Jackson State University
Department of Computer Science
CSC 437/539 Computer Security
Fall 2013
Instructor: Dr. Natarajan Meghanathan

Lab Project # 3: Simulating DHCP Snooping and DNS Cache Poisoning through a Man-in-the-Middle (MITM) Attack using Backtrack 5

Due: November 7, 2013: 7.30 PM

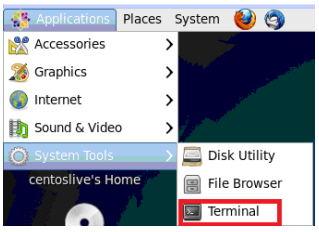
This project is for educational and awareness purposes only. We are not responsible for anyone using this project for any malicious intent. The objective is to understand how a system/network can be vulnerable to a man-in-the-middle (MITM) attack. We will explain the MITM attack in the context of DHCP Snooping. You will do this project in a virtual machine environment. You will need to download VMware Player which is the virtualization software that will be used for this project. You will also need to download CentOS and Backtrack 5 to complete this project.

Installing VMWare Player

Download the latest version (v.5 or v.6) of VMware Player for your Operating System from https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/5_0

Downloading and Installing CentOS

1. Download CentOS (CentOS-6.4-i386-LiveCD.iso) http://centos.icyboards.com/6.4/isos/i386/ and save it somewhere on your computer
2. Open up VMWare Player
3. Click on **Create a New Virtual Machine**
4. Select Installer disc image file (iso): browse for your CentOS .iso file and click **Next**
5. For Guest Operating System, choose Linux --> CentOS (**do not choose** CentOS 64-bit): we are using x86 version. Click **Next**. Give the VM - the name you want.
5. On the next page, select **Store virtual disk as a single file**, and click **Next**.
6. Click **Finish** on the next page.
7. Now Select CentOS from the VM Player menu and click **Play Virtual Machine.** Go through the OS installation process.
8. You can setup automatic login without requiring a password. If you wish to setup a password, you could also do so. You should be now logged into the CentOS system.
9. Click the **Player** menu, and go to **Manage** then **Virtual Machine settings.**
10. When the settings come up, make sure that the **Network Adapter** is set to **NAT**, and click **OK**.
11. Launch a terminal from the Applications --> System --> Terminal menu.

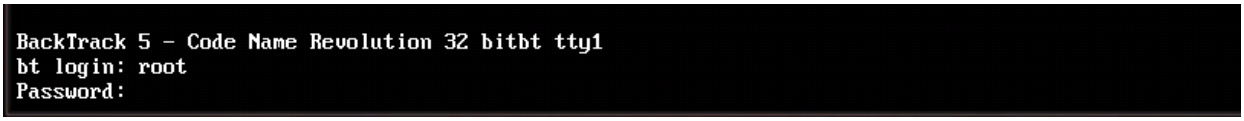


Downloading and Installing Backtrack 5

1. Download **Backtrack 5** (**not** Backtrack 5 R1, R2, or R3) from
http://www.backtrack-linux.org/downloads/

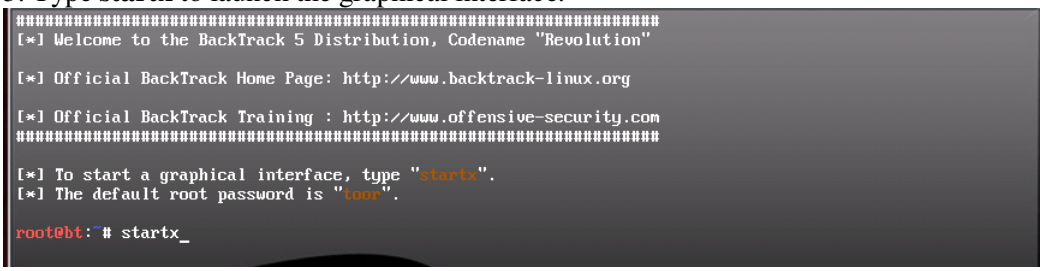
Download the GNOME 32-bit version .iso file, directly to a location in your physical host.
Then create a virtual machine instance of the Backtrack system on the VMWare Player. Choose the Guest Operating System to be Linux - Version: Other Linux 2.6.x kernel. Name the VM as **Backtrack-5.** You could set up the RAM to 512 MB or higher, as feasible for your host machine. The rest of the installation steps should be similar to that you went through for the CentOS VM.

2. When the VM starts, press enter in a black screen where is says **boot:** and press enter again to boot in text mode (the first option) when the Backtrack boot menu appears. If you are not already logged in as root, type in **root** for username and **toor** for password.

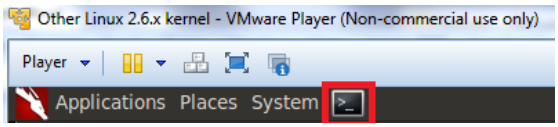


Note: You may need to press **Ctrl+Alt** when you need to bring your mouse pointer out of the Backtrack 5 virtual machine.

3. Type **startx** to launch the graphical interface.



4. You could launch a terminal by clicking the top >_ terminal icon.



6. Click the **Player** menu, and go to **Manage** then **Virtual Machine settings**.

7. When the settings come up, make sure that the **Network Adapter** is set to **NAT**, and click **OK**.

8. If Wireshark is not installed in your Backtrack VM, we will first install **Wireshark.** On your Backtrack VM, open a terminal by clicking the top >_ terminal icon.

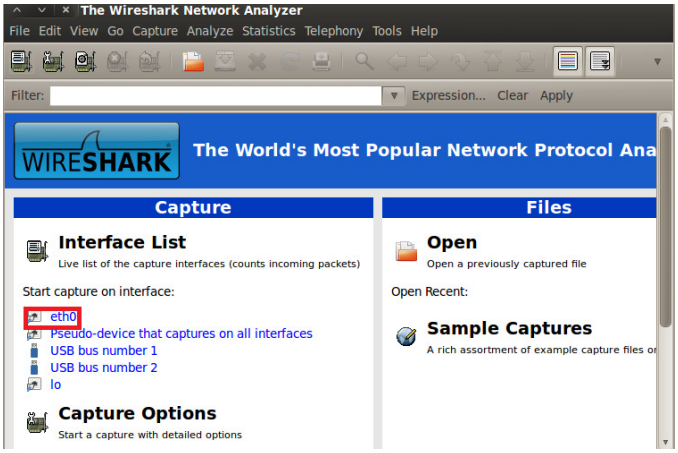
You need to have 'super-user' root access to install and run wireshark. You need to set a root password using the 'sudo passwd root' command. It may ask for a password (if you had setup one at the time of installing your Backtrack VM). Or (as shown in the screenshot below), you may be directly prompted to select a UNIX password, enter a password of your choice and confirm that. Make sure your UNIX root password can be easily remembered (but difficult to be guessed!!).

```
root@root:~# sudo passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@root:~#
```

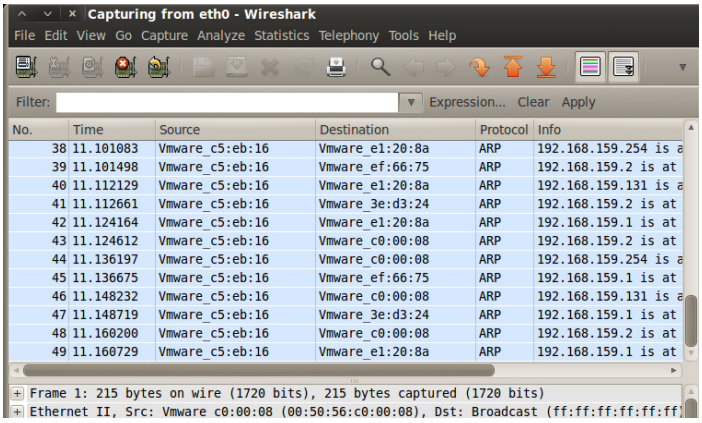
Now, login as root by running the command ‘su root’. You may be prompted to enter the root password that you selected just now.

Now, run the **sudo apt-get install wireshark** command to install wireshark. Depending on the case, it may sometimes say Wireshark is already installed in your system and there is no more updates to it.

After Wireshark is installed, run **sudo wireshark** to launch the wireshark program. You should see the wireshark frontend GUI as below. Discard the warning message that may appear with regards to running wireshark as root user and under group root.



5. Now, click the **eth0** line on the Wireshark screen (marked in the screenshot above) and launch the packet capture window. You may already see some packets captured (as seen in the screenshot below).



Understanding DHCP and DNS

Steps and Tasks

1. In your CentOS terminal, type **su root** and press enter, to become root. If you do not have root access, you would be required to setup a root access using the **sudo passwd root** command. After you setup root access or if you already have root access, your role will be automatically changed to a root user when you run the **su root** command (like in the screenshot below).

```
[centoslive@livecd ~]$ su root
[root@livecd centoslive]#
```

2. Now, type **cd ..** and press enter. Do it one more time. Now, you are in the root folder. Then type **cd var/lib/dhclient**. In the dhclient folder, you would see a DHCP file that has an extension **.lease**. Look for files in the directory by typing the **ls** command.

Task 1: 3. Print the contents of the .lease file using the **cat** command, along with the name of the .lease file (screenshot shown below in my case). **Identify the IP address of the CentOS VM, the DHCP server and DNS server.** In my case, as indicated in the screenshot, the IP address of the CentOS VM is 192.168.159.132; the IP address of the DHCP server is 192.168.159.254 and the IP address of the DNS server is 192.168.159.2. You may observe different IP address(es) for each of them in your case.

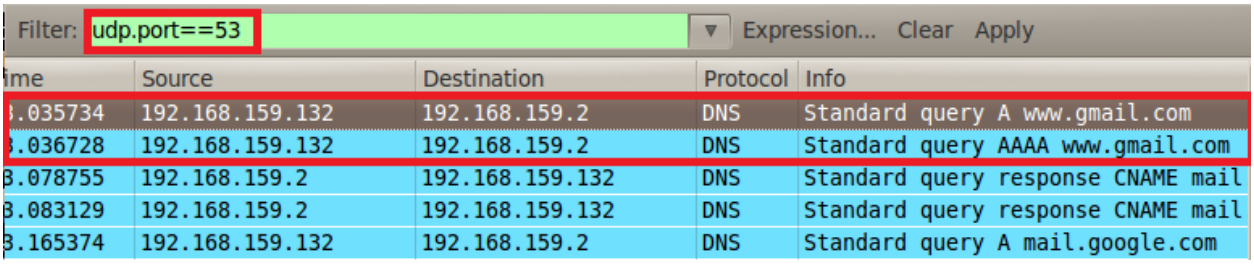
```
[root@livecd /]# cd var/lib/dhclient
[root@livecd dhclient]# ls
dhclient-daa8a8b6-5b1d-4e64-ae60-28ed44242932-eth0.lease
[root@livecd dhclient]# cat dhclient-daa8a8b6-5b1d-4e64-ae60-28ed44242932-eth0.l
ease
lease {
  interface "eth0";
  fixed-address 192.168.159.132;
  option subnet-mask 255.255.255.0;
  option routers 192.168.159.2;
  option dhcp-lease-time 1800;
  option dhcp-message-type 5;
  option domain-name-servers 192.168.159.2;
  option dhcp-server-identifier 192.168.159.254;
  option broadcast-address 192.168.159.255;
  option domain-name "localdomain";
  renew 1 2013/05/20 07:41:37;
  rebind 1 2013/05/20 07:53:16;
  expire 1 2013/05/20 07:57:01;
}
[root@livecd dhclient]#
```

DHCP (Dynamic Host Configuration Protocol): Hosts in a network are assigned either static or dynamic IP addresses. A static IP address stays the same with the machine every time it boots. On the other hand, a dynamic IP address is an IP address that a host leases from the DHCP server. After a machine boots up, it contacts the DHCP server and requests for an IP address; the DHCP server maintains a pool of available IP addresses and assigns an available IP address from this pool.

DNS Server: The Domain Name Server (DNS) is the server contacted by a local host when it needs to resolve the domain/host name (say, a website address) of a host whose IP address it does not know. This, typically happens when you visit a website for the first time or after a long time from your computer. Your computer maintains a DNS cache storing the IP addresses of the recently contacted domain/host

names. When it could not find such a mapping in its DNS cache for the website you want to visit, the computer contacts the DNS server (that typically maintains a longer list of domain names - IP addresses) to obtain the mapping. If the local DNS server does not know the mapping, it contacts the DNS servers in the Internet (there is a hierarchy of DNS servers in the Internet, all the way to the backbone) until one of them responds with the appropriate IP address, if the domain/host name is a valid one. Hence, it is important for a host to know the correct IP address of the DNS server in order to contact the latter to resolve any domain/host name.

Task 2: 4. With Wireshark running in your Backtrack VM, launch the Firefox web browser in your CentOS VM and visit a website that you have not yet visited from the VM. If you have just installed the CentOS VM, you could basically visit any website. Now, go back to the Wireshark screen in the Backtrack VM and **stop** packet capture by selecting the **Capture** menu. Now, type **dns** on the filter field. [As an alternative, as shown in the screenshot, you could also use **udp.port==53** as a filter, where 53 is the port at which DNS runs]. You could see one or more packets exchanged between the CentOS VM and the DNS server (in my case, between the IP addresses 192.168.159.132 and 192.168.159.2 representing the CentOS VM and DNS server respectively, as shown in the screenshot below when I visited www.gmail.com for the first time from the VM). Capture a screenshot of the DNS packets in Wireshark.



You can then close the packet capture window by clicking the X button on the top of the screen as marked in the screenshot below. You do not need to save any packets. So, select the first option of *continuing without saving*.

Task 3: We can similarly see how the CentOS VM interacts with the DHCP server. In this pursuit, we will execute the following steps in this order (make sure you are a root user in the CentOS VM terminal):

5. Make the CentOS VM to release its IP address by executing the command **ifconfig eth0 down** in the terminal. [Note that eth0 (eth followed by number 0) is the name of the interface]

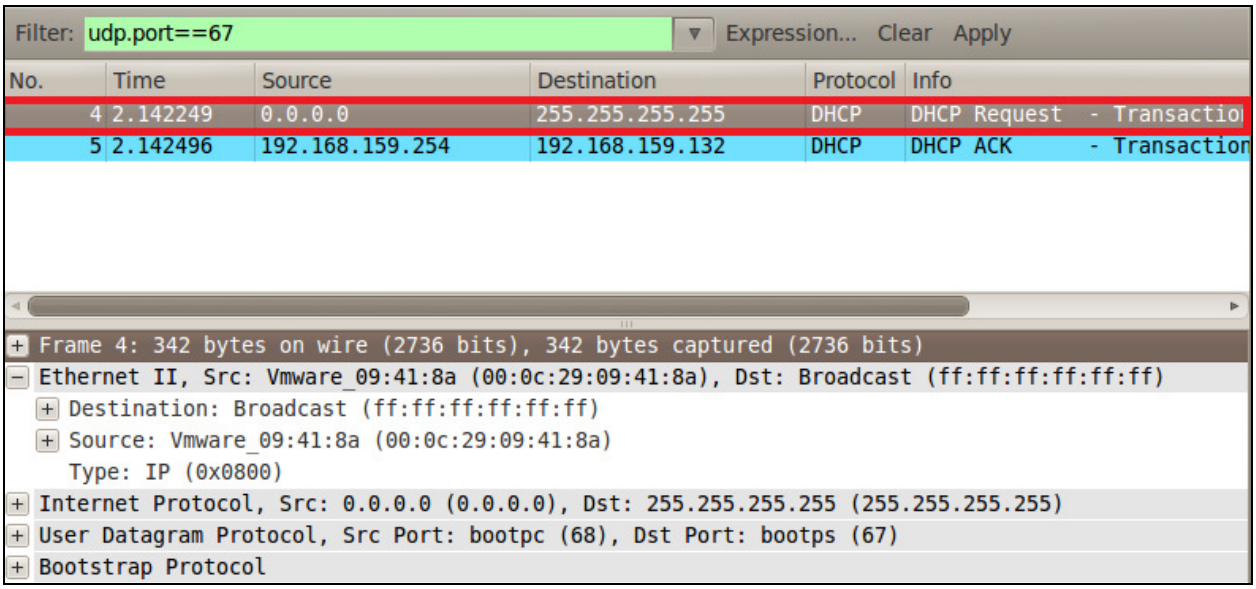
6. Start the Wireshark packet capture in the Backtrack VM.

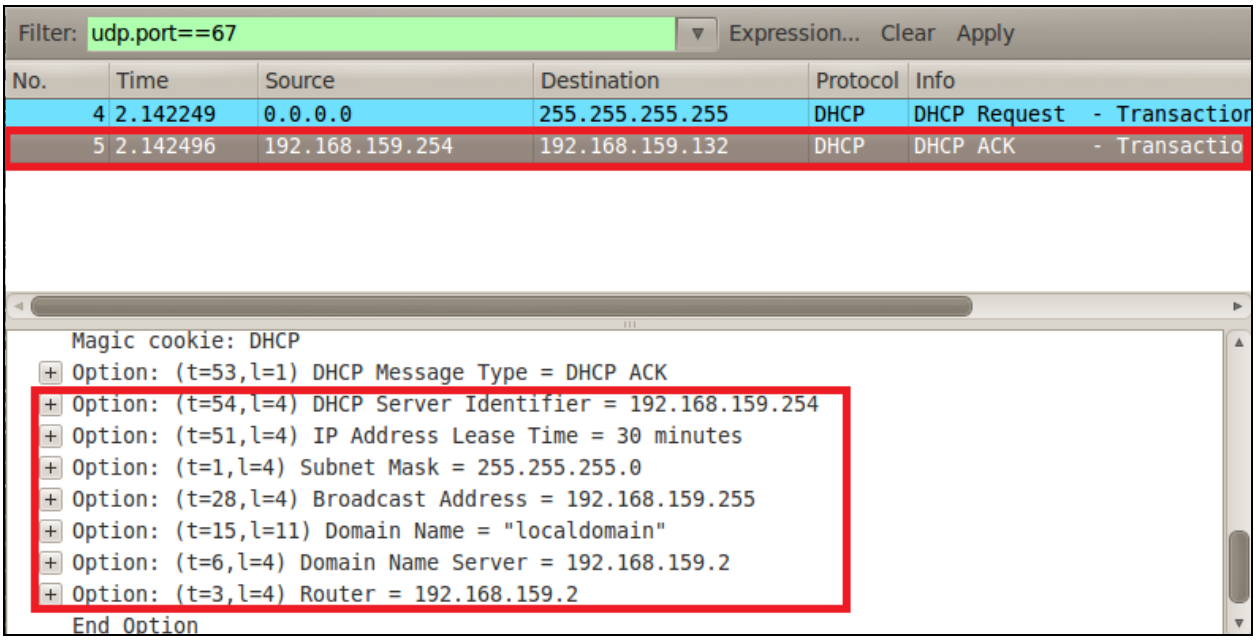
7. Run the command **ifconfig eth0 up** in the CentOS terminal.

8. The Wireshark packet capture screen will now be updated with several packets. When you observe there are no more packets added to the screen, **Stop** the Wireshark packet capture in the Backtrack VM and filter the packets by typing **udp.port == 67** as the filter, where 67 is a port number associated with DHCP. You could see that the CentOS VM did a DHCP Request broadcast looking for a DHCP server and the DHCP server picked up the request (in my case, the IP address of the DHCP server is 192.168.159.254) and responded with an IP address (192.168.15.132) that the CentOS VM can basically own on a lease basis. In the screenshot below, frame 4 corresponds to the DHCP Request packet broadcast by the CentOS VM at the network level; frame 5 is the ACK/response from the DHCP server assigning the dynamic IP address to the CentOS VM. We can also see that the DHCP response contains

critical details such as the IP addresses of the DNS server, the gateway router, the broadcast IP address and the IP address of the DHCP server itself.

Likewise, capture screenshots in your case, for the DHCP Request and DHCP ACK showing the details, similar to the one seen in the screenshots below.





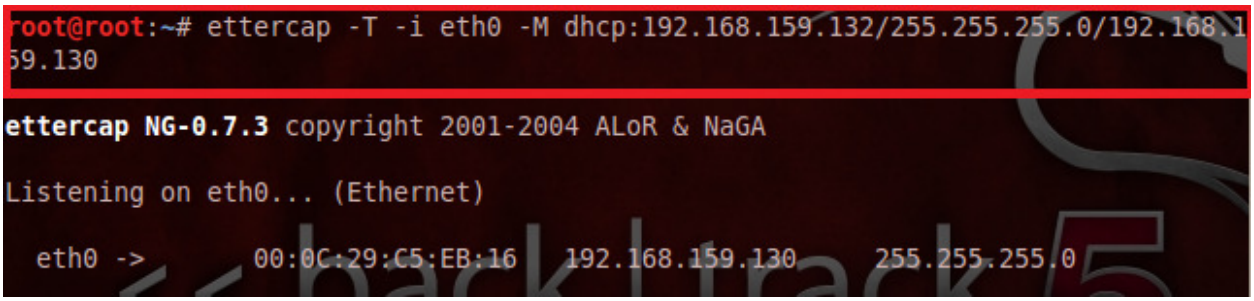
Simulating the DHCP Snooping and DNS Cache Poisoning Attack

The DHCP Snooping attack is a kind of Man-in-the-middle (MITM) attack in which a host (under the control of the attacker) listens to the network in promiscuous mode and responds to the DHCP Request of a victim host with a DHCP ACK that contains a leased IP address (assigned of the attacker's choice) as well as wrong DNS server and gateway router addresses (the IP address of the attacker/intruding host is informed to be IP address for the DNS server and gateway router so that all packets from the victim host reach the attacker, which may either drop them or forward further).

In our simulations in this project, the victim is the CentOS VM; the attacker is the Backtrack VM and we will also run the Wireshark on the Backtrack VM to capture the packets.

Task 4:

9. Open a new terminal in the Backtrack VM (make sure you are the root; if needed, run the **su root** command to become the root user), and type the following **ettercap** command in text mode (note that ettercap is the program that we will use to simulate the DHCP Snooping/MITM attack), as shown in the screenshot below. As indicated in the screenshot, I am making the ettercap program to be assigned the expected IP address of 192.168.159.132 (same IP address that was assigned in the earlier section - Step 7 under Task 3 - when there was no MITM attack, so that no suspicion arises to the user working on the victim host), the subnet mask of 255.255.255.0 and the DNS server IP address to that of the Backtrack VM itself (in my case, the Backtrack VM is assigned the IP address 192.168.159.130). Likewise, for your project, you need to pass the IP address that got assigned to the CentOS VM when you did the previous section (Task 3/Step 7) and pass the IP address of your Backtrack VM (you can run the **ifconfig** command on another Backtrack terminal to find out the IP address assigned to your VM) to be the DNS server IP address for the ettercap command. Include appropriate screenshot in your documentation.



After launching the ettercap command, your Backtrack VM starts running in promiscuous mode. Let the ettercap command to run till the end. After you are done with all your steps, you can press Ctrl + C and stop the command.

You can open another terminal in the Backtrack VM to be used for launching the Wirehsark analyzer.

Execute the following sequence of actions (Steps 10 through 13), in the order specified below:

IMPORTANT: Note that the DHCP Snooping attack need not be always successful because of the race factor involved. That is, the genuine DHCP Server (in my case, it is 192.168.159.254) will also respond (with an IP address in the ACK; in my case, it is expected to be 192.168.159.132) to the DHCP Request. The requesting host will accept the first DHCP ACK received. So, there are good chances that the DHCP ACK from the genuine DHCP Server reaches the targeted victim - the CentOS VM.

So, in order to successfully, simulate this attack, you may have to perform steps 9 through 15 several times, until you are able to successfully launch the attack. **As part of your report documentation, write the number of times you had to try.** In my case, I got it working in the second attempt.

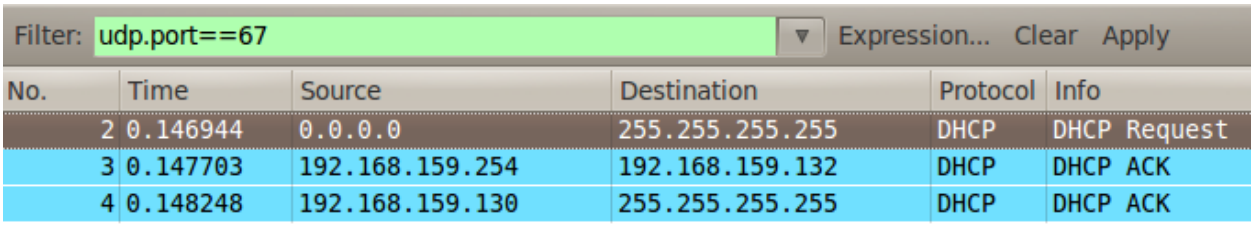
10. Make your CentOS VM to release its IP address using the command **ifconfig eth0 down**

11. **Start** Wireshark (**sudo wireshark** from a terminal in the Backtrack VM) and initiate packet capture on interface eth0 by clicking on the text.

12. As the ettercap program is running (waiting for a DHCP Request), go to the CentOS VM and run the command **ifconfig eth0 up**.

Task 5:

13. **Stop** the Wireshark packet capture and filter using **udp.port == 67**. If the DHCP ACK from the genuine DHCP Server reaches the victim ahead of the ACK from the MITM attacker (as shown in the screenshot below), then we need to continue steps 9 through 13 again. You can even check that the targeted victim's DNS cache is not corrupted by trying to visit any website by opening the Firefox web browser on the CentOS VM. Show the screenshots as part of your documentation.



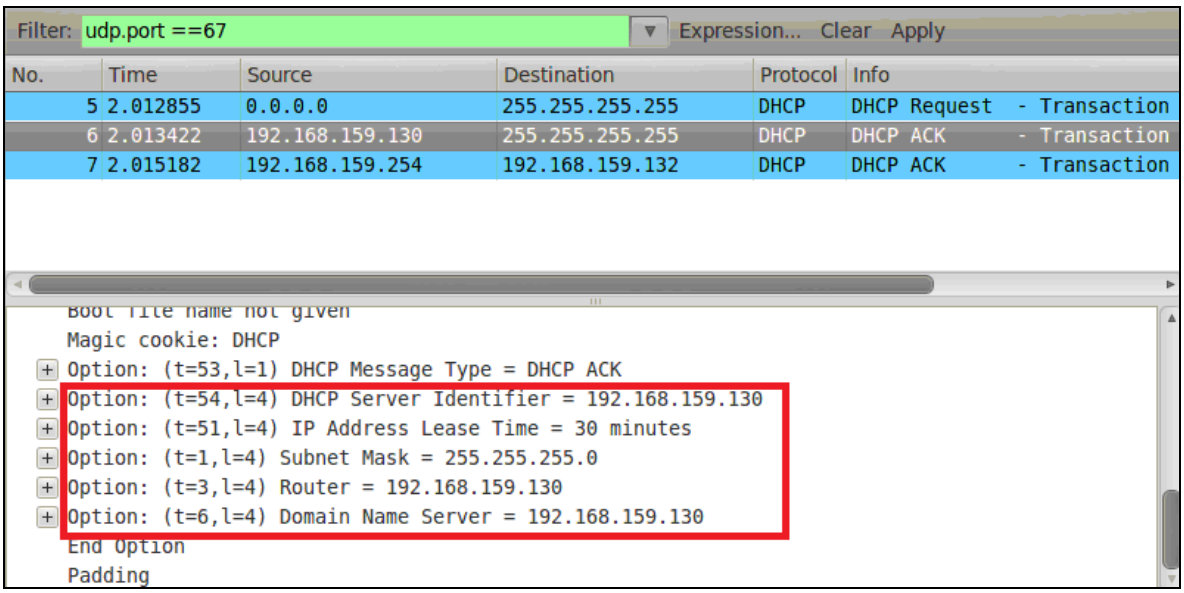
If the DHCP ACK from the MITM attacker (in my case, from IP address 192.168.159.130) reaches the victim ahead of the ACK from the genuine DHCP Server (in my case, the IP address of the genuine DHCP server is 192.168.159.254), as shown in the screenshot below, then it means that you have successfully launched the DHCP Snooping/MITM attack. Include appropriate screenshots for your case.

You can further validate it by attempting to visit a website of your choice on the CentOS VM and you will not be able to visit. You will get an error message telling that the website could not be loaded/visited.

What is the reason that you cannot visit a website when the DHCP Snooping attack was successful?

Clearly indicate the IP addresses of your Backtrack VM, the genuine DHCP Server, the genuine DNS Server, the IP address expected/assigned to the victim and the IP addresses of the DHCP Server and DNS Server perceived by the victim.

14. Stop the ettercap program in the terminal of the Backtrack VM by pressing Ctrl + C.



To restore back the normal working of the CentOS VM, just reboot the machine.

What to Submit:

Video: Record a video of your execution of Tasks 4 and 5. Note that Task 5 may have to be executed several times until you are able to successfully launch the MITM attack. Let your video be recorded for all these trials. For each trial, you should also show the DHCP packets captured in Wireshark at the Backtrack VM as well as your attempts to visit a website from the CentOS VM.

You could try using one of the following **desktop recording software** (or anything of your choice):
CamStudio: http://sourceforge.net/projects/camstudio/files/legacy/
Debut: http://www.nchsoftware.com/capture/index.html

Upload your video to GoogleDrive or Dropbox and share it with my email address: natarajan.meghanathan@jsums.edu

Hard copy of the report: (1) Provide appropriate answers and screenshots under the tasks 1 through 5 listed in the project description. Also, provide answers for the questions in bold under Tasks 4 and 5. (2) Provide a summary (of at least 300 words) of what you understood from this project.

Submit a hard copy of the report in class on the due date/time as well as ***e-mail*** me.