Статья Установка Kali Linux на Raspberry Pi 3 Model B+

yarr · 15.09.2018 · alfa 036 | alfa 036ach | alfa 036n | alfa 036nha | kali linux | nexmon | raspberry pi | raspberry pi 3 | rtl sdr | установка kali linux

yarr
Red Team
05.10.2017 305 576

15.09.2018 #1

В последнее время на форуме стали появляться вопросы про Raspberry Pi 3 и установку на него Kali Linux. На форуме уже имеется подобная статья, но я решил вынести тему в отдельную в связи с наличием альтернативного образа и варианта для установки системы.

Если Вы хотели купить себе компактный одноплатный компьютер для пентеста, но не можете выбрать, то советую взять Raspberry Pi 3 Model B+, которая вышла в марте 2018 года. На сегодняшний эта плата является наиболее мощным вариантом из линейки Raspberry Pi.

Спойлер

Новая модель работает быстрее за счет разогнанного из коробки процессора Broadcom BCM2837 (64-бит, 4 ядра Cortex-A53, работает на частоте 1.4 Ггц). Тем не менее сильно греться новая модель не будет за счет улучшенной целостности питания и теплоотводу, так же желательно поставить на CPU и чипсет USB/Ethernet алюминиевые радиаторы.

Обновился радиочастотный модуль, над которыми теперь установлен металлический экран (CYW43455 от Cypress - двухдиапазонный беспроводной модуль на 2.4 и 5 ГГц и Bluetooth 4.2 / BLE). Новый контроллер Ethernet LAN7515 позволяет работать со скоростью до 300 Мбит/с.

Спойлер

Само собой лучше покупать не голую плату, а еще набор радиаторов (два для данной модели), корпус (лучше металлический), SD карту (от 16 ГБ Class 10 - скорость записи не менее 10 МБ/с).

Одноплатный компьютер удобен тем, что его можно использовать как отдельную независимую платформу для обучению тестирования на проникновения с помощью Kali Linux. Почему именно Raspberry Pi? Хорошая поддержка сообщества. Это мы увидим ниже, когда перейдем к установке Kali на устройство. Естественно использовать Kali не обязательно, есть много других ОС, которые заточены под использование на одноплатниках Raspberry Pi.

Как я выше упомянул у модели B+ есть новый модуль для беспроводной связи, поддерживающий Wi-Fi на 5 ГГц. Именно для этого модуля разработчики из Германии (Secure Mobile Networking Lab), которые занимаются широко известным в узких кругах проектом Nexmon создали драйвер, позволяющий перевести встроенный в малину чипсет BCM43455c0 в режим монитора. Но это еще не все! Этот чип указан еще в одном проекте от тех же разработчиков - Nexmon SDR. Я думаю, что объяснять, что такое SDR не нужно. Малина так же поддерживает работу с RTL-SDR с помощью программы rpitx.

Если использовать Raspberry Pi 3 B+ для аудита безопасности беспроводных сетей, то понадобится один или два внешних адаптера. Я бы рекомендовал использовать Alfa 036 NHA, Alfa 036 ACH или Alfa 036 NH.

Перейдем непосредственно к установке. Инструкцию по установке я сделал для Windows.

1. Для начала необходимо установить пакет некоторых программ

Спойлер

2. Теперь вернемся к тому, что я сказал ранее про поддержку сообществом.

Благодаря ядру от Re4son (сборки на его основе работали с Raspberry Pi 3 Model B+ еще до того, как официальный релиз был доступен на Offensive Security). улучшенные спецификация и производительность сетевого оборудования могут использоваться с инструментами тестирования на проникновение, которые предлагает Kali Linux. В это ядро так же входят:

- поддержка Nexmon
- исправление проблем с работой bluetooth
- нативная поддержка оптимизация компиляции модулей
- поддержка подключения по SSH через USB (с помощью переходника USB/Ethernet)
- имеет поддержку работы с tft дисплеями и скрипт, позволяющий настроить автоматический вход в систему
- интегрирована поддержка драйвера для перевода адаптера TL-WN722N v2 в режим монитора (чипсет RTL8188EU).
- интегрирована поддержка драйвера для адаптера Alfa 036 ACH (монитор, инъекция и т.д.).
- полный список твиков, а так же подробные инструкции (настройка дисплеев и т.д. можно найти на сайте Re4son. Там имеется форум и достаточно подробные инструкции.

На сайте есть так же специальная сборка с небольшим комплектом программ и предустановленным ядром от Re4son.

Скачиваем образ. Так же скачаем новое ядро (в готовой сборке стоит 4.9, новое версии 4.14).

Спойлер

4. Следующие пункты опциональны, в зависимости от того, если ли в наличии HDMI кабель и монитор/телевизор с поддержкой HDMI.

5. В случае, если в наличии есть HDMI кабель и монитор/телевизор с поддержкой HDMI, то включаем и настраиваем наш монитор/телевизор, цепляем к малинке кабель Ethernet (идущий к роутеру), HDMI и в конце подключаем питание. Если HDMI не взлетел, то вырубаем питание и пробуем снова.

Теперь, когда система загружена и подключена к сети нам понадобится проводная клавиатура и мышь. Для работы через монитор мышь понадобится в любом случае, от клавиатуры можно отказаться в пользу виртуальной, однако для первичной настройки необходима проводная. Если нету клавиатуры и/или мыши, то переходим к следующим пунктам, то есть подключаемся по SSH. Если они есть, то входим с логином root и паролем toor.

6. В случае, если в наличии нет монитора с HDMI и/или проводной клавиатуры с мышью, то будем подключаться через SSH. Для этого необходимо подсоединить Ethernet кабель от роутера к малинке и подключить к ней питание.

Нам потребуется узнать ip адрес малинки, сделать это можно разными путями, один из них – установить на ПК программу Advanced IP Scanner. Стоит помнить, что ваша сеть может быть закрыта от подобного сканирования firewall, и тогда надо будет временно отключить защиту в роутере. Так же данная программа иногда не очищяет кеш сканирования, воспользуйтесь другим способом узнать ip малины, если есть подозрение, что Вы нем ожете получить правильный ip для подключения по SSH.

Когда увидим наш kali-pi, то запоминаем её ip и заходим в Putty, где прописываем ip (подключение по SSH и порт 22 выбираются по умолчанию). В процессе подключения появится окно с просьбой подтвердить подключение, нажимаем «Да». Имя пользователя – root, пароль – toor.

Спойлер

7. Авторизовавшись с помощью пункта 5 или 6 необходимо будет расширить наш образ на все дисковое пространство.

Код:

```
sudo fdisk /dev/mmcblk0

Command (m for help): p

Device Boot Start End Sectors Size Id Type
/dev/mmcblk0p1 1 125000 125000 61M c W95 FAT32 (LBA)
/dev/mmcblk0p2 125001 15523839 15398839 7.4G 83 Linux
```

Обратим внимание на значение 125001, у Вас оно может быть другое.

Код:

```
Select (default p): p
Partition number (2-4, default 2): 2
First sector (125001-31116287, default 126976): 125001
Last sector, +sectors or +size{K,M,G,T,P} (125001-31116287, default 31116287):
Do you want to remove the signature? [Y]es/[N]o: N
Command (m for help): w
```

Перезагрузите систему.

Код:

```
sudo resize2fs /dev/mmcblk0p2
```

8. Меняем пароль учетной записи на свой:

Код:

```
passwd
```

Удаляем встроенную учетную запись pi:

Код:

```
deluser --remove-all-files pi
```

9. Изменим ключи ssh по умолчанию:

Код:

```
cd /etc/ssh/
dpkg-reconfigure openssh-server
update-rc.d -f ssh remove
update-rc.d -f ssh defaults
service ssh restart
update-rc.d -f ssh enable 2 3 4 5
```

10. Установим vnc-server:

Код:

```
apt purge tightvncserver -y
&& wget https://www.realvnc.com/download/file/vnc.files/VNC-Server-6.3.1-Linux-ARM.deb
&& sudo dpkg -i VNC-Server-6.3.1-Linux-ARM.deb
&& rm VNC-Server*
```

Запустим vncserver:

Код:

```
vncserver :1 -geometry 1920x1080 -depth 24 -dpi 96
```

Теперь подключимся к нему с помощью установленного на ПК VNC Viever:

Код:

```
cd /usr/local/src
&& wget -O re4son-kernel_current.tar.xz https://re4son-kernel.com/download/re4son-kernel-current/
&& tar -xJf re4son-kernel_current.tar.xz
&& rm -rf re4son-kernel_current.tar.xz
&& cd re4son-kernel_4.14.50-20180721
&& ./install.sh
```

На все вопросы отвечаем «Y»

Теперь поставим более новое ядро 4.14 на замену 4.9. Хочу отметить, что команду apt-get dist-upgrade выполнять не следует, т.к. это кастомное ядро, обновления которого нужно брать с сайта.

12. Настроим время и дату:

Код:

```
dpkg-reconfigure tzdata
```

13. Добавим vnc sever в автозагрузку (через настройки автозагрузки xfce):

Перейдем в Applications => Sessions and Startup => ищем меню автозагрузки и добавляем нашу программу:

Спойлер

14. Настроим автозагрузку xfce, поддержку tft экранов и беспроводных модулей:

Код:

```
/usr/local/src/re4son-kernel_4.14.50-20180721/re4son-pi-tft-setup -a root
```

На все предложения отвечаем "y".

В итоге получим автовстарт vnc после загрузки малины, рекомендую добавить в малину пароль от wifi чтобы подключаться к ней без кабеля.

15. Установим виртуальную клавиатуру xvkbd и leafpad.

Код:

```
apt-get install xvkbd  leafpad -y
```

Виртуальную клавиатуру я так же советую поставить в автозагрузку, чтобы подключать к монитору только мышку.

16. Проверяем работу Bluetooth:

```
default-agent
scan on
```

Для подключения используйте

Код:

```
pair XX:XX:XX:XX:XX:XX
```

17. Для перевода встроенного адаптера в режим монитора используйте команду:

Код:

```
iw phy phy0 interface add mon0 type monitor
```

18. Для русификации системы редактируем locale:

Код:

```
nano /etc/default/locale
```

изменяем на:

Код:

```
LANG="ru_RU.UTF-8"
LC_ALL="ru_RU.UTF-8"
```

19. В самом начале инструкции была установленая программа Win32DiskImager, она понадобится для создания бекапа. Он будет занимать столько места, сколько размечено на флешке под систему (в моем случае это 32 ГБ).
Вставьте ридер с micro SD в разъем ПК, запустите программу, укажите путь для сохранения бекапа и нажмите "Read".

Спойлер

Умоляю, помогите уйти с Kali Linux ©

Valera252, id2746, Vander и еще 17

Жалоба | Нравится | + Цитата | Ответ

U

Underwood

15.09.2018 #2

Отличная статья!