BUUCTF——firmwork

原创

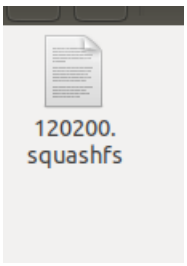
chan3301 于 2019-08-01 16:54:09 发布 920 收藏 2

分类专栏： 逆向题目练习 文章标签： 逆向 BUUCTF

本文链接：https://blog.csdn.net/sjt670994562/article/details/98071249

这是前几天做的一道逆向题，固件里面的bin文件分析，学了不少的姿势，所以单独拿出来记录一下

开始我使用binwallk看得，果然binwalk出了不少的文件，发现有一个Squashfs文件，说明他用了Squashfs 文件系统



但是一直没办法解压，通过查阅大量资料，终于找到解压的办法。

先运行

hexdump -C 1.bin | grep -n “hsqs” //得出位移为0x00120200

再提取一个从0x00120200开始的一百个字节并定义为squash的文件

dd if=1.bin bs=1 count=100 skip=1180160 of=squash

file一下

file squash： //得出字节数为2774624

dd if=1.bin bs=1 count=2774624 skip=1180160 of=1.squash //提取

然后安装firmware-mod-kit解压缩工具，后面连接有大佬教程连接，这里把代码带过来

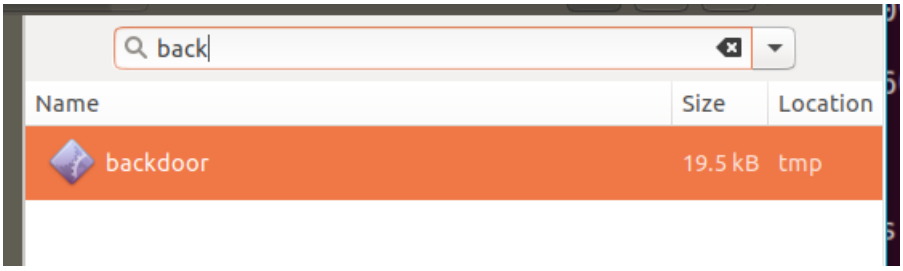
```
git clone https://github.com/mirror/firmware-mod-kit.git

sudo apt-get install build-essential zlib1g-dev libz1zma-dev python-magic

./configure && make
```

在firmware-mod-kit的目录下运行unsquashfs_all.sh 1.squash，成功解压

流程图：

```
chan@chan:~/ida$ hexdump -C 1.bin | grep -n "hsqs"
55243:00120200  68 73 71 73 07 02 00 00  c8 8d 2b 55 00 00 02 00  |hsqs
......+U....|
chan@chan:~/ida$ dd if=1.bin bs=1 count=100 skip=1180160 of=squash
100+0 records in
100+0 records out
100 bytes copied, 0.00045647 s, 219 kB/s
chan@chan:~/ida$ file squash :
squash: Squashfs filesystem, little endian, version 4.0, 2774624 bytes,
 519 inodes, blocksize: 131072 bytes, created: Mon Apr 13 09:35:04 2015
: :     cannot open `: ' (No such file or directory)
chan@chan:~/ida$ dd if=1.bin bs=1 count=2774624 skip=1180160 of=1.squas
h
2774624+0 records in
2774624+0 records out
2774624 bytes (2.8 MB, 2.6 MiB) copied, 5.01465 s, 553 kB/s
chan@chan:~/ida$
```


找到backdoor文件



发现有一个UPX壳，去掉，查询字符串

```
LOAD:000…  00000006    C    write
LOAD:000…  00000006    C    ntohl
LOAD:000…  00000005    C    free
LOAD:000…  0000000A    C    GLIBC_2.4
.rodata:…  00000014    C    echo.byethost51.com
.rodata:…  00000005    C    root
.rodata:…  00000006    C    admin
.rodata:…  00000005    C    user
```

找到我们要的地址
这是他的端口

```
strcpy(&s, (&comm
v3 = 36667;
if ( strchr(&s, 58
```

然后变成MD5，ok啦

最后附上大神的文章，感觉固件这一块挺有趣的，可以玩一玩
https://www.cnblogs.com/blacksunny/p/7208451.html?utm_source=itdadao&utm_medium=referral