

buuctf——firmware

原创

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

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 版权协议，转载请附上原文出处链接和本声明。

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

版权

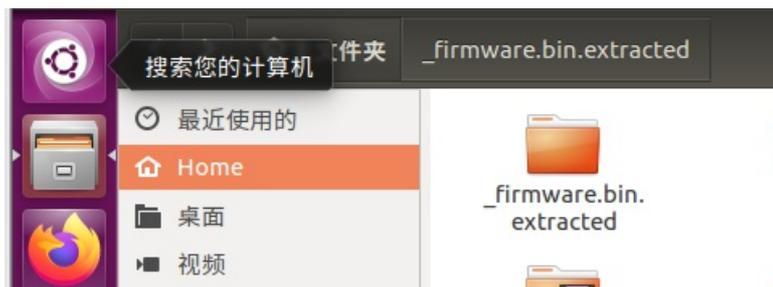
1.得到bin文件。在Ubuntu系统中用binwalk提取。

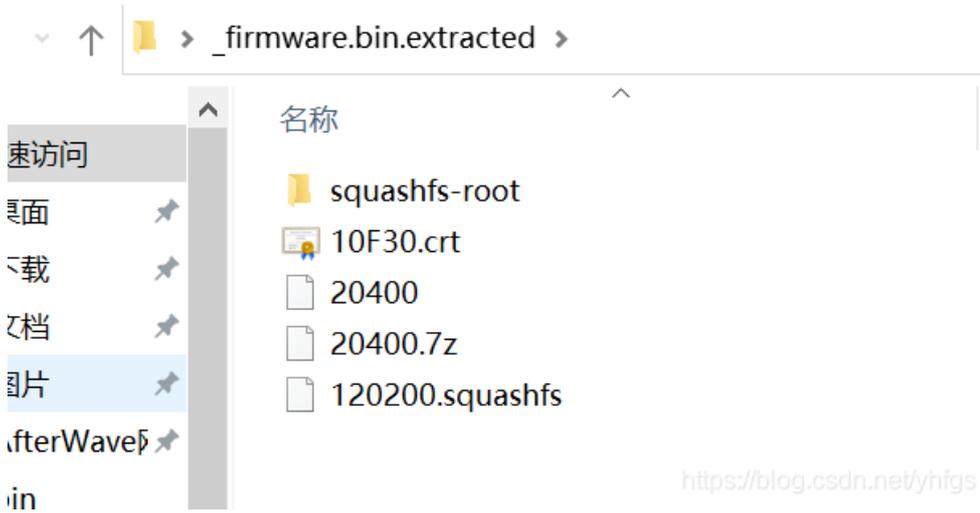
(binwalk下载：<https://blog.csdn.net/QQ1084283172/article/details/65441110>)

binwalk -e firmware.bin(路径)

```
by@by-virtual-machine: ~
General Error: Cannot open file : [Errno 2] No such file or directory: 'firmware
.bin'
by@by-virtual-machine:~$ binwalk -e '/home/by/桌面/firmware.bin'
DECIMAL          HEXADECIMAL      DESCRIPTION
-----
0                0x0              TP-Link firmware header, firmware version: 1.-2043
2.3, image version: "", product ID: 0x0, product version: 155254791, kernel load
address: 0x0, kernel entry point: 0x80002000, kernel offset: 4063744, kernel le
ngth: 512, rootfs offset: 772784, rootfs length: 1048576, bootloader offset: 288
3584, bootloader length: 0
69424           0x10F30          Certificate in DER format (x509 v3), header length
: 4, sequence length: 64
94080           0x16F80          U-Boot version string, "U-Boot 1.1.4 (Aug 26 2013
- 09:07:51)"
94256           0x17030          CRC32 polynomial table, big endian
131584          0x20200          TP-Link firmware header, firmware version: 0.0.3,
image version: "", product ID: 0x0, product version: 155254791, kernel load addr
ess: 0x0, kernel entry point: 0x80002000, kernel offset: 3932160, kernel length:
512, rootfs offset: 772784, rootfs length: 1048576, bootloader offset: 2883584,
bootloader length: 0
132096          0x20400          LZMA compressed data, properties: 0x5D, dictionary
size: 33554432 bytes, uncompressed size: 2203728 bytes
WARNING: Extractor.execute failed to run external extractor 'sasquatch -p 1 -le
-d '%squashfs-root%' '%e': [Errno 2] No such file or directory
WARNING: Extractor.execute failed to run external extractor 'sasquatch -p 1 -be
-d '%squashfs-root%' '%e': [Errno 2] No such file or directory
1180160         0x120200         Squashfs filesystem, little endian, version 4.0, c
ompression:lzma, size: 2774624 bytes, 519 inodes, blocksize: 131072 bytes, creat
ed: 2015-04-13 09:35:04
by@by-virtual-machine:~$
```

得到文件夹（_firmware.bin.extracted）。



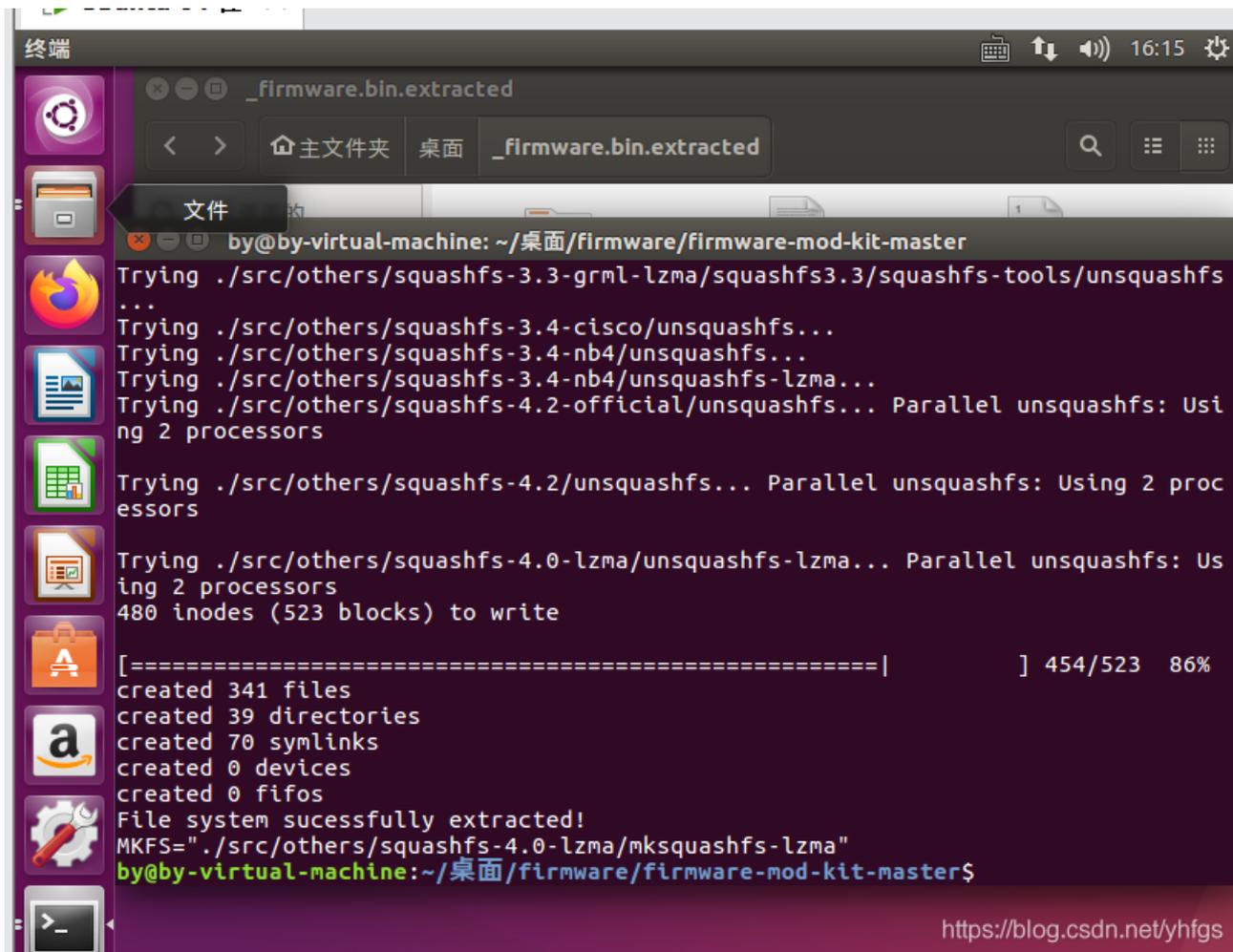


<https://blog.csdn.net/yhfgs>

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](#))



<https://blog.csdn.net/yhfgs>

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

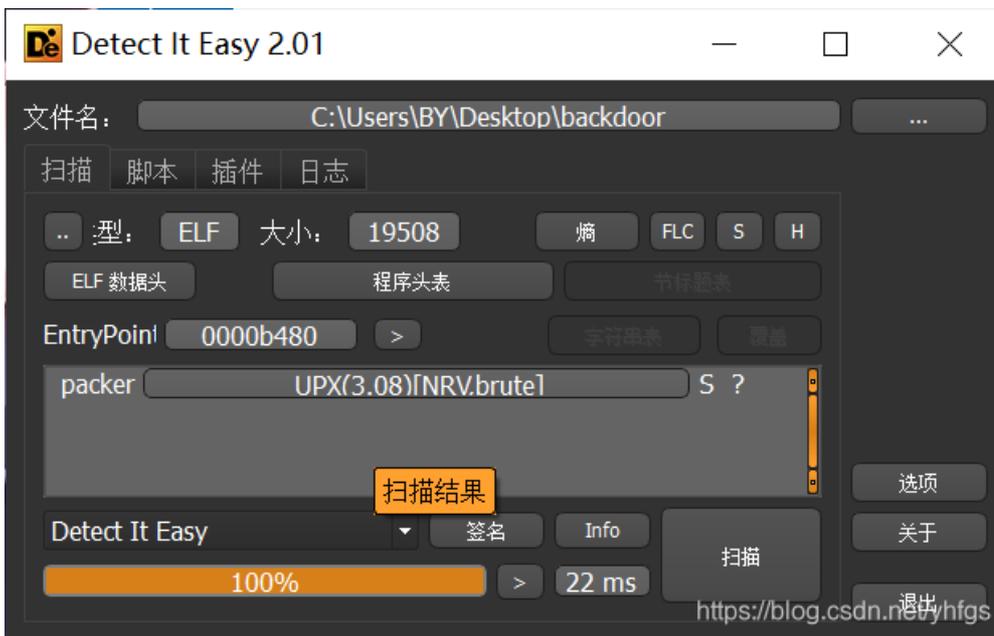


在其中找到backdoor。

```
find: 'backdoor': 没有那个文件或目录
by@by-virtual-machine:~/桌面/squashfs-root$ find -name "*backdoor"
./tmp/backdoor
```

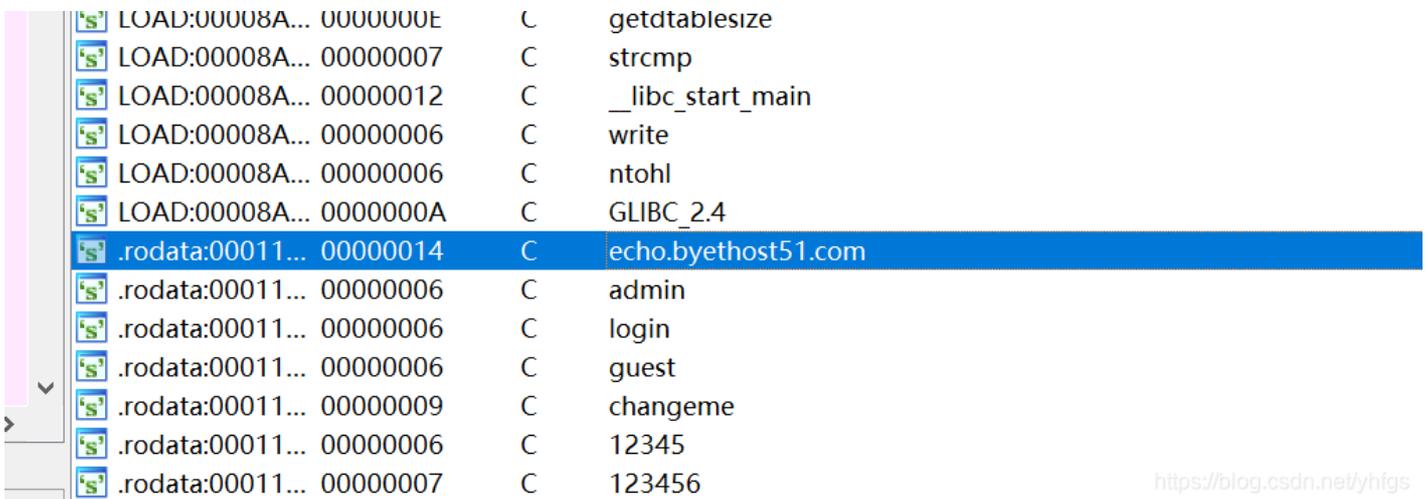
3.对backdoor查壳。

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  setuid(0);
61  chdir("/");
62  for ( i = signal(13, (__sig_handler_t)1); ; i = (__sig_handler_t)
63  {
64  while ( initConnection(i) )
65  {
66  puts("Failed to connect...");
67  i = (__sig_handler_t)sleep(5u);
68  }
69  v9 = mainCommSock;
70  v10 = (const char *)getBuild();
71  sockprintf(v9, "BUILD %s", v10);
```

00009044 main:64 (11044) <https://blog.csdn.net/yhfgs>

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 {
10 close(mainCommSock);
11 mainCommSock = 0;
12 }
13 if ( currentServer )
14 ++currentServer;
15 else
16 currentServer = 0;
17 strcpy(s, (&commServer)[currentServer]);
18 v3 = 36667;
19 if ( strchr(s, 58) )
20 {
21 v0 = strchr(s, 58);
22 v3 = atoi(v0 + 1);
23 *strchr(s, 58) = 0;
24 }
25 mainCommSock = socket(2, 1, 0);
26 return connectTimeout(mainCommSock, s, v3, 30) == 0;
27 }
```

<https://blog.csdn.net/yhfgs>

得到端口36667

4.根据题目对改字符串加密。

[加密/解密](#) [散列/哈希](#) [BASE64](#) [图片转 BASE64](#) [进制转换](#) [URL转码](#) [ASCII转换](#) [UTF-8编码](#) [htpasswd生成器](#) [迅雷|快车|旋风URL加解密](#) [MD5加密](#)

[\[点我\]==>](#) 新版MD5加密解密工具，支持 32位、16位大小写，还支持部分MD5代码解密哦

echo.byethost51.com:36667

33a422c45d551ac6e4756f59812a954b

32位[小]

加密 清空

<https://blog.csdn.net/yhfgs>

5.get flag

flag{33a422c45d551ac6e4756f59812a954b}