BUUCTF--firmware

原创

Hk_Mayfly 于 2020-03-31 23:41:00 发布 484 收藏

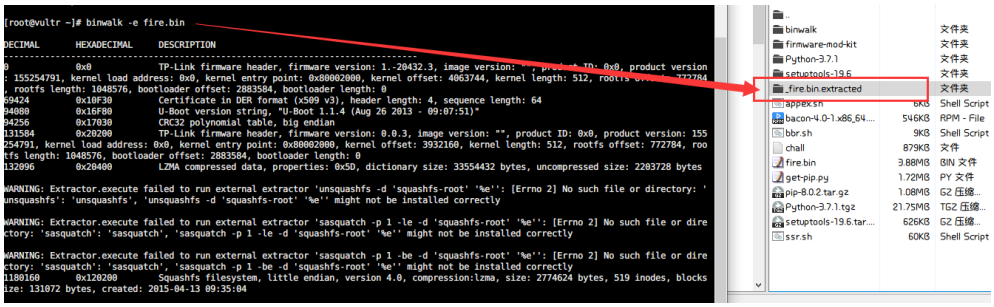
测试文件：https://www.lanzous.com/iaup43c

文件提取

binwalk

首先需要使用binwalk对文件进行提取。安装教程：https://blog.csdn.net/QQ1084283172/article/details/65441110

> **binwalk -e fire.bin**



firmware-mod-kit分析

安装

```
sudo yum install git build-essential zlib1g-dev liblzma-dev python-magic
git clone https://github.com/mirror/firmware-mod-kit.git
cd firmware-mod-kit/src
./configure
make
```

说明

extract-firmware.sh 解包固件

build-firmware.sh 重新封包

check_for_upgrade.sh 检查更新

unsquashfs_all.sh 解包提取出来的squashfs文件

将_fire.bin.extracted文件夹中的120200.squashfs文件，转存到firmware-mod-kit文件夹

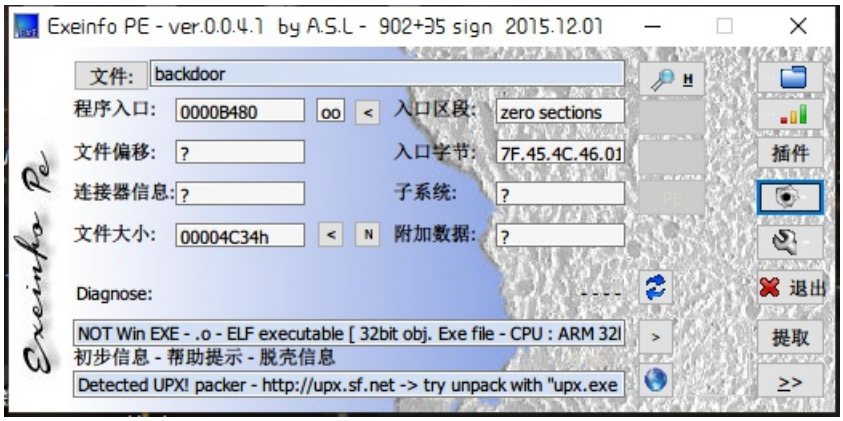
```
mv /root/_fire.bin.extracted/120200.squashfs /root/firmware-mod-kit

cd firmware-mod-kit

./unsquashfs_all.sh 120200.squashfs

cd squashfs-root/tmp/

dir
```

第三条指令，可以使用绝对路径，不过我报错了，所以用的相对路径。

```
[root@vultr firmware-mod-kit]# ./unsquashfs_all.sh 120200.squashfs
./unsquashfs_all.sh: line 85: ./src/binwalk: No such file or directory
Attempting to extract SquashFS .X file system...


Trying ./src/squashfs-2.1-r2/unsquashfs...
Trying ./src/squashfs-2.1-r2/unsquashfs-lzma...
Trying ./src/squashfs-3.0/unsquashfs...
Trying ./src/squashfs-3.0/unsquashfs-lzma...
Trying ./src/squashfs-3.0-lzma-damn-small-variant/unsquashfs-lzma...
Trying ./src/others/squashfs-2.0-nb4/unsquashfs...
Trying ./src/others/squashfs-3.0-e2100/unsquashfs...
Trying ./src/others/squashfs-3.0-e2100/unsquashfs-lzma...
Trying ./src/others/squashfs-3.2-r2/unsquashfs...
Trying ./src/others/squashfs-3.2-r2-lzma/squashfs3.2-r2/squashfs-tools/unsquashfs...
Trying ./src/others/squashfs-3.2-r2-hg612-lzma/unsquashfs...
Trying ./src/others/squashfs-3.2-r2-wnr1000/unsquashfs...
Trying ./src/others/squashfs-3.2-r2-rtn12/unsquashfs...
Trying ./src/others/squashfs-3.3/unsquashfs...
Trying ./src/others/squashfs-3.3-lzma/squashfs3.3/squashfs-tools/unsquashfs...
Trying ./src/others/squashfs-3.3-grml-lzma/squashfs3.3/squashfs-tools/unsquashfs...
Trying ./src/others/squashfs-3.4-cisco/unsquashfs...
Trying ./src/others/squashfs-3.4-nb4/unsquashfs...
Trying ./src/others/squashfs-3.4-nb4/unsquashfs-lzma...
Trying ./src/others/squashfs-4.2-official/unsquashfs... Parallel unsquashfs: Using 1 processor

Trying ./src/others/squashfs-4.2/unsquashfs... Parallel unsquashfs: Using 1 processor

Trying ./src/others/squashfs-4.0-lzma/unsquashfs-lzma... Parallel unsquashfs: Using 1 processor
480 inodes (523 blocks) to write

[=========================|                                                                                                                    ] 123/523  23%F
ile system sucessfully extracted!
MKFS="./src/others/squashfs-4.0-lzma/mksquashfs-lzma"
[============================================================-                                                                            ] 306/523  58%[
[=============================================================================================================================================\] 523/523 100%
created 341 files
created 39 directories
created 70 symlinks
created 69 devices
created 0 fifos
[root@vultr firmware-mod-kit]# cd squashfs-root/tmp/
[root@vultr tmp]# dir
backdoor
[root@vultr tmp]#
```

提取出的backdoor就是我们需要的文件。

文件分析

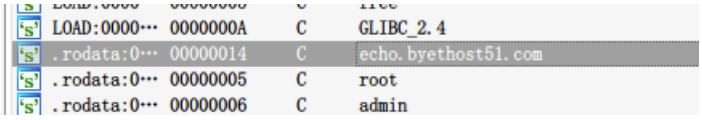


upx脱壳

```
C:\Users\10245\Desktop>upx -d backdoor
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95w       Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     54907 <-     19508   35.53%    linux/arm    backdoor

Unpacked 1 file.
```

代码分析

因为题目中是让我们找网址+端口的md5加密结果，因此我们只需要在String window找网址和端口就行。



找到源处

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

  memset(&s, 0, 0x200u);
  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;
}
```

即：**echo.byethost51.com:36667**

get flag！

> **flag{33a422c45d551ac6e4756f59812a954b}**