

MANUAL DE USUARIO PPDRON.

DIEGO ARMANDO SIERRA SIERRA
LARRY MAURICIO PORTOCARRERO
ANDREA KATHERINE VELANDIA

UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA
FACULTAD DE INGENIERÍA
ESCUELA INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
TUNJA
2016

MANUAL DE USUARIO PPDRON.

Presentado a:

INGENIERA ANDREA CATHERINE ALARCON ALDANA

UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA
FACULTAD DE INGENIERÍA
ESCUELA INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
TUNJA
2016

INTRODUCCIÓN.

El presente documento pretende mostrar al usuario el funcionamiento de la aplicación PPDRON. Para utilizar la aplicación correctamente, es necesario contar con determinadas herramientas, a continuación se explicarán los pasos para descargar e instalar cada una de ellas así como una explicación de su funcionamiento.

1. INSTALACIÓN AIRCRACK.

Aircrack-ng es una suite llena de herramientas para el testeo de redes e interfaces wireless. Permite poner en modo monitor o modo promiscuo una interfaz wifi, inyectar paquetes, realizar ataques para testear nuestra seguridad.

Para descargar e instalar aircrack hay que seguir los siguientes pasos:

```
$ echo "deb-src http://ftp.fr.debian.org/debian sid main contrib non-free" > /etc/apt/sources.list.d/removeme.list
```

```
$ apt-get update
```

```
$ apt-get build-dep aircrack-ng
```

```
$ rm /etc/apt/sources.list.d/removeme.list
```

```
$ apt-get install xterm iw macchanger tar gzip
```

```
$ wget http://download.aircrack-ng.org/aircrack-ng-1.1.tar.gz -O -|tar xvz
```

```
$ wget http://airoscrip.t.googlecode.com/files/airoscrip-ng_1.1.tgz -O -|tar xvz
```

```
$ make -C aircrack-ng-1.1 && make -C aircrack-ng-1.1 install
```

```
$ make -C airoscript-ng
```

2. INSTALACIÓN ETHTOOL.

Ethtool se puede utilizar para consultar y cambiar parámetros como la velocidad, autonegociación y la descarga de la suma de verificación en muchos dispositivos de red, especialmente dispositivos Ethernet. Para instalar esta herramienta se deben seguir los siguientes pasos:

```
# apt-get update
```

```
# apt-get install ethtool
```

```
# ethtool eth0
```

3. INSTALACIÓN DE REAVER.

Reaver implementa un ataque de fuerza bruta contra el WiFi Protected Setup (WPS) PIN de registro con el fin de recuperar contraseñas WPA/WPA2. Para descargar e instalar se deben seguir los siguientes pasos:

Descargar:

```
wget http://reaver-wps.googlecode.com/files/reaver-1.4.tar.gz
```

Instalar:

```
apt-get install build-essential libpcap0.8-dev libsqlite3-dev
```

Desempaquetar:

```
tar xvf reaver-1.4.tar.gz
```

Al descomprimir se crea el directorio /reaver-1.4 y dos subdirectorios /docs y "/src". En este último hay que ubicarse y lanzar :

```
./configure
```

```
make
```

```
make install
```

4. INSTALACIÓN DE PIXIE WPS.

Pixiewps es una herramienta escrita en C utiliza para ataque de fuerza bruta sin conexión el PIN WPS explotación de la entropía baja o inexistente de algunos puntos de acceso, el llamado "ataque polvo mágico" descubierto por Dominique Bongard en el verano de 2014. Está destinado a fines educativos solamente. Para descargar e instalar se deben seguir los siguientes pasos:

```
pi@crozono~$ git clone https://github.com/wiire/pixiewps.git
```

```
pi@crozono~$ cd src
```

```
pi@crozono~$ sudo make
```

```
pi@crozono~$ sudo make install
```

5. INSTALACIÓN DE MACCHANGER.

MacChanger es una herramienta de GNU/Linux para la visualización y manipulación de direcciones MAC de cada interfaz de red en tu computador.

Se puede descargar de:

<https://github.com/alobbbs/macchanger>

Se puede instalar con el comando:

```
sudo apt-get install macchanger macchanger-gtk
```

6. INSTALACIÓN LIBRERÍAS DE PYTHON.

Para descargar los paquetes necesarios, es posible ir al sitio web del paquete o acceder al repositorio en Github. Sin embargo, existe un método mucho más eficaz para descargar e instalar los paquetes necesarios para un proyecto desarrollado con Python. Este método involucra utilizar un archivo de texto, en el cual se anotan los paquetes para que pip se encargue de instalarlos de forma automática. El archivo en cuestión se le llama *requirements.txt* y tiene un formato específico para anotar cada una de los paquetes a instalar. Por lo general se ubica en el directorio raíz del proyecto.

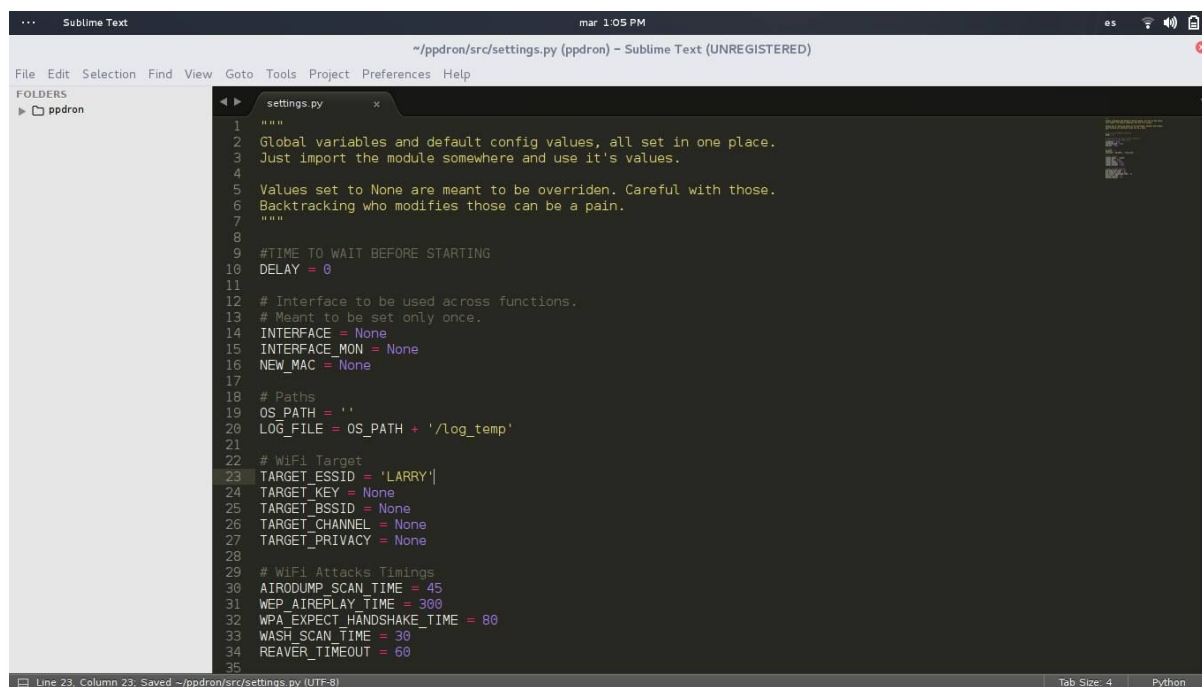
Simplemente se ejecuta el siguiente comando en la terminal:

```
$ pip install -r requirements.txt
```

El comando anterior debe ejecutarse en el directorio dónde se encuentra el archivo *requirements.txt*.

7. CONFIGURACIÓN ARCHIVO SETTINGS.PY.

Para que el sistema PPDRON pueda iniciar, se debe modificar el archivo Settings.py (ver Figura N° 1). En este archivo se debe configurar con los siguientes datos: nombre de la red teniendo en cuenta mayúscula y minúscula, interfaz, tiempo de escaneo del espectro, la MAC del AP y el tiempo destinado para realizar el escaneo.

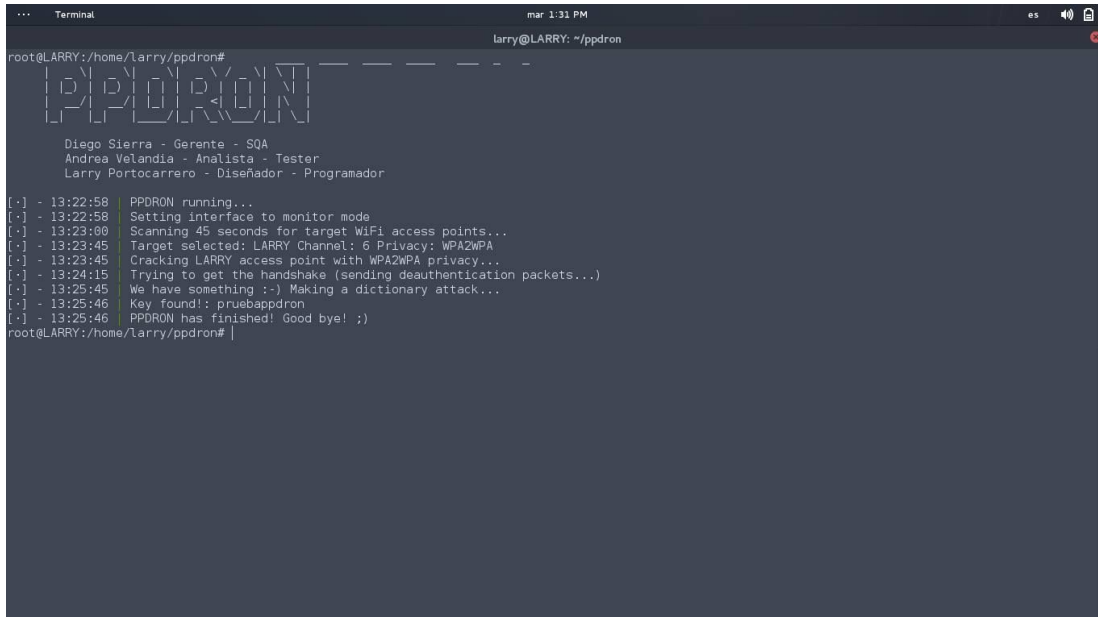


```
1  """
2  Global variables and default config values, all set in one place.
3  Just import the module somewhere and use it's values.
4
5  Values set to None are meant to be overridden. Careful with those.
6  Backtracking who modifies those can be a pain.
7  """
8
9  #TIME TO WAIT BEFORE STARTING
10 DELAY = 0
11
12 # Interface to be used across functions.
13 # Meant to be set only once.
14 INTERFACE = None
15 INTERFACE_MON = None
16 NEW_MAC = None
17
18 # Paths
19 OS_PATH = ''
20 LOG_FILE = OS_PATH + '/log_temp'
21
22 # WiFi Target
23 TARGET_ESSID = 'LARRY|'
24 TARGET_KEY = None
25 TARGET_BSSID = None
26 TARGET_CHANNEL = None
27 TARGET_PRIVACY = None
28
29 # WiFi Attacks Timings
30 AIRODUMP_SCAN_TIME = 45
31 WEP_AIREPLAY_TIME = 300
32 WPA_EXPECT_HANDSHAKE_TIME = 80
33 WASH_SCAN_TIME = 30
34 REAVER_TIMEOUT = 60
35
```

Figura N° 1. Configuración Archivo Settings.py

8. PANTALLA EJECUCIÓN PPDRON.

La pantalla de ejecución de PPDRON (ver Figura N° 2), se muestra el canal, el tipo de seguridad, el tiempo de escaneo, el nombre la red, el tipo de ataque utilizado.



```
root@LARRY:/home/larry/ppdrón#
PPDRON

Diego Sierra - Gerente - SQA
Andrea Velandia - Analista - Tester
Larry Portocarrero - Diseñador - Programador

[.] - 13:22:58 | PPDRON running...
[.] - 13:22:58 | Setting interface to monitor mode
[.] - 13:23:00 | Scanning 45 seconds for target WiFi access points...
[.] - 13:23:45 | Target selected: LARRY Channel: 6 Privacy: WPA2WPA
[.] - 13:23:45 | Cracking LARRY access point with WPA2WPA privacy...
[.] - 13:24:15 | Trying to get the handshake (sending deauthentication packets...)
[.] - 13:25:45 | We have something :-| Making a dictionary attack...
[.] - 13:25:46 | Key found!: pruebappdrón
[.] - 13:25:46 | PPDRON has finished! Good bye! ;)
root@LARRY:/home/larry/ppdrón#
```

Figura N° 2. Pantalla Ejecución PPDRON.

9. REPORTE.

El usuario podrá extraer el reporte (ver Figura N° 3), en esta pantalla se muestran: objetivo, canal, encriptación, tipo de ataque, contraseña de acceso, error, recomendación.



AP Objetivo	Canal	Encriptación	Ataque	Clave
LARRY	6	WPA2WPA	Ataque de diccionario	pruebappdrón

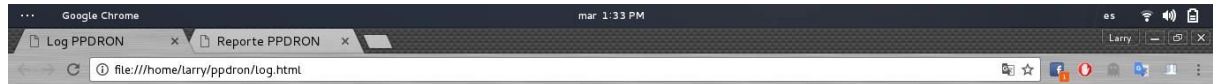
Recomendaciones

- Uso de contraseñas robustas, se debe evitar claves que puedan ser adivinadas por un atacante fácilmente, la implementación de una política de claves seguras y cambio de estas periódicamente es necesario para este punto de acceso.
- Establecimiento de cifrado WPA/WPA2 - PSK: Es lo más robusto que hay hoy en día, aunque no es ni mucho menos infalible, ya que existen formas de atacar un red con WPA/WPA2-PSK, pero es lo más que podemos tener en cuanto a cifrado de red en entornos domésticos.
- Cambio de la clave por defecto. El punto de acceso objetivo contiene una configuración por defecto. Un atacante utiliza la implementación de los algoritmos que usaron los fabricantes para establecer claves por defecto.
- Ocultar el SSID: Al ocultar el SSID del punto de acceso, se evita que emita los beacon frames con el nombre de la red. Limitando la difusión del punto de acceso a personas ajenas a la red.
- Cambiar periódicamente del SSID y clave: al realizar este proceso periódicamente se evita que la configuración de acceso al punto de acceso termine almacenada en bases de datos públicas y cualquier persona logre ingresar a la red.
- Desactivación del WPS (WiFi Protected Setup): Esta característica permite que un equipo se conecte a la WiFi utilizando un código temporal que simplifica todo el proceso de "enrollment" de un nuevo equipo. Por desgracia las implementaciones de muchos routers no detectan los ataques de fuerza bruta y en unos minutos un atacante lograría ingresar a la red WiFi.
- Filtración por direcciones MAC de conexión: No es una medida definitiva, pero dificulta el trabajo del atacante, además ayuda a identificar y localizar a los atacantes.
- Implementación de WPA/WPA2 - Enterprise: Esta tipo de configuración de red está pensada para diseños empresariales, que agrega un nivel de seguridad adicional.
- Deshabilitar el punto de acceso cuando no esté en uso.

Figura N° 3 Pantalla Reporte.

10. PANTALLA LOG.

En esta pantalla (ver Figura N° 4), se visualiza el canal, el tipo de seguridad, el tiempo de escaneo, el nombre la red, el tipo de ataque utilizado. Durante el tiempo de ejecución con la hora del sistema en formato hora, minuto y segundo.



Log PPDRON

```
13:22:58 [ PPDRON running... ]
13:22:58 [ Setting interface to monitor mode ]
13:23:00 [ Scanning 45 seconds for target WiFi access points... ]
13:23:45 [ Target selected: LARRY Channel: 6 Privacy: WPA2WPA ]
13:23:45 [ Cracking LARRY access point with WPA2WPA privacy... ]
13:24:15 [ Trying to get the handshake (sending deauthentication packets...) ]
13:25:45 [ We have something :-). Making a dictionary attack... ]
13:25:46 [ Key found!: pruebappdron ]
13:25:46 [ PPDRON has finished! Good bye! ;) ]
```

Figura N° 3 Pantalla Log.