

UNIVERSIDAD INCA GARCILASO DE LA VEGA SUDAMERICA PERÚ LIMA REGIÓN 09

RAMA ESTUDIANTIL IEEE - UIGV





UNIVERSIDAD INCA GARCILASO DE LA VEGA SUDAMERICA PERÚ LIMA REGIÓN 09

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



UNIVERSIDAD INCA GARCILASO DE LA VEGA SUDAMERICA PERÚ LIMA REGIÓN 09

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 \rightarrow BackTrack \rightarrow Exploitation Tools \rightarrow Wireless Exploitation Tools \rightarrow WLAN Exploitation \rightarrow gerix-wifi-cracker-ng.



1.- CONFIGURACION





UNIVERSIDAD INCA GARCILASO DE LA VEGA SUDAMERICA PERÚ LIMA REGIÓN 09

RAMA ESTUDIANTIL IEEE - UIGV

2.- SELECIONAMOS NUESTRA TARJETA RED INALAMBRICA

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

	Welcome Configuration WEP WPA Fake AP Cracking Database Credits	
	General configurations and network selection.	
	Directory for session files (logs, .cap,):	
	/root/.gerix-wifi-cracker/ Clean old session files	
	Select the interface:	
	Interface MAC Chipset Driver Mode	
	e0:ca:94:64:1c Atheros AR928! ath9k - [phy1] Managed	
	Set fairful MAC address in Enable/Unsable Monton Mode F Select the target network: Essid Bssid Channel Signal	
< <	Essid Bassid Channel Signal Enc	
	09:23:39 - database reloaded: /root/.gerix-wifi-cracker/key-database.db [Success]	
	the en	
	Goriy IT	

- 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.

\rightarrow		Gerix w	ifi cracker		~ ~ ~ ~	×	
Install ackTrack	Welliome Configuratio	WEP WPA Fa	ke AP Crackin	g Database	Credits		
	Directory for session fi	les (logs, .cap,):					
	/root/.gerix-wifi-cracke	/root/.gerix-wifi-cracker/					
	Select the interface:						
	Interface	MAC Chine	ot Drivo	rMode			
	mon0	E0:CA:94:64:1C Ather	os AR928! ath9k	- [phy1] Monit	pr		
	2 wlan0	eu:ca:94:64:1C Athen	05 AR928: atn9k	- [pny1] Manag	ged		
	Reload wireless inte	rfaces Set rando	m MAC address	Enable/Disat	le Monitor Mode		
	Select the target net	work:					
	Essid	Bssid	Channel	Signal	Enc		
AQUI ESCOJEIVIOS LA	1 RED_WIFI	F4:EC:38:A1:44:AA	2	-77	WEP WEP		
RED A DESENCRIPTAR	2 CFD74E	D8:5D:4C:CF:D7:4E	1	L -77	WPA TKIP PSK		
	Channel: all channel:	Seconds: 10	racker/key-datab	Rescan networ	ks 1		
	09:25:43 - Monitor on: wi 09:26:32 - rescan networ 09:28:45 - rescan networ 09:29:23 - rescan networ	ano [Success] ks [Success] ks [Success] ks [Success]		<u> 1</u> 5			
		Genx	security so	lutions			
🤹 📴 💽 Gerix wifi cracker 🖆 root : :	scrot	ե վայ 🛞 📃	09:29 am 💪			(A)	



UNIVERSIDAD INCA GARCILASO DE LA VEGA SUDAMERICA PERÚ LIMA REGIÓN 09

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



10. - ASSOCIATE WITH AP USING FAKE AUTH → ASOCIASION FALSA. 11.- FRAGMENTATION ATACK→ CAPTURA LOS PAQUETES PARA DESPUES INYECTARLOS.

Welcome in WEP Attacks Control Panel	F4:EC:38:A1:44:AA -38 100 1682 17 0 2 11 WEP WEP OPN RED_WIFI
General functionalities	RSSID <u>STATION PWR Rate Lost</u> Packets Probes
WEP Attacks (no-client)	E4:EC:38:A1:44:AA E0:CA:94:64:1C:79 0 0 - 1 0 62
ChopChop attack	
Start false access point Authentication on victim	
Start the ChopChop attack	
Create the ARP packet to be injected on the victim access point	
Inject the created packet on victim access point	
Fragmentation attack	
Associate with AP using fake auth	bash -c "aireplay-ng -5 -b F4:EC:38:A1:44:AA -h E0:CA:94:64:1C 🗙 🔨 🗙
Fragmentation att ck	09:32:04 Waiting for beacon frame (BSSID: F4:EC:38:A1:44:AA) on channel 2
Create the APP packet to be injector	Read 2363 packets
create the Air packet to be injected and in access point	Size: 86, FromDS: 1, ToDS: 0 (WEP)
Inject the created packet on victim access point	BSSID = F4:EC:38:A1:44:AA
	Source MAC = 00:30:67:18:42:EC
WEP Attacks (with clients)	0x00001: 0842 0000 ffff ffff ffff f4ec 38a1 44aa .B8.D.
WEP Attack (with clients, in Access Point and Ad-Hoc mode)	0x0020: c0e4 429d f879 ff59 80c7 eb70 a12e b5fcBy.Yp 0x0030: 226d d322 b1a4 d965 8827 d2ac f606 406d " " 8
00-28-4F second a function	0x0040: bd55 4352 e2e ff 17 3933 c77f 1c7f 3004 .UCR930.
09:29:23 - rescan networks [Success]	
09:29:58 - Sniffing and logging started with mon0	
09:31:42 - Fragmentation attack started, using mon0	
09:32:03 - Fragmentation attack started, using mon0	



UNIVERSIDAD INCA GARCILASO DE LA VEGA SUDAMERICA PERÚ LIMA REGIÓN 09

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.



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**.



UNIVERSIDAD INCA GARCILASO DE LA VEGA SUDAMERICA PERÚ LIMA REGIÓN 09

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

Welcome Configuration WEP WPA Fake AP Cracking Database Credits	CH 2][Elapsed: 11 mins][2012-06-29 09:41
Welcome in Cracking Control Panel	BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
WEP cracking	F4:EC:38:A1:44:AA -38 100 6645 45884 493 2 11 WEP WEP OPN RED_WIFI
Normal cracking When you have enougth packets (>5000) you can try to decrypt the password. Aircrack-ng - Decrypt WEP password	BSID STATION PWR Rate Lost Packets Probes F4:EC:38:A1:44:AA E0:CA:94:64:1C:79 0 0 - 1 474 108630
Aircrack-log.txt; read; "	Output_FORGED2 mon0: read: 0 </td
U00100001 lested 8 keys (got 33855 1%s) KB depth byte(vote) 0/2 255(50155) 765(4125) 216(4980) 251(2512) F01(45656) 1 0/2 255(1015) 765(4125) 216(4980) 251(45	0.012 0.012 <td< td=""></td<>
09:38 09:39 09:39 09:39 09:39 09:41 20	▲ Use this packet ? y Swing chasen packet in replay_src-0629-093963.cap You should also start airodump-ng to capture replies. Bent 46144 packets(500 pps)
Gerix IT security solutions	