TL-WR841N固件分析入门

```
wget https://static.tp-link.com/2018/201804/20180403/TL-
WR841N%28EU%29_V14_180319.zip
```

1、信息收集

解压后得到bin文件

1.1 file

```
file TL-WR841Nv14_EU_0.9.1_4.16_up_boot\[180319-rel57291\].bin
```

```
root@kali:~/desktop桌面/share/IOT/f固件安全# file TL-WR841Nv14_EU_0.9.1_4.16_up_boot\[180319-rel57291\].bin
TL-WR841Nv14_EU_0.9.1_4.16_up_boot[180319-rel57291].bin: data
root@kali:~/desktop桌面/share/IOT/f固件安全#
```

是二进制文件，可以直接用二进制工具（hexdump和string）读取其内容信息

1.2 hexdump

先将其二进制内容写入文件中，再逐步分析查看

```
hexdump -C TL-WR841Nv14_EU_0.9.1_4.16_up_boot\[180319-
rel57291\].bin > hex-out.txt
```

(hexdump -C 能够获取较多的信息，输出的格式为hex+ASCII的方式)

```
root@kali:~/desktop桌面/share/IOT/f固件安全# hexdump -C TL-WR841Nv14_EU_0.9.1_4.16_up_boot\[180319-rel57291\].bin > hex-out.txt
root@kali:~/desktop桌面/share/IOT/f固件安全# ls
 hex-out.txt   'TL-WR841N(EU)_V14_180319.zip'   'TL-WR841Nv14_EU_0.9.1_4.16_up_boot[180319-rel57291].bin'
root@kali:~/desktop桌面/share/IOT/f固件安全#
```

先查看下是否写入成功：先查看前几行即可

```
more hex-out.txt
```

```
root@kali:~/desktop桌面/share/IOT/f固件安全# more hex-out.txt
00000000  03 00 00 00 76 65 72 2e  20 32 2e 30 00 ff ff ff  |....ver. 2.0....|
00000010  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
00000030  ff ff ff ff 08 41 00 14  00 00 00 01 00 00 00 14  |.....A..........|
00000040  e1 62 6d f8 0b 9e 2e 18  94 a9 39 12 3b 80 66 50  |.bm.......9.;.fP|
00000050  00 00 00 00 ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
00000060  ff ff ff ff ff ff ff ff  00 00 00 80 50 c1 00 80  |............P...|
00000070  00 3e 02 00 00 01 04 00  00 0e e0 4f 00 0f 00 00  |.>.........O....|
00000080  00 2d 50 00 00 00 00 00  00 00 fd 74 55 aa 04 10  |.-P........tU...|
00000090  a5 00 09 01 b6 29 dd be  ff ff ff ff ff ff ff ff  |.....)..........|
000000a0  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
000000d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000001d0  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
00000200  ff 00 00 10 00 00 00 00  fd 00 00 10 00 00 00 00  |................|
00000210  0b 03 00 10 00 00 00 00  09 03 00 10 00 00 00 00  |................|
00000220  07 03 00 10 00 00 00 00  05 03 00 10 00 00 00 00  |................|
00000230  03 03 00 10 00 00 00 00  01 03 00 10 00 00 00 00  |................|
00000240  ff 02 00 10 00 00 00 00  fd 02 00 10 00 00 00 00  |................|
00000250  fb 02 00 10 00 00 00 00  f9 02 00 10 00 00 00 00  |................|
00000260  f7 02 00 10 00 00 00 00  f5 02 00 10 00 00 00 00  |................|
00000270  f3 02 00 10 00 00 00 00  f1 02 00 10 00 00 00 00  |................|
00000280  ef 02 00 10 00 00 00 00  ed 02 00 10 00 00 00 00  |................|
00000290  eb 02 00 10 00 00 00 00  e9 02 00 10 00 00 00 00  |................|
000002a0  e7 02 00 10 00 00 00 00  e5 02 00 10 00 00 00 00  |................|
000002b0  e3 02 00 10 00 00 00 00  e1 02 00 10 00 00 00 00  |................|
000002c0  df 02 00 10 00 00 00 00  dd 02 00 10 00 00 00 00  |................|
```

1.3 strings

strings 工具能够提取出bin文件中的字符串，提取后先写入到文本文件中：

```
strings TL-WR841Nv14_EU_0.9.1_4.16_up_boot\[180319-rel57291\].bin > str-out.txt
```

```
root@kali:~/desktop桌面/share/IOT/f固件安全# strings TL-WR841Nv14_EU_0.9.1_4.16_up_boot\[180319-rel57291\].bin > str-out.txt
root@kali:~/desktop桌面/share/IOT/f固件安全# ls
 hex-out.txt   str-out.txt  'TL-WR841N(EU)_V14_180319.zip'  'TL-WR841Nv14_EU_0.9.1_4.16_up_boot[180319-rel57291].bin'
root@kali:~/desktop桌面/share/IOT/f固件安全#
```

查看前几行试试

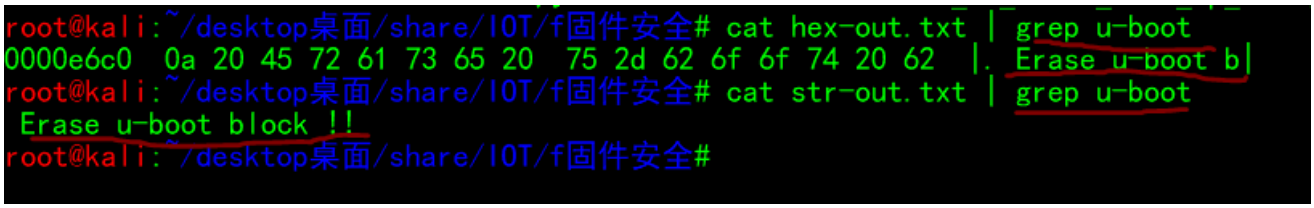
```
root@kali:~/desktop桌面/share/IOT/f固件安全# head -n 5 str-out.txt
ver. 2.0
$'X`
$$H*
$$Xm
$%Xm
root@kali:~/desktop桌面/share/IOT/f固件安全#
```

1.4 cat .. | grep

接下来可以直接在导出的文本文件中查找敏感的信息，如固件版本等

eg：搜索一下文件系统常用的boot loader名字u-boot

```
cat hex-out.txt | grep u-boot
cat str-out.txt | grep u-boot
```



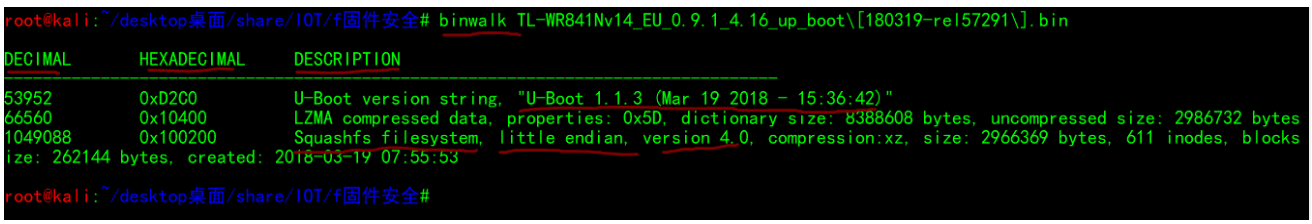
2、固件提取 binwalk

收集完相应的信息后，可以利用binwalk进行固件提取操纵

2.1 binwalk

先直接用binwalk 进行固件信息探测

```
binwalk TL-WR841Nv14_EU_0.9.1_4.16_up_boot\[180319-rel57291\].bin
```



可以获取很多有用的信息，系统文件信息，大小端信息，版本信息等

（PS：分析结果主要分为三个部分进行展示：文件地址的十进制和十六进制展示以及对应位置发现的详细描述）

确认此处使用的boot loader就是U-boot

2.2 binwalk -e

接下来用binwalk -e来对固件的各个部分进行提取

```
root@kali:~/desktop桌面/share/IOT/f固件安全# binwalk -e TL-WR841Nv14_EU_0.9.1_4.16_up_boot\[180319-rel57291\].bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
53952         0xD2C0          U-Boot version string, "U-Boot 1.1.3 (Mar 19 2018 - 15:36:42)"
66560         0x10400         LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size:
1049088       0x100200        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2966369 bytes, 611 i
ize: 262144 bytes, created: 2018-03-19 07:55:53

root@kali:~/desktop桌面/share/IOT/f固件安全# ls
 hex-out.txt                    'TL-WR841Nv14_EU_0.9.1_4.16_up_boot[180319-rel57291].bin'
 str-out.txt                    '_TL-WR841Nv14_EU_0.9.1_4.16_up_boot[180319-rel57291].bin.extracted'
'TL-WR841N(EU)_V14_180319.zip'
root@kali:~/desktop桌面/share/IOT/f固件安全#
```

提取完后可以进入文件系统中查看具体的文件目录信息，该固件就是一个小的操作系统的重要核心信息

binwalk其他参数解释：-Mre

```
-M：递归扫描提取的文件

-r：提取后删除剩余文件

-e：自动提取已知文件类型
```

所以一般会使用binwalk -Mre file.bin来提取固件中的信息。

2.3 dd

其实也可以使用dd命令来对特定位置的文件来提取 ，结果与binwalk 提取相同

提取的主要内容为固件的文件系统，所以直接从文件系统Squashfs filesystem的位置偏移地址往后开始提取即可

先用binwalk 查看该固件的大致信息：

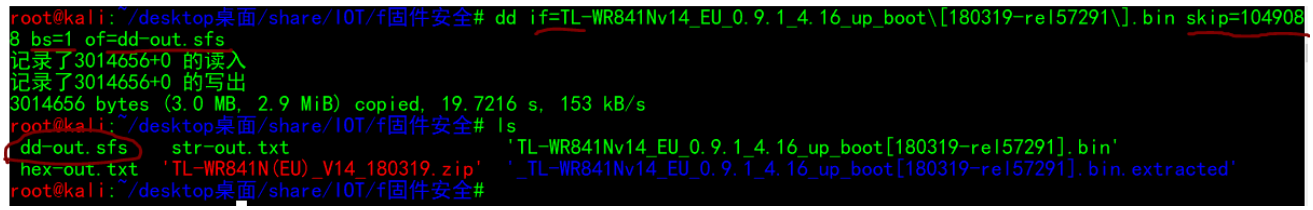
```
root@kali:~/desktop桌面/share/IOT/f固件安全# binwalk TL-WR841Nv14_EU_0.9.1_4.16_up_boot\[180319-rel57291\].bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
53952         0xD2C0          U-Boot version string, "U-Boot 1.1.3 (Mar 19 2018 - 15:36:42)"
66560         0x10400         LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 2986732 bytes
1049088       0x100200        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2966369 bytes, 611 inodes, blocks
ize: 262144 bytes, created: 2018-03-19 07:55:53

root@kali:~/desktop桌面/share/IOT/f固件安全#
```

其Squashfs filesystem 文件系统的偏移地址为 1049088

直接提取该地址之后的内容

```
dd if=TL-WR841Nv14_EU_0.9.1_4.16_up_boot\[180319-rel57291\].bin
skip=1049088 bs=1 of=TP.sfs
```

（PS： sfs是一个存储Squashfs文件系统的文件，一般用于linux下）



dd 参数解释：

```
dd 可以跨文件、设备、分区和卷 复制数据
if 标准文件输入 即准备被dd的固件
of 标准文件输出 即dd后保存的文件，文件系统的后缀名一般为sfs
bs 块大小 （bs=1 即每一块扫描过去）
skip用于跳过指向固件二进制映像中特定地址的指针 即跳过的地址
```

dd提取后得到一个sfs 的系统文件，通常这是一种 Squashfs File Archive 的压缩格式

还需要进行解压

2.4 unsquashfs

对sfs压缩文件可以使用 unsquashfs 工具来对其中的文件系统进行提取

```
unsquashfs dd-out.sfs
```

```
root@kali:~/desktop桌面/share/IOT/f固件安全# unsquashfs dd-out.sfs
Parallel unsquashfs: Using 4 processors
568 inodes (586 blocks) to write

[=============================================================================================]

created 419 files
created 43 directories
created 60 symlinks
created 89 devices
created 0 fifos
root@kali:~/desktop桌面/share/IOT/f固件安全# ls
 dd-out.sfs      'TL-WR841N(EU)_V14_180319.zip'
 hex-out.txt     'TL-WR841Nv14_EU_0.9.1_4.16_up_boot[180319-rel57291].bin'
 squashfs-root   '_TL-WR841Nv14_EU_0.9.1_4.16_up_boot[180319-rel57291].bin.extracted'
 str-out.txt
root@kali:~/desktop桌面/share/IOT/f固件安全#
```

提取后得到一个 squashfs-root

这就是该固件的文件系统

```
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root# ls
bin  dev  etc  lib  linuxrc  mnt  proc  sbin  sys  usr  var  web
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root#
```

其实就是一个linux 的系统目录

至此，我们已经提取了固件的整个文件系统，现在我们可以开始分析文件系统中存在的二进制文件或者某些文件

3、固件 文件系统分析

固件中的文件系统分析与linux 系统分析类似，

直奔etc目录，查看密码文件 passwd ， shadow等

3.1 etc/passwd

```
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root/etc# ls
default_config.xml  init.d          MT7628_AP_2T2R-4L_V15.BIN  passwd.bak                resolv.conf  services
fstab               inittab         MT7628_EEPROM_20140317.bin ppp                       RT2860AP.dat SingleSKU_CE.dat
group               iptables-stop   passwd                     reduced_data_model.xml    samba        TZ
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root/etc# cat passwd
cat: passwd: 没有那个文件或目录
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root/etc# cat passwd.bak
admin:$1$$iC.dUsGpxNNJGeOm1dFio/:0:0:root:/:/bin/sh
dropbear:x:500:500:dropbear:/var/dropbear:/bin/sh
nobody:*:0:0:nobody:/:/bin/sh
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root/etc#
```

发现了admin用户的passwd信息，拿去 john解hash 试试

```
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root/etc# ls
default_config.xml  init.d          MT7628_AP_2T2R-4L_V15.BIN   passwd.bak              resolv.conf   services
fstab               inittab         MT7628_EEPROM_20140317.bin  ppp                     RT2860AP.dat  SingleSKU_CE.dat
group               iptables-stop   passwd                      reduced_data_model.xml  samba         TZ
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root/etc# john passwd.bak
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])
No password hashes left to crack (see FAQ)
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root/etc# john passwd.bak --show
admin:1234:0:0:root:/:/bin/sh

1 password hash cracked, 0 left
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root/etc#
```

直接可得到该系统的admin 用户，弱口令 为1234

3.2 etc/init.d

在/etc 目录下，init.d是linux 文件系统的启动项目录，查看其内容

```
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root/etc# ls
default_config.xml  init.d          MT7628_AP_2T2R-4L_V15.BIN   passwd.bak              resolv.conf   services
fstab               inittab         MT7628_EEPROM_20140317.bin  ppp                     RT2860AP.dat  SingleSKU_CE.dat
group               iptables-stop   passwd                      reduced_data_model.xml  samba         TZ
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root/etc# cd init.d/
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root/etc/init.d# ls
rcS
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root/etc/init.d# cat rcS
#!/bin/sh

mount -a
# added by yangcaiyong for sysfs
mount -t sysfs /sys /sys
# ended add

/bin/mkdir -m 0777 -p /var/lock
/bin/mkdir -m 0777 -p /var/log
/bin/mkdir -m 0777 -p /var/run
/bin/mkdir -m 0777 -p /var/tmp
/bin/mkdir -m 0777 -p /var/Wireless/RT2860AP
/bin/mkdir -m 0777 -p /var/tmp/wsc_upnp
cp -p /etc/SingleSKU_FCC.dat /var/Wireless/RT2860AP/SingleSKU.dat
```

简单来看

```
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root/etc/init.d# cat rcS
#!/bin/sh

mount -a
# added by yangcaiyong for sysfs
mount -t sysfs /sys /sys
# ended add

/bin/mkdir -m 0777 -p /var/lock
/bin/mkdir -m 0777 -p /var/log
/bin/mkdir -m 0777 -p /var/run
/bin/mkdir -m 0777 -p /var/tmp
/bin/mkdir -m 0777 -p /var/Wireless/RT2860AP
/bin/mkdir -m 0777 -p /var/tmp/wsc_upnp
cp -p /etc/SingleSKU_FCC.dat /var/Wireless/RT2860AP/SingleSKU.dat

/bin/mkdir -m 0777 -p /var/tmp/dropbear

/bin/mkdir -m 0777 -p /var/dev
cp -p /etc/passwd.bak /var/passwd
/bin/mkdir -m 0777 -p /var/l2tp

echo 1 > /proc/sys/net/ipv4/ip_forward
#echo 1 > /proc/sys/net/ipv4/tcp_syncookies
echo 1 > /proc/sys/net/ipv6/conf/all/forwarding

echo 30 > /proc/sys/net/unix/max_dgram_qlen
```

该系统启动后，会执行以上命令，如 导入更新passwd密码，开启转发功能等

3.3 /bin

回退到bin 目录下

```
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root/bin# ls
ash  busybox  cat  chmod  cp  date  df  echo  kill  login  ls  mkdir  mount  netstat  pidof  ping  ping6  ps  rm  sh  sleep  umount
root@kali:~/desktop桌面/share/IOT/f固件安全/squashfs-root/bin#
```

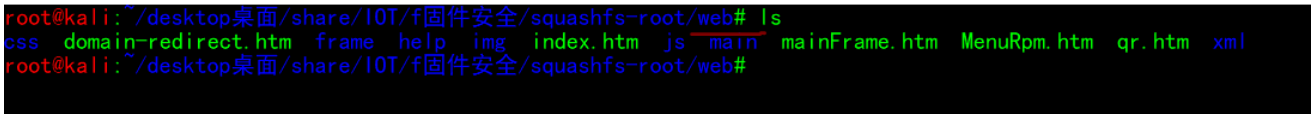
发现该系统能够执行以上的命令

可以对其中的操作逻辑进行逆向分析，发现其中的漏洞，如命令执行，绕过登录等

eg：利用IDA或者Ghidra等工具对“login”进行逆行分析，发现其登录逻辑中的漏洞

3.4 web

进入文件系统的web目录下，对web进行源码审计，挖掘漏洞



4、其他分析方法

在整个二进制文件 .bin 中搜索字符串

```
r2 TL-WR841Nv14_EU_0.9.1_4.16_up_boot\[180319-rel57291\].bin
izz | more
```