run.sh 框架分析

笔记本:	FirmAE源码解读		
创建时间:	2022/4/10 20:46	**更新时间:**	2022/4/21 10:09
作者:	dreamingctf@163.com		

输出日志

```
ubuntu@ubuntu:~/Desktop/DIR600/FirmAE$ sudo ./run.sh -r dir600 ./firmwares/FIRMWARE_DIR600B1_B2_v2.01-tomizone-1.1.0.bin
[*] ./firmwares/FIRMWARE_DIR600B1_B2_v2.01-tomizone-1.1.0.bin emulation start!!!
[*] extract done!!!
[*] get architecture done!!!
mke2fs 1.44.1 (24-Mar-2018)
e2fsck 1.44.1 (24-Mar-2018)
[*] infer network start!!!
[IID] 1
[MODE] run
[+] Network reachable on 192.168.0.1!
[+] Web service on 192.168.0.1
Creating TAP device tap1_0...
Set 'tap1_0' persistent and owned by uid 0
Initializing VLAN...
Bringing up TAP device...
Starting emulation of firmware... 192.168.0.1 true true 2.072803854 3.231474404
```

```
[*] extract done!!! - Line 141, -Line 114, ./sources/extractor/extractor.py
删除多行：第 3 - 5 行
3, 5d
删除多行：第 10 到最后一行
10, $d

echo "$UID"
echo "$PID"

sudo ./part.sh -r dir600 ./firmwares/FIRMWARE_DIR600B1_B2_v2.01-tomizone-1.1.0.bin
[*] ./firmwares/FIRMWARE_DIR600B1_B2_v2.01-tomizone-1.1.0.bin emulation start!!!
/home/ubuntu/Desktop/DIR600/FirmAE/scratch/1
[*] extract done!!!


check
sudo ./run.sh -c dir645 ./firmwares/DIR645A1_FW102B08.bin

analyze
ubuntu@ubuntu:~/Desktop/DIR600/FirmAE$ sudo ./run.sh -a dir645 ./firmwares/DIR645A1_FW102B08.bin
[sudo] password for ubuntu:
[*] ./firmwares/DIR645A1_FW102B08.bin emulation start!!!
[*] extract done!!!
[*] get architecture done!!!
[*] ./firmwares/DIR645A1_FW102B08.bin already succeed emulation!!!

[IID] 4
[MODE] analyze
[+] Network reachable on 192.168.0.1!
[+] Web service on 192.168.0.1
[*] Waiting web service...
Creating TAP device tap4_0...
Set 'tap4_0' persistent and owned by uid 0
Initializing VLAN...
Bringing up TAP device...
Starting emulation of firmware... 192.168.0.1 true true 11.251085030 30.828259229
[+] start pentest!
[*] FirmAE web server initializer
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-12 18:48 PDT
Nmap scan report for 192.168.0.1
Host is up (0.00099s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  D-Link 524, DIR-300, or WBR-1310 WAP telnetd
53/tcp    open  domain  dnsmasq 2.45
80/tcp    open  http    D-Link DIR-645 WAP http config 1.02
49152/tcp open  upnp    D-Link DIR-645 WAP UPnP 1.02 (UPnP 1.0)
MAC Address: 00:DE:FA:1A:01:00 (Unknown)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; Device: WAP; CPE: cpe:/h:dlink:dir-645:1.02, cpe:/o:linux:linux_kernel, cpe:/h:d-link:dir-645


OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.50 seconds
[*] fuzzer
[*] rsf
/home/ubuntu/Desktop/DIR600/FirmAE/analyses
[*] analyzer finished
/home/ubuntu/Desktop/DIR600/FirmAE
qemu-system-mipsel: terminating on signal 15 from pid 3324 (/bin/bash)
Bringing down TAP device...
```

```
Removing VLAN...
Deleting TAP device tap4_0...
Set 'tap4_0' nonpersistent
Done!
[*] cleanup
======================================

run
sudo ./run.sh -r dir645 ./firmwares/DIR645A1_FW102B08.bin

debug
ubuntu@ubuntu:~/Desktop/DIR600/FirmAE$ sudo ./run.sh -d dir645 ./firmwares/DIR645A1_FW102B08.bin
[*] ./firmwares/DIR645A1_FW102B08.bin emulation start!!!
[*] extract done!!!
[*] get architecture done!!!
[*] ./firmwares/DIR645A1_FW102B08.bin already succeed emulation!!!


[IID] 4
[MODE] debug
[+] Network reachable on 192.168.0.1!
[+] Web service on 192.168.0.1
[+] Run debug!
Creating TAP device tap4_0...
Set 'tap4_0' persistent and owned by uid 0
Initializing VLAN...
Bringing up TAP device...
Starting emulation of firmware... 192.168.0.1 true true 9.201040481 28.721388372
[*] firmware - DIR645A1_FW102B08
[*] IP - 192.168.0.1
[*] connecting to netcat (192.168.0.1:31337)
[+] netcat connected
------------------------------
|       FirmAE Debugger      |
------------------------------
1. connect to socat
2. connect to shell
3. tcpdump
4. run gdbserver
5. file transfer
6. exit
> 2
Trying 192.168.0.1...
Connected to 192.168.0.1.

boot
sudo ./run.sh -b dir645 ./firmwares/DIR645A1_FW102B08.bin

sudo ./part.sh -r dir645 ./firmwares/DIR645A1_FW102B08.bin
[*] ./firmwares/DIR645A1_FW102B08.bin emulation start!!!
/home/ubuntu/Desktop/DIR600/FirmAE/scratch/4
[*] extract done!!!


extractor.py 来将文件解包
timeout --preserve-status --signal SIGINT 300 ./sources/extractor/extractor.py -b dir645 -sql 127.0.0.1 -np -nk
./firmwares/DIR645A1_FW102B08.bin image

./scripts/util.py get_iid ./firmwares/DIR645A1_FW102B08.bin 127.0.0.1
```

```
ubuntu@ubuntu:~/Desktop/DIR600/FirmAE/scratch/4$ ls -al
total 92644
drwxrwxrwx  3 root root       4096 Dec 27 22:36 .
drwxrwxrwx 10 root root       4096 Feb 27 23:47 ..
-rwxrwxrwx  1 root root          7 Apr 10 18:57 architecture
-rwxrwxrwx  1 root root          7 Apr 10 18:57 brand
-rwxrwxrwx  1 root root         15 Dec 27 22:31 current_init
-rwxrwxrwx  1 root root        262 Dec 27 22:36 emulation.log
-rwxrwxrwx  1 root root      61449 Apr 10 18:57 fileList
-rwxrwxrwx  1 root root        153 Apr 10 18:57 fileType
drwxrwxrwx  2 root root       4096 Dec 27 22:31 image
-rwxrwxrwx  1 root root 1073741824 Apr  8 18:58 image.raw
-rwxrwxrwx  1 root root         55 Dec 27 22:31 init
-rwxrwxrwx  1 root root         12 Dec 27 22:36 ip
-rwxrwxrwx  1 root root         11 Dec 27 22:35 ip.0
-rwxrwxrwx  1 root root          1 Dec 27 22:35 ip_num
-rwxrwxrwx  1 root root          5 Dec 27 22:35 isDhcp
-rwxrwxrwx  1 root root          0 Apr 10 18:57 kernelCmd
-rwxrwxrwx  1 root root          0 Apr 10 18:57 kernelInit
-rwxrwxrwx  1 root root         94 Apr 10 18:57 kernelVersion
-rwxrwxrwx  1 root root       1969 Dec 27 22:31 makeImage.log
-rwxrwxrwx  1 root root        600 Dec 27 22:36 makeNetwork.log
-rwxrwxrwx  1 root root         18 Apr 10 18:57 name
-rwxrwxrwx  1 root root          5 Dec 27 22:36 ping
-rwxrwxrwx  1 root root    1445888 Apr  8 18:58 qemu.final.serial.log
-rwxrwxrwx  1 root root     344751 Dec 27 22:35 qemu.initial.serial.log
-rwxrwxrwx  1 root root          5 Apr  8 18:27 result
lrwxrwxrwx  1 root root          8 Dec 27 22:36 run_analyze.sh -> ./run.sh
lrwxrwxrwx  1 root root          8 Dec 27 22:36 run_boot.sh -> ./run.sh
lrwxrwxrwx  1 root root          8 Dec 27 22:36 run_debug.sh -> ./run.sh
-rwxrwxrwx  1 root root       3192 Dec 27 22:35 run.sh
-rwxrwxrwx  1 root root          0 Dec 27 22:31 tar2db.log
-rwxrwxrwx  1 root root         11 Apr 10 18:57 time_arch
-rwxrwxrwx  1 root root         11 Apr 10 18:57 time_extract
-rwxrwxrwx  1 root root         12 Dec 27 22:31 time_image
-rwxrwxrwx  1 root root         14 Dec 27 22:36 time_network
-rwxrwxrwx  1 root root         13 Dec 27 22:36 time_ping
-rwxrwxrwx  1 root root         12 Dec 27 22:31 time_tar
-rwxrwxrwx  1 root root         13 Dec 27 22:36 time_web
```

```
-rwxrwxrwx  1 root root          5 Dec 27 22:36 web
```

```
get brand
ubuntu@ubuntu:~/Desktop/DIR600/FirmAE$ ./scripts/util.py get_brand ./firmwares/DIR645A1_FW102B08.bin 127.0.0.1
dir645

./scripts/util.py
def get_brand(infile, psql_ip):
    md5 = io_md5(infile)
    q = "SELECT brand_id FROM image WHERE hash = '%s'" % md5
    brand_id = query_(q, psql_ip)

    if brand_id:
        q = "SELECT name FROM brand WHERE id = '%s'" % brand_id
        brand = query_(q, psql_ip)
        if brand:
            return brand[0]
        else:
            return ""
    else:
        return ""
```

连接本地数据库

```
def check_connection(psql_ip):
    try:
        dbh = psycopg2.connect(database="firmware",
                               user="firmadyne",
                               password="firmadyne",
                               host=psql_ip)
        dbh.close()
        return 0
    except:
        return 1
```

```
ubuntu@ubuntu:~/Desktop/DIR600/FirmAE/images$ ls
1.kernel  1.tar.gz  2.kernel  2.tar.gz  3.kernel  3.tar.gz  4.kernel  4.tar.gz  5.kernel  5.tar.gz  6.kernel  7.kernel  7.tar.gz  8.kernel  8.tar.gz

./scripts/getArch.py ./images/4.tar.gz 127.0.0.1
mipsel
```

emulation

```
./scripts/tar2db.py -i 4 -f ./images/4.tar.gz -h 127.0.0.1

把文件信息和数据库信息对应
def insertObjectToImage(iid, files2oids, links, cur):
    query = """INSERT INTO object_to_image (iid, oid, filename, regular_file, uid, gid, permissions) VALUES (%(iid)s, %(oid)s, %
(filename)s, %(regular_file)s, %(uid)s, %(gid)s, %(mode)s)"""
```

logs

```
FIRMWARE = ./firmwares/DIR645A1_FW102B08.bin
run_emulation
[*] ./firmwares/DIR645A1_FW102B08.bin emulation start!!!
INFILE = ./firmwares/DIR645A1_FW102B08.bin
BRAND = dir645
FILENAME = DIR645A1_FW102B08
PSQL_IP = 127.0.0.1
WORK_DIR = /home/ubuntu/Desktop/DIR600/FirmAE/scratch/4
/home/ubuntu/Desktop/DIR600/FirmAE/scratch/4
FILENAME = DIR645A1_FW102B08
BRAND = dir645
[*] extract done!!!
t_start = {1649812871.369866645}
t_end = {1649812871.704626636}
time_extract = .334759991
WORK_DIR = /home/ubuntu/Desktop/DIR600/FirmAE/scratch/4
time_extract = .334759991
ARCH = mipsel
4
[*] get architecture done!!!
time_arch = .325423370
time_tar = .348621405
makeImage.sh
IID = 4
ARCH = mipsel
4
FILENAME = DIR645A1_FW102B08
mke2fs 1.44.1 (24-Mar-2018)
e2fsck 1.44.1 (24-Mar-2018)
time_image = 6.231062141
[*] infer network start!!!
FIRMAE_NET = true
```

```
Line185
```

```
./scripts/makeImage.sh $IID $ARCH $FILENAME 2>&1 > ${WORK_DIR}/makeImage.log

makeImage.sh 学习

./scripts/mytest.sh 4 mipsel DIR645A1_FW102B08
Error: This script requires root privileges!

sudo ./scripts/mytest.sh 4 mipsel DIR645A1_FW102B08
----Running----
WORK_DIR = /home/ubuntu/Desktop/DIR600/FirmAE/scripts/scratch/4
IMAGE = /home/ubuntu/Desktop/DIR600/FirmAE/scripts/scratch/4/image.raw
IMAGE_DIR = /home/ubuntu/Desktop/DIR600/FirmAE/scripts/scratch/4/image/


echo -e "o\nn\np\n1\n\n\nw"
o
n
p
1


w

/sbin/fdisk /home/ubuntu/Desktop/DIR600/FirmAE/scratch/4/image.raw
Welcome to fdisk (util-linux 2.31.1).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.
Command (m for help): o
Created a new DOS disklabel with disk identifier 0x9b9151b3.
Command (m for help): n
Partition type
   p   primary (0 primary, 0 extended, 4 free)
   e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-2097151, default 2048):
Last sector, +sectors or +size{K,M,G,T,P} (2048-2097151, default 2097151):
Created a new partition 1 of type 'Linux' and of size 1023 MiB.
Command (m for help): w
The partition table has been altered.
Syncing disks.
```

```
        # ================================
        # make qemu image
        # ================================
        t_start="$(date -u +%s.%N)"
        ./scripts/tar2db.py -i $IID -f ./images/$IID.tar.gz -h $PSQL_IP \
            2>&1 > ${WORK_DIR}/tar2db.log
```

make qemu_image

```
        # ================================
        # make qemu image
        # ================================
        t_start="$(date -u +%s.%N)"
        ./scripts/tar2db.py -i $IID -f ./images/$IID.tar.gz -h $PSQL_IP \
            2>&1 > ${WORK_DIR}/tar2db.log
        t_end="$(date -u +%s.%N)"
        time_tar="$(bc <<<"$t_end-$t_start")"
        echo $time_tar > ${WORK_DIR}/time_tar

sudo ./scripts/tar2db.py -i 4 -f ./images/4.tar.gz -h 127.0.0.1
```

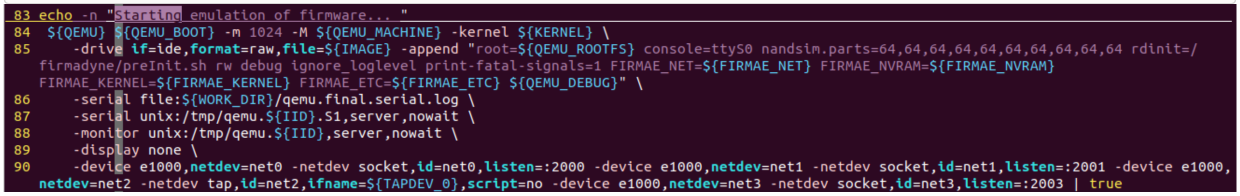
infer network interface

```
        t_start="$(date -u +%s.%N)"
        ./scripts/makeImage.sh $IID $ARCH $FILENAME \
            2>&1 > ${WORK_DIR}/makeImage.log
        t_end="$(date -u +%s.%N)"

sudo ./scripts/makeImage.sh 4 mipsel DIR645A1_FW102B08
cat /home/ubuntu/Desktop/DIR600/FirmAE/scratch/4/makeImage.log
```

```
        # ================================
        # just run mode
        # ================================
        check_network ${IP} false &
        ${WORK_DIR}/run.sh

/home/ubuntu/Desktop/DIR600/FirmAE/scratch/4/run.sh
cat /home/ubuntu/Desktop/DIR600/FirmAE/scratch/4/run.sh
```



```
echo -n "Starting emulation of firmware... "
 ${QEMU} ${QEMU_BOOT} -m 1024 -M ${QEMU_MACHINE} -kernel ${KERNEL} \
    -drive if=ide,format=raw,file=${IMAGE} -append "root=${QEMU_ROOTFS} console=ttyS0 nandsim.parts=64,64,64,64,64,64,64,64,64,64 rdinit=/firmadyne/preInit.sh rw debug ignore_loglevel print-fatal-signals=1 FIRMAE_NET=${FIRMAE_NET} FIRMAE_NVRAM=${FIRMAE_NVRAM} FIRMAE_KERNEL=${FIRMAE_KERNEL} FIRMAE_ETC=${FIRMAE_ETC} ${QEMU_DEBUG}" \
    -serial file:${WORK_DIR}/qemu.final.serial.log \
    -serial unix:/tmp/qemu.${IID}.S1,server,nowait \
    -monitor unix:/tmp/qemu.${IID},server,nowait \
    -display none \
    -device e1000,netdev=net0 -netdev socket,id=net0,listen=:2000 -device e1000,netdev=net1 -netdev socket,id=net1,listen=:2001 -device e1000,netdev=net2 -netdev tap,id=net2,ifname=${TAPDEV_0},script=no -device e1000,netdev=net3 -netdev socket,id=net3,listen=:2003 | true
```

boot mode

```
    elif [ ${OPTION} = "boot" ]; then
        # ================================
        # boot debug mode
        # ================================
        BOOT_KERNEL_PATH=`get_boot_kernel ${ARCH} true`
        BOOT_KERNEL=./binaries/`basename ${BOOT_KERNEL_PATH}`
        echo -e "[\033[32m+\033[0m] Connect with gdb-multiarch -q ${BOOT_KERNEL} -ex='target remote:1234'"
        ${WORK_DIR}/run_boot.sh
```

linux 管理设备文件

```
https://linux.cn/article-8099-1.html
```

```
https://www.cnblogs.com/lanchang/p/8150249.html
/dev这个目录包含了所有Linux系统中使用的外部设备
```