

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего
профессионального образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И
РАДИОЭЛЕКТРОНИКИ» (ТУСУР)
Кафедра комплексной информационной безопасности электронно-вычислительных систем
(КИБЭВС)

УТВЕРЖДАЮ

заведующий каф. КИБЭВС

_____ А.А. Шелупанов

«_____» _____ 2015г.

ПАССИВНЫЙ ПЕРЕХВАТ ПАКЕТОВ ПО БЕСПРОВОДНОЙ СЕТИ ИНТЕРНЕТ (WI-FI)

Курсовая работа по дисциплине «Безопасность сетей ЭВМ»

Пояснительная записка

Выполнила:

студентка гр. 722

_____ М.В. Мейта

«_____» _____ 2015г.

Научный руководитель:

аспирант каф. КИБЭВС

_____ А.К. Новохрестов

«_____» _____ 2015г.

РЕФЕРАТ

Курсовая работа содержит 18 страниц, 21 рисунок, 0 таблиц, 2 источника, 0 приложение.

RASPBERRY PI, UBUNTU, WI-FI, TCPDUMP, PCAP, RASPBIAN, WIRESHARK, BASH, СНИФФЕР, СЕТЕВОЙ ТРАФИК.

Цель работы — разработать и настроить систему пассивного перехвата пакетов по беспроводной сети Интернет (Wi-Fi) в научно-образовательных целях.

Проект выполнен с использованием следующих программных и аппаратных средств:

- ОС Linux Ubuntu 15.04;
- ОС Linux Raspbian Jessie Light 4.1;
- Wi-Fi-адаптер TP-Link TL-WN722NC;
- tcpdump — консольная утилита Unix для перехвата и анализа сетевого трафика;
- Wireshark — программа-анализатор сетевого трафика с графическим пользовательским интерфейсом.

Пояснительная записка выполнена при помощи системы компьютерной вёрстки L^AT_EX.

Содержание

| | |
|--|----|
| Введение | 4 |
| 1 Используемые программные и аппаратные средства, обоснование выбора и их описание | 5 |
| 1.1 Raspberry Pi + TPLink | 5 |
| 1.2 Ubuntu | 5 |
| 1.3 Raspbian | 5 |
| 1.4 tcpdump | 5 |
| 1.5 wireshark | 5 |
| 2 Проектирование и настройка пакетного sniffера | 6 |
| 2.1 Установка ОС Raspbian | 6 |
| 2.2 настройка сети (Ethernet) | 6 |
| 2.3 Установка ssh-соединения | 11 |
| 2.4 Установка драйвера TP-Link | 12 |
| 2.5 Настройка режима monitor mode | 13 |
| 2.6 tcpdump | 16 |
| 2.7 wireshark | 16 |
| Заключение | 17 |
| Список использованных источников | 18 |

Введение

Беспроводные сети небезопасны, особенно открытые. Но и зашифрованные не являются на
100

тут надо сочинение на эту тему

склепать сниффер

В качестве задания на курсовую работу была поставлена задача разработать пассивный перехватчик пакетов на базе Raspberry Pi. ????

Задачи: установить настроить сниффить анализировать

1 Используемые программные и аппаратные средства, обоснование выбора и их описание

1.1 Raspberry Pi + TPLink

1.2 Ubuntu

1.3 Raspbian

1.4 tcpdump

1.5 wireshark

2 Проектирование и настройка пакетного sniffера

2.1 Установка ОС Raspbian

Для установки операционной системы Raspbian на Raspberry Pi необходимо перейти на страницу загрузок на официальном сайте [1] и скачать необходимый образ ОС (рис. 2.1), затем установить загруженный образ на SD-карту, которая впоследствии будет подключена к Raspberry Pi и с которой непосредственно будет загружаться система.



Рисунок 2.1 – Официальная страница загрузок ОС Raspbian

Инструкцию по установке образа системы на SD-карту можно найти, перейдя по ссылке [2].

После распаковки загруженного архива с образом системы, необходимо вставить SD-карту в слот и выполнить следующие команды:

```
$ df -h    # увидеть все примонтированные устройства
$ umount /dev/<ИМЯ_УСТРОЙСТВА>    # отмонтировать SD-карту
$ dd bs=4M if=2015-11-21-raspbian-jessie.img of=/dev/sdd    # записать образ
$ sync
```

Далее достаточно извлечь SD-карту и установить ее в соответствующий разъем Raspberry Pi.

2.2 настройка сети (Ethernet)

Все остальные настройки оставить по умолчанию.

Изменение Проводное соединение 1

Название соединения: Проводное соединение 1

Общий Ethernet Защита 802.1x DCB Параметры IPv4 Параметры IPv6

Способ настройки: Предоставить сеть другим компьютерам

Адреса

| Адрес | Маска сети | Шлюз |
|-------|------------|------|
| | | |

Добавить
Удалить

Серверы DNS:

Поисковый домен:

ID клиента DHCP:

☒ Требовать адресацию IPv4 для этого соединения

Маршруты...

Отменить Сохранить

Рисунок 2.2 – Параметры IPv4 для проводного соединения

Изменение Проводное соединение 1

Название соединения: Проводное соединение 1

Общий Ethernet Защита 802.1x DCB Параметры IPv4 Параметры IPv6

Способ настройки: Игнорировать

Адреса

| Адрес | Префикс | Шлюз |
|-------|---------|------|
| | | |

Добавить
Удалить

Серверы DNS:

Поисковый домен:

IPv6 privacy extensions: Выключено

☐ Требовать адресацию IPv6 для этого соединения

Маршруты...

Отменить Сохранить

Рисунок 2.3 – Параметры IPv6 для проводного соединения

Изменение ZyX

Название соединения: ZyX

Общий Wi-Fi Защита Wi-Fi **Параметры IPv4** Параметры IPv6

Способ настройки: Автоматически (DHCP)

Адреса

| Адрес | Маска сети | Шлюз |
|-------|------------|------|
| | | |

Добавить
Удалить

Дополнительные серверы DNS:

Дополнительные поисковые домены:

ID клиента DHCP:

☒ Требовать адресацию IPv4 для этого соединения

Маршруты...

Отменить Сохранить

Рисунок 2.4 – Параметры IPv4 для беспроводного соединения

Изменение ZyX

Название соединения: ZyX

Общий Wi-Fi Защита Wi-Fi Параметры IPv4 **Параметры IPv6**

Способ настройки: Игнорировать

Адреса

| Адрес | Префикс | Шлюз |
|-------|---------|------|
| | | |

Добавить
Удалить

Серверы DNS:

Поисковый домен:

IPv6 privacy extensions: Выключено

☐ Требовать адресацию IPv6 для этого соединения

Маршруты...

Отменить Сохранить

Рисунок 2.5 – Параметры IPv6 для беспроводного соединения

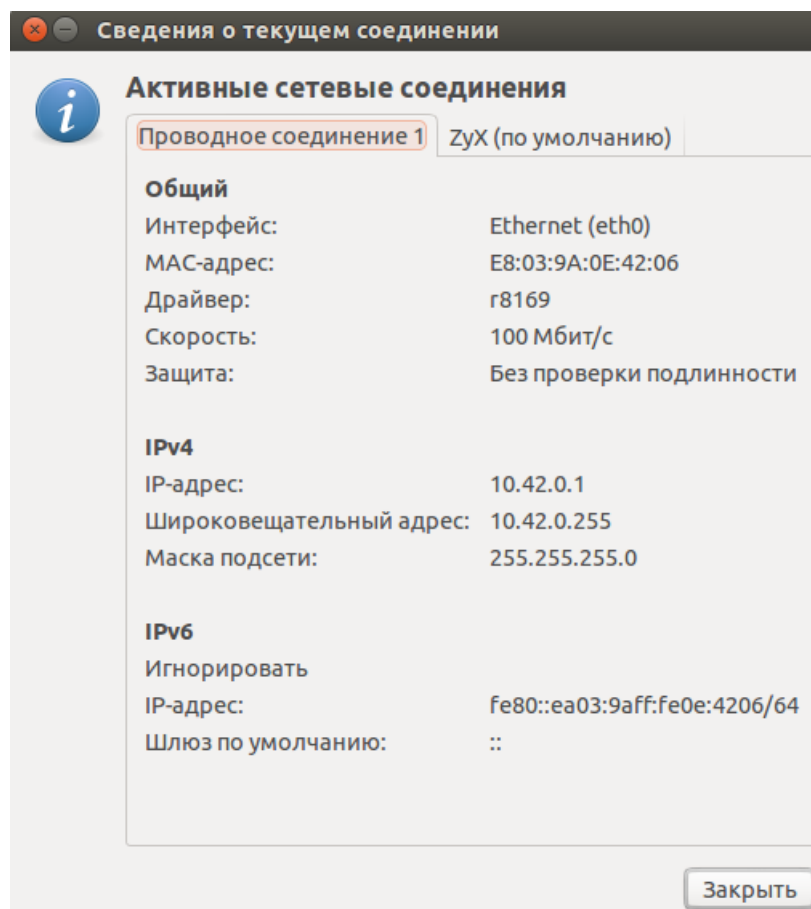


Рисунок 2.6 – Сведения о проводном соединении

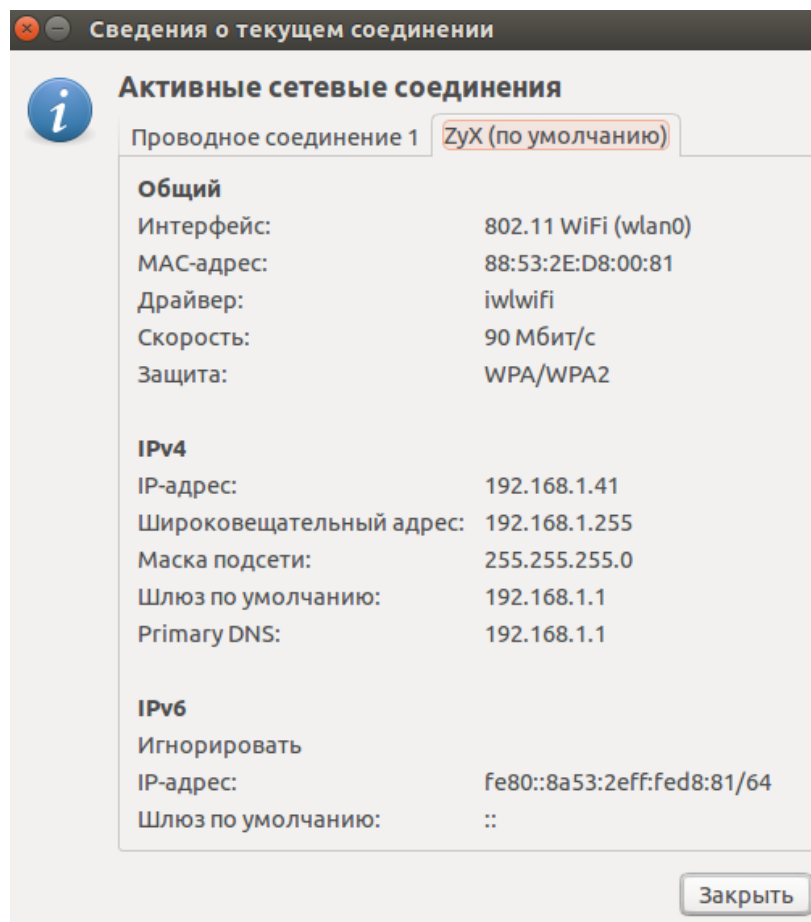


Рисунок 2.7 – Сведения о беспроводном соединении

2.3 Установка ssh-соединения

arp -vn:

```
marina@marina-530U3BI-530U4BI-530U4BH:~$ arp -vn
Адрес HW-тип HW-адрес Флаги Маска Интерфейс
192.168.1.1 ether c8:6c:87:40:4f:b3 C
10.42.0.67 ether b8:27:eb:5f:e4:39 C
Записей: 2 на Пропущено: 0 Найдено: 2
marina@marina-530U3BI-530U4BI-530U4BH:~$
```

Рисунок 2.8 – Параметры IPv4 для проводного соединения

connect ssh:

```
marina@marina-530U3BI-530U4BI-530U4BH:~$ ssh pi@10.42.0.67
ssh: connect to host 10.42.0.67 port 22: Connection refused
marina@marina-530U3BI-530U4BI-530U4BH:~$ sudo ssh pi@10.42.0.67
The authenticity of host '10.42.0.67 (10.42.0.67)' can't be established.
ECDSA key fingerprint is 36:b0:32:77:0b:4f:bf:d8:2b:ee:cc:d0:4f:c0:19:93.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.42.0.67' (ECDSA) to the list of known hosts.
pi@10.42.0.67's password:
Linux raspberrypi 4.1.13+ #826 PREEMPT Fri Nov 13 20:13:22 GMT 2015 armv6l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jan 3 14:12:43 2016 from 10.42.0.1
pi@raspberrypi ~ $ ls -la
total 1644
drwxr-xr-x 15 pi pi 4096 Jan 3 15:17 .
drwxr-xr-x 3 root root 4096 Jan 1 1970 ..
```

Рисунок 2.9 – Параметры IPv4 для проводного соединения

все,мы в системе

2.4 Установка драйвера TP-Link

Узнаем версию системы и проверяем устройства USB

```
pi@raspberrypi / $ uname -a
Linux raspberrypi 4.1.13+ #826 PREEMPT Fri Nov 13 20:13:22 GMT 2015 armv6l GNU/Linux
```

Рисунок 2.10 – Узнаем версию системы

```
pi@raspberrypi / $ lsusb
Bus 001 Device 002: ID 0424:9512 Standard Microsystems Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 003: ID 0424:ec00 Standard Microsystems Corp.
Bus 001 Device 004: ID 0bda:8179 Realtek Semiconductor Corp.
```

Рисунок 2.11 – проверяем устройства USB

тут ссылка на то, как устанавливать драйвер согласно версии системы
<https://www.raspberrypi.org/forums/viewtopic.php?p=462982>

Скачиваем драйвер:

```
pi@raspberrypi ~ $ wget https://dl.dropboxusercontent.com/u/80256631/8188eu-20151113.tar.gz
--2016-01-03 16:26:02-- https://dl.dropboxusercontent.com/u/80256631/8188eu-20151113.tar.gz
Resolving dl.dropboxusercontent.com (dl.dropboxusercontent.com)... 199.47.217.69
Connecting to dl.dropboxusercontent.com (dl.dropboxusercontent.com)|199.47.217.69|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 416724 (407K) [application/octet-stream]
Saving to: '8188eu-20151113.tar.gz'
100%[=====]
2016-01-03 16:26:11 (221 KB/s) - '8188eu-20151113.tar.gz' saved [416724/416724]
```

Рисунок 2.12 – Скачиваем драйвер

установим и ребутнемся

```
pi@raspberrypi ~ $ tar -zxvf 8188eu-20151113.tar.gz
8188eu.ko
8188eu.conf
install.sh
pi@raspberrypi ~ $ ./install.sh
sudo cp 8188eu.conf /etc/modprobe.d/.
sudo install -p -m 644 8188eu.ko /lib/modules/4.1.13+/kernel/drivers/net/wireless
sudo depmod 4.1.13+
Reboot to run the driver.
If you have already configured your wifi it should start up and connect to your wireless network.
If you have not configured your wifi you will need to do that to enable the wifi.
pi@raspberrypi ~ $ sudo reboot
```

Рисунок 2.13 – Устанавливаем драйвер

Проверим командой ifconfig

```

pi@raspberrypi ~ $ ifconfig
eth0: Link encap:Ethernet HWaddr b8:27:eb:5f:e4:39
      inet addr:10.42.0.67 Bcast:10.42.0.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
      RX packets:169 errors:0 dropped:0 overruns:0 frame:0
      TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:19389 (18.9 KiB) TX bytes:21375 (20.8 KiB)

lo:    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      UP LOOPBACK RUNNING  MTU:65536 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

wlan0: Link encap:Ethernet HWaddr c0:4a:00:25:6e:40
      UP BROADCAST MULTICAST  MTU:1500 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

```

Рисунок 2.14 – ifconfig

2.5 Настройка режима monitor mode

Для начала попробуем установить Wi-Fi соединение и подсоединиться к RPi без Ethernet-соединения.

```

pi@raspberrypi ~ $ sudo iwlist wlan0 scan | grep ESSID
storage
ESSID:"ZyX"
ESSID:"Prohorova "
tusu
ESSID:"SSA_WIFI"
pi@raspberrypi ~ $

```

Рисунок 2.15 – просканировали сеть

```

pi@raspberrypi ~ $ nano /etc/network/interfaces

```

Рисунок 2.16 – путь к config

```

auto lo
iface lo inet loopback
iface eth0 inet dhcp

allow-hotplug wlan0
auto wlan0

iface wlan0 inet dhcp
wpa-ssid "NETWORK NAME"
wpa-psk "PASSWORD"

```

Рисунок 2.17 – config

```

pi@raspberrypi ~ $ iwconfig
wlan0 unassociated Nickname:"<WIFI@REALTEK>"
      Mode:Managed Frequency=2.412 GHz Access Point: Not-Associated
      Sensitivity:0/0
      Retry:off RTS thr:off Fragment thr:off
      Power Management:off
      Link Quality=0 Signal level:0 Noise level:0
      Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
      Tx excessive retries:0 Invalid misc:0 Missed beacon:0

lo no wireless extensions.

eth0 no wireless extensions.

```

Рисунок 2.18 – config

```

pi@raspberrypi ~$ iwconfig
wlan0 IEEE 802.11bgn ESSID:"ZyX" Nickname:"<WIFI@REALTEK>"
      Mode:Managed Frequency=2.412 GHz Access Point: C8:6C:87:40:4F:B3
      Bit Rate:150 Mb/s Sensitivity:0/0
      Retry:off RTS thr:off Fragment thr:off
      Power Management:off
      Link Quality=100/100 Signal level=59/100 Noise level=0/100
      Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
      Tx excessive retries:0 Invalid misc:0 Missed beacon:0
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

lo no wireless extensions.

lo Link encap:Local Loopback

eth0 no wireless extensions.

```

Рисунок 2.19 – config

подняли сетку в режиме Managed

тут можно рассказать про разные режимы адаптеров (их 6) и про мониторинг режим. Устройство может в определенный момент времени находиться только в одном режиме.

Настроим адаптер в режим приема пакетов. Для этого необходимо ввести команду `sudo iwconfig wlan0 mode monitor` При попытке ввести данную команду видим следующее сообщение:

```

pi@raspberrypi ~ $ sudo iwconfig wlan0 mode monitor
Error for wireless request "Set Mode" (8B06) :
  SET failed on device wlan0 ; Device or resource busy.

```

Рисунок 2.20 – ресурс занят

это связано с тем, что в системе работает `network interface plugging daemon` (ссылка на raspberrypi.org) необходимо его отключить для того, чтобы перевести устройство в другой режим работы

напишем небольшой `bash`-скрипт, который будет переводить адаптер в режим перехвата пакетов и содержать следующие команды: `sudo service ifplugd stop` останавливаем работу демона `sudo ifconfig wlan0 down` отключаем wi-fi соединение `sudo iwconfig wlan0 mode monitor` включаем прослушивающий режим `sudo ifconfig wlan0 up` включаем wi-fi соединение `sudo service ifplugd start` запускаем демона `iwconfig` проверяем настройки

результат работы скрипта приведен на рисунке ... Устройство теперь в режиме перехвата пакетов. Данный скрипт необходимо запускать снова при перезапуске системы, поскольку по умолчанию устройство переходит в режим `managed`

```

pi@raspberrypi ~/sniff $ cat start_monitoring.sh
#!/bin/bash

sudo service ifplugd stop
sudo ifconfig wlan0 down
sudo iwconfig wlan0 mode monitor
sudo ifconfig wlan0 up
iwconfig
pi@raspberrypi ~/sniff $ ./start_monitoring.sh
[ ok ] Network Interface Plugging Daemon...stop eth0...stop wlan0...done.
wlan0 IEEE 802.11bgn Mode:Monitor Frequency:2.412 GHz Tx-Power=20 dBm
        Retry short limit:7 Retry RTS thr:off Fragment thr:off
        Power Management:off
lo Обзоры wireless extensions.
eth0 storage no wireless extensions.
pi@raspberrypi ~/sniff $

```

Рисунок 2.21 – результат выполнения скрипта

2.6 tcpdump

2.7 wireshark

Заключение

Список использованных источников

- 1 Raspbian [Электронный ресурс]. URL: <https://www.raspberrypi.org/downloads/raspbian/> (дата обращения: 25.09.2015).
- 2 Installing Operating System Images on Linux [Электронный ресурс]. URL: <https://www.raspberrypi.org/documentation/installation/installing-images/README.md> (дата обращения: 25.09.2015).