

RAMA ESTUDIANTIL IEEE - UIGV



RAMA ESTUDIANTIL IEEE - UIGV

UNIVERSIDAD PARTICULAR

“INCA GARCILASO DE LA VEGA”

I-EEE UIGV

PRESIDENTE RAMA IEEE UIGV

JIMY A. ESPINOZA RONDÁN

VICEPRESIDENTE

JENKIS PILLPE CANGANA

CONSEJERO

P. TRONCOSO C.

ORGANIZADOR DE TALLER: VICTOR DE LA CRUZ BAUTISTA

PONENTE: MIEMBRO IEEE UIGV CESAR DIAZ CAMACHO

DATOS: :- Correo: cesardc17@hotmail.com

:- Cel: 986533404

FISCT

LIMA - PERÚ

2012

RAMA ESTUDIANTIL IEEE - UIGV

MANUAL BACTRACK 5-R2 PARA REDES CON SEGURIDAD WEP

Antes de entrar en materia, debemos recordar que esta distribución, como su uso, depende del usuario. Estas herramientas y este manual/tutorial no están diseñados para fines delictivos. Por tanto la responsabilidad del uso que se haga de ello, depende únicamente de ustedes. Hacer buen uso de esta información.

Utilizaremos un programa llamado Gerix Wifi Cracker. El programa se encuentra en: Inicio → BackTrack → Exploitation Tools → Wireless Exploitation Tools → WLAN Exploitation → gerix-wifi-cracker-ng.



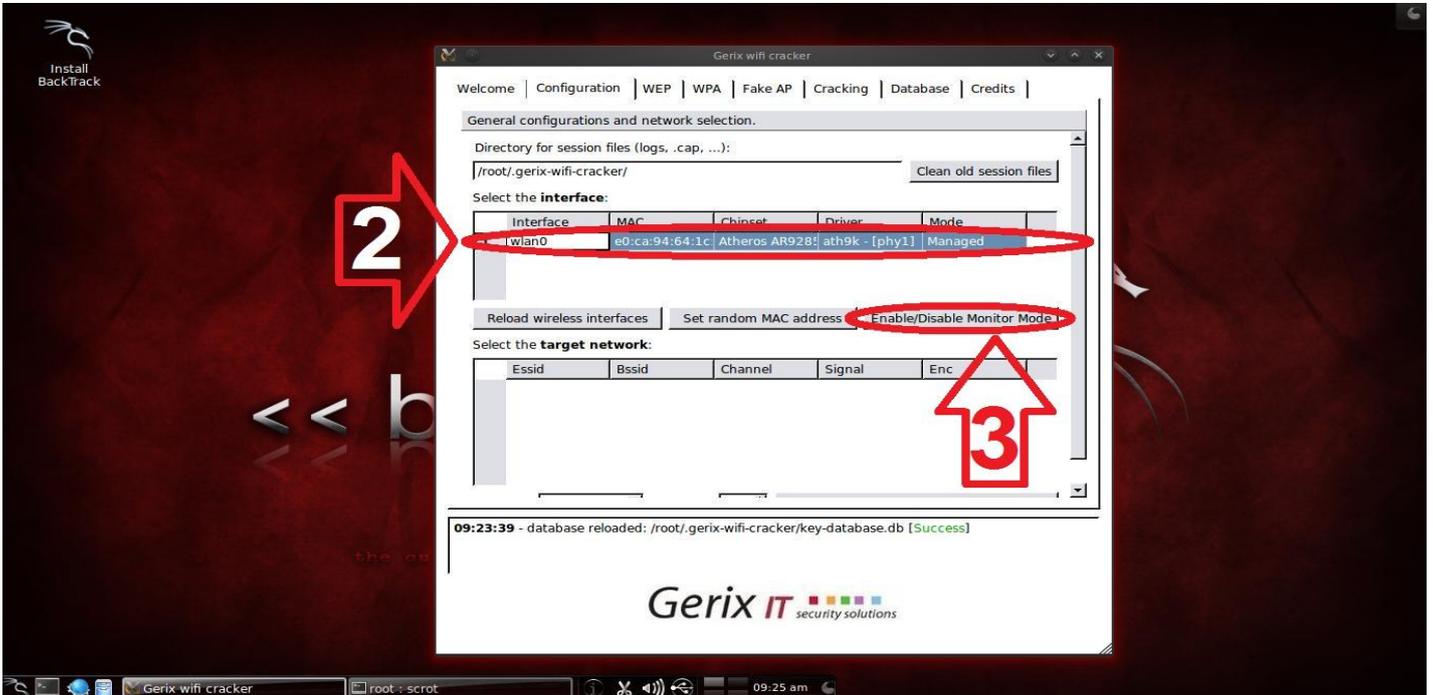
1.- CONFIGURACION



RAMA ESTUDIANTIL IEEE - UIGV

2.- SELECCIONAMOS NUESTRA TARJETA RED INALAMBRICA

3.- ENABLE/DISABLE MONITOR MODE → HABILITA EL MODO MONITOR DE NUESTRA TARJETA DE RED

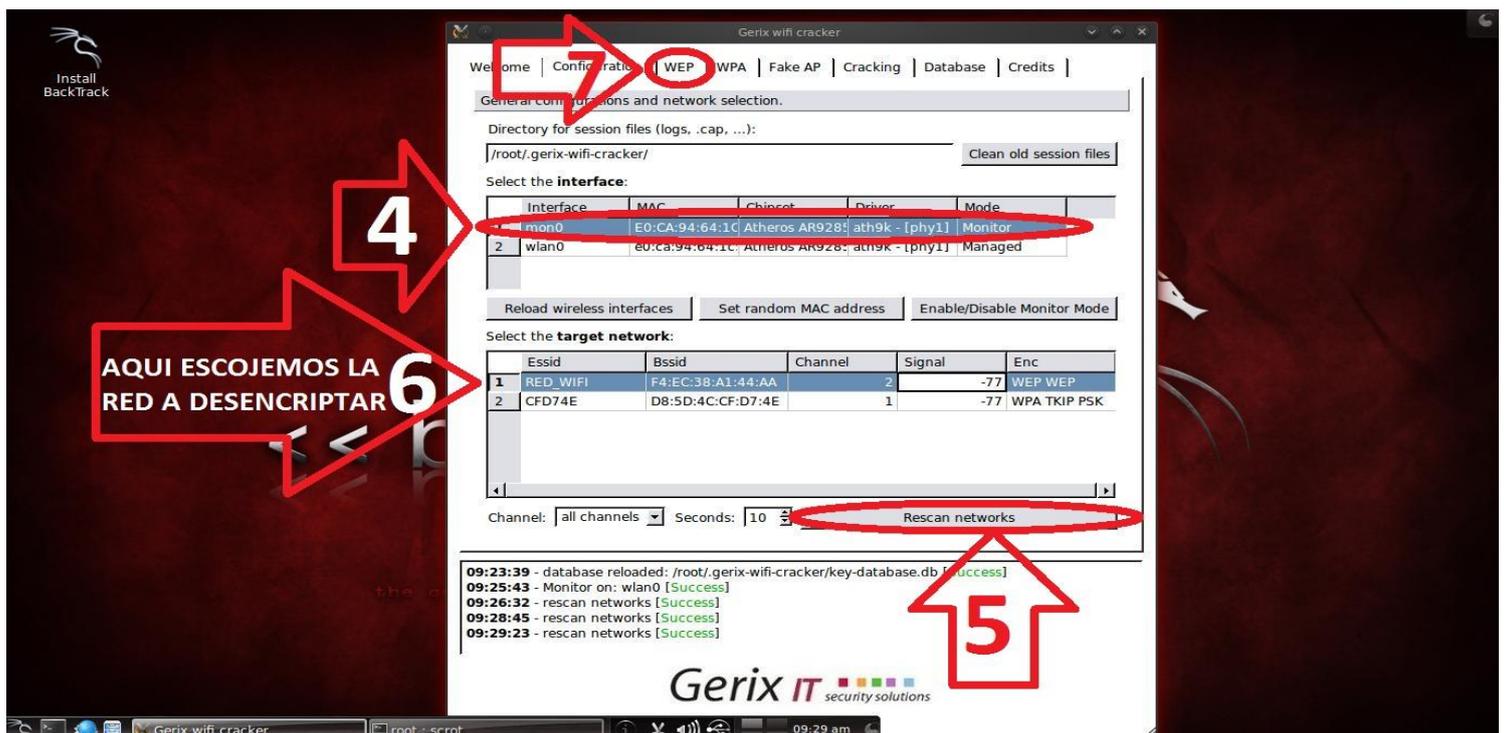


4.- SELECCIONAMOS LA NUEVA SUB INTERFACE CREADA LLAMADA **mon0**.

5.- RESCAN NETWORKS → ESCANEMOS LAS REDES EXISTENTES ALREDEDOR.

6.- ESCOJEMOS LA RED A DESENCRIPTAR.

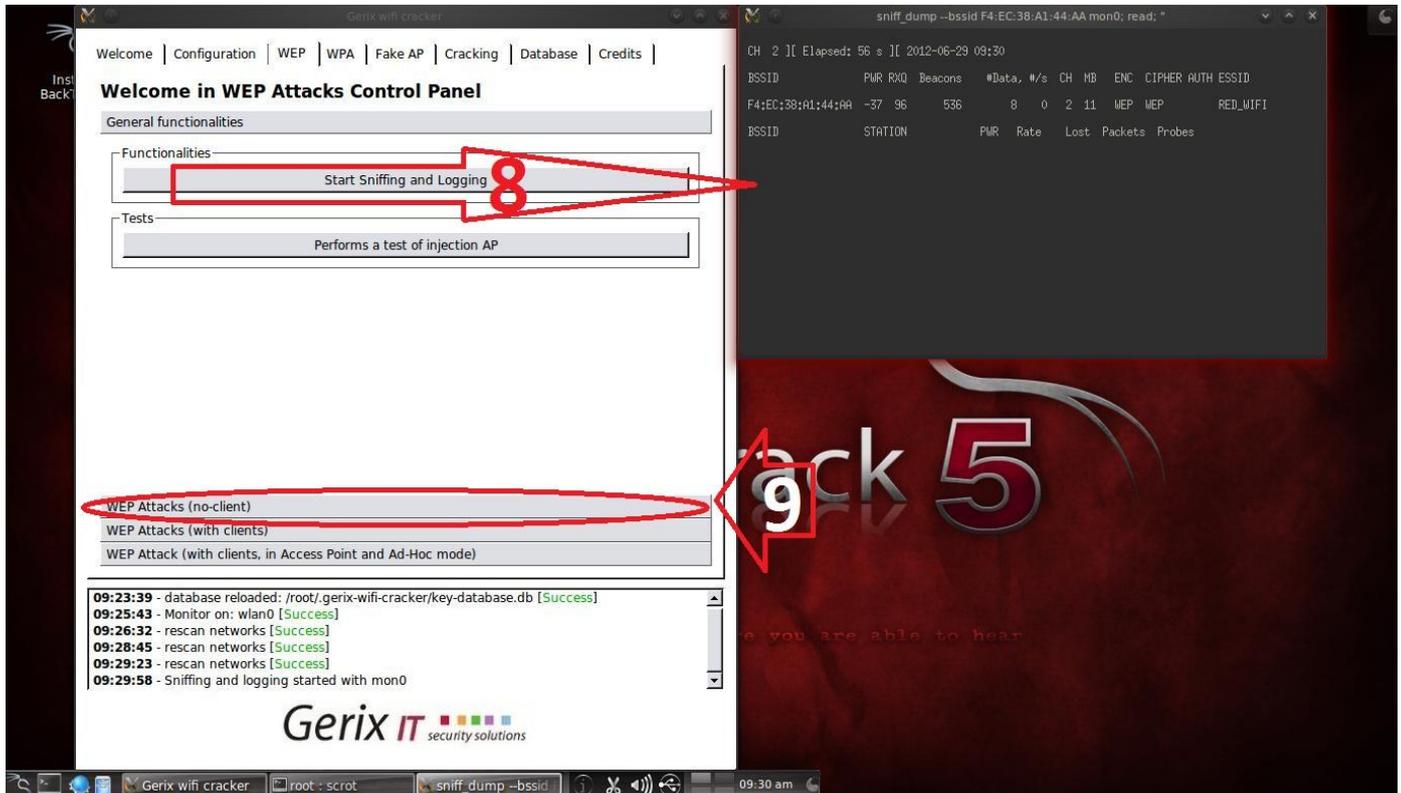
7.- NOS DIRIGIMOS A LA PESTAÑA **WEP**.



RAMA ESTUDIANTIL IEEE - UIGV

8.- STAR SNIFFING AND LOGGING → SE HABRE UN TERMINAL CON LA RED QUE DESEAMOS DESENCRIPTAR.

9.- WEP ATTACKS(no clients) → PARA COMENSAR EL ATAQUE



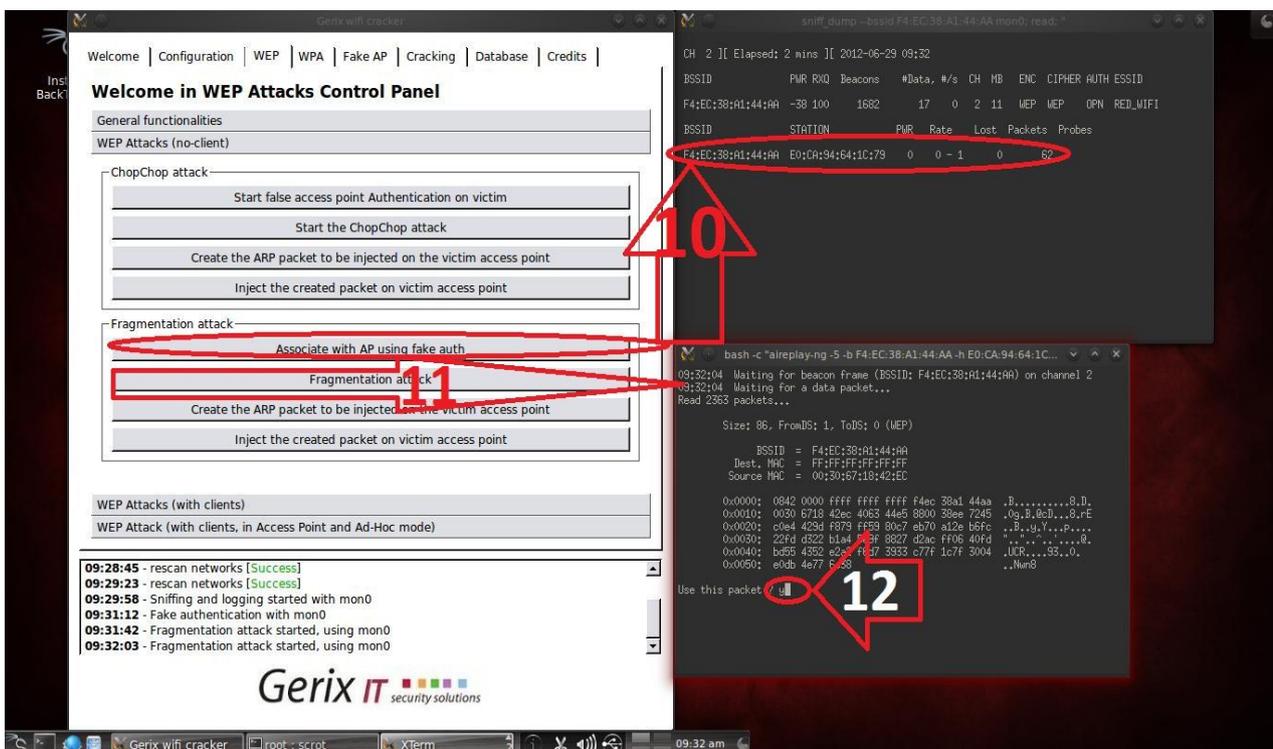
The screenshot shows the Gerix WiFi Cracker web interface. In the 'General functionalities' section, the 'Start Sniffing and Logging' button is circled in red with the number '8'. Below it, the 'WEP Attacks (no-client)' option is also circled in red with the number '9'. To the right, a terminal window displays the output of a sniffing operation, including a table of network statistics:

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
F4:EC:38:A1:44:AA	-37	96	536	8 0	2 11	WEP	WEP	RED_WIFI		

A large 'Back 5' watermark is overlaid on the terminal window.

10. - ASSOCIATE WITH AP USING FAKE AUTH → ASOCIACION FALSA.

11.- FRAGMENTATION ATTACK → CAPTURA LOS PAQUETES PARA DESPUES INYECTARLOS.



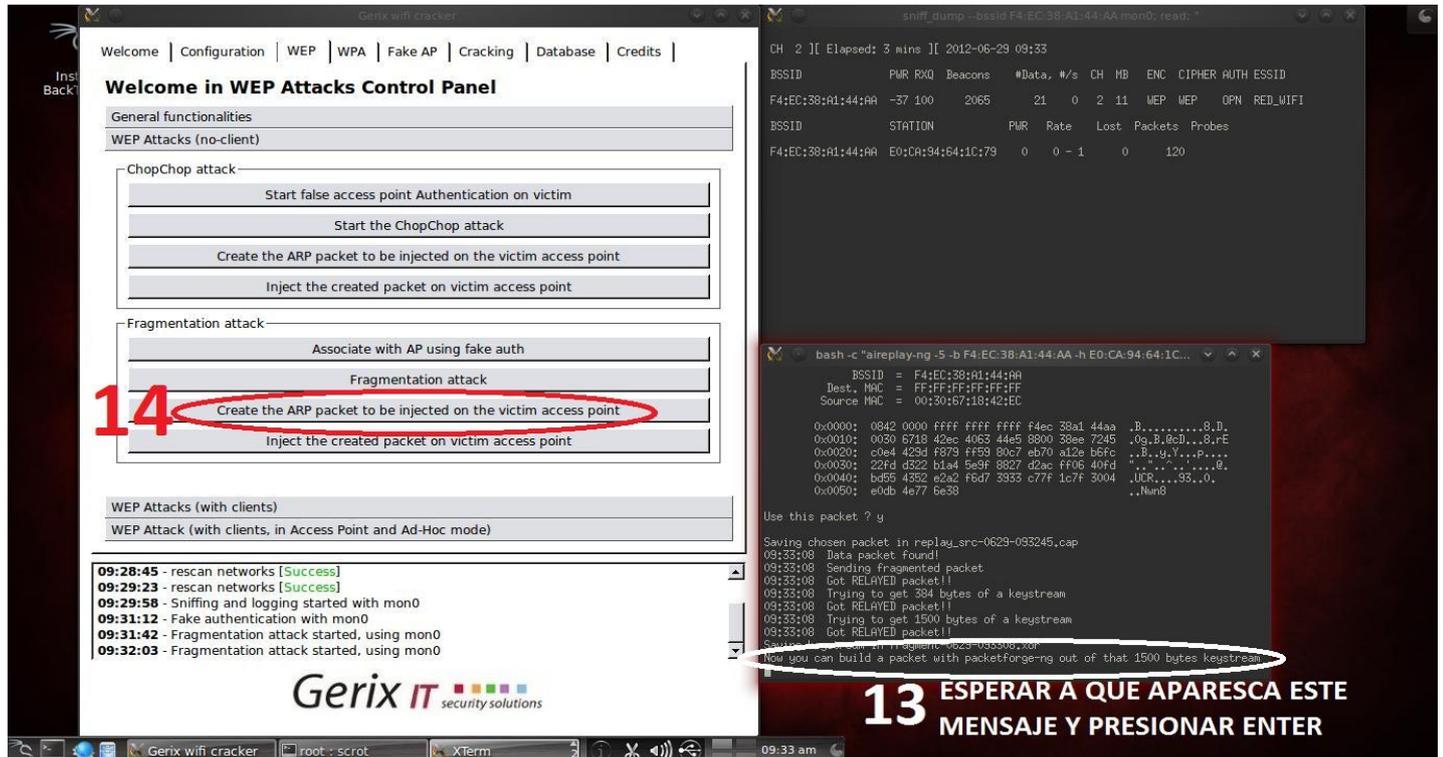
The screenshot shows the Gerix WiFi Cracker web interface. In the 'WEP Attacks (no-client)' section, the 'Associate with AP using fake auth' button is circled in red with the number '10'. Below it, the 'Fragmentation attack' button is also circled in red with the number '11'. To the right, a terminal window displays the output of a sniffing operation, including a table of network statistics:

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
F4:EC:38:A1:44:AA	E0:CA:94:64:1C:79	0	0	1	0	62

A large 'Back 5' watermark is overlaid on the terminal window.

RAMA ESTUDIANTIL IEEE - UIGV

- 12.- PONERMOS "Y" Y APRETAMOS ENTER PARA COMENZAR LA CAPURA DE PAQUETES.
- 13.- ESPERAR A QUE APARESCA ESE MENSAJE Y PRESIONAR ENTER PARA CERRARLO.
- 14.- CREATE THE ARP PACKET TO BE INJECTEC ON THE VICTIM AP → CREA EL PAQUETE ARP A INYECTAR.

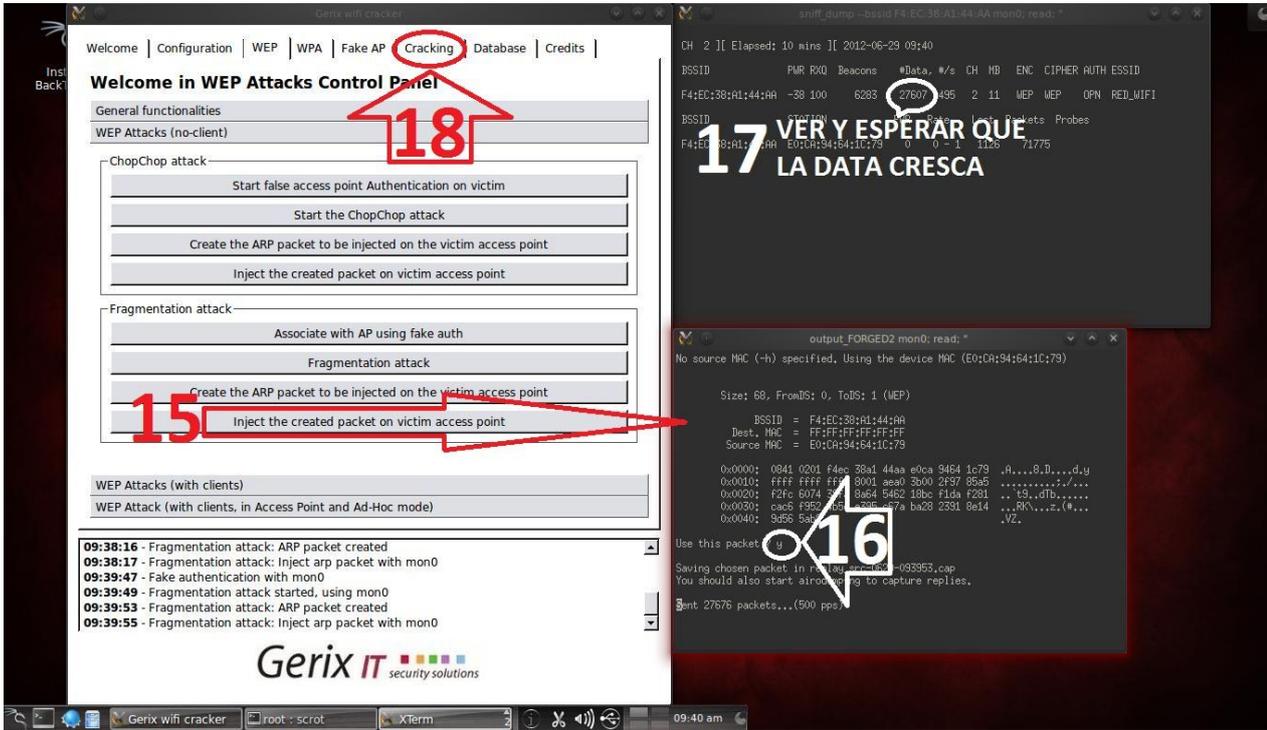


14 Create the ARP packet to be injected on the victim access point

13 ESPERAR A QUE APARESCA ESTE MENSAJE Y PRESIONAR ENTER

- 15.- INJECT THE CREATED PACKET ON VICTIM AP → INYECTA EL PAQUETE CREADO EN EL AP DE LA VICTIMA
- 16.- PONERMOS "Y" Y APRETAMOS ENTER PARA COMENZAR LA INYECCION DE PAQUETES.
- 17.- VEMOS COMO LA DATA AUMENTA Y ESPERARAMOS PARA COTINUAR CON EL SIGUIENTE PASO.
- 18.- NOS DIRIGIMOS A LA PESTAÑA **CRACKING**.

RAMA ESTUDIANTIL IEEE - UIGV



- 19.- AIRCRACK-NG DECRYPT WEP PASSWORD → ABRE LA TERMINAL QUE DESCIFRA LA CLAVE WEP.
- 20.- VEMOS LA CLAVE DE LA RED VICTIMA EN HEXADECIMAL Y ASCII

