

Curso de Hacking Ético Wi-Fi

*Introducción práctica a la seguridad inalámbrica del protocolo 802.11 con la distribución de seguridad **Backtrack 4** y la suite **Aircrack-ng***

v1.0

Curso de Hacking Ético Wi-Fi Prácticas con Backtrack y Aircrack ng



<< back | track 4

<< back | track 4

ÍNDICE

IEEE 802.11	8
IEEE	8
Comités.....	8
Estándares y enmiendas 802.11.....	9
IEEE 802.11	9
Canales y Frecuencias.....	13
Funcionamiento del estándar 802.11.....	15
Introducción	15
Modos de operación 802.11.....	15
Modo de Infraestructura	15
Modo Ad Hoc.....	16
Modo Monitor y modo Promiscuo	16
Paquetes 802.11 comunes y su estructura	17
Estructura	17
Cabecera (Header).....	17
Datos (Data).....	19
Secuencia de control de trama (FCS).....	19
Tramas de control (control frames).....	19
ACK	20
PS-Poll.....	20
RTS/CTS.....	21
Tramas de Administración.....	24
Beacon (Trama Baliza)	25
Request (Petición)	26
Response (Respuesta)	27
Authentication (Autenticación).....	28
Association / Reassociation (Asociación / Reasociación)	29

Disassociate / Deauthentication (Desasociar / Deautenticación)	32
Atim	34
Action frames (tramas de acción).....	34
Data frames (tramas de datos).....	35
Data frames. Trama de datos	35
Null frame. Trama null.....	38
Interactuando con las redes	40
Probe	41
Probe request	41
Probe response.....	44
Autenticación	48
Autenticación abierta	48
Shared authentication. Autenticación compartida	51
Asociación.....	58
Encriptaciones	61
Redes abiertas	61
WEP. Wired Equivalent Privacy	68
WPA. Wi-Fi Protected Access	70
Algoritmos. Un pequeño vistazo	71
Conexión a la red	71
Hardware.....	78
Eligiendo hardware.....	78
Diferentes tipos de adaptadores.....	78
Ordenadores Portátiles	80
bB, dBm, dBi, mW, W	80
Antenas.....	81
Elegir una tarjeta	81
Antenas.....	83

Aircrack-ng en profundidad.....	88
Airmon-ng.....	88
Descripción.....	88
Uso.....	88
Ejemplos de uso.....	88
Usos típicos.....	88
Modo monitor de driver Madwifi-ng	88
Recomendaciones de uso.....	90
Ejercicios.....	90
Airodump-ng	91
Descripción.....	91
Uso.....	91
Pistas de uso.....	91
Sugerencias de optimización de uso	93
Problemas de uso	93
Ejercicios.....	94
Aireplay-ng	94
Descripción.....	94
Uso de los ataques.....	95
Uso.....	95
Ataque de Fragmentación vs. Chopchop.....	96
Sugerencias de optimización de uso	97
Problemas de uso	97
Aireplay se cuelga sin mostrar nada en pantalla.....	98
Write failed: Cannot allocate memory wi_write(): Illegal seek	99
Inyección lenta: "rtc: lost some interrupts at 1024Hz".....	99
Inyección lenta en general	99
Mensaje de error: "open(/dev/rtc) failed: Device or resource busy"	99

Mensaje de error: "Interface MAC doesn't match the specified MAC"	99
SSID oculto "<length: ?>"	100
Ataque 9 Aireplay – Test de inyección (Injection test)	100
Ataque 0 Aireplay – Deautenticación	104
Ataque 1 Aireplay – Falsa autenticación	105
Ataque Aireplay 2 – Reinyección de paquetes interactiva	110
Ataque Aireplay 3 – Inyección de tramas ARP	114
Ataque Aireplay 4 – KoreK chopchop	118
Ataque 5 Aireplay – Ataque de Fragmentación	123
Estoy inyectando pero los IVs no aumentan	126
Packetforge-ng	129
Trucos de uso	133
Problemas de uso	133
Prácticas	133
Aircrack-ng	133
Descripción	133
¿Cómo funciona?	134
Explicación de la profundidad (depth) y del Fudge Factor	135
Uso	136
Ejemplos de uso	137
WPA	140
Trucos de uso	141
Problemas de uso	143
Airdecap-ng	145
Uso	145
Ejemplos de uso	145
Recomendaciones de uso	145
Prácticas	145

Airtun-ng.....	145
Descripción	145
Uso.....	146
Escenarios.....	146
Inyección WEP	147
Inyección PRGA.....	147
Conectándose a dos puntos de acceso.....	148
Copiar paquetes desde la interface opcional	148
Prácticas	150
Wesside-ng.....	150
Descripción	150
Uso.....	151
Easside-ng.....	152
Estableciendo Conectividad	152
¿Qué papel juega el amigo servidor (buddy server)?.....	153
Comunicación con la red WIFI.....	153
Técnica de Fragmentación.....	154
Técnica de expansión linear del keystream.....	154
Easside-ng comparado con Wesside-ng	155
¿Porqué easside-ng cuando aircrack-ng tiene ptw?.....	155
Uso.....	155
Escenarios.....	156
Ejemplo de uso para el escaneo de APs	157
Prácticas	157
Airolib-ng	158
Descripción	158
Uso.....	158
Ejemplos de uso.....	159

Trucos de uso.....	163
Problemas de uso	163
Airserv-ng	163
Descripción	163
Uso.....	164
Ejemplos de uso.....	164
Problemas de uso	166
Airpwn	167
Tarjetas soportadas	167
Cómo funciona airpwn	167
Archivos de configuración de airpwn:	169
Kismet.....	170
Características de Kismet	170
Arquitectura de Kismet	170
Usando Kismet.....	171
Configurando Kismet.....	171
Iniciando kismet	171
Uso.....	172