buuctf——firmware

原创

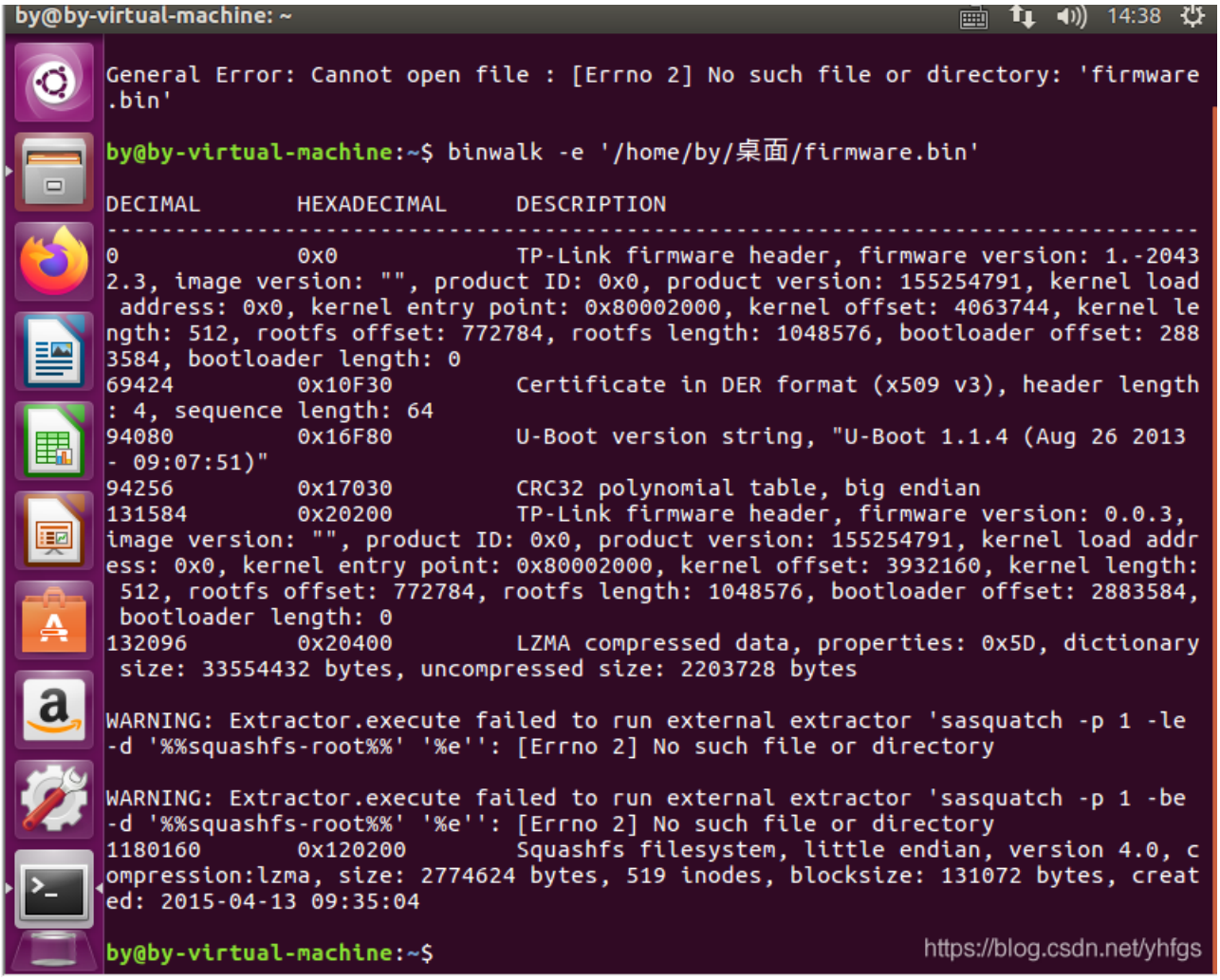
re3sry 于 2021-06-10 16:40:06 发布 151 收藏

本文链接：https://blog.csdn.net/yhfgs/article/details/117779638

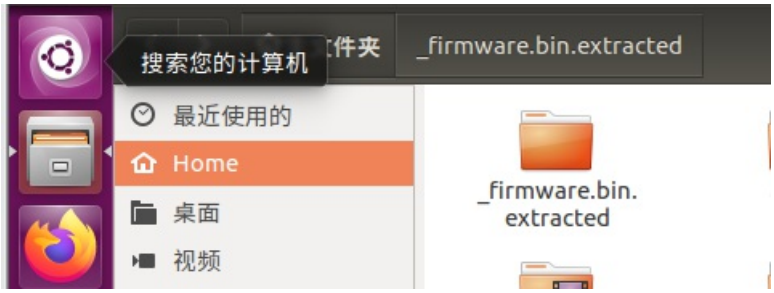
1.得到bin文件。在Ubuntu系统中用binwalk提取。

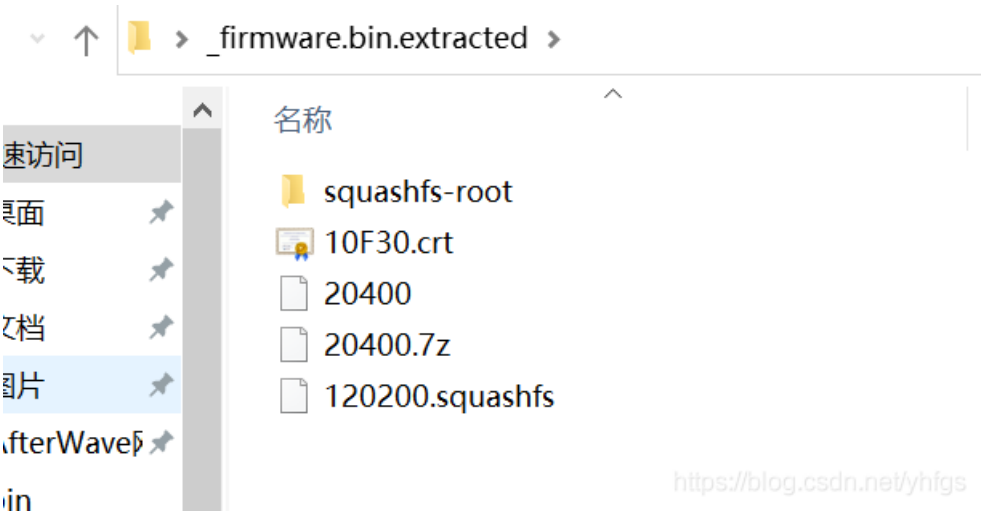
（binwalk下载：https://blog.csdn.net/QQ1084283172/article/details/65441110）

binwalk -e firmware.bin(路径)



得到文件夹（_firmware.bin.extracted）。

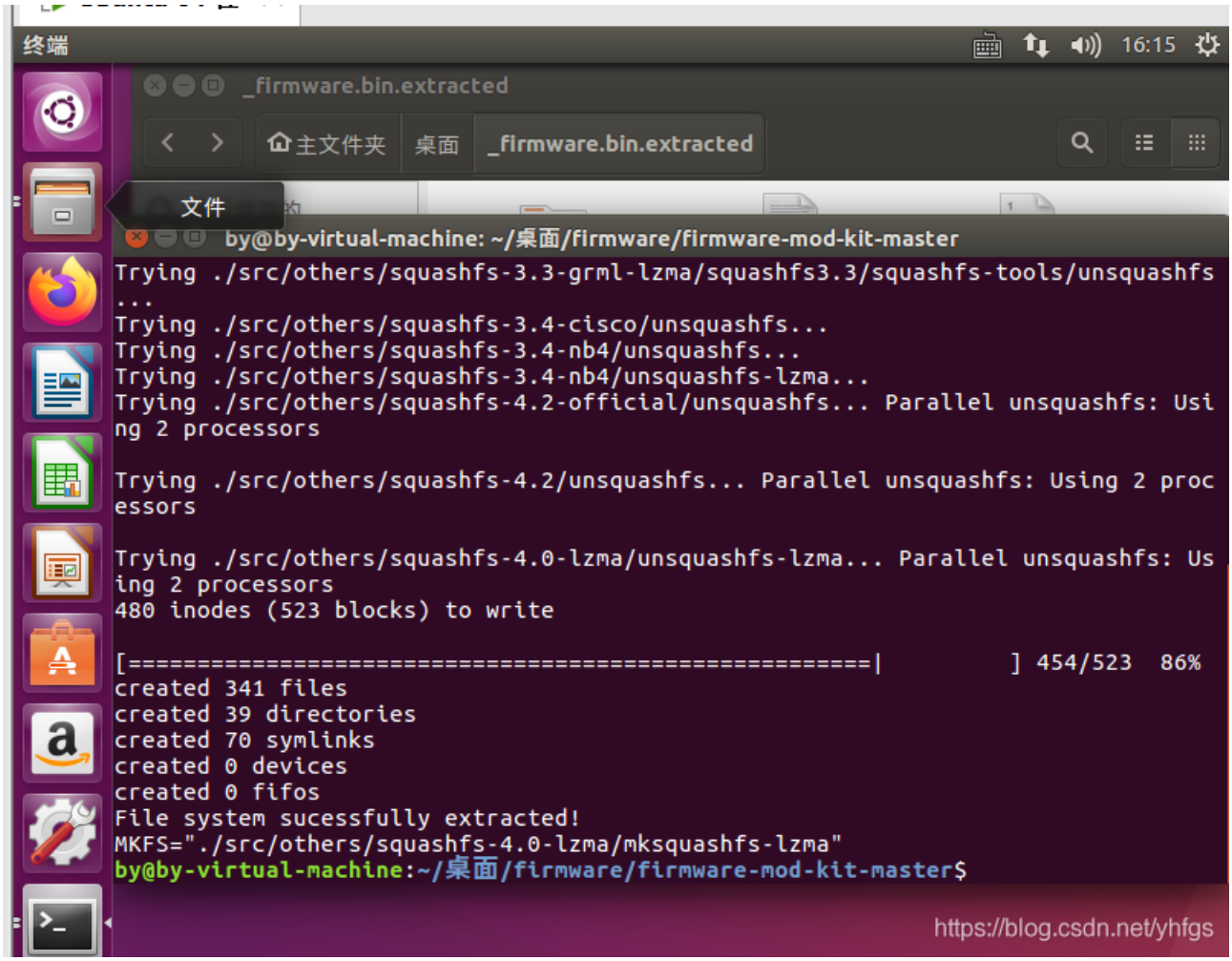




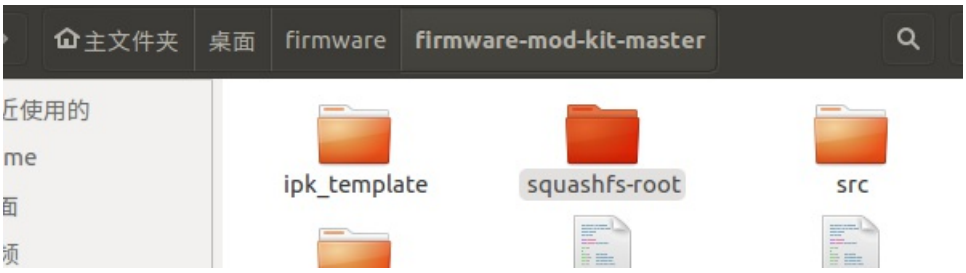
2.120200.squashfs是一个linux的压缩文件

用firmware-mod-kit工具解压。

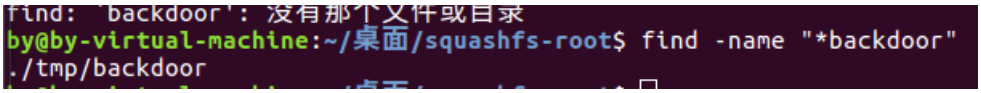
（firmware-mod-kit下载：firmware-mod-kit工具安装和使用说明_LDWJ2016的博客-CSDN博客_firmware-mod-kit）



在firmware-mod-kit-master目录下得到squashfs-root文件夹。

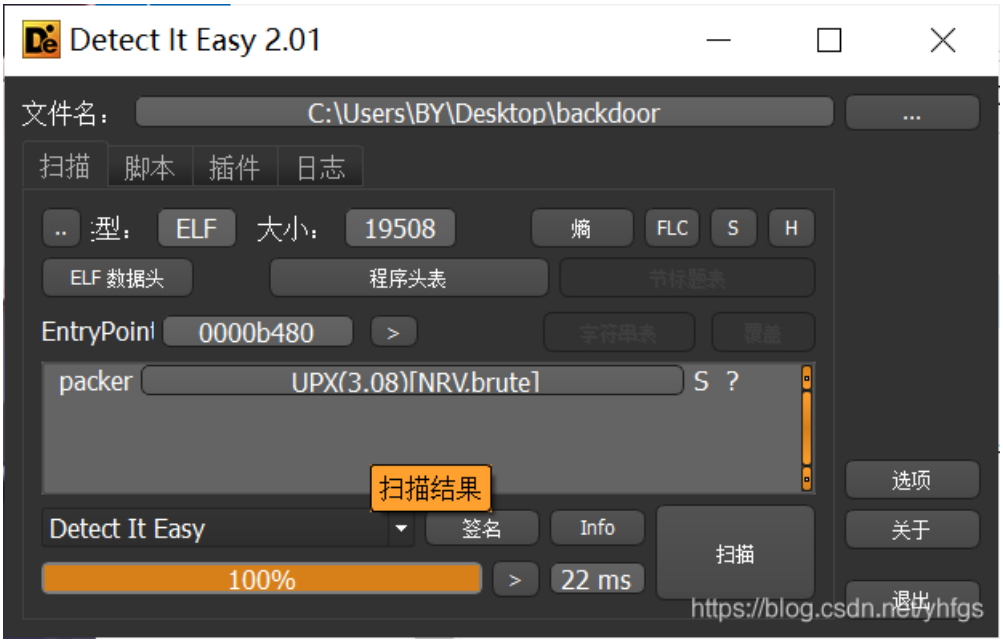


在其中找到backdoor。



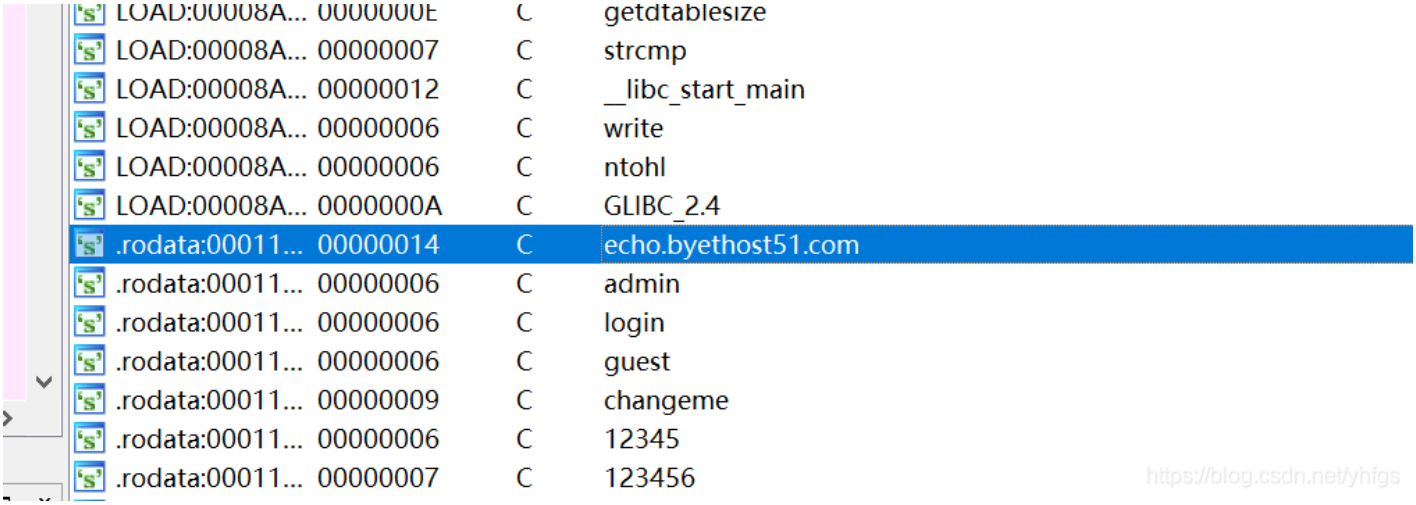
3.对backdoor查壳。

upx加壳，



脱壳，IDA反编译。

查看字符串



得到网址：echo.byethost51.com

继续找端口：找到initConnection函数

```
60  setsid();
61  chdir("/");
62  for ( i = signal(13, (__sighandler_t)1); ; i = (__sighandler_
63  {
64    while ( initConnection(i) )
65    {
66      puts("Failed to connect...");
67      i = (__sighandler_t)sleep(5u);
68    }
69    v9 = mainCommSock;
70    v10 = (const char *)getBuild();
71    sockprintf(v9, "BUILD %s", v10);
00009044 main:64 (11044)
```


找到initConnection函数，进入

```
2 {
3   char *v0; // r0
4   char s[512]; // [sp+4h] [bp-208h] BYREF
5   int v3; // [sp+204h] [bp-8h]
6
7   memset(s, 0, sizeof(s));
8   if ( mainCommSock )
9   {
.0    close(mainCommSock);
.1    mainCommSock = 0;
.2  }
.3  if ( currentServer )
.4    ++currentServer;
.5  else
.6    currentServer = 0;
.7  strcpy(s, (&commServer)[currentServer]);
.8  v3 = 36667;
.9  if ( strchr(s, 58) )
:0  {
:1    v0 = strchr(s, 58);
:2    v3 = atoi(v0 + 1);
:3    *strchr(s, 58) = 0;
:4  }
:5  mainCommSock = socket(2, 1, 0);
:6  return connectTimeout(mainCommSock, s, v3, 30) == 0;
:7 }
```


得到端口36667

4.根据题目对改字符串加密。

5.get flag

flag{33a422c45d551ac6e4756f59812a954b}