# RASPBERRY: la portable penetration testing machine

Indice:

# 1) Introduzione

## Perché nasce questa guida?

Questo piccolo manuale nasce poiché in molti, dopo l'acquisto di un Raspberry, vogliono cimentarsi nel vasto mondo del penetrationtesting con questo piccolo dispositivo, tanto piccolo quanto utile, senza però sapere né da dove partire, né tantomeno quali strumenti utilizzare. Decidono così di installare Kali piuttosto che Parrot, occupando numerosa memoria sul piccolo Pi, e iniziano a incontrare diverse difficoltà.
Questa guida nasce quindi con l'intento di ovviare a tutte queste piccole difficoltà, rimpiazzando Kali con il nativo OS Raspbian e personalizzandolo nei tools e quantaltro.

## Cosa si può fare dopo aver installato tutto il necessario?

Beh, le cose che si possono fare sono davvero un infinità!
Si potranno testare applicativi web, generare exploit e payload, creare dizionari ed effettuare attacchi Brute-Force piuttosto che attacchi MITM o di ingegneria sociale (ovviamente il tutto nei limiti delle prestazioni di un Raspberry, non aspettatevi gli stessi risultati in fatto di tempo ecc rispetto a un PC!).

## Lo consiglieresti a un neofito dell'informatica?

Sì, anche perché la pratica rende perfetti, nessuno nasce che sa già le cose. Un po' di esercizio, abbinato alle giuste dosi di teoria e studio, può fare in modo che anche un utente inesperto possa approcciarsi a questo mondo senza averne le piene competenze. Poi per chiunque disponga di un Pi, sicuramente potrebbe essere interessante vederne anche questo aspetto, quindi in un caso o nell'altro, può sempre servire ed essere interessante oltre che utile.

# 2) Requisiti

Per l'installazione e la configurazione del Pi avremo bisogno di un paio di software (SW) e dell'hardware (HW) necessario.
Cominciamo dall'HW.Ciò che ovviamente ci servirà è:

- **Raspberry** (ma dai?!?)
- **SD** di almeno **8GB** (meglio se superiore) preferibilmente di **classe10**
- **Monitoresterno** (può essere il nostro cellulare, uno schermo LCD o il nostro TV in base alle esigenze)
- **Tastiera** e **mouse esterni** (meglio se bluetooth)

- **Adattatore** per **SD**
- **Cavo di rete** (opzionale)
- **Scheda di rete esterna** (opzionale)

I SW invece che ci serviranno sono:

- **Win32DiskImager** (https://sourceforge.net/projects/win32diskimager/)
- **Raspbian Stretch OS** (https://downloads.raspberrypi.org/raspbian_latest)
- **SDformatter**(opzionale)

# 3) Elenco dei tools + descrizioni

I tools che installeremo sono i seguenti:

- **Aircrack-ng**:
  Suite di programmi per testare la sicurezza delle reti Wi-Fi. Permette di rilevare tutti gli hotspot, visibili e non, intercettarne i pacchetti e gli handshake, eseguire attacchi bruteforce per cercare le credenziali di accesso e tanto altro.
- **Crunch**:
  Programma da riga di comando che permette la creazione dettagliata di dizionari per attacchi basati su wordlist .
- **Wireshark**:
  Il più diffuso e utilizzato sniffer di rete/network protocolanalyzer.
- **SET (Social Engineer Toolkit)**:
  Vasto insieme di programmi per attacchi di ingegneria sociale di tutti i tipi. Permette di copiare pagine html, inviare SMS e email personalizzate, creare siti di phishing e quant'altro.
- **Metasploit**:
  Framework per il testing di qualsiasi dispositivo. Permette di creare o utilizzare exploit già esistenti, settare e modificare payload, avviare sessioni su un host remoto e tante altre cose.
- **John-the-ripper**:
  Uno dei più famosi e potenti software per il cracking di password.
- **THC-Hydra**:
  Programma per il cracking di login e siti, molto veloce e flessibile.

# 4) Installazione

Nelle prossime pagine vedremo come installare i programmi precedentemente citati sul nostro raspberry. Per chi non si fidasse, può tranquillamente installare tutto su una macchina virtuale ed eseguire le prove da lì, riportando poi gli stessi passaggi sul proprio Pi.

## a. Scaricare, installare e avviare Raspbian

Come prima cosa, per creare la nostra macchina da hacking, avremo bisogno di installare raspbian sulla sd. Scarichiamo quindi Win32Diskimager e Raspbian dai link del capitolo 2 e procediamo all'installazione. Formattiamo la nostra sd tramite un'apposita app oppure da riga di comando (io lo farò da riga di comando su Windows).

Avviamo il **CMD** e digitiamo

```
>> diskpart
```

Si avvierà così il programma per formattare la nostra sd. Procediamo elencando tutti i dispositivi con il comando

```
>> listdisk
```

e selezioniamo la nostra SD (nel mio caso il disco 1)

```
>> select disk 1
```

ora avremo bisogno di ripulire tutto il vecchio contenuto, creare una nuova partizione da zero e riformattarla. Digitiamo quindi:

```
>> clean
>> create partition primary
>> format fs=fat32 quick
```

Ecco fatto! Ora siamo pronti per installare il nostro sistema operativo. Apriamo quindi Win32DiskImager, selezioniamo la nostra sd, il nostro file .iso e installiamo il tutto. Alla fine del caricamento avremo la nostra memorietta esterna con sopra Raspbian, pronta ad essere inserita nel Raspberry e avviata. Accendiamo quindi il nostro Pi collegandolo alla corrente, settiamo tutte le impostazioni che ci servono (come monitor, tastiera esterna, servizio SSH ecc.) e prepariamoci a installare tutti i tools che vogliamo!

## b. Installare Aircrack-ng

Prima di procedere all'installazione della suite, aggiorniamo tutti i riferimenti delle repo con

```
$ sudo apt-get update
```

Ora siamo davvero pronti: per installare e far funzionare Aircrack e affiliati dobbiamo installare un po' di programmi. Digitiamo:

$ sudo apt-get install subversion libssl1.0-dev libnl-3-dev libnl-gen1-3-dev ethtool build-essential libsqlite3-dev

Conclusa l'installazione di tutti questi software spostiamoci nella cartella dei Download del nostro Raspberry e scarichiamo l'archivio compresso di air crack (verificate sul sito l'ultima versione):

$ cd /home/pi/Download

$ wget http://download.aircrack-ng.org/aircrack-ng-1.2-rc4.tar.gz

Ora che abbiamo il file compattato, scompattiamolo, compiliamo il contenuto e installiamo air crack

$ tar –zxvf aircrack-ng-1.2-rc4.tar.gz

$ cd aircrack-ng-1.2-rc4

$ sudo make

$ sudo make install

Perfetto, abbiamo così Aircrack-ng e tutti i suoi componenti! Per provare, se disponiamo di una scheda di rete che supporta la modalità monitor, digitiamo:

$ sudo airmon-ng start wlan1

e osserviamo la nostra scheda di rete entrare in modalità monitor.

## c. Installare Crunch

Rispetto ad Aircrack-ng, l'installazione di crunch risulta 100 volte più semplice. Ci basterà aprire il terminale e digitare:

$ sudo apt-get install crunch

Semplice no?

Proviamo ora a generare un semplice dizionario con parole di sole 3 lettere terminanti con 'a'. Scriviamo:

$ sudo crunch 3 3 –t @@a –o ./dizionario.txt

Se tutto ha funzionato correttamente, ci trverete nella cartella indicata (nel mio caso la corrente) il file di testo con le vostre psw.

## d. Installare Wireshark

Come per Crunch, anche l'installazione di Wireshark risulta essere particolarmente semplice. Basterà digitare nella CLI:

$ sudo apt-get install wireshark

e attendere il completamento dell'installazione.

**ATTENZIONE:**

alla domanda se si voglia rendere eseguibile wireshark per tutti gli utenti e non solo i root, digitiamo (o premiamo) 'YES'.

Alla fine dell'installazione non ci resta che eseguire wireshark con l'apposito comando:

$ sudo wireshark

e goderci il nostro nuovo tool.

**ATTENZIONE x2:**

In caso comparisse un errore riferito al file init.lua, per risolverlo dovremo andare nella cartella di wireshark, editare init.lua e cambiare il valore del flag disable_lua

$ cd usr/share/wireshark

$ sudo leafpad init.lua

disable_lua = false >> disable_lua = true

(https://askubuntu.com/questions/454734/running-wireshark-lua-error-during-loading)

## e. Installare SET

Siamo giunti all'installazione del Social Engineer Toolkit. Innanzitutto dovremo scaricarlo da github, quindi dirigiamoci nella nostra solita cartella dei Download e scarichiamolo lì:

$ cd /home/pi/Download

$ sudo git clone https://github.com/trustedsec/social-engineer-toolkit /set

$cd set

Bene, una volta dentro la cartella, leggiamo il file readme in modo da capire quali softeare installare per far sì che non ci siano errori

$ sudo cat README.md

Vediamo che servono un bel po' di programmi, installiamo quindi ciò che serve:

$ sudo apt-get -force-yes -y install git apache2 python-requests libapache2-mod-php

$ sudo apt-get -force-yes -y install python-pymssql build-essential python-pexpect python-pefile python-crypto python-openssl

Fatto questo siamo pronti per concludere l'installazione del SET

$ sudo python setup.py install

## f. Installare Metasploit

L'installazione di Metasploit è una delle più complesse nonché lunghe. Iniziamo installando un po' di programmi che ci aiutano a risolvere le dipendenze:

$ sudo apt-get install build-essential zlib1g zlib1g-dev libxml2 libxml2-dev libxslt-dev locate libreadline6-dev libcurl4-openssl-dev git-core libssl-dev libyaml-dev openssl autoconf libtool ncurses-dev bison curl wget postgresql postgresql-contrib libpq-dev libapr1 libaprutil1 libsvn1 libpcap-dev

Finito di installare tutto, continuiamo con l'installazione di altri software:

$ sudo apt-get install git-core postgresql curl ruby1.9.3 nmap gem

$ sudo gem install wirble sqlite3 bundler nokogiri

Finito di installare anche questi programmi, scarichiamo metasploit da github e installiamolo

$ cd /opt

$ sudo git clone https://github.com/rapid7/metasploit-framework.git

$ cd mtasploit-framework

$ sudo bundle install

**ATTENZIONE:**

In caso si verificassero errori, molto probabilmente è perché la versione di ruby non è quella giusta. Dovrete allora aggiungere una nuova repo alla lista delle esistenti e scaricare l'ultima versione di ruby da lì. Scriviamo:

$ sudo leafpad /etc/apt/source.list

Aggiungiamo

deb http://archive.raspbian.org/raspbian/ stretch main

Salviamo, usciamo, aggiorniamo e installiamo l'ultima versione di ruby

$ sudo apt-get update

$ sudo apt-get install build-essential patch ruby-dev zlib1g-dev liblzma-dev

$ sudo gem install nokogiri

A questo punto tutto dovrebbe esser stato installato correttamente. Non ci resta che dirigerci nella cartella di metasploit ed avviare

$ sudo ./msfconsole

## g. Installare John-the-ripper

Dopo aver installato msf, john-the-ripper risulta più semplice che bere un bicchier d'acqua. Indovinate un po' come si fa?

Esatto:
$ sudo apt-get install john

Più facile di così!

### h. Installare THC-Hydra

Siamo arrivati all'ultimo tool, e come il precedente, anche per questo basterà un solo comando:
$ sudo pat-get install hydra hydra-gtk

**Abbiamo così finito di installare tutto!**

## 5) Conclusioni

Spero che questo piccolo manuale possa esser stato utile a qualcuno. L'idea è quella di non scaricare un SO con già tutto sopra ma sbattersi e mettere le mani in pasta per imparare a usare e capire il mondo attorno a linux e raspberry.
Inoltre specifico che non rispondo di ciò che farete con i tools scaricati tramite questo libro. Non mi assumo responsabilità in caso di utilizzo errato dei medesimi contenuti, ma vi ringrazio per la lettura.
Ricordate sempre che 'da grandi poteri derivano grandi responsabilità'.
Detto questo, grazie di tutto.

- Bl4ckD0t