/embark.git; cd embark; sudo ./installer.sh -d
```

缺啥装啥，pipenv要用pip装，github issue说了不要用apt否则会太老旧。

> 装了快三天了！好在终于好了。

然后，修改/`etc/hosts`的embark.local前面为127.0.0.1而不是0.0.0.0，然后vm配置虚拟网口，让主机能够访问即可。

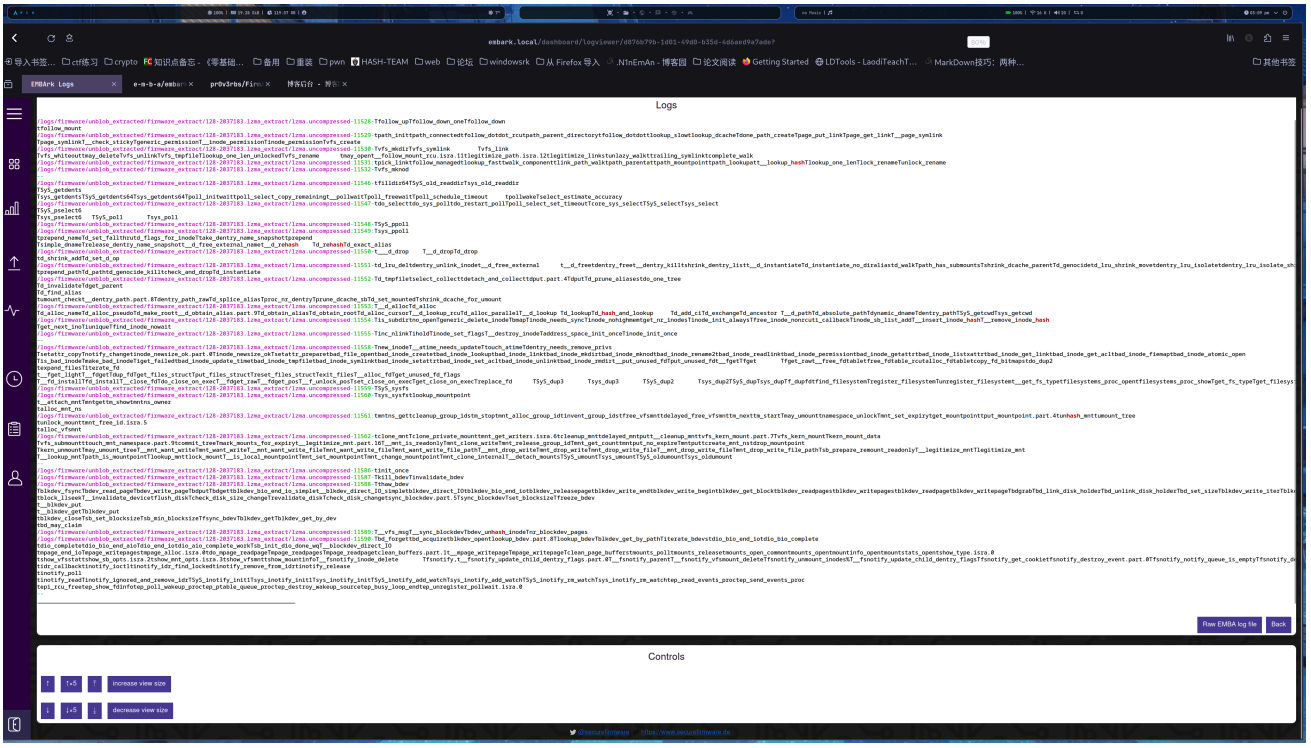
方法：https://blog.51cto.com/gwj1314/6168174

和上面的差不多，不过arch方便多了，直接vm修改就好。

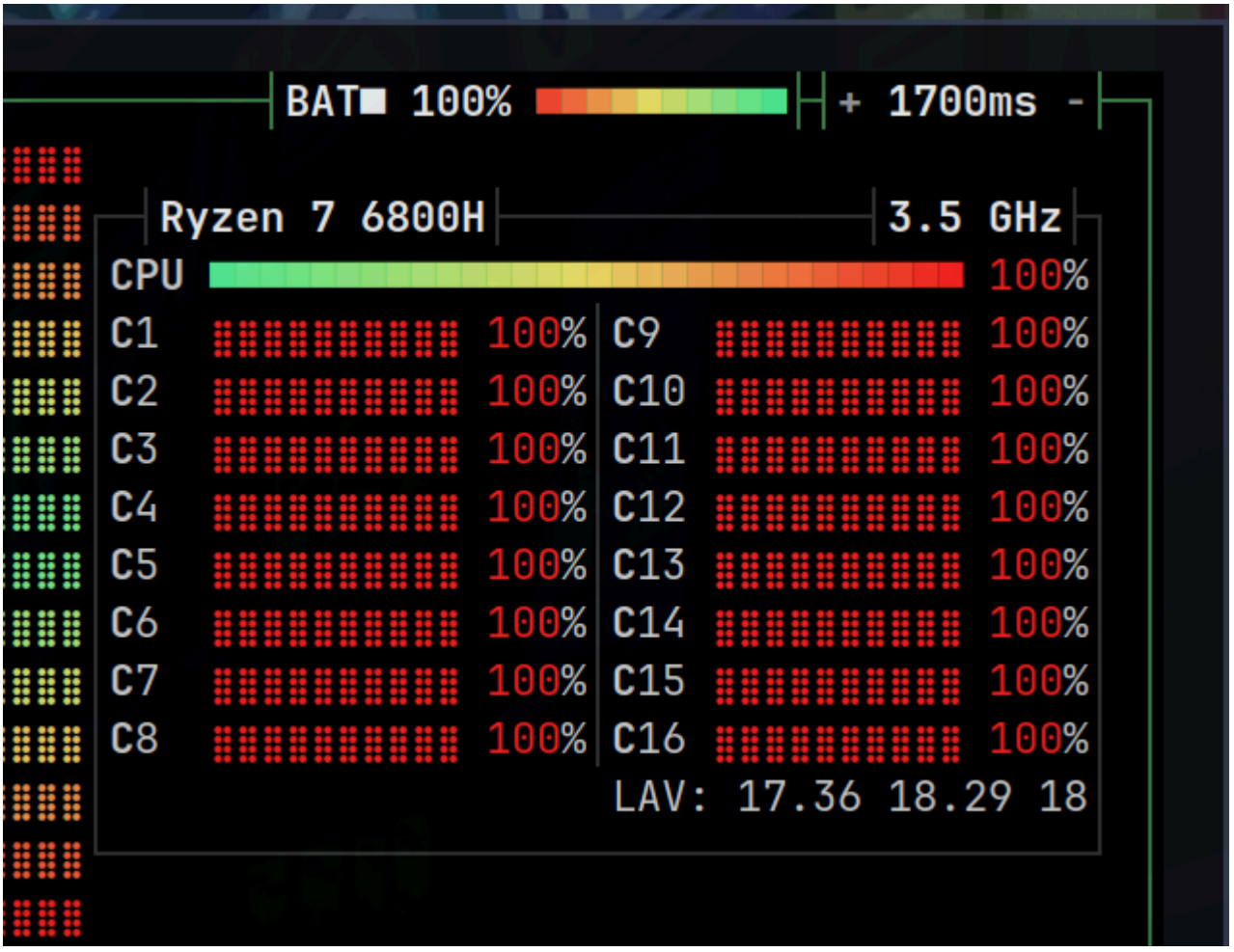
虚拟机用`ip addr`看网卡地址，是然后开启NAT网络方式，把ip输进去，设置一下端口。

然后主机的`/etc/hosts`加上一行，刚才获得的`ip embark.local`。这样就可以直接访问了。

> 有了这个方法，后面可以虚拟机模拟固件，然后主机直接打。调试可以再想一下办法，应该可以远程调试。



跑得够刺激，直接满了。



FirmAE

这个项目好像也很牛逼，不过还没上手使用。等我手头这个emba跑完了试试。

这个项目根据oneshell师傅所说主要是用于仿真和调试。没什么特殊的，主要就是端口转发啥的。

我的环境是22.04LTS ubuntu。

binwalk模块无法导入

```
git clone https://github.com/ReFirmLabs/binwalk.git
cd binwalk
sudo python setup.py install
```

CVE提交方式

存一下，刚查了这个版本的固件没漏洞，准备开造。

https://www.freebuf.com/articles/web/342909.html

https://blog.csdn.net/weixin_48421613/article/details/120719338#commentBox

开始复现

2024.3.2

这几天搞了半天，根本连怎么用python交互都不知道。从头开始一点点复现学习吧。然后自己喂了一些给机器人让他和我一起学。

https://www.iotsec-zone.com/

今天开始阅读《揭秘路由器》了。

路由器漏洞基本知识

路由器作为连接网络的关键设备，其安全性至关重要。了解路由器漏洞的基本知识是进行漏洞分析和挖掘的必要前提。

漏洞分类

路由器漏洞可以按照不同的特征进行分类，以便更好地理解和应对这些漏洞。

密码破解漏洞

密码破解漏洞是通过对WiFi加密密码进行破解来获取未授权访问权限的一种漏洞。攻击者可以利用WPS的PIN爆破、WiFi弱密码爆破或管理员账号密码爆破等方式来获取路由器的控制权。

WEB漏洞

WEB漏洞是指存在于路由器的Web服务器中的漏洞。这些漏洞可能包括SQL注入、命令执行、跨站请求伪造（CSRF）和跨站脚本攻击（XSS）等。

后门漏洞

后门漏洞是由开发人员为了方便后续调试而故意留下的安全漏洞。然而，一旦黑客发现这些后门，就会对路由器的安全性造成严重威胁。

溢出漏洞

溢出漏洞是指由于缓冲区溢出等原因导致的内存溢出问题。攻击者可以通过利用这些漏洞来执行恶意代码，实现对路由器的攻击和控制。

HTTP协议

请求行

```
Method Request-URI HTTP-Version CRLF
```

如

```
POST /registez.aspx HTTP/ (CRLE)
```

消息报头

```
名字+:+空格+值
```

如

```
Accept:image/gif
```

表示请求GIF图像格式的资源。

完整如

```
GET /index.html HTTP/1.1 (CRLF)
Accept:image/gif, image/x-xbitmap,*/* (CRLF)
Accept-Language:zh-cn (CRLF)
Accept-Encoding:gzip, deflate (CRLF)
User-Rgent:Mozilla/4.0(compatible;MSIE6.0;Windows NT 5.0) (CRLF)
Host:www.baidu.com (CRLF)
Connection:Keep-Alive (CRLF)
(CRLF)
```

请求正文

如

```
Usernarme=admin&password=admin
```

实际上可以有更多内容。

DIR-815多次溢出漏洞

2024.3.6

昨晚终于花了三天复现了DIR815的漏洞，等过会合天发出来了贴在这。在这里记录一个好文章：

https://bbs.kanxue.com/thread-277386.htm