buuctf——firmware



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: ~ 📺 🚺 🜒) 14:38 😲 General Error: Cannot open file : [Errno 2] No such file or directory: 'firmware Ô .bin' by@by-virtual-machine:~\$ binwalk -e '/home/by/桌面/firmware.bin' DECIMAL HEXADECIMAL DESCRIPTION TP-Link firmware header, firmware version: 1.-2043 0 0x0 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 Certificate in DER format (x509 v3), header length 0x10F30 : 4, sequence length: 64 U-Boot version string, "U-Boot 1.1.4 (Aug 26 2013 94080 0x16F80 - 09:07:51)" 94256 0x17030 CRC32 polynomial table, big endian TP-Link firmware header, firmware version: 0.0.3, 131584 0x20200 image version: "", product ID: 0x0, product version: 155254791, kernel load addr 2 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 https://blog.csdn.net/yhfgs by@by-virtual-machine:~\$

得到文件夹(_firmware.bin.extracted)。



\sim \uparrow	📕 > _fir	rmware.bin.extracted >	
速访问 電 [、] 载 ζ档 晶片 ufterWav	∧ ★ ★ ★ ★	 名称 squashfs-root 10F30.crt 20400 20400.7z 120200.squashfs 	^ https://blog.csdn.net/yhfgs
In			

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)

终端		è ↑	↓ ●))	16:15 🔱
6	🛛 🖶 🗉 _firmware.bin.extracted			
	く > 企 主文件夹 桌面 _firmware.bin.extracted		۹	
	文件 20 次件 20 非 20	1	2	
	🛛 🔍 🔍 by@by-virtual-machine: ~/桌面/firmware/firmware-mod-kit-master			
	Trying ./src/others/squashfs-3.3-grml-lzma/squashfs3.3/squashf	s-too	ls/uns	quashfs
	Trying ./src/others/squashfs-3.4-clsco/unsquashfs			
	Trying ./src/others/squashfs-3.4-nb4/unsquashfs-lzma	-		
	Trying ./src/others/squashfs-4.2-official/unsquashfs Parall	el un	squash	ifs: Usi
	Trying ./src/others/squashfs-4.2/unsquashfs Parallel unsqua	shfs:	Using	2 ргос
	Trying ./src/others/squashfs-4.0-lzma/unsquashfs-lzma Paral	lel u	nsquas	hfs: Us
	1ng 2 processors 480 inodes (523 blocks) to write			
-8-				
A	[=====================================] ·	454/52	3 86%
	created 39 directories			
a	created 70 symlinks			
	created 0 devices created 0 fifos			
122	File system sucessfully extracted!			
	MKFS="./src/others/squashfs-4.0-lzma/mksquashfs-lzma"			
	by why were the contraction of the second seco			
: >_	A http	os://blo	g.csdn.	net/yhfgs

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

	企 主文件夹	桌面	firmware	firmware-mod-kit-master	۹
丘使	用的			-	
me			ipk_templa	ate squashfs-root	SFC
面					In the second se
须				Hornessen H H H H H H H H H H H H H	Terrational and the second sec

在其中找到backdoor。

find: backdoor': 没有那个又件或目录 by@by_victual-machine:~/桌面/squashfs-roots	find -name	"*backdoor"
./tmp/backdoor		Duckdoor

3.对backdoor查壳。

upx加壳,

Detect It Easy 2.01			_		\times
文件名: C:\ 扫描 脚本 插件 日志	Users\BY\Desktop	\backdoor	-		
··· ;型: ELF 大小: ELF 数据头 EntryPoint 0000b480	19508 程序头表 >	熵 FL 学行串表	CS NEA	H	
packer UPX/	3.08)[NRV.brute]) S ?		选项
Detect It Easy	▼	Info 22 ms	扫描 https://bl	og.csdn.	关于 n褐嵌yhfgs

脱壳, IDA反编译。

查看字符串

	's' LOAD:00008A 0000000E	C	getdtablesize	
	🔄 LOAD:00008A 00000007	С	strcmp	
	🔄 LOAD:00008A 00000012	С	libc_start_main	
	🔄 LOAD:00008A 00000006	С	write	
	🔄 LOAD:00008A 00000006	С	ntohl	
	🔄 LOAD:00008A 0000000A	С	GLIBC_2.4	
	😨 .rodata:00011 00000014	С	echo.byethost51.com	
	🔄 .rodata:00011 00000006	С	admin	
	🔄 .rodata:00011 00000006	С	login	
	🔄 .rodata:00011 00000006	С	guest	
×	🔄 .rodata:00011 00000009	С	changeme	
	🔄 .rodata:00011 00000006	С	12345	
 	🔄 .rodata:00011 00000007	С	123456	

得到网址: echo.byethost51.com

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

```
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);
      mainCommSock = 0;
.1
.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
      v_3 = atoi(v_0 + 1);
!3
      *strchr(s, 58) = 0;
:4
   }
:5
   mainCommSock = socket(2, 1, 0);
    return connectTimeout(mainCommSock, s, v3, 30) == 0;
:6
:7 }
```

得到端口36667

4.根据题目对改字符串加密。

加密/解密 制列/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

5.get flag

flag{33a422c45d551ac6e4756f59812a954b}