Introduction

The **Network Vulnerabilities** module provides you with the instruction and Server hardware to develop your hands on skills in the defined topics. This module includes the following exercises:

1) Network Footprinting

2) Packet Sniffing

3) MitM with ARP Spoofing

4) Denial of Service

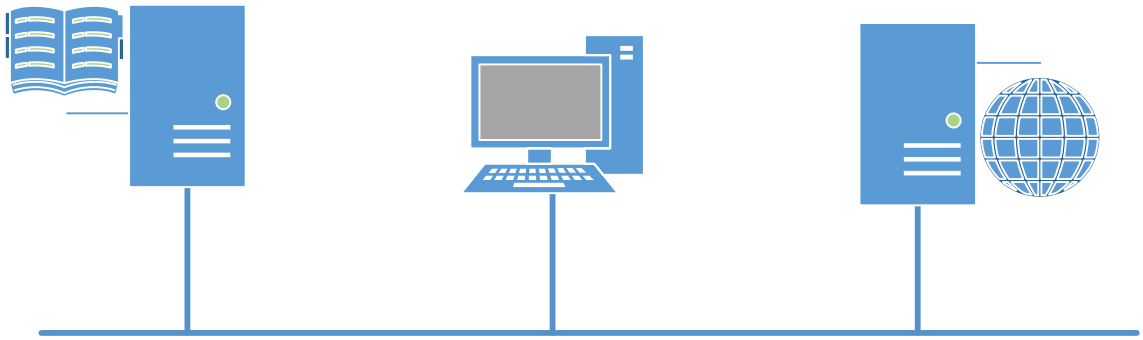
Lab Diagram

During your session you will have access to the following lab configuration.

SERVER1
(Domain Controller)
192.168.0.1 /24

CLIENT1
(Windows XP Workstation)
192.168.0.2 /24

BackTrack Server



Connecting to your lab

In this module you will be working on the following equipment to carry out the steps defined in each exercise.

- SERVER1 (Domain Controller)
- CLIENT1 (XP Workstation)

Each exercise will detail which console you are required to work on to carry out the steps.

To start simply click on the named Server from the device list (located on the left hand side of the screen) and click the **Power on** from the in tools bar. In some cases the devices may power on automatically.

During the boot up process an activity indicator will be displayed in the name tab:

- Black - Powered Off

- Orange - Working on your request
- Green - Ready to access

If the remote console is not displayed automatically in the main window (or popup) click the **Connect** icon located in the tools bar to start your session.

If the remote console does not appear please try the following option:

- Switch between the HTML 5 and Java client versions in the tools bar.

In the event this does not resolve your connectivity problems please visit our Help / Support pages for additional resolution options.

Copyright Notice

Exercise 1 - Network Footprinting

In this lab, you will practise attack strategies such as footprinting, spoofing, and Denial of Service.

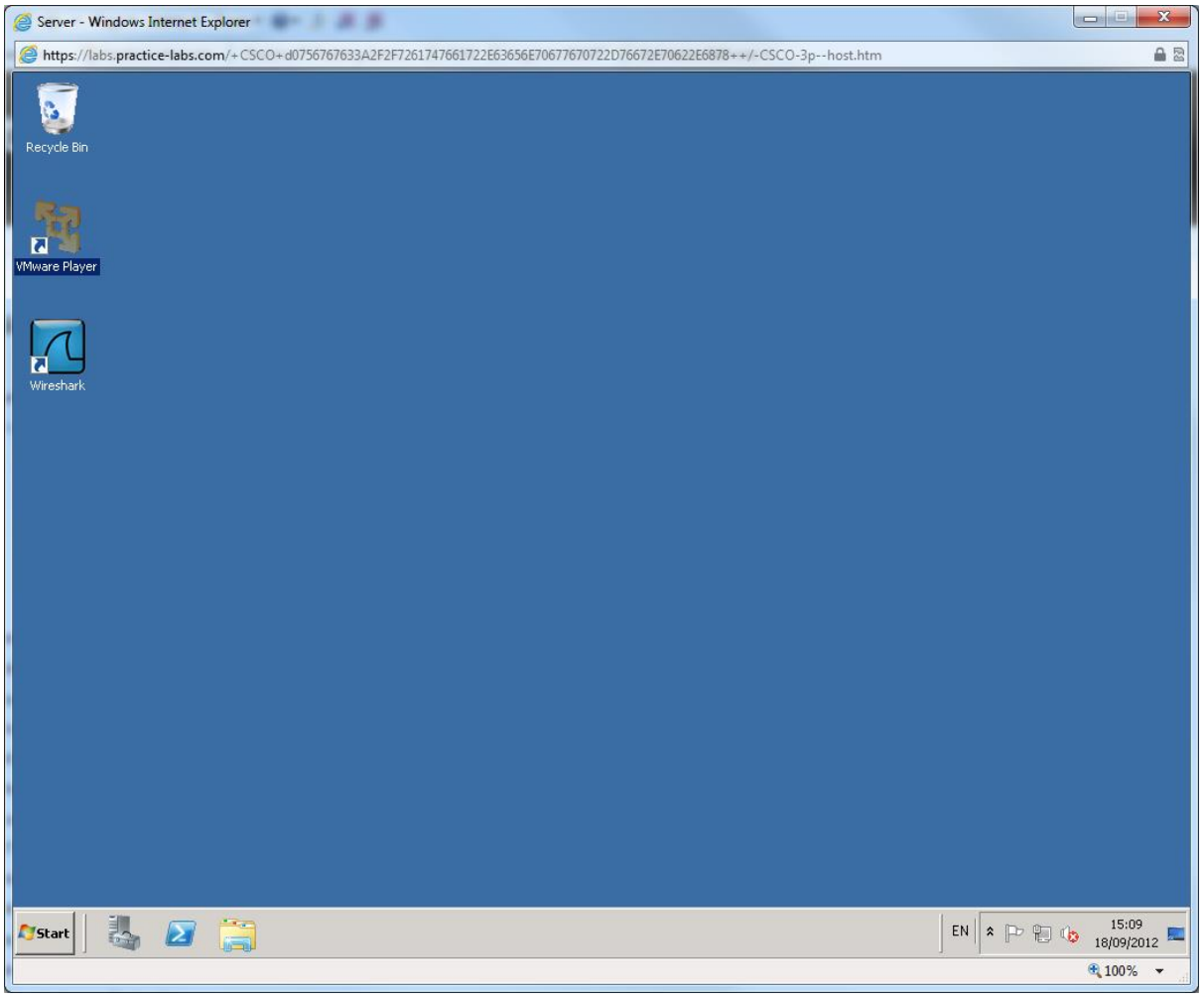
A network scan is usually the first step in an attempt to penetrate security (or indeed to establish what needs defending). Footprinting establishes the topology and protocols deployed on the network while fingerprinting determines the services and other configuration details of a target host.

One of the most popular scanning tools in nmap. This is a command-line program operated using scripts. A GUI version (Zenmap) can perform several very useful pre-configured scans though.

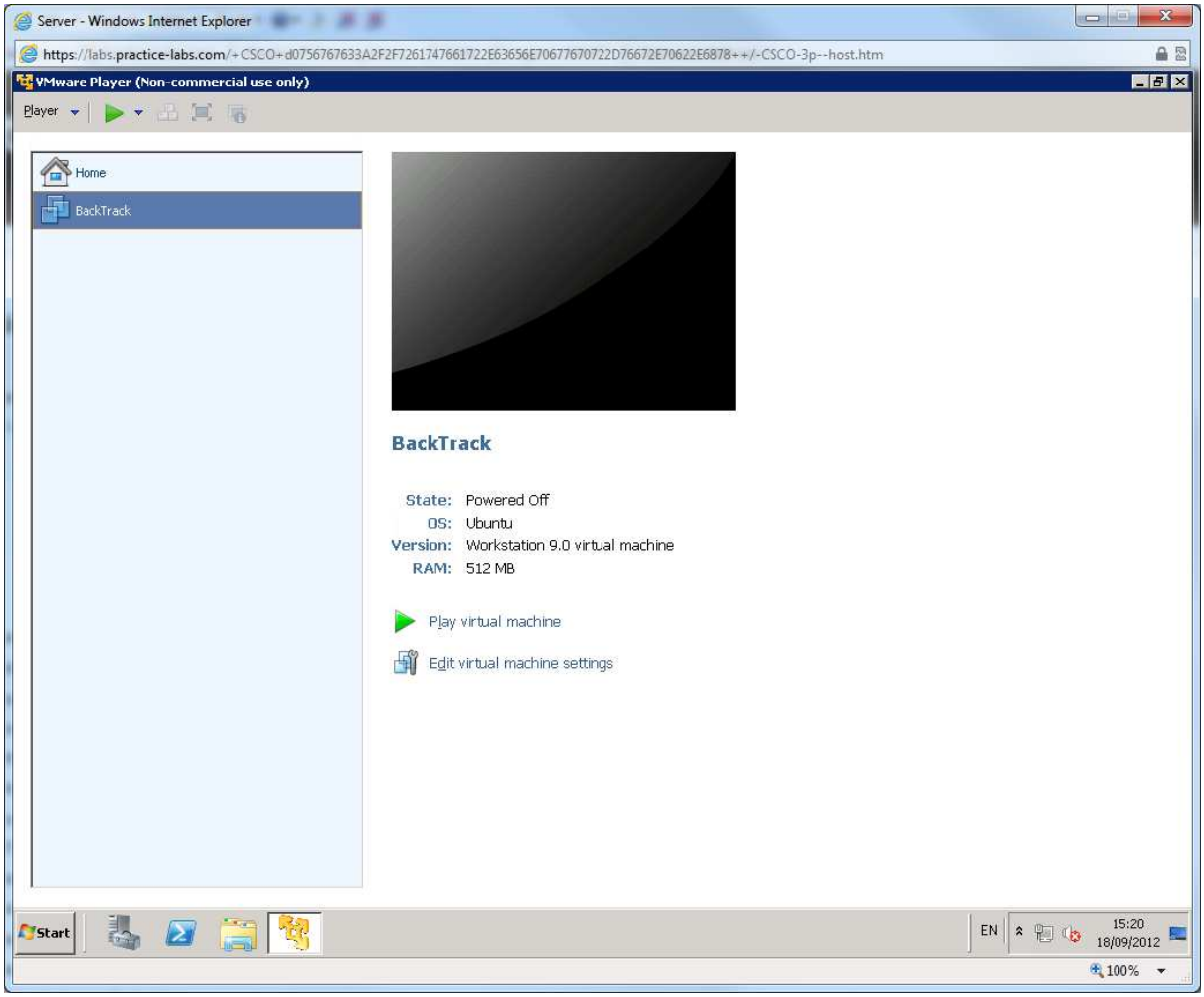
From the Practice-Lab application power on the **Server, and Client** devices.

Select the "**Connect**" button when it becomes available to logon to **Server**.

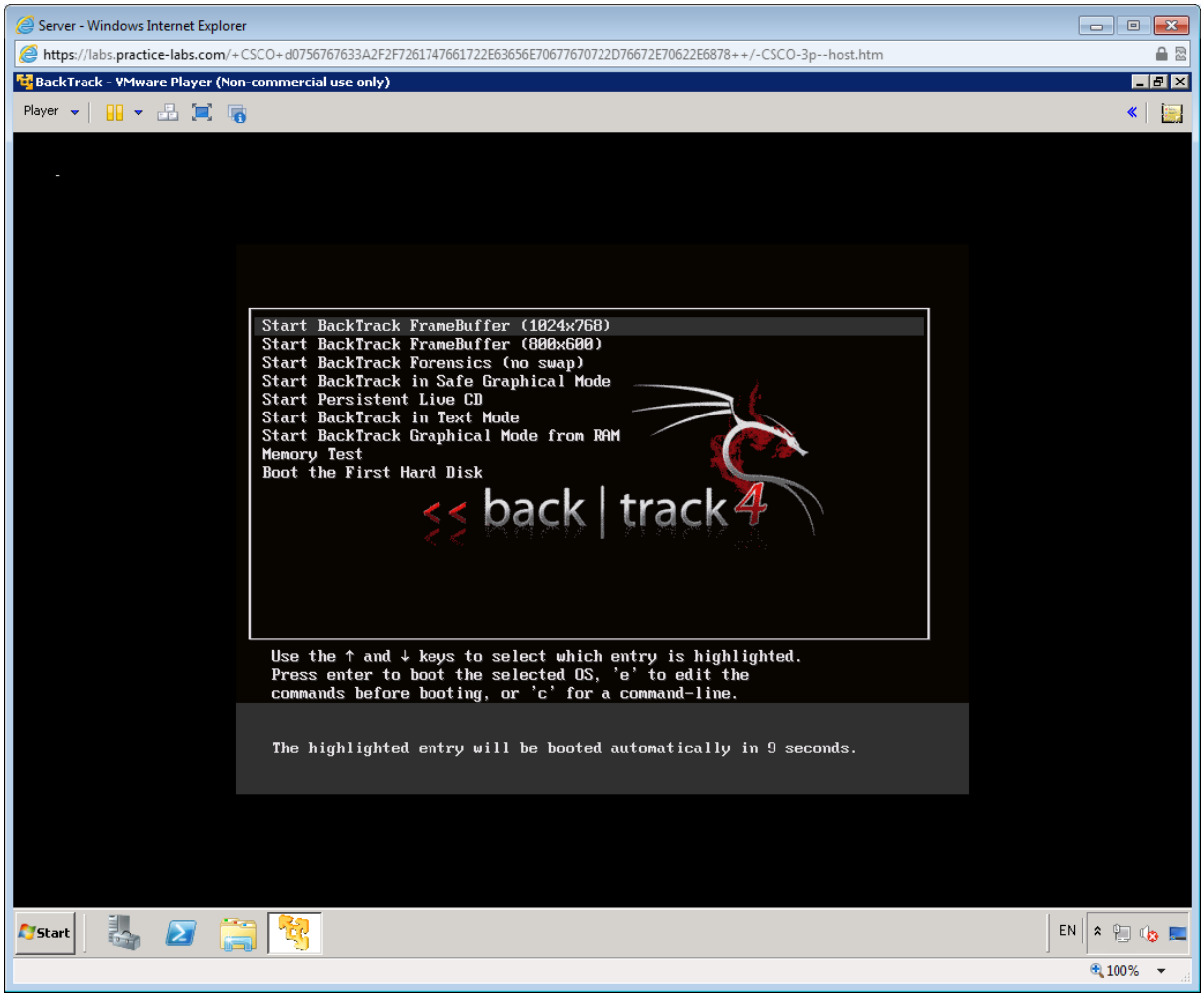
Once you have logged in double click on the **VMware Player** icon located on the desktop.



Double click the **BackTrack** icon to start the server.



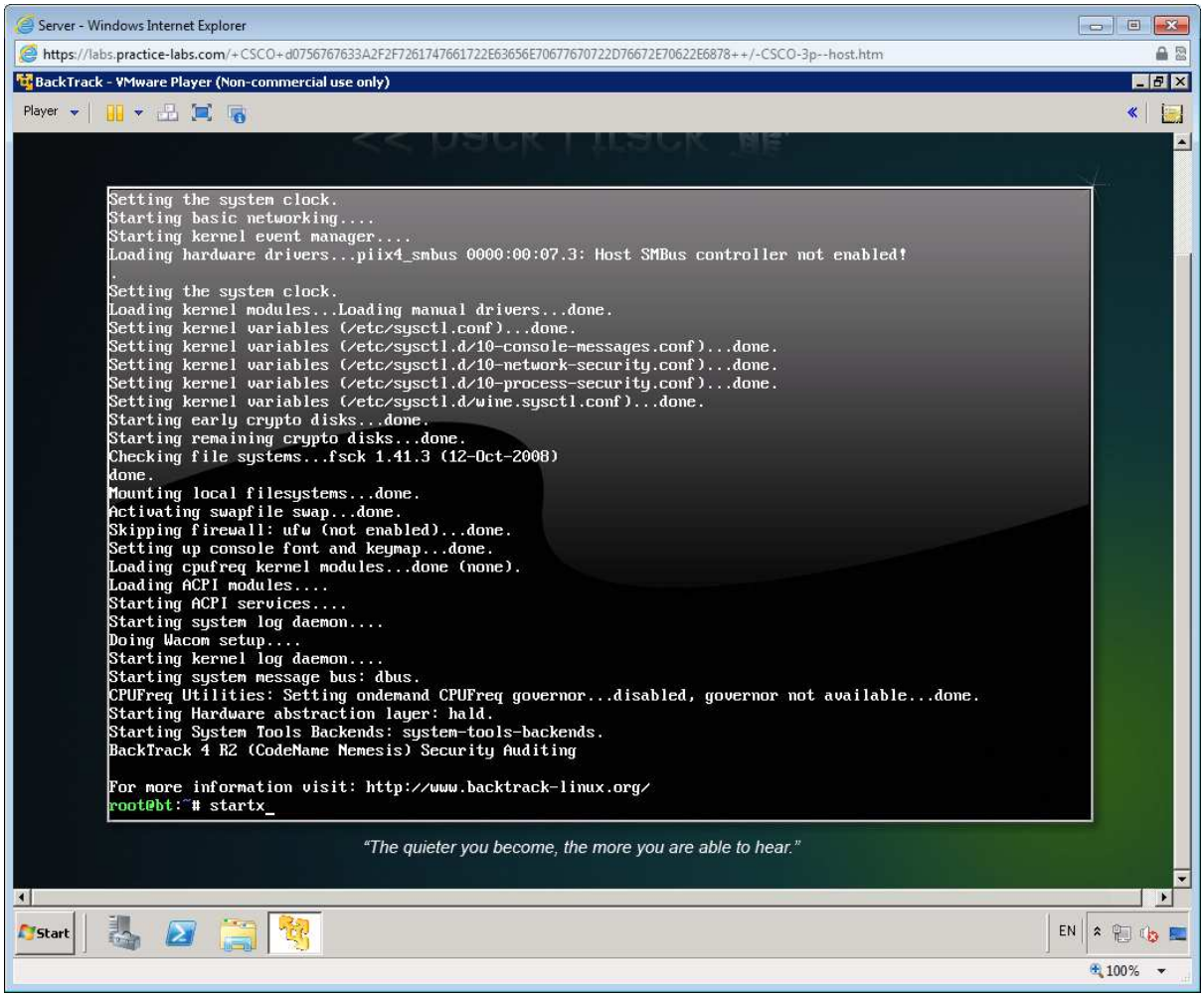
Click in the Black window and Press **Enter** to select the default graphics mode (or use the **Arrow** key to select 800x600 if you have a low resolution display).



When Backtrack has booted, type the following at the # prompt

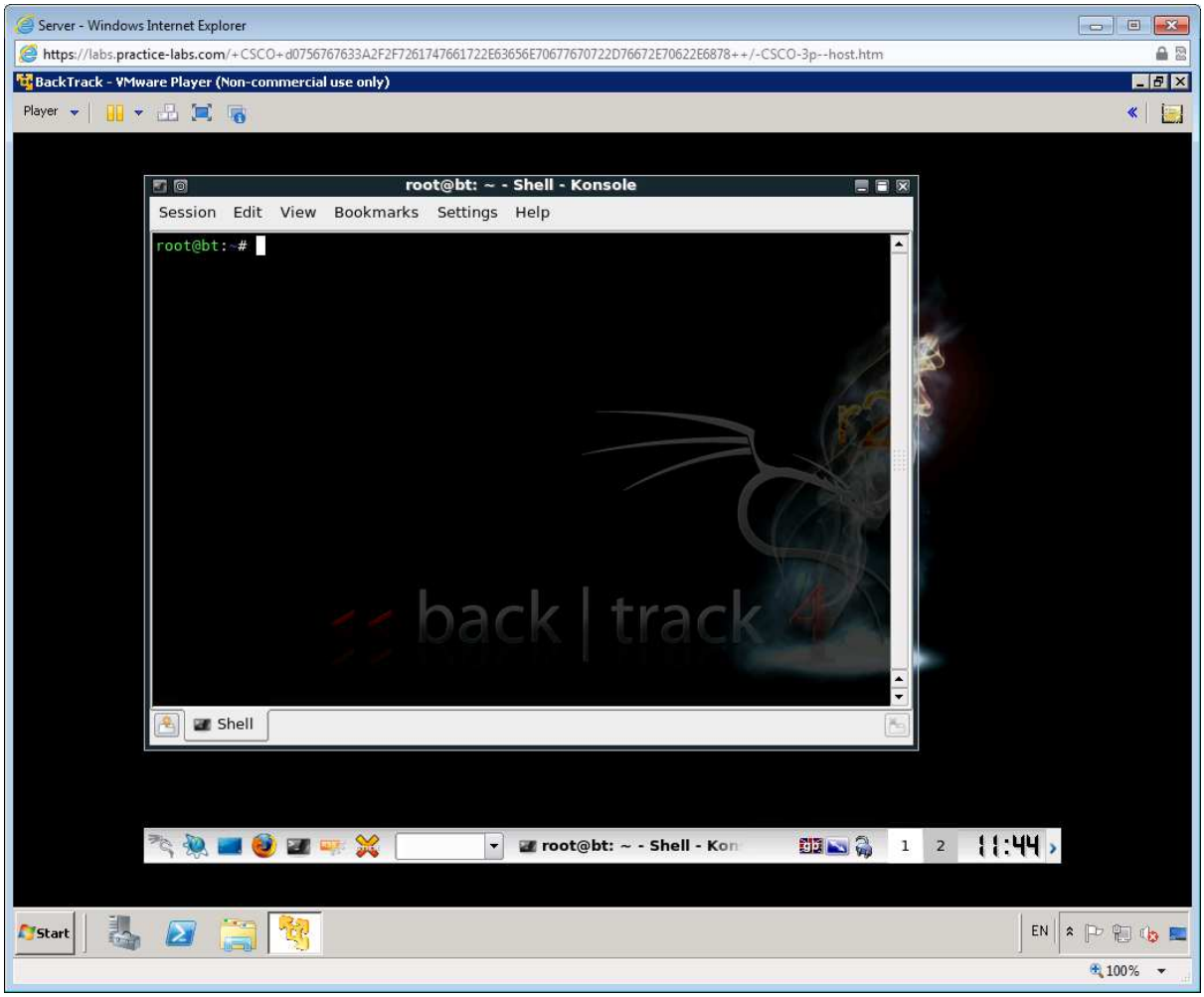
startx

Press Enter to load the GUI.



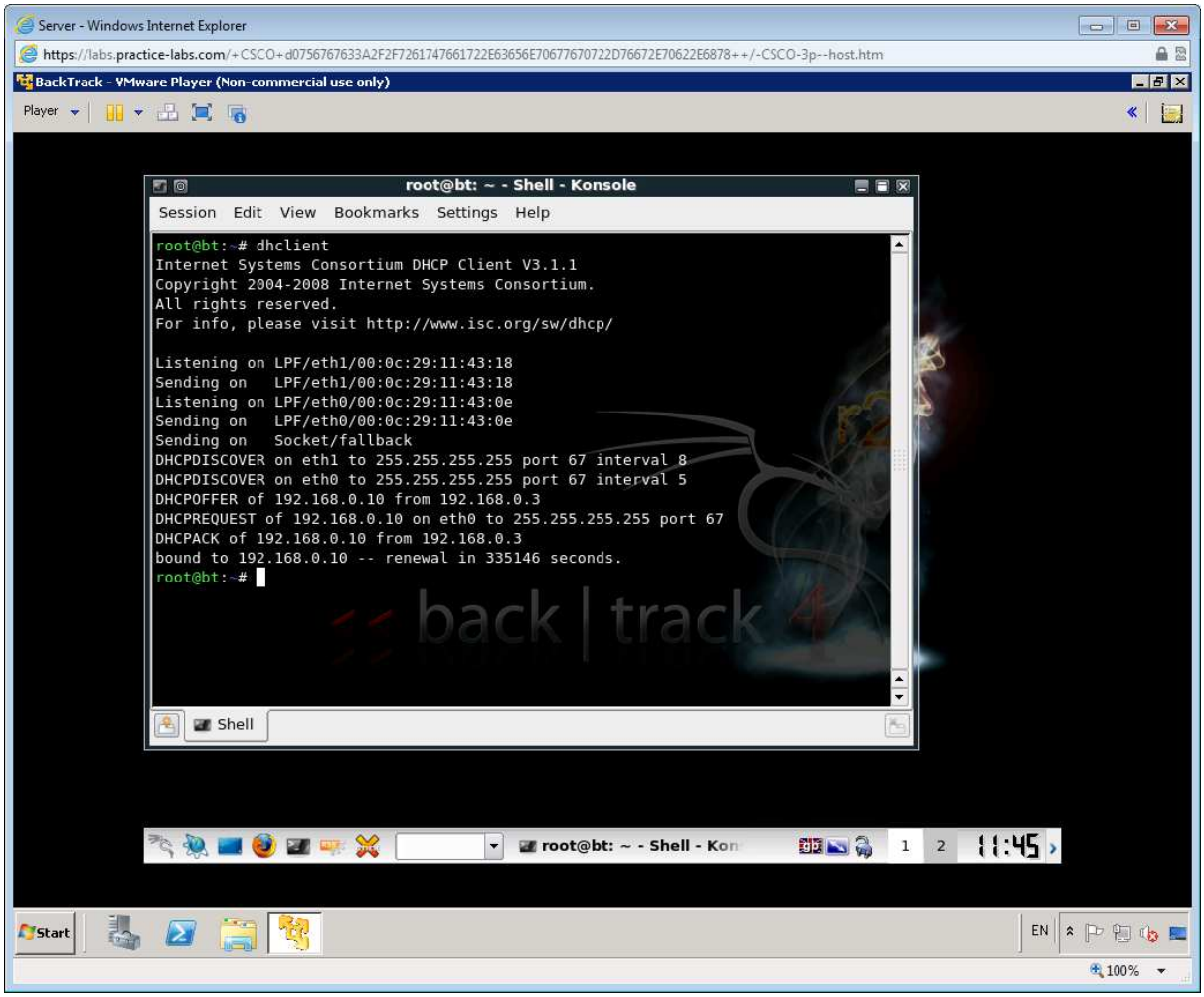
Right-click the flag icon on the taskbar to select the appropriate regional keyboard layout and settings.

Click the Konsole icon to open a command shell.



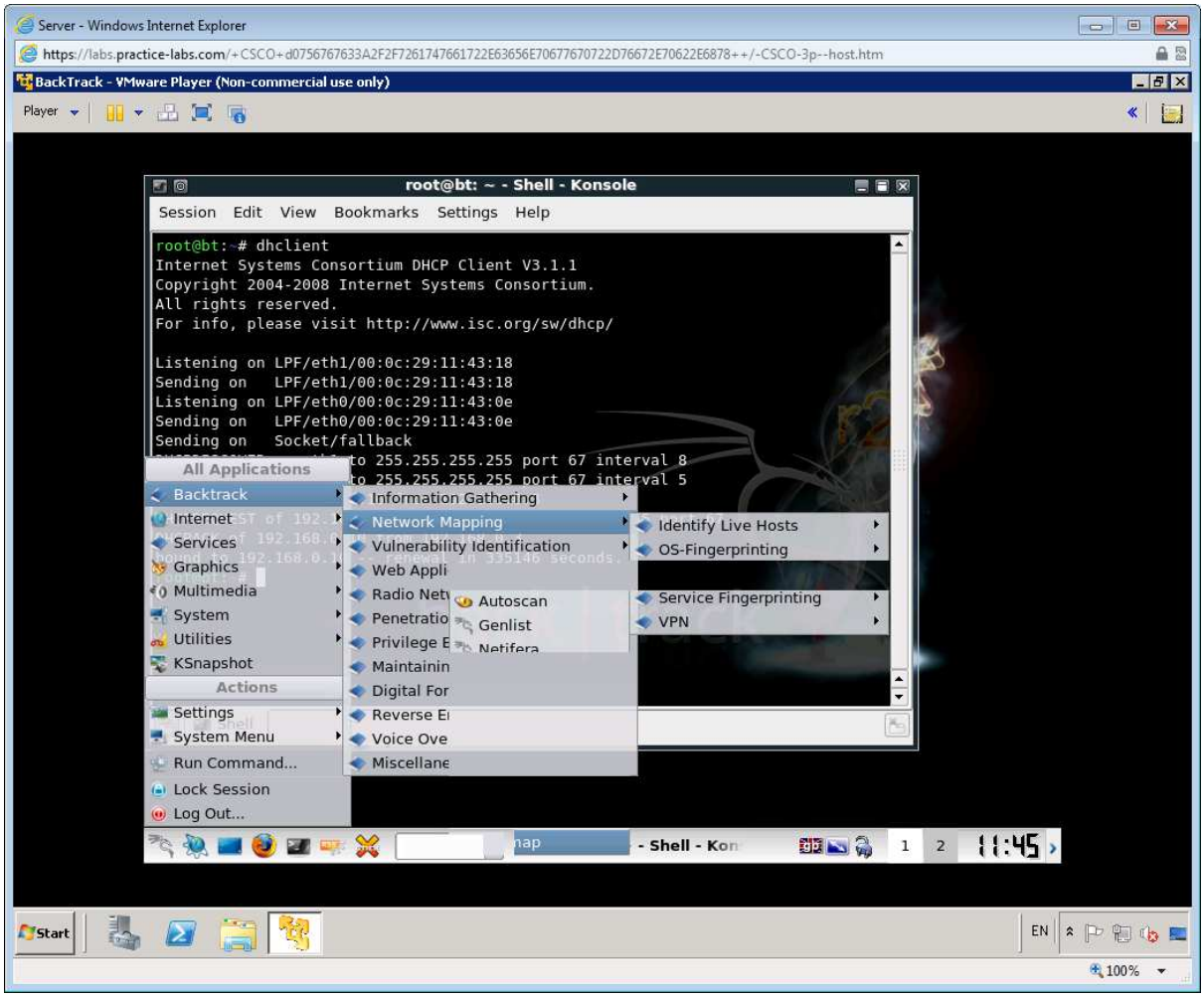
To connect the BackTrack Server to the same network as the CLIENT machine (using the DHCP server on SERVER), enter the following command:

dhclient

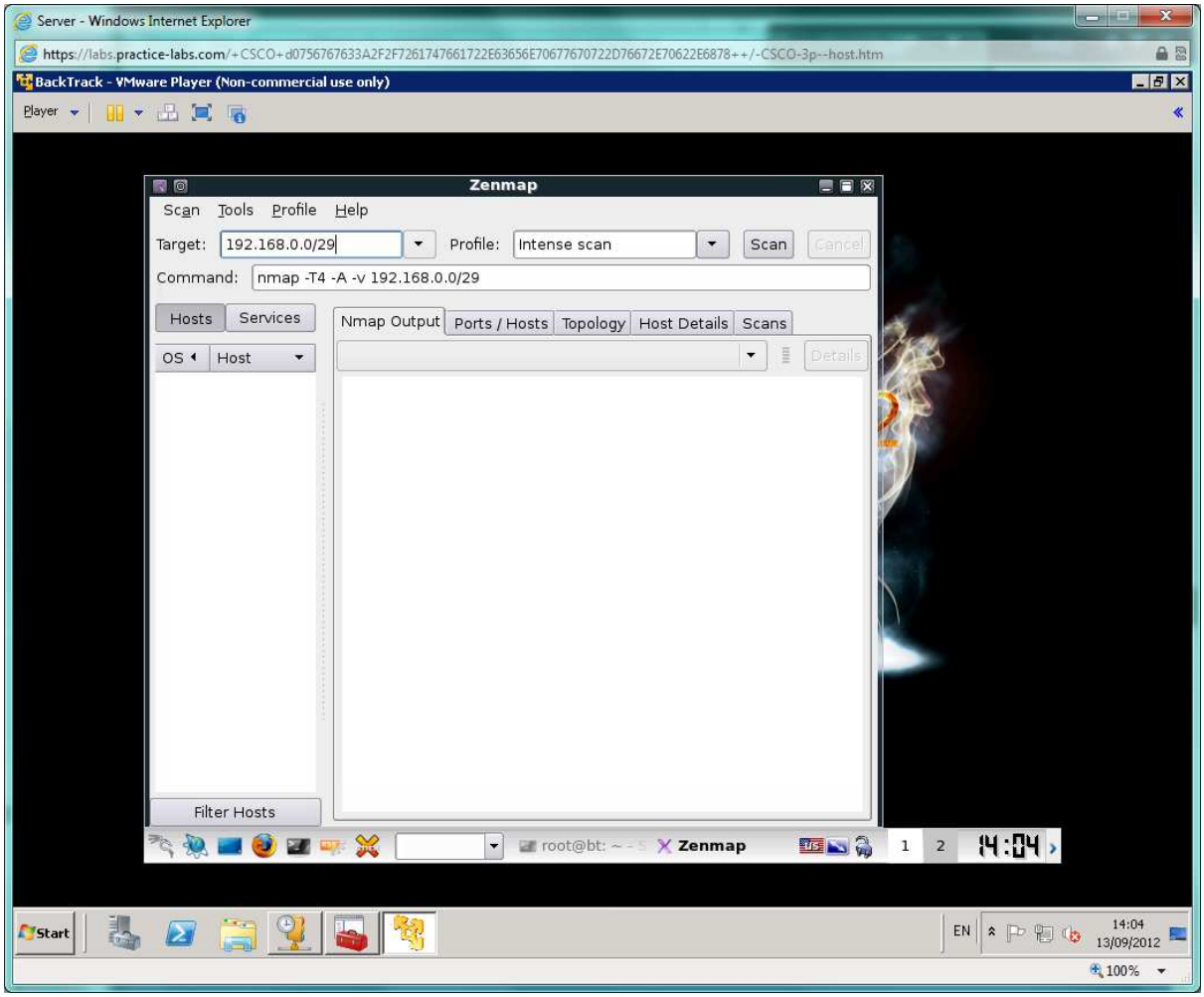


The DEVICE should receive an address in the 192.168.0.0 - 100 range. (Normally 192.168.0.10)

Use the K(onqueror) menu to open **Backtrack > Network Mapping > Portscanning > Zenmap**.

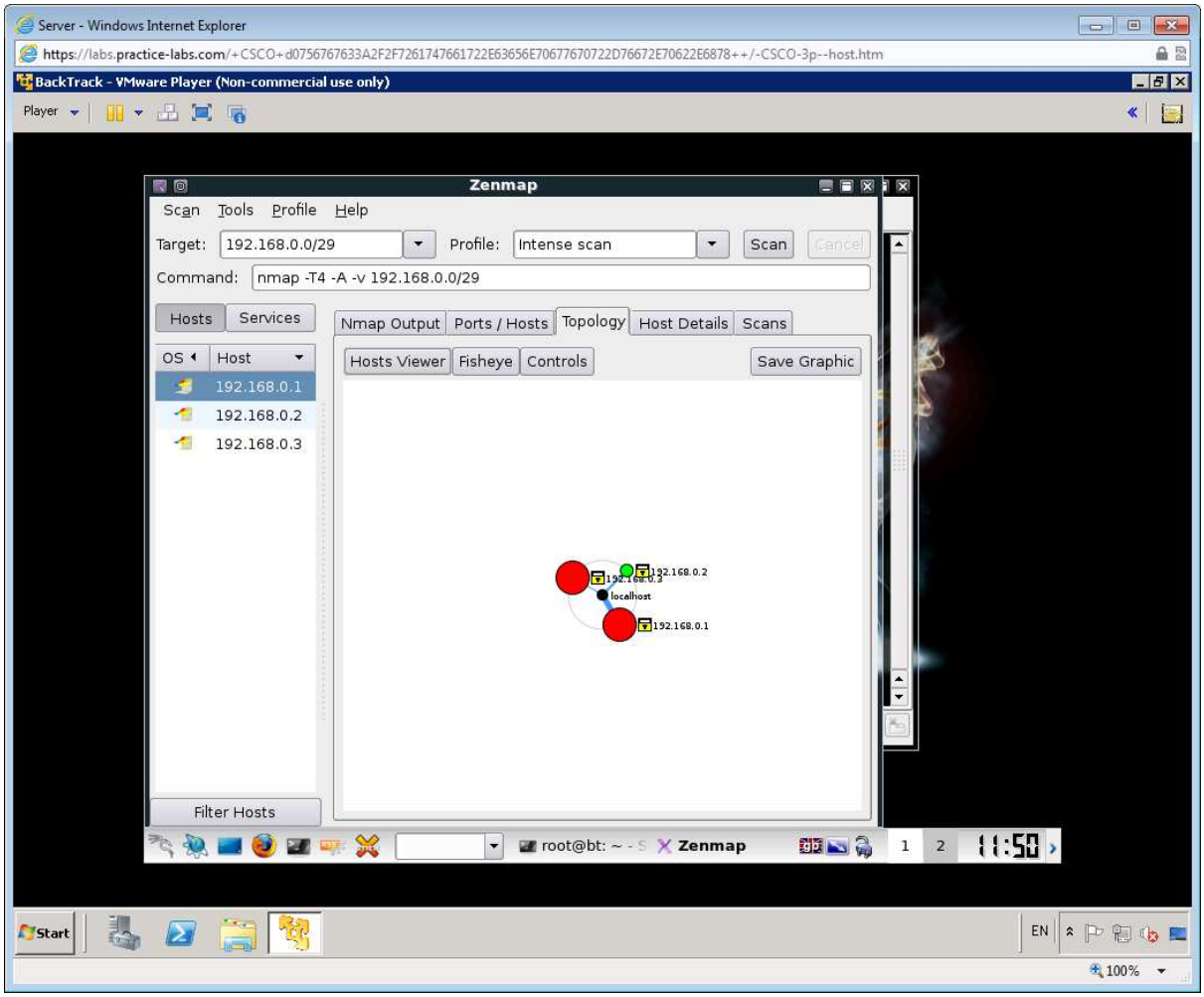


Enter 192.168.0.0/29 into the "Target" box. Click **Scan**.



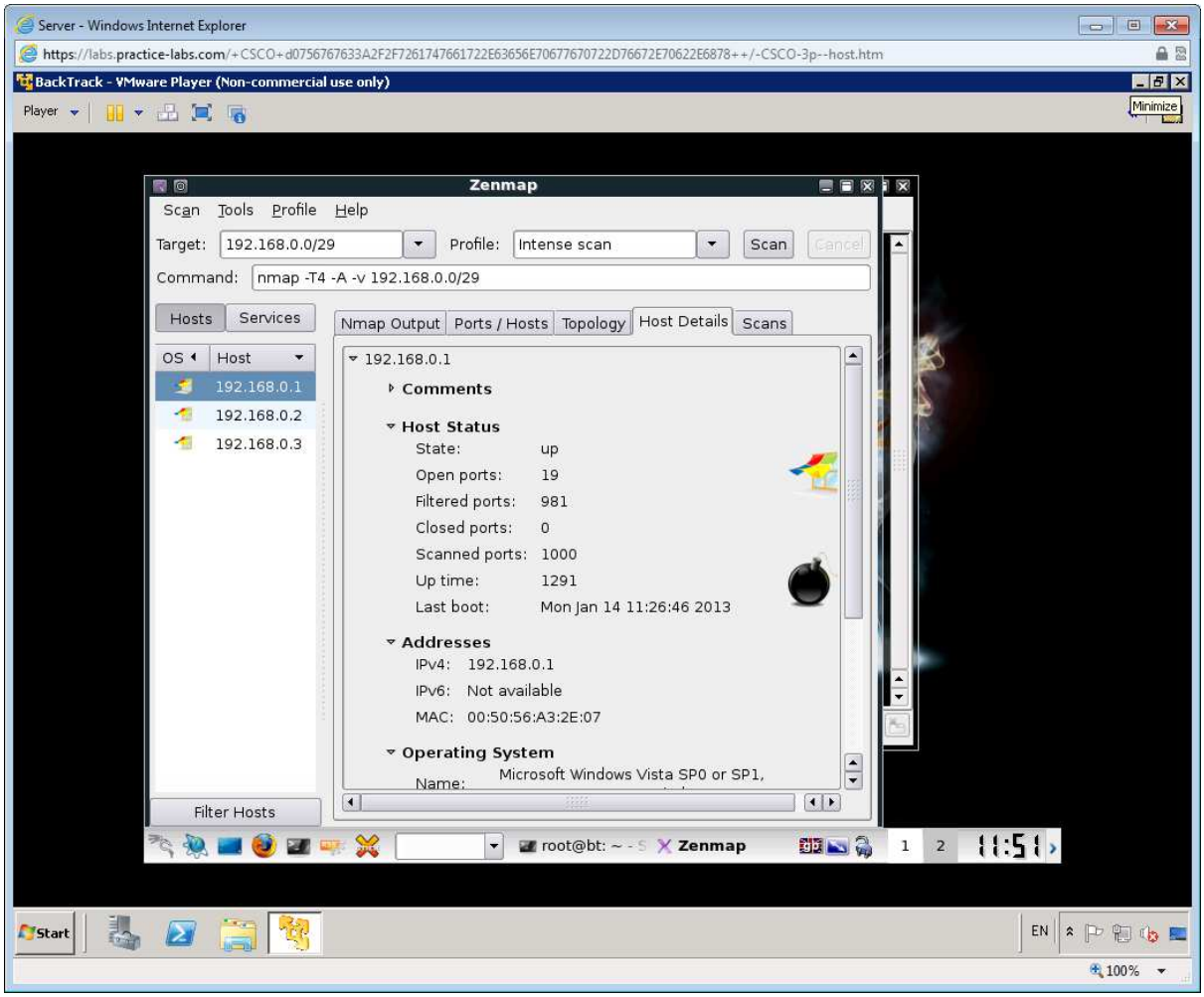
The scan will take a few minutes to complete and should finish with an "Nmap done" status message.

Click the **Topology** tab - this shows the hosts found via the scan, in this case restricted to the local subnet. You should be able to see all three DEVICEs.

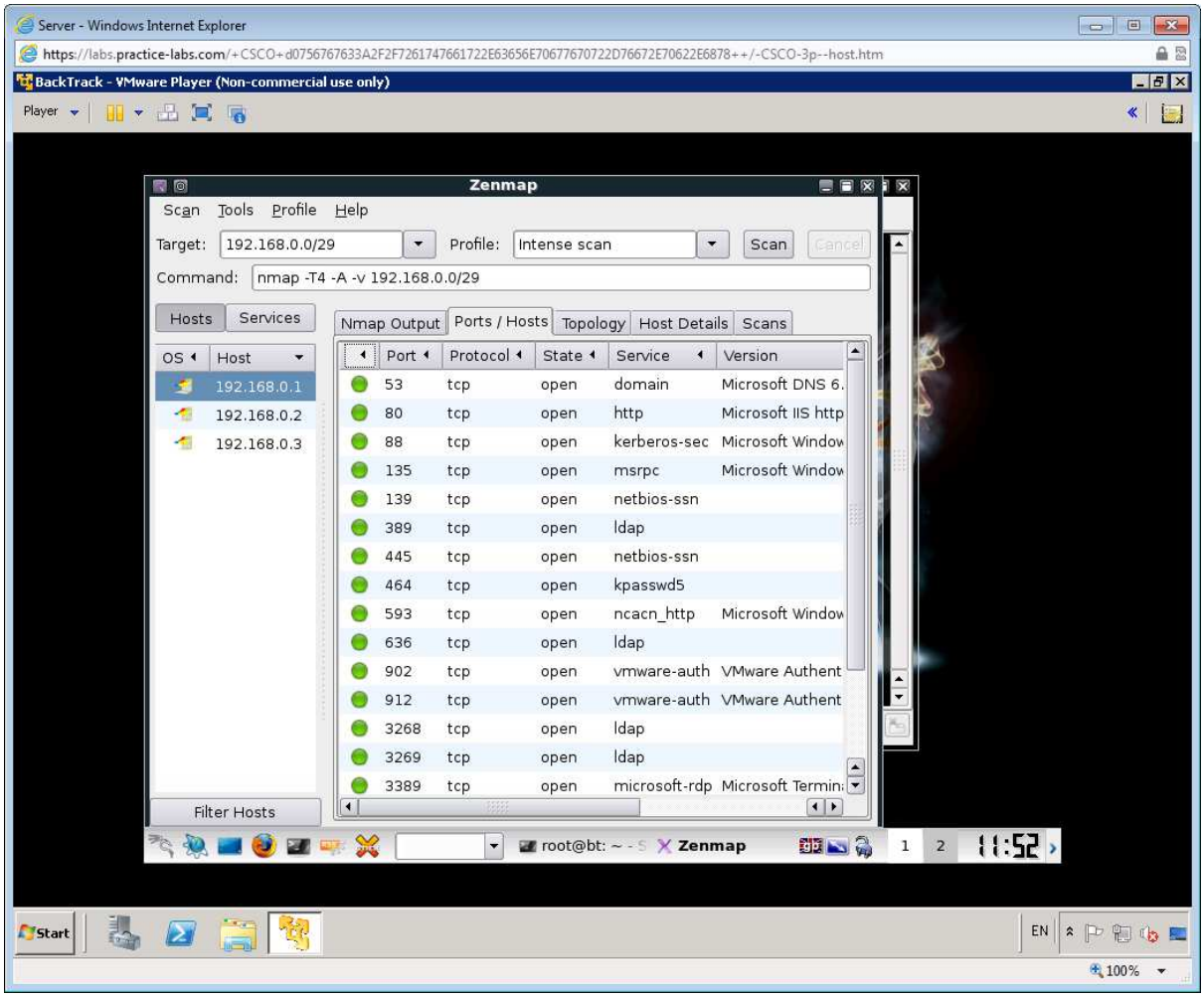


Click the **Host Details** tab. This shows the scan's attempt to identify the OS. Click the different hosts in the left-hand panel to view them. Note that the bomb icon shown on the SERVER DEVICE indicates lots of open ports.

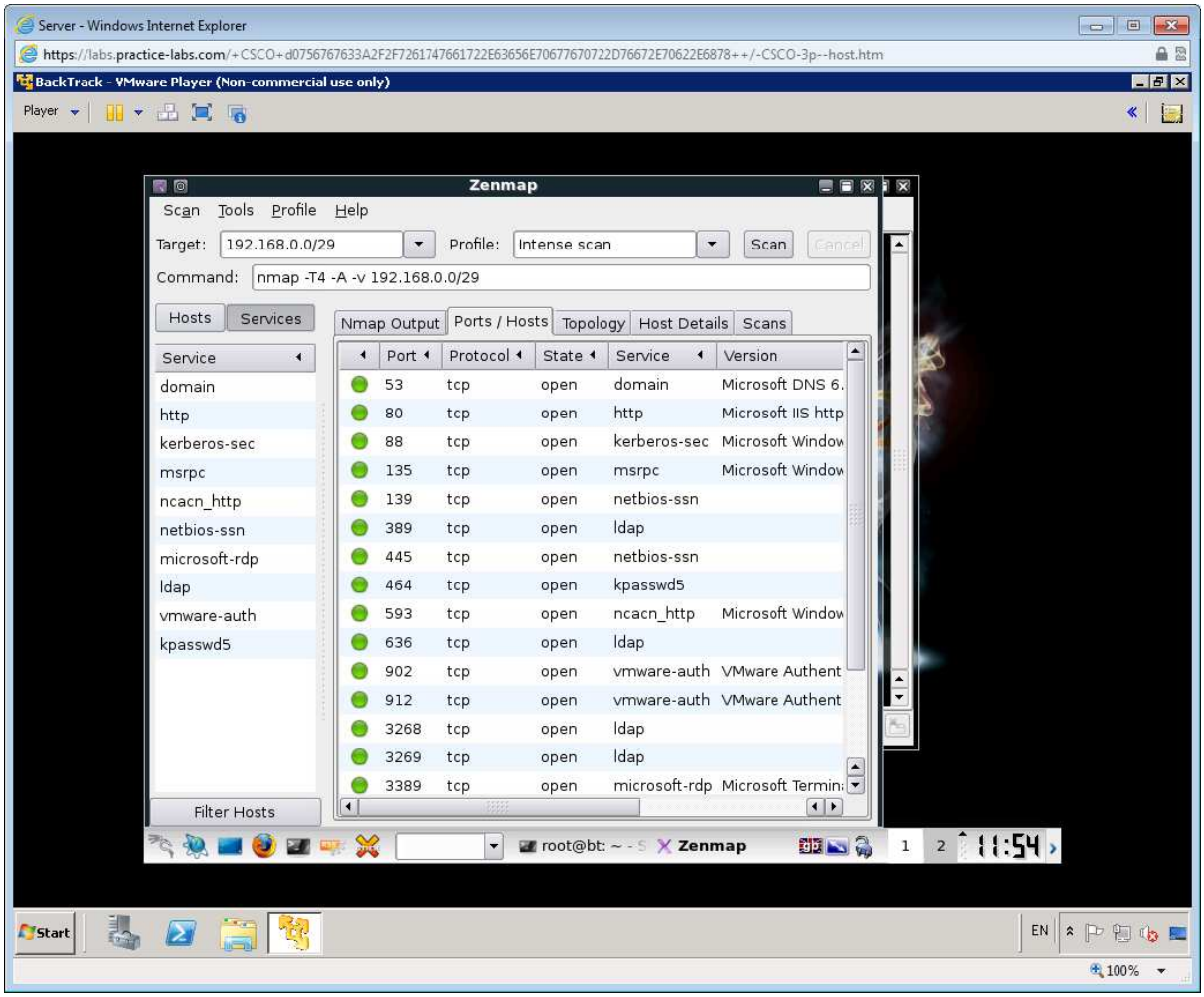
Note: Zenmap provides a GUI to the port scanning tool nmap



Click the **Ports / Hosts** tab. This shows precisely which ports are open on each host and in some cases the model and version of the server hosting them.



Finally, click the **Services** tab - this sorts the display by service rather than host. For any service you are interested in attacking (or defending) you can see which host(s) are running it.



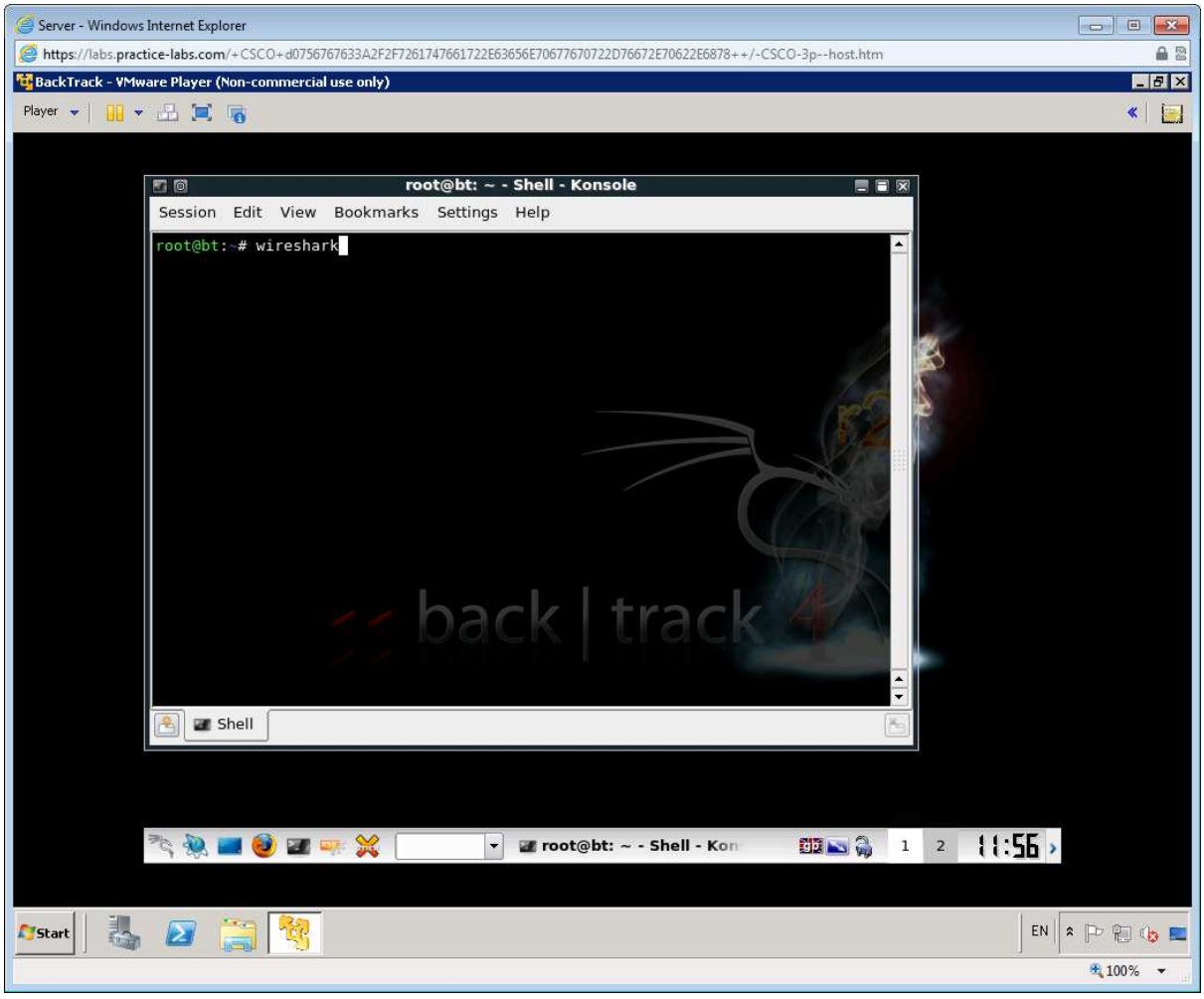
Close Zenmap, discarding any changes.

Continue to the next exercise to discover more network vulnerability tools.

Exercise 2 - Packet Sniffing

Another critical information gathering tool is a protocol analyzer. This tool captures unicast packets sent to the host and broadcast packets on the same subnet. The most widely used is Wireshark, which is bundled with Backtrack.

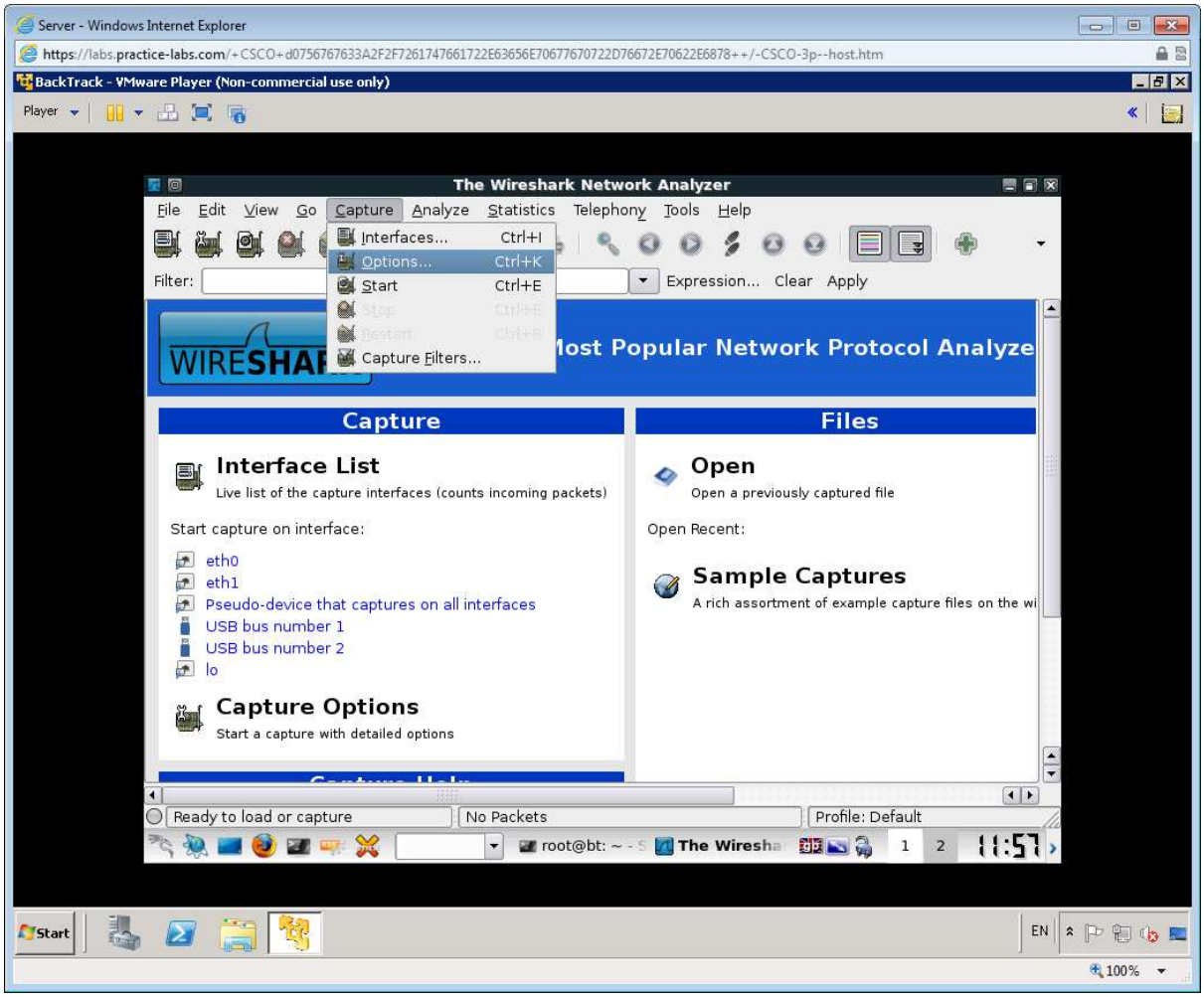
From the console, type **wireshark** and press Enter.



Click **OK** to the warning.

Maximize the window.

Click the Capture Options button.

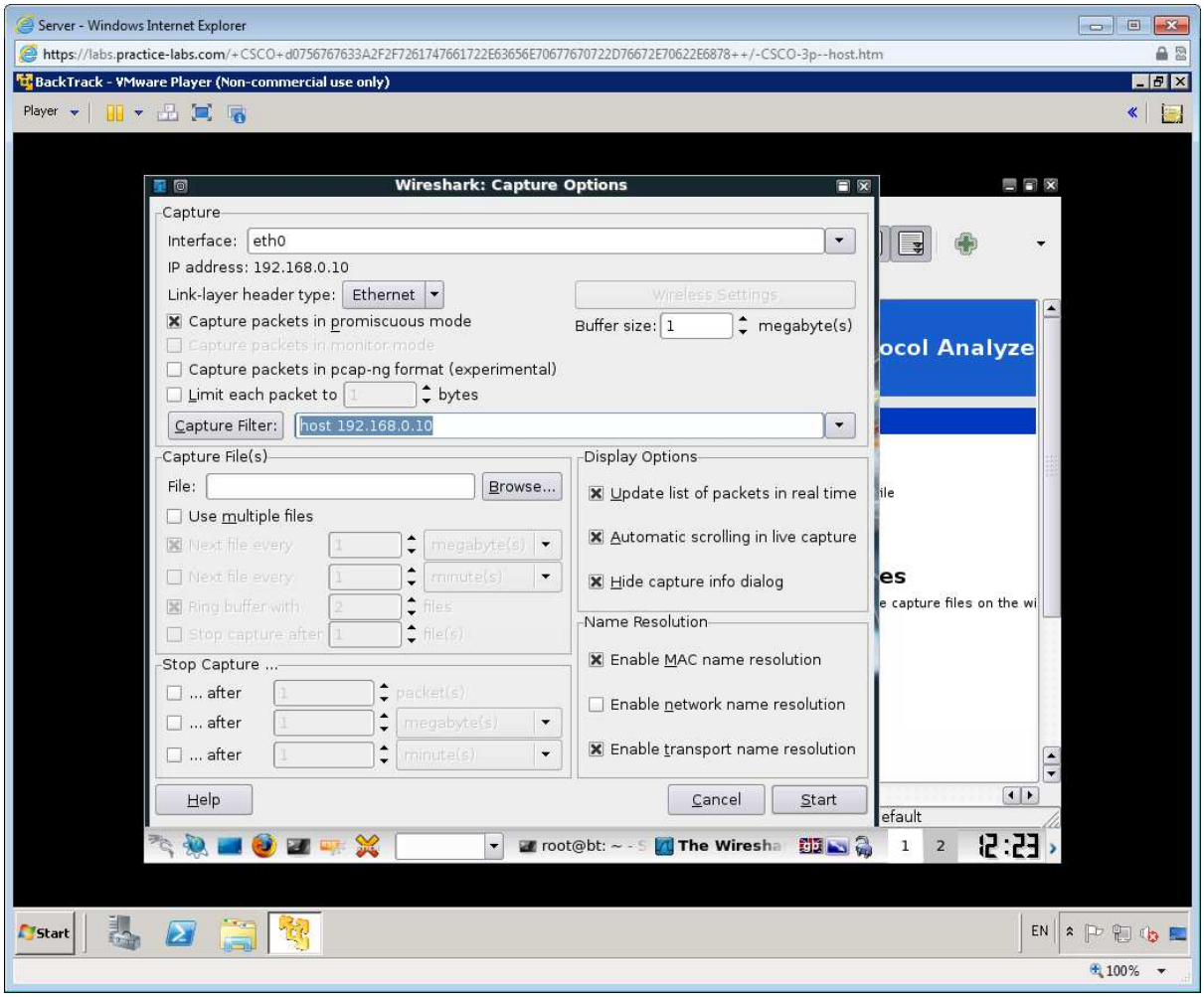


In the "Capture Filter" box, type:

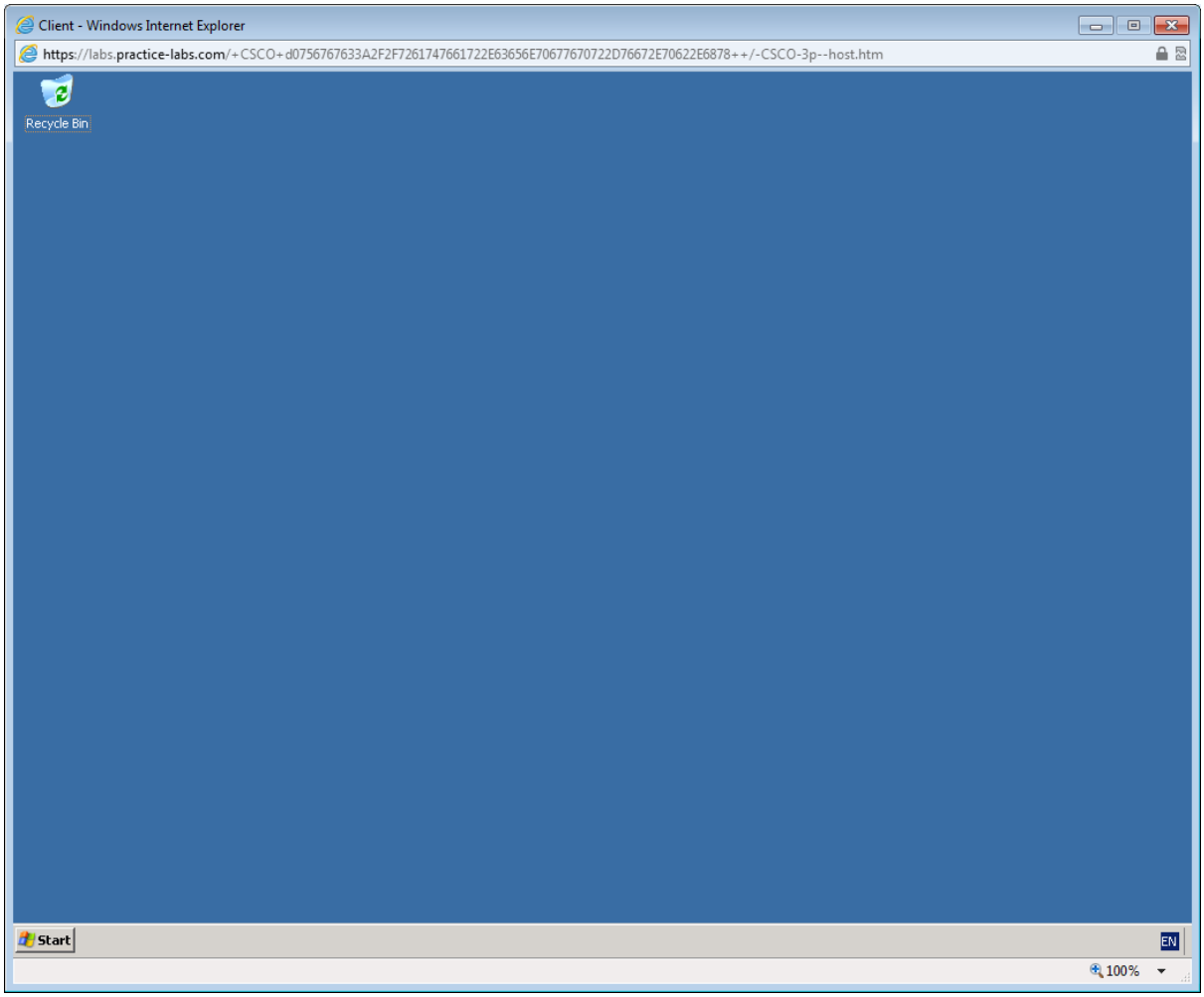
host 192.168.0.10

(A capture filter is used to restrict the type of packets processed by Wireshark)

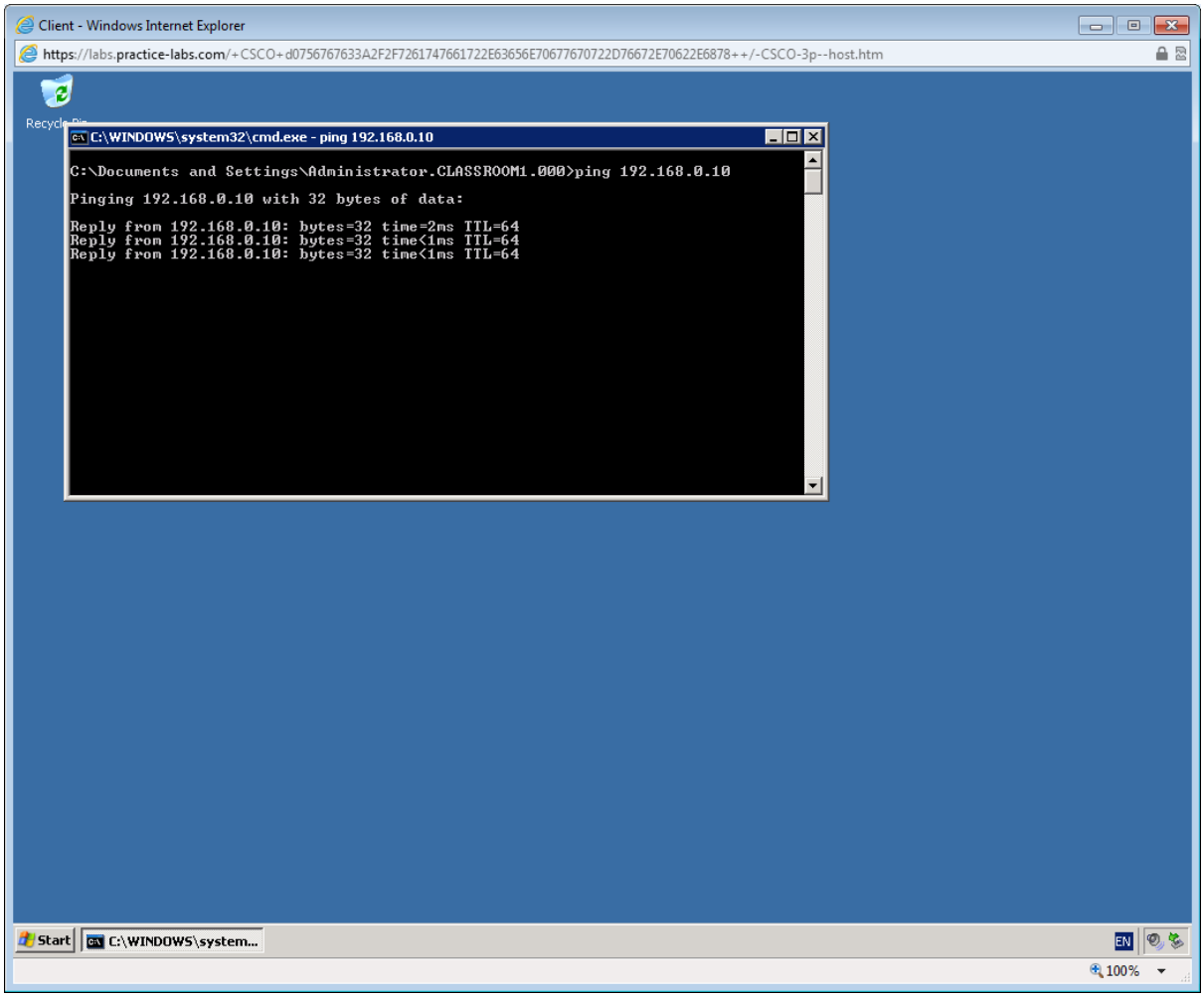
Click **Start**.



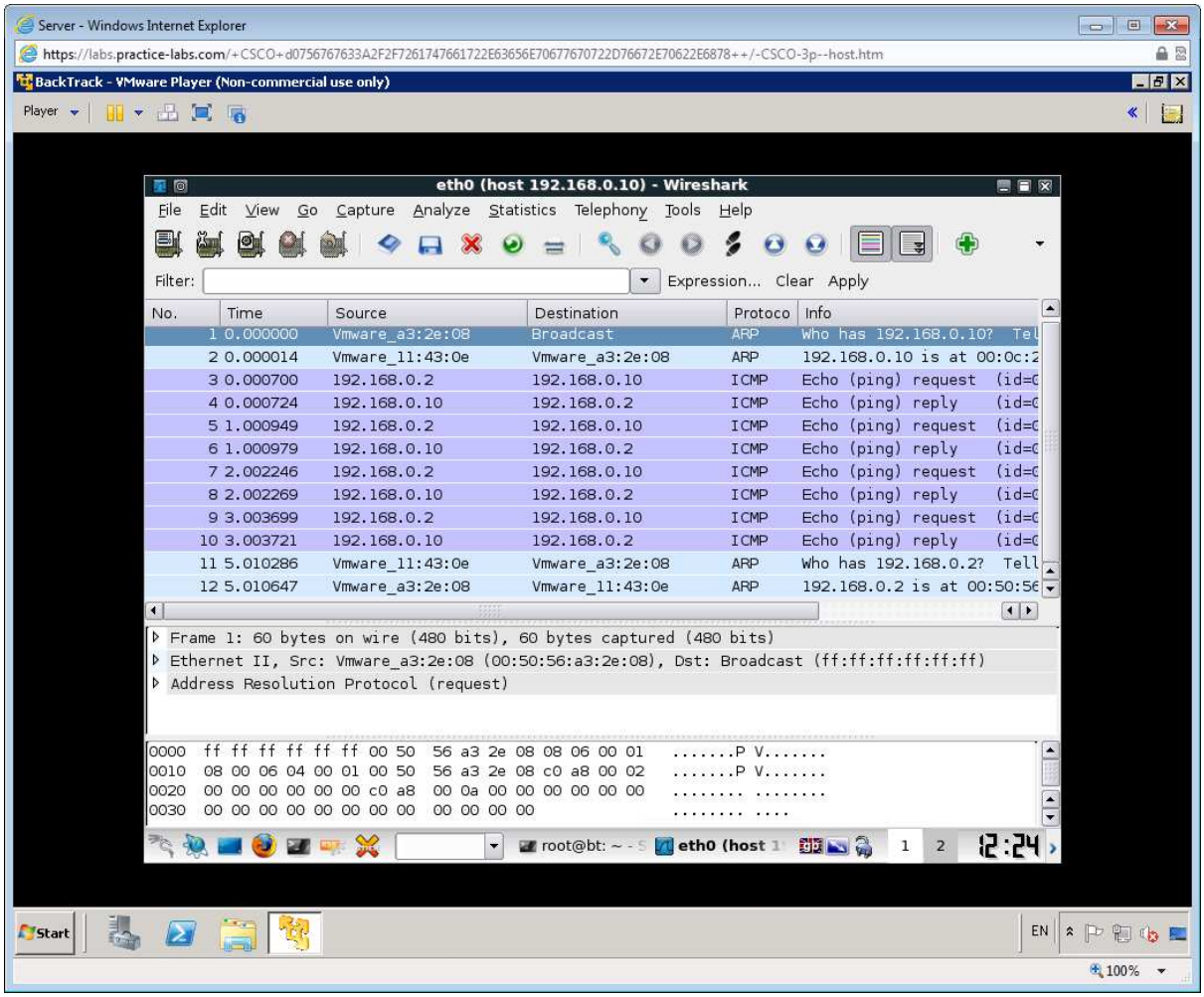
Connect to the **CLIENT** device using the Practice-Labs application.



Open a command prompt and ping the IP address of BackTrack (192.168.0.10).



Switch back to Backtrack and stop the capture and note what has been captured.



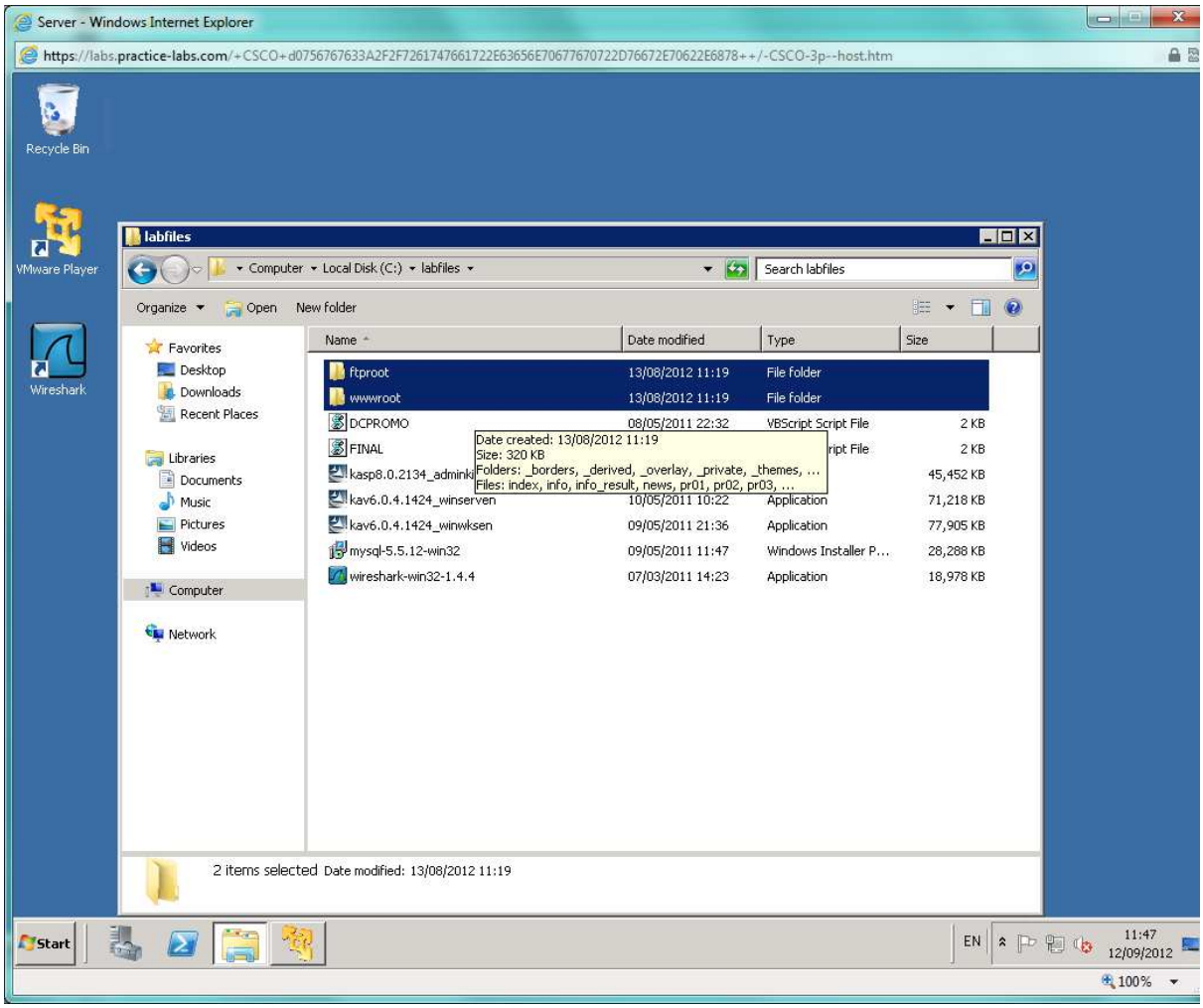
Continue to the next exercise to learn about Man in the middle attacks.

Exercise 3 - MitM with ARP Spoofing

As an attacker, you may be more interested in finding out what information a different host on the network is receiving and possibly to modify the transmissions between two hosts - a Man in the Middle (MitM) attack. Ettercap is one of the most widely used tools for launching MitM attacks. On a local network, one of the most powerful techniques is ARP spoofing.

Connect to SERVER Practice-Lab device.

*Open Explorer and copy the **ftproot** and **wwwroot** folders from **C:\labfiles**.*

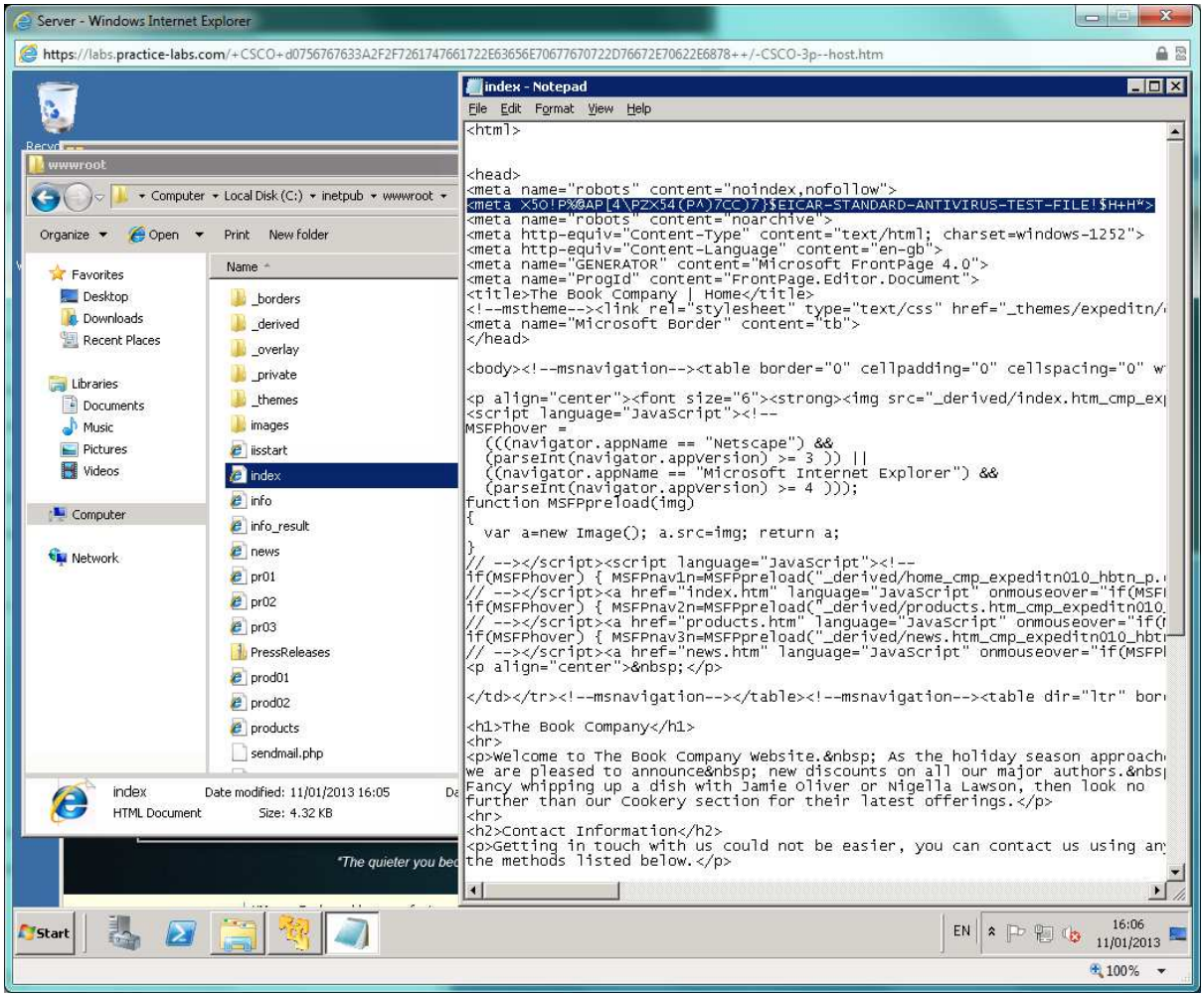


Open **C:\inetpub** and paste the folders, choosing to merge with the existing folders.

Browse to **C:\inetpub\wwwroot**

Right click the **Index.htm** file and open with **Notepad.**

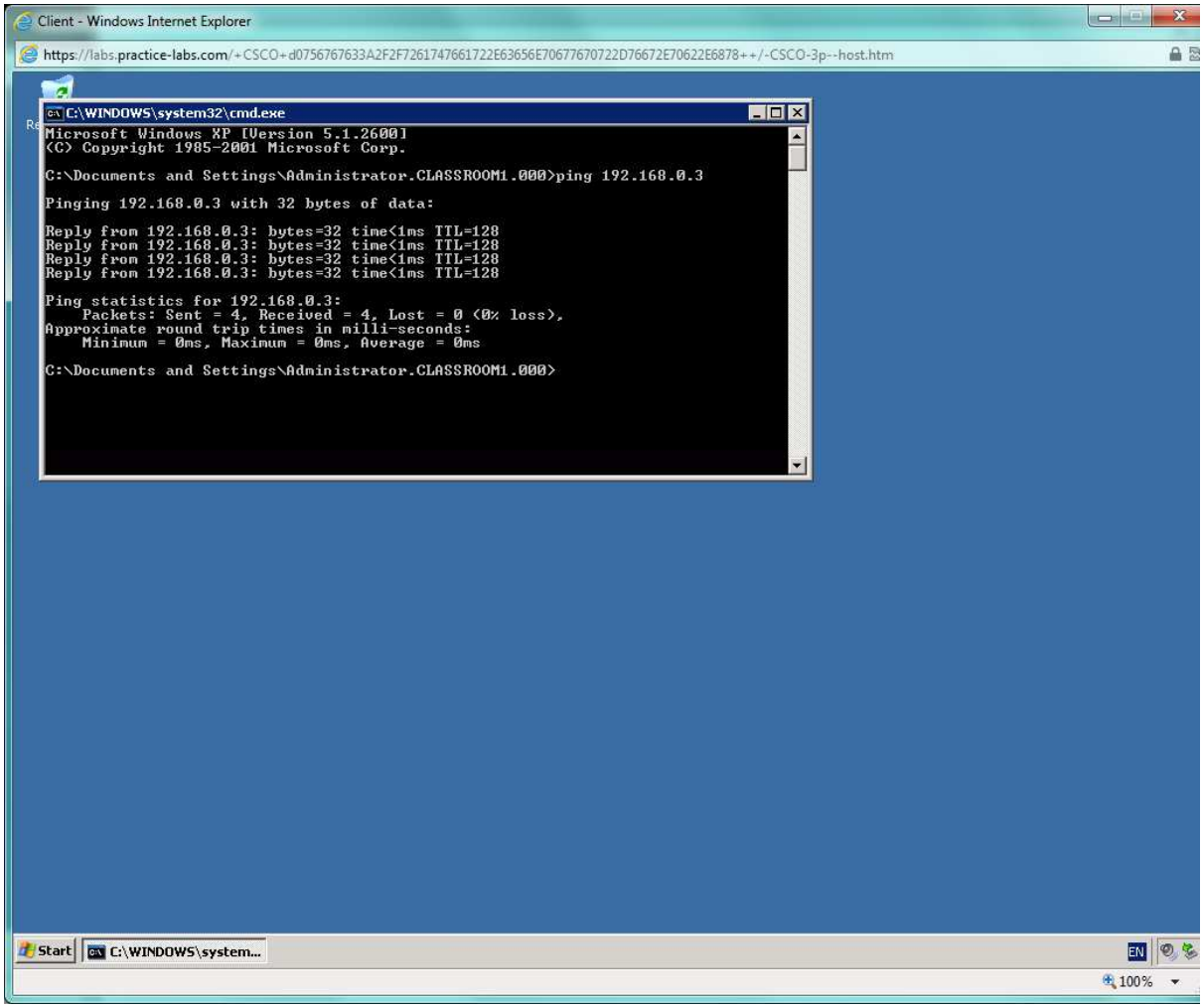
Find and delete this line: *meta X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H**



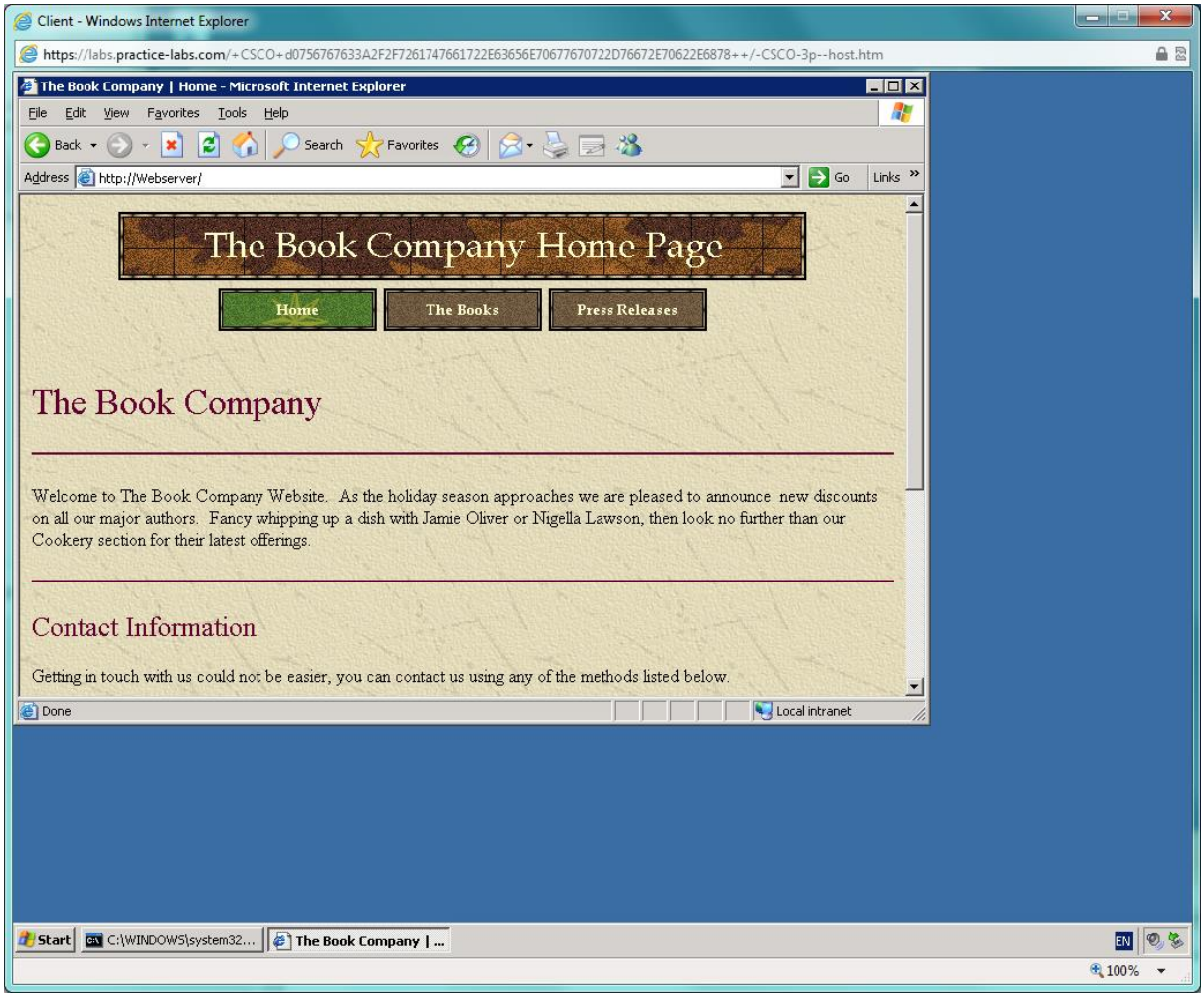
Save and close the file.

Connect to the CLIENT device in your Practice-Lab and open a command prompt.

Type **ping 192.168.0.3** to check connectivity with the SERVER.



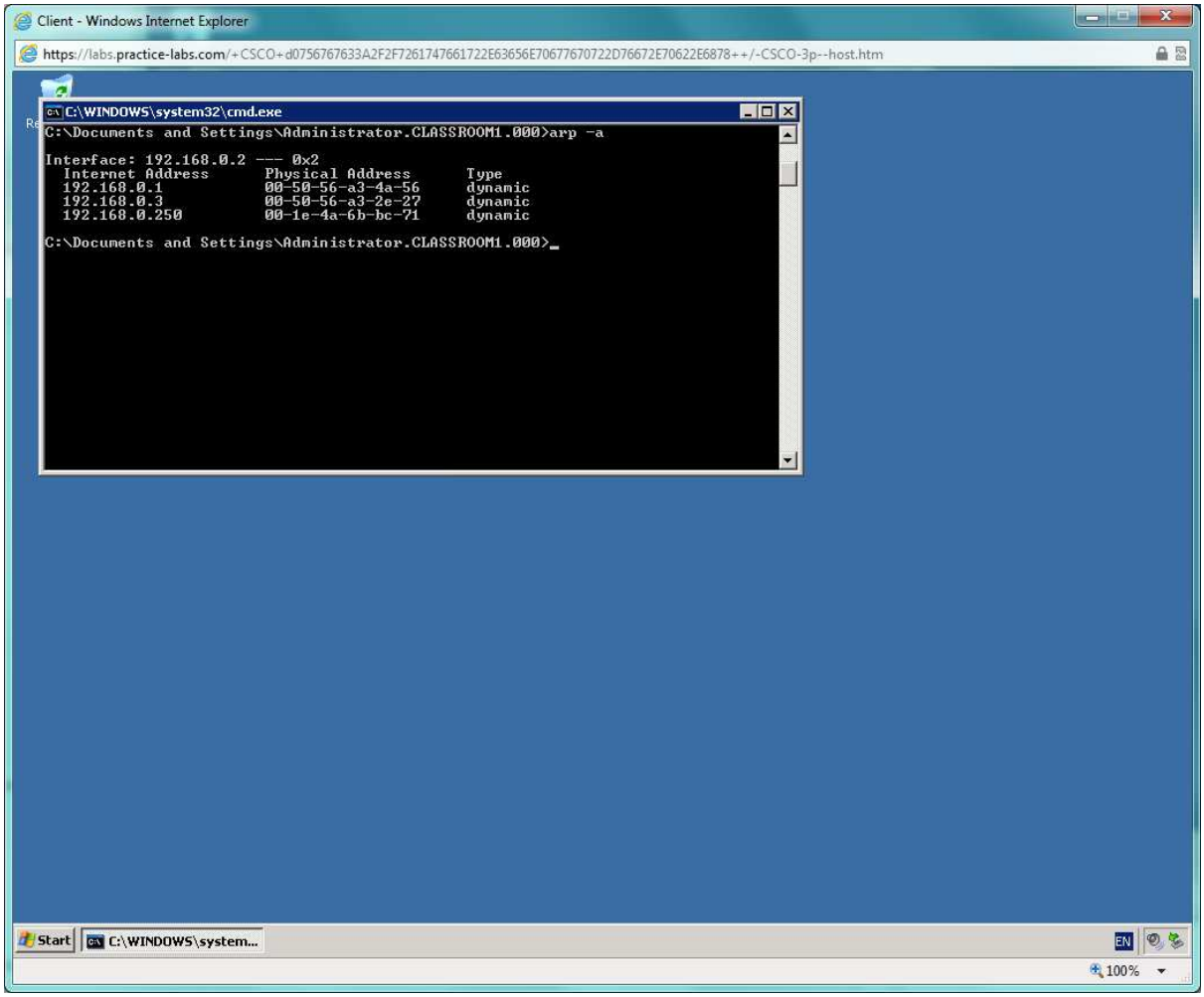
Open Internet Explorer and load [http ://webserver](http://webserver)



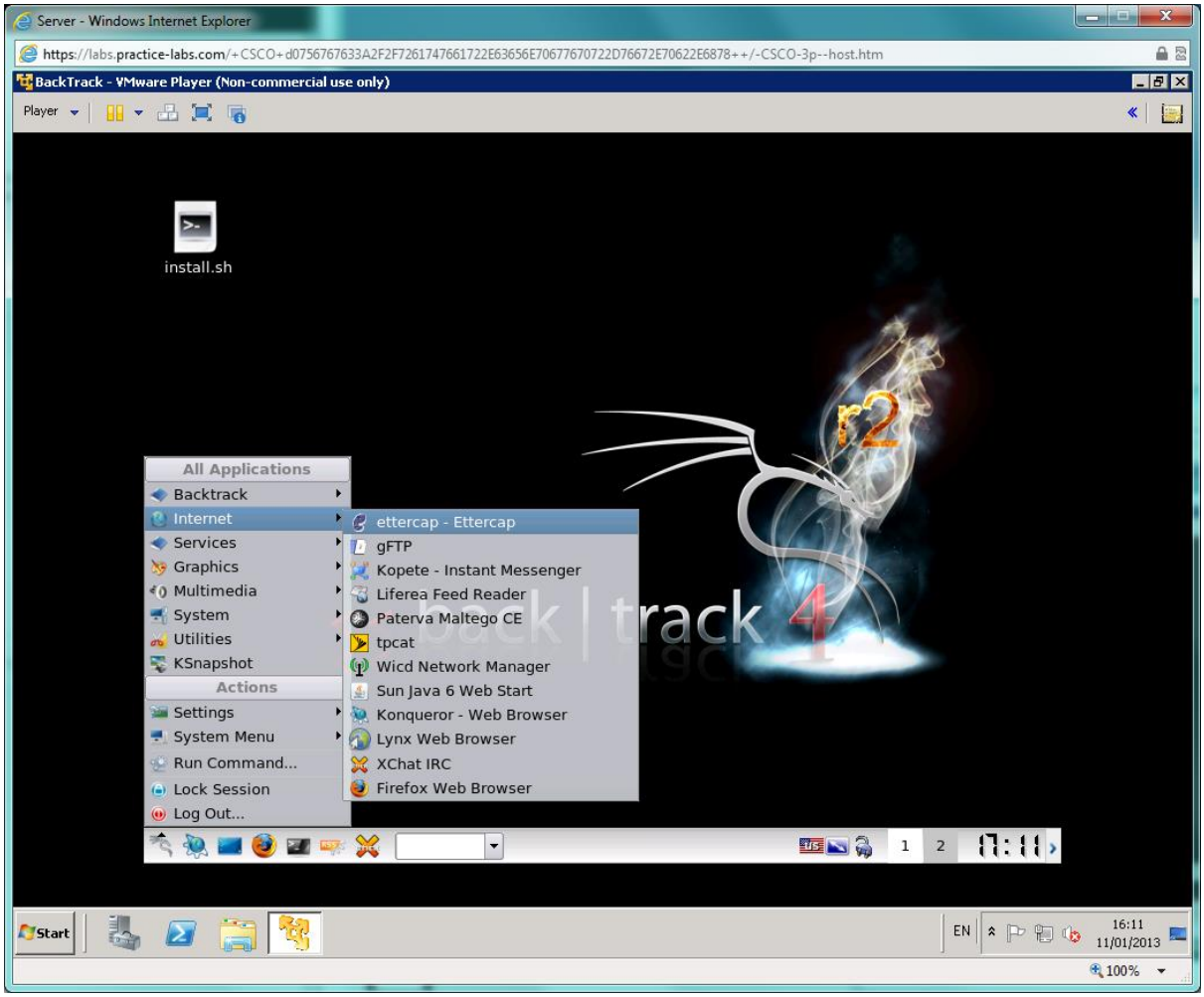
In the command prompt, type

arp -a

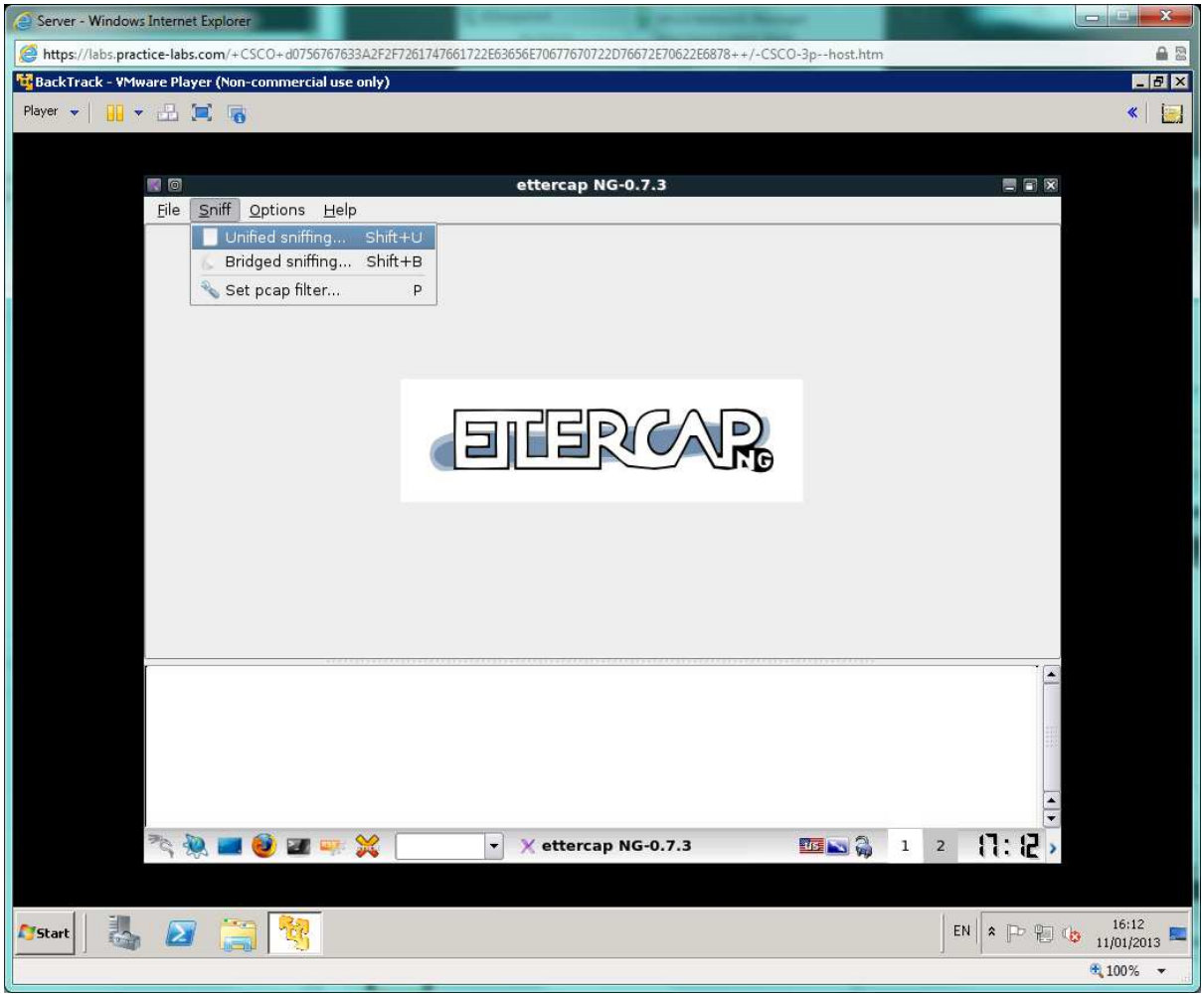
This will show you a view the ARP cache. Make a note of SERVER's MAC address:



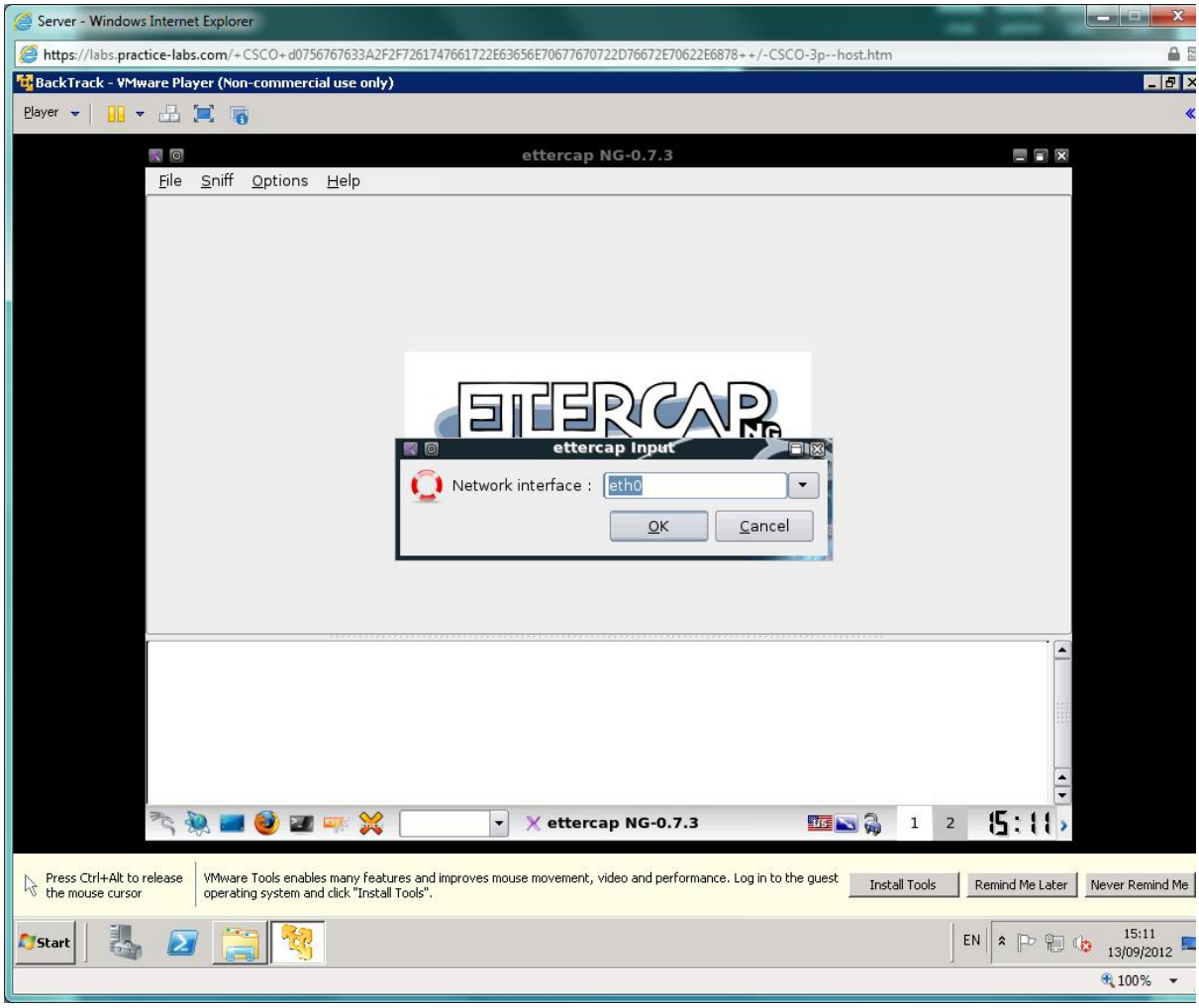
Switch to Backtrack. From the **K(onqueror)** menu, select **Internet > Ettercap**. Maximize the window.



Select **Sniff > Unified Sniffing**

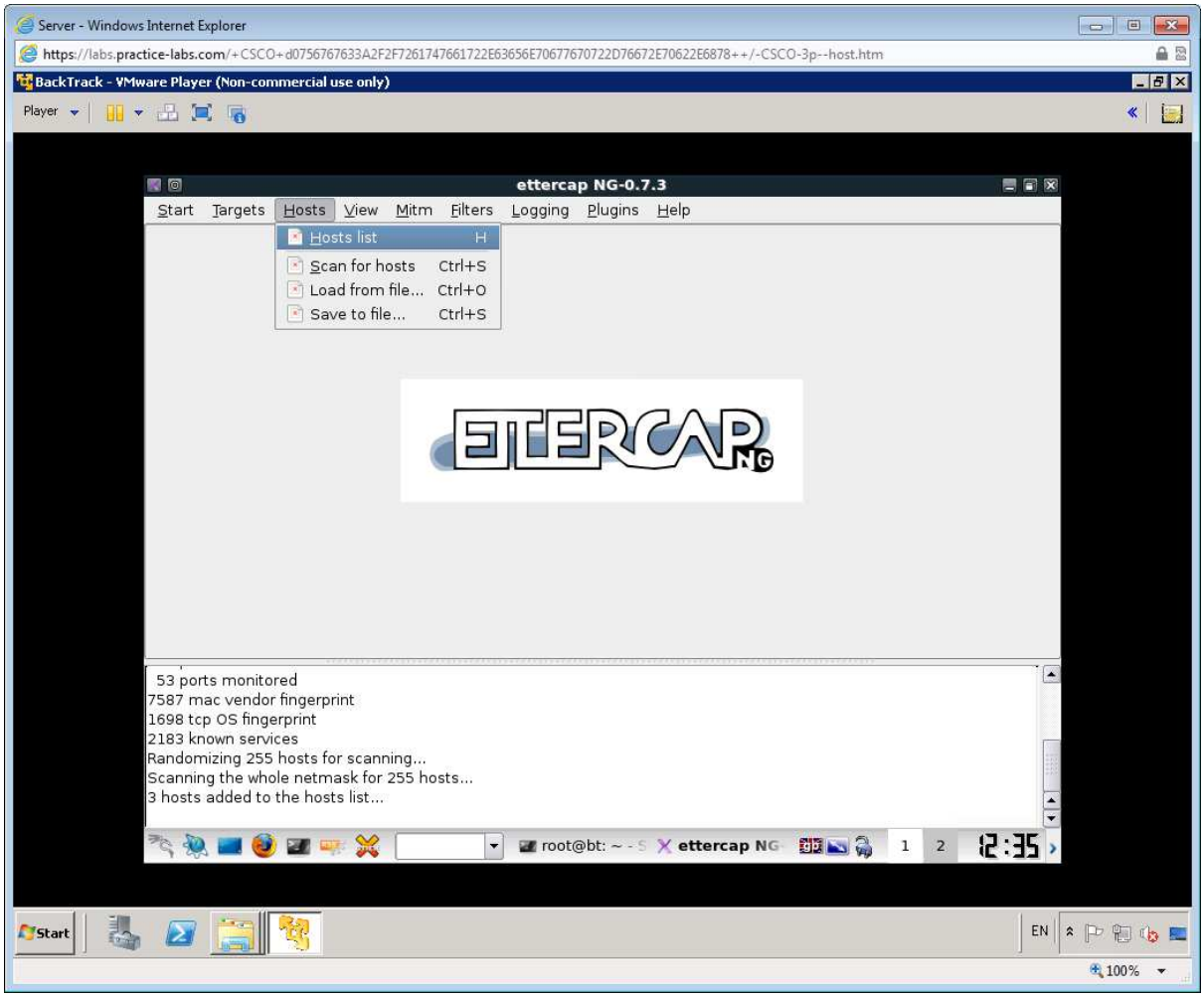


Check that the interface “eth0 " is selected and click OK.

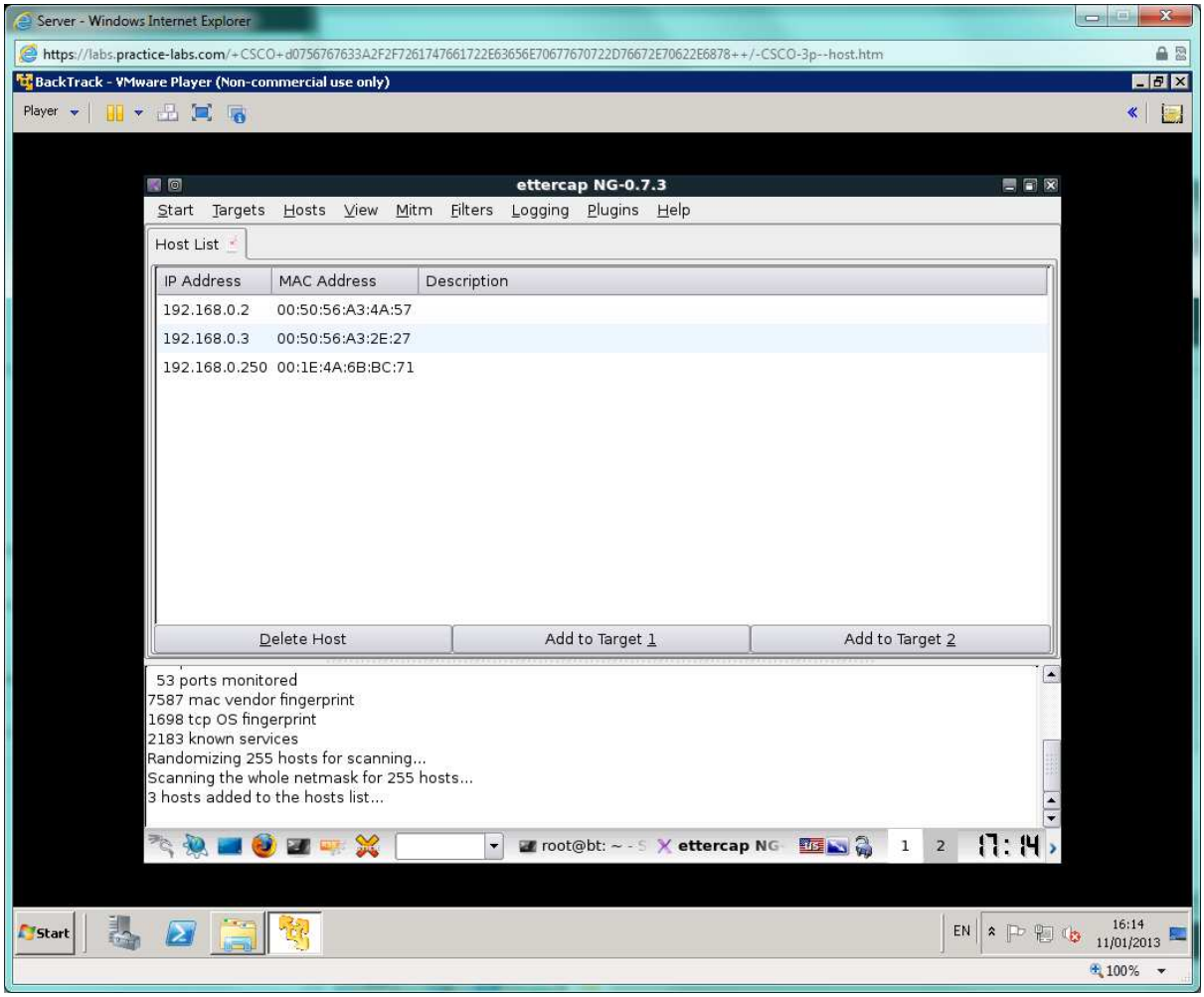


Select **Hosts > Scan for hosts**. This should return three results.

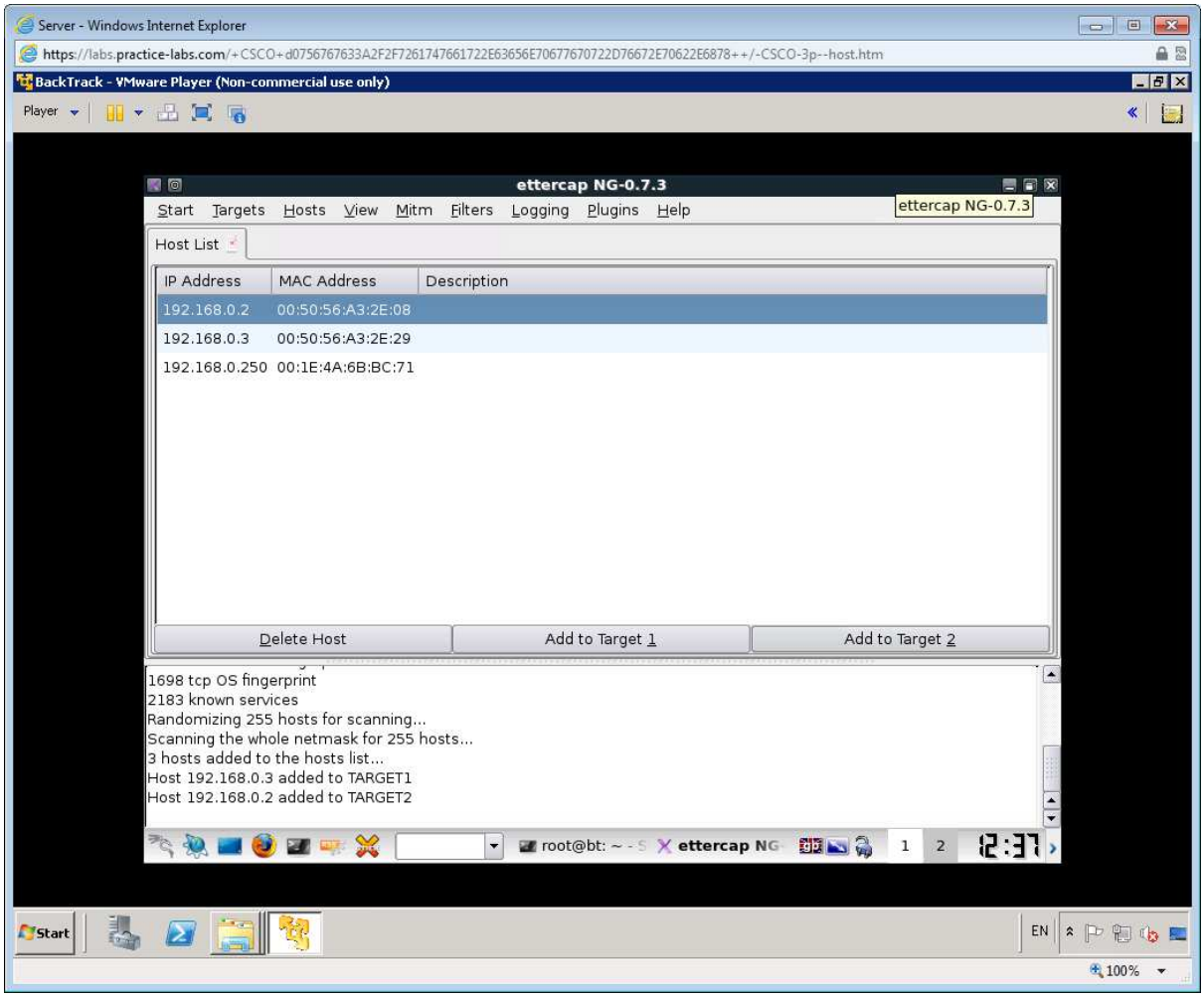
Once the scan has completed Select **Hosts > Hosts list**



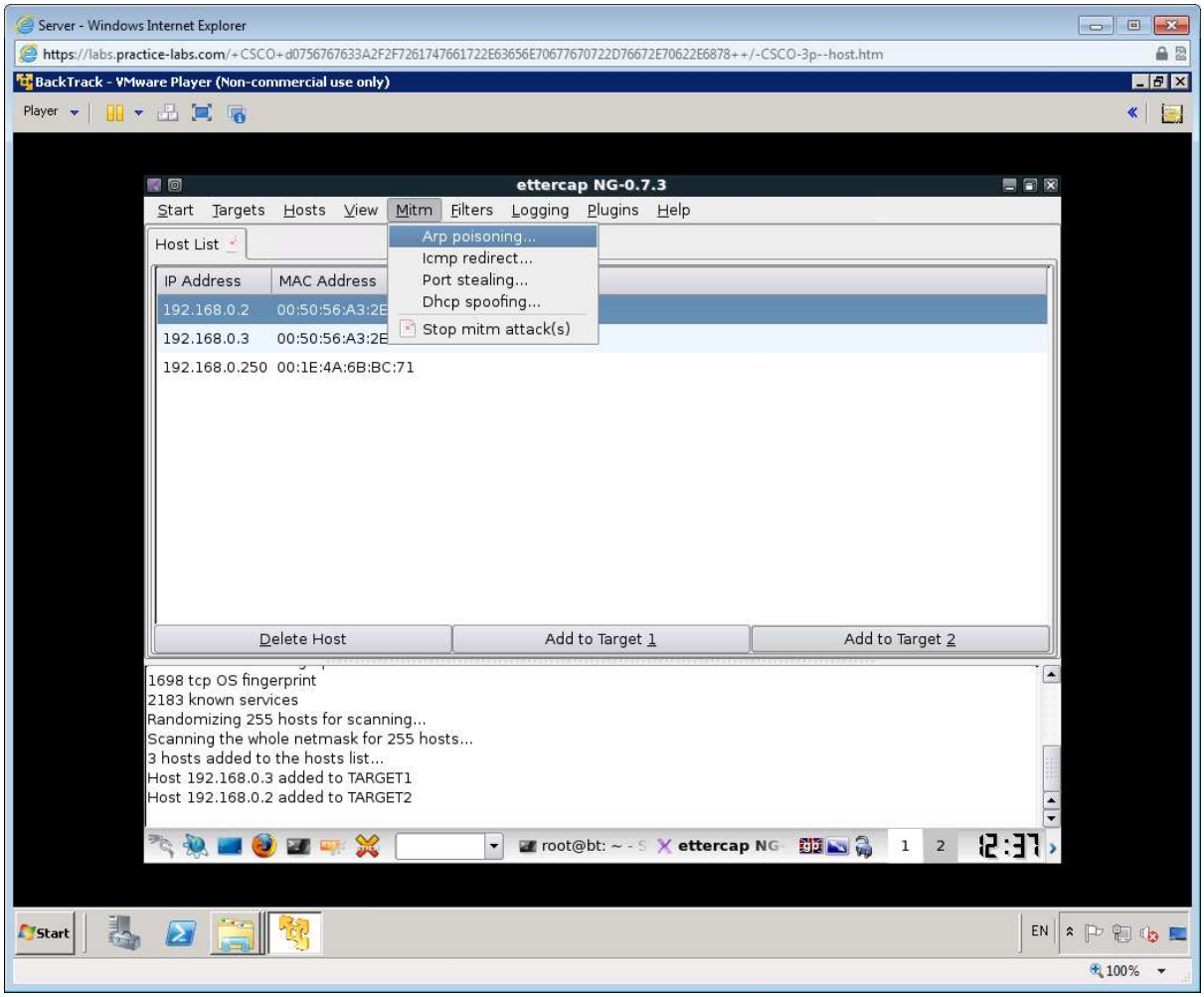
This will show you a list of discovered hosts.



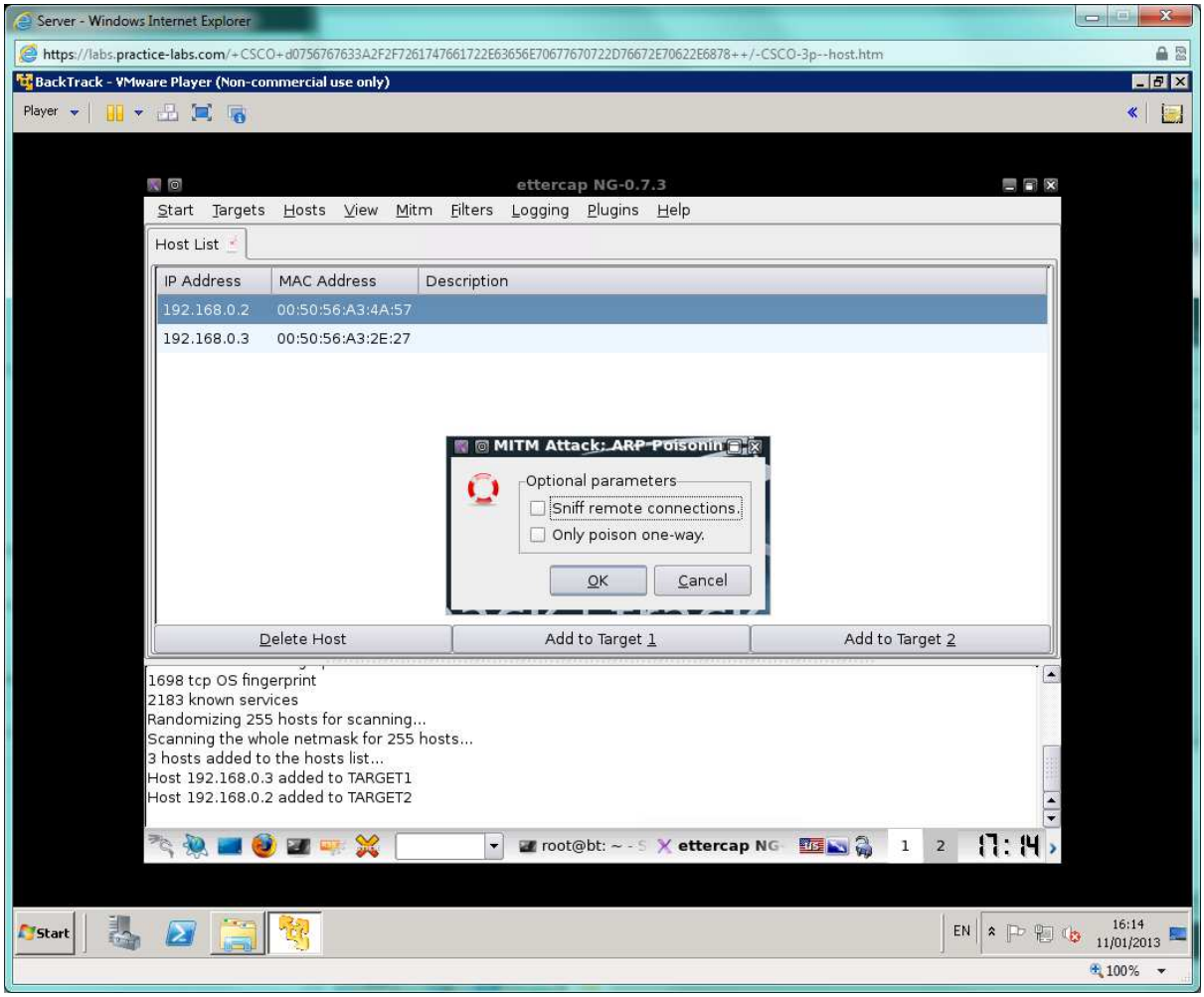
Select 192.168.0.3 and click **Add to Target 1** then select 192.168.0.2 (CLIENT's IP address) and click **Add to Target 2**.



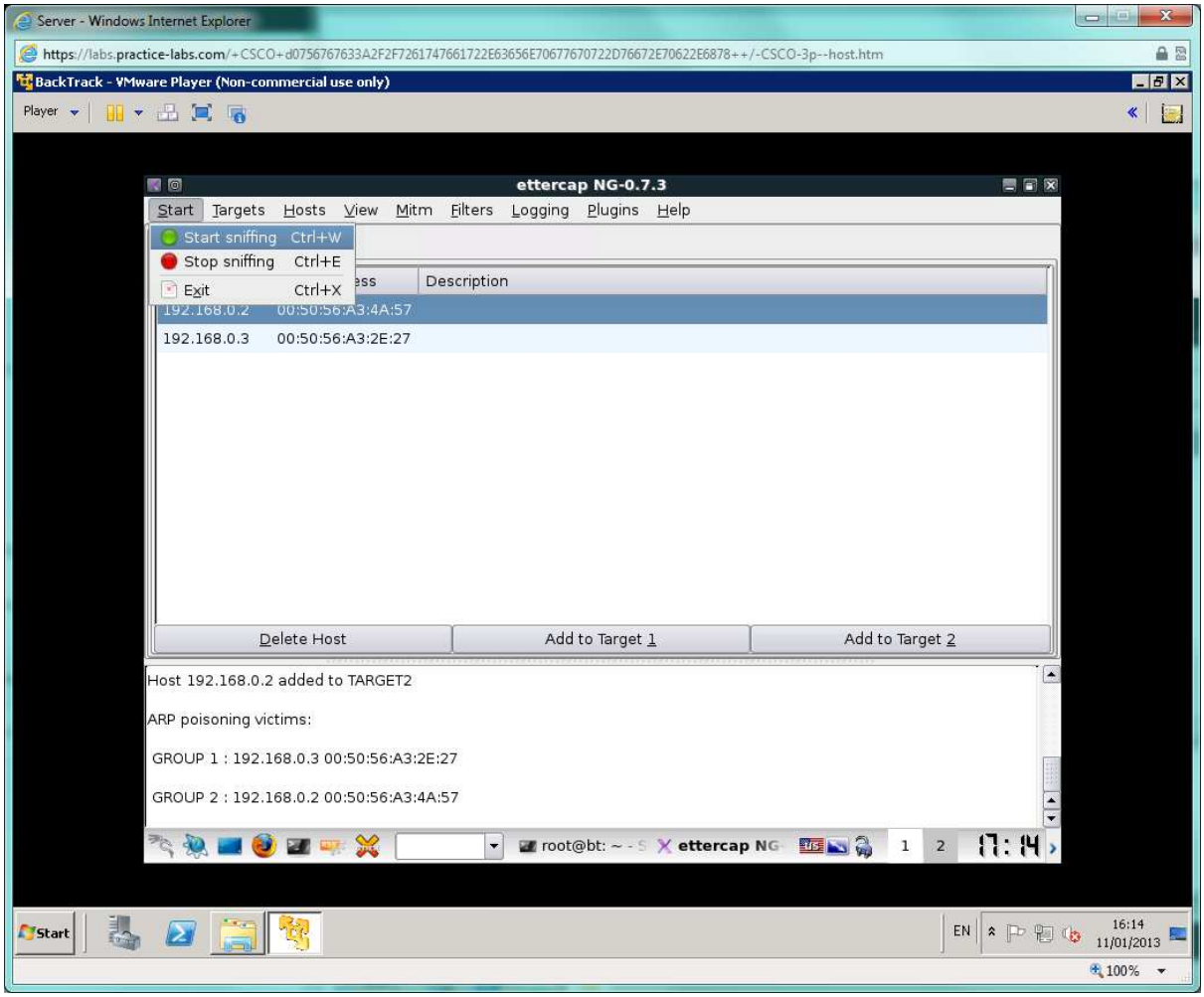
Select **Mitm > Arp poisoning**. Click OK.



Select OK to the displayed message

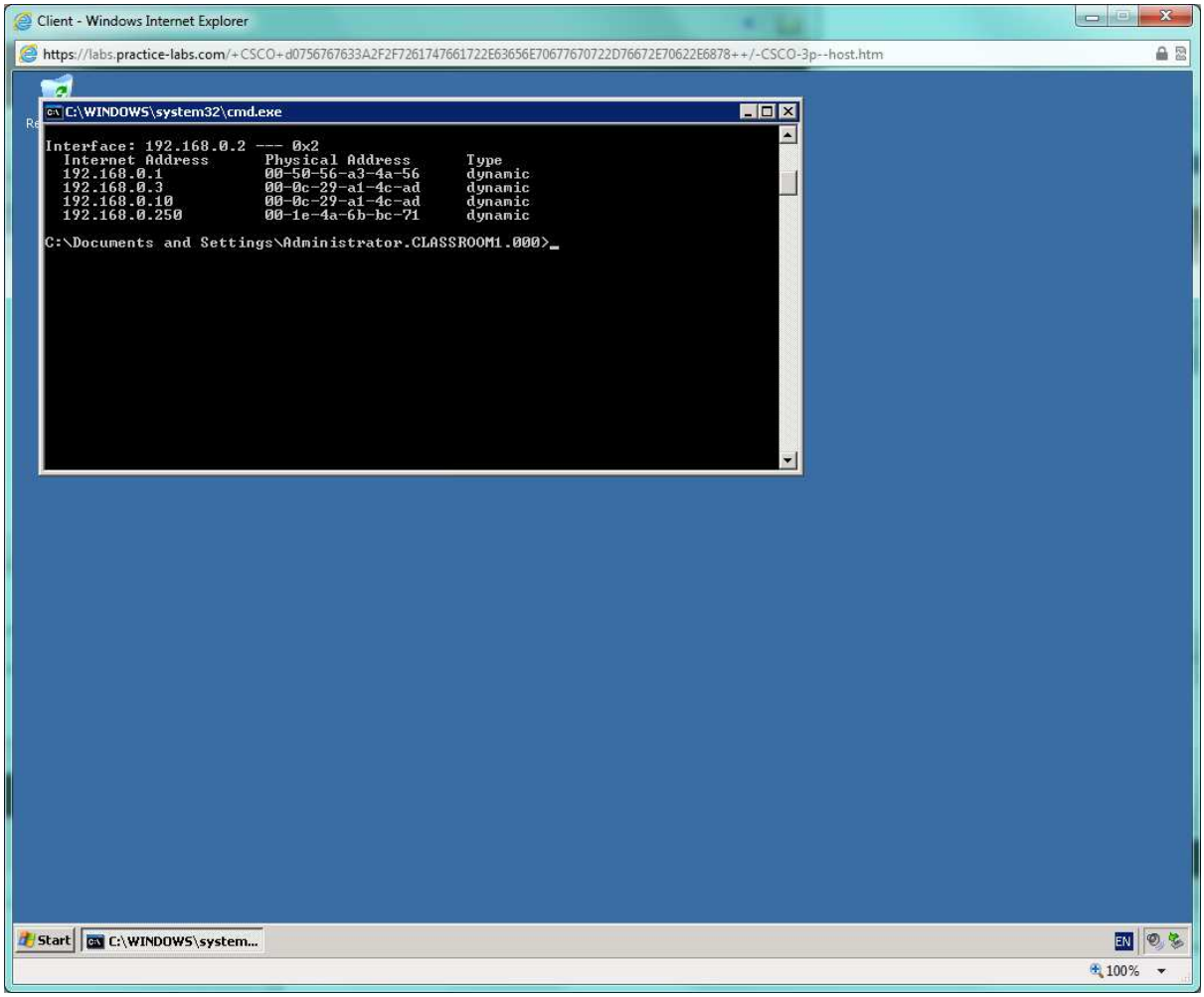


Select **Start > Start sniffing**.



Switch to the CLIENT workstation and ping 192.168.0.3 again.

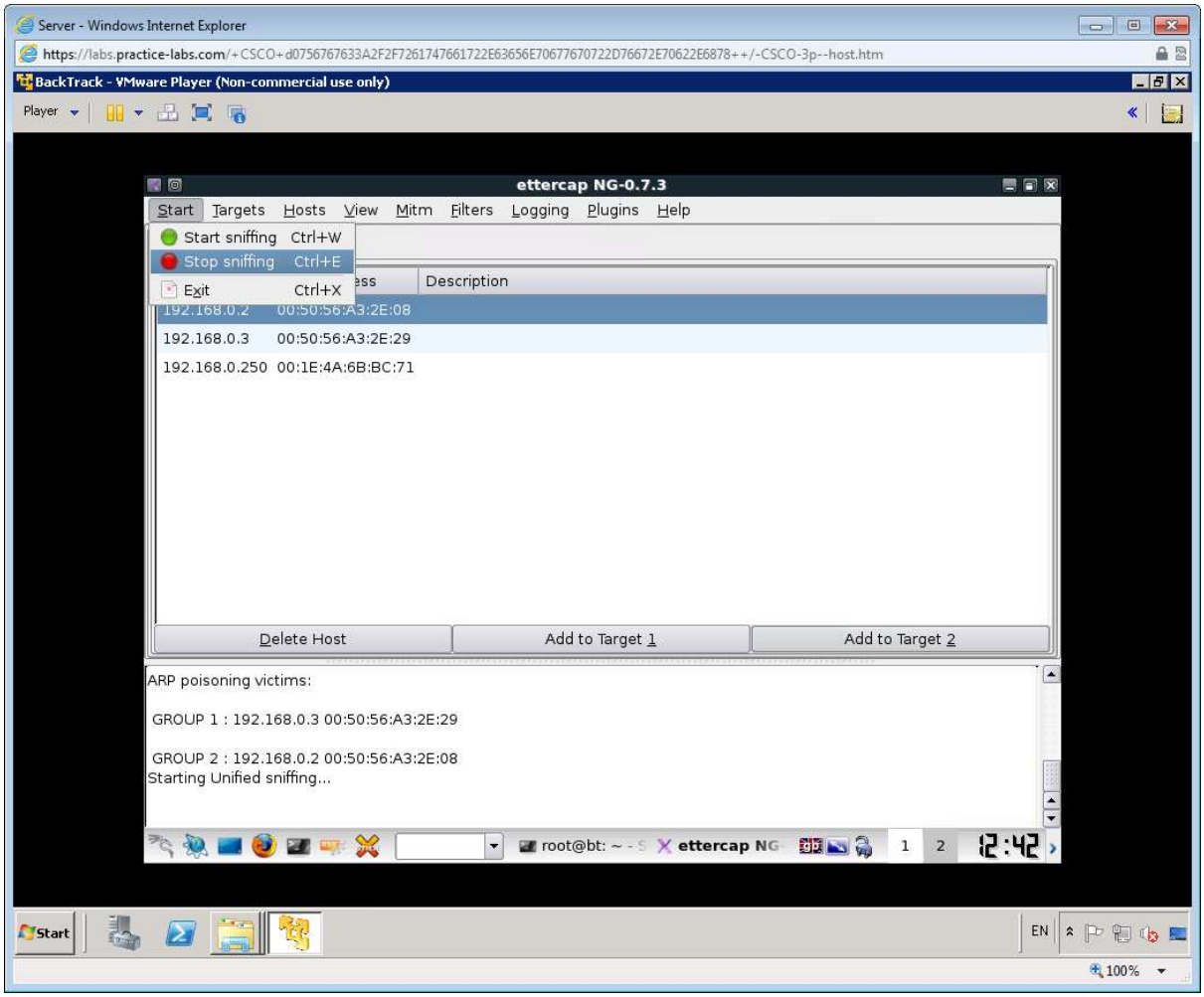
Enter **arp -a** to view the ARP cache. Make a note of SERVER's MAC address:



Note that you can see BACKTRACK IP address and MAC and that the MACs for BACKTRACK and SERVER are identical. The attack we are launching is quite unsophisticated - it is possible to be a lot sneakier.

As a simple example of doing some content rewriting, we will design a filter to subvert the web server hosted on SERVER.

Switch back to the BACKTRACK SERVER and **Stop** the **Arp poisoning** and **Sniffing.**

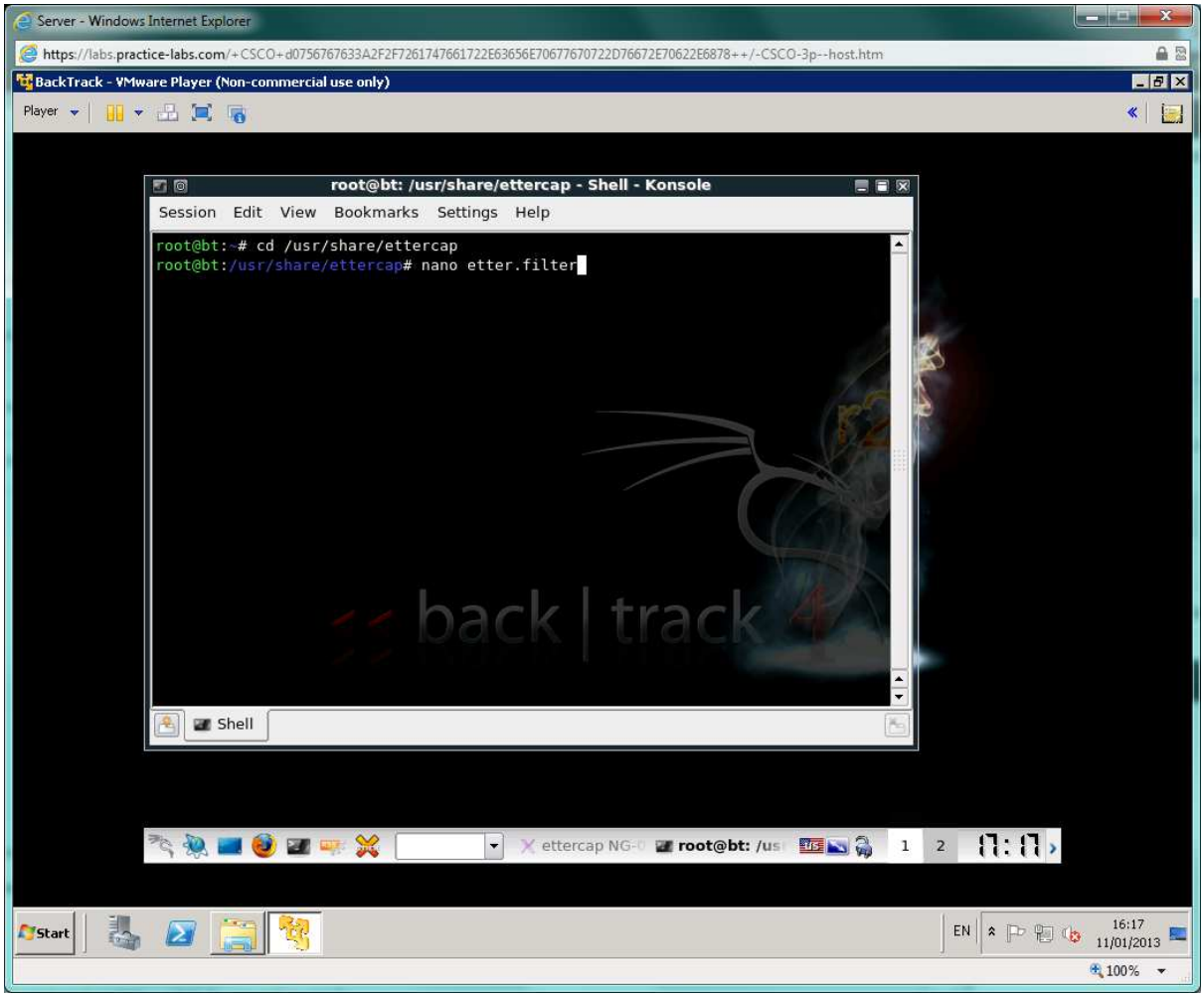


Open a console and enter:

cd /usr/share/ettercap

Then edit the etter.filter file by using the nano editor.

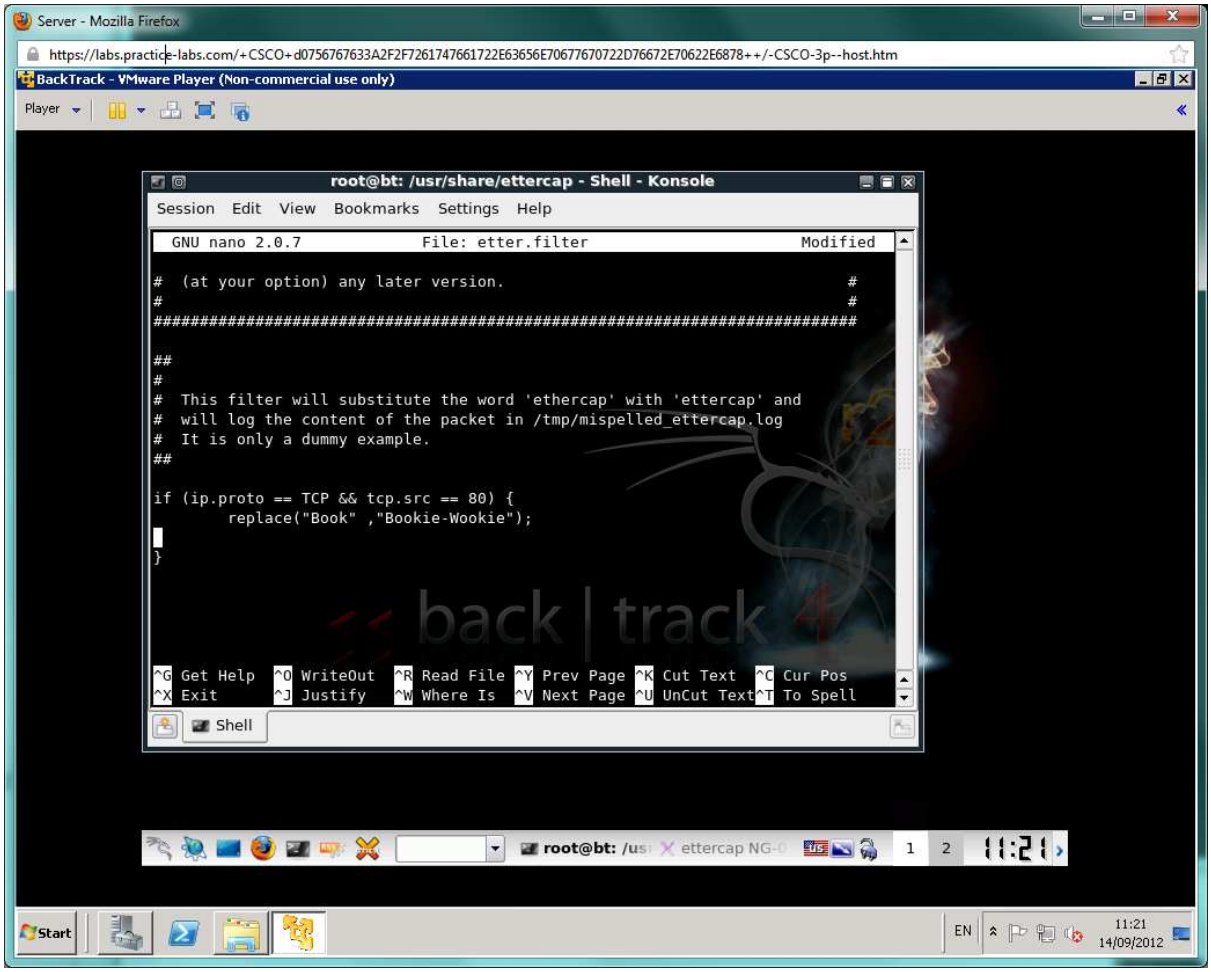
nano etter.filter



Delete the existing code and insert the following syntax:

if (ip.proto == TCP && tcp.src == 80) {

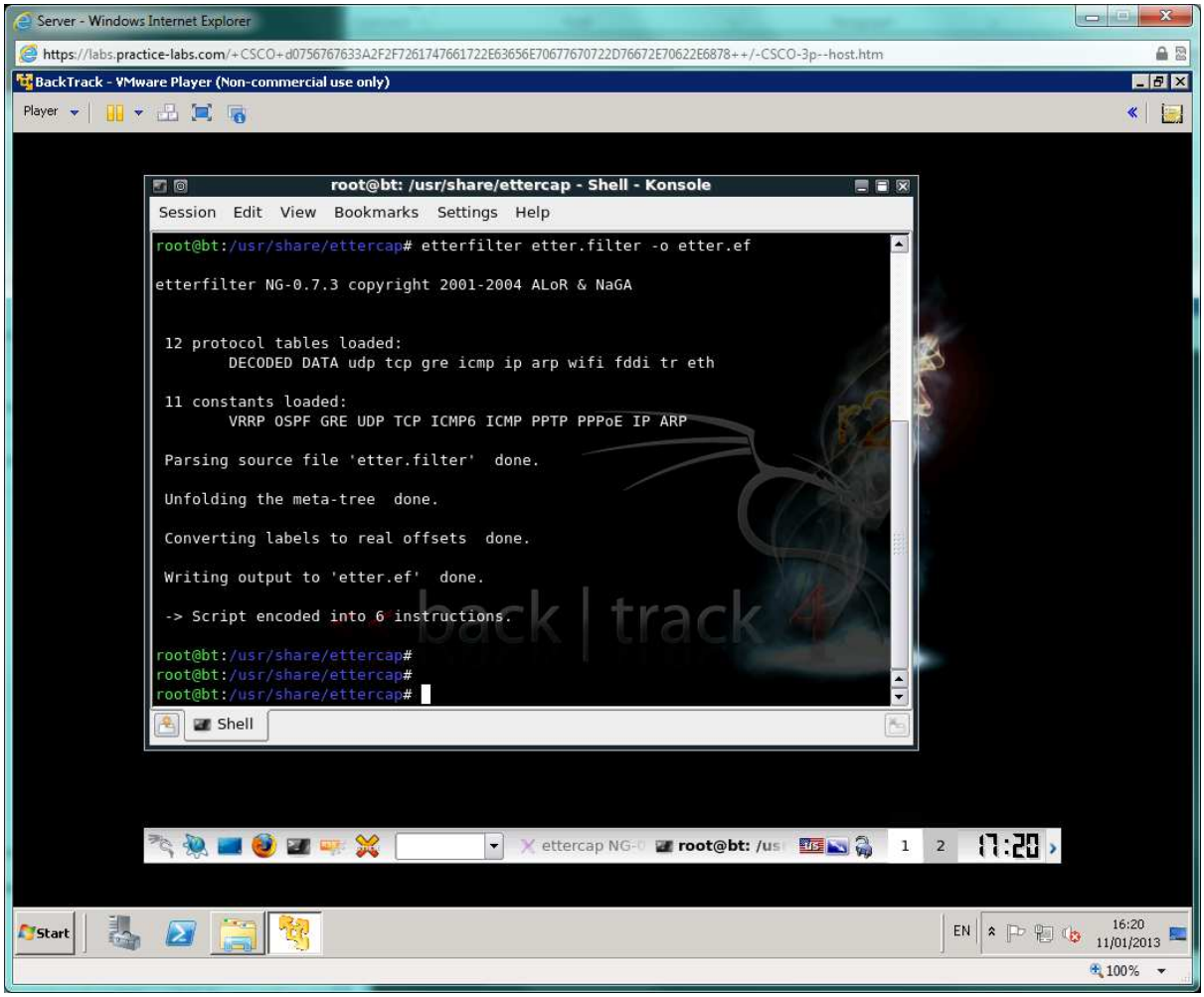
replace("Book", "Bookie-Wookie");}



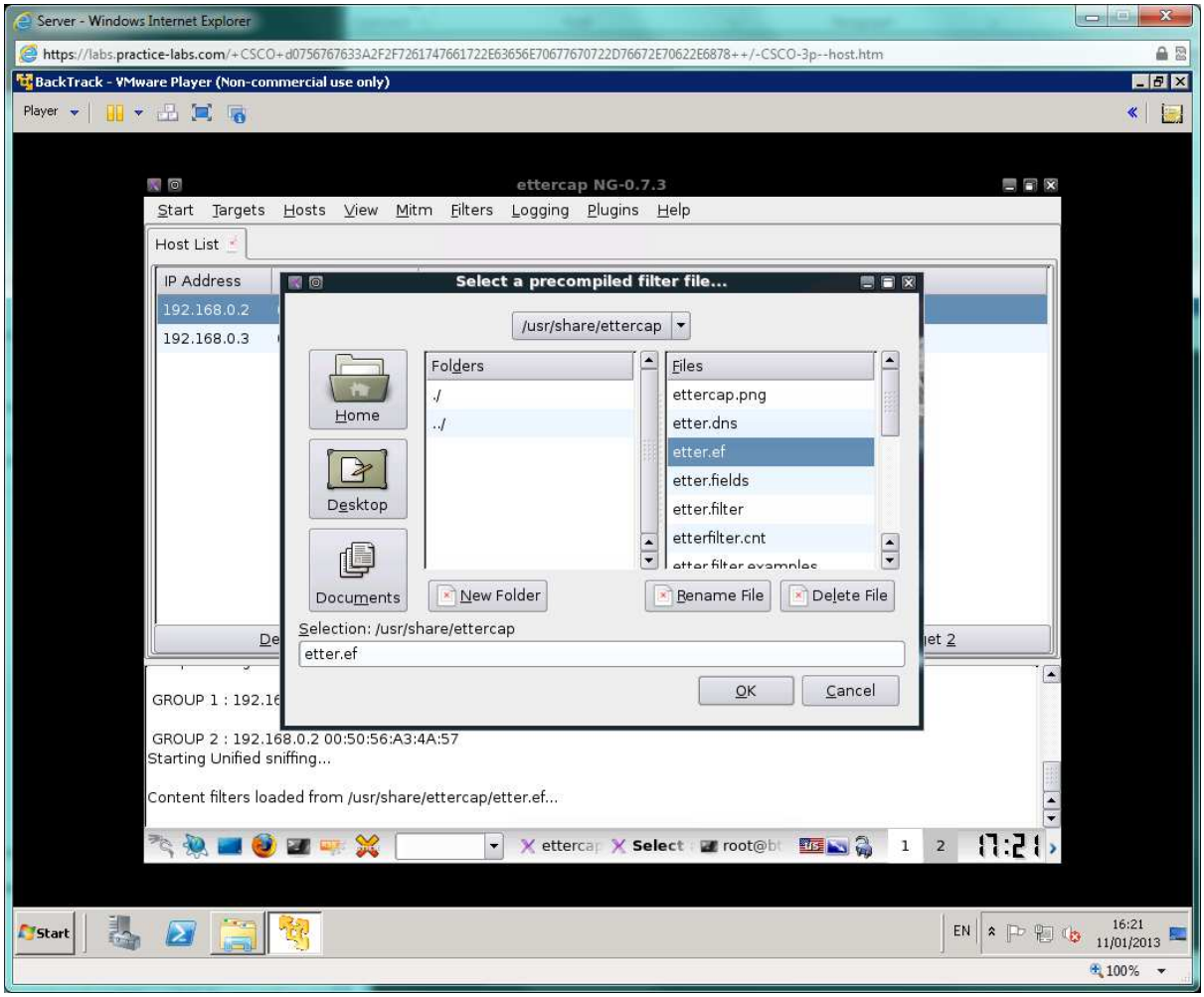
Press **Ctrl+O** then Enter to save the file then **Ctrl+X** to exit.

To compile the script (to make it usable in Ettercap), use the following command in the konsole:

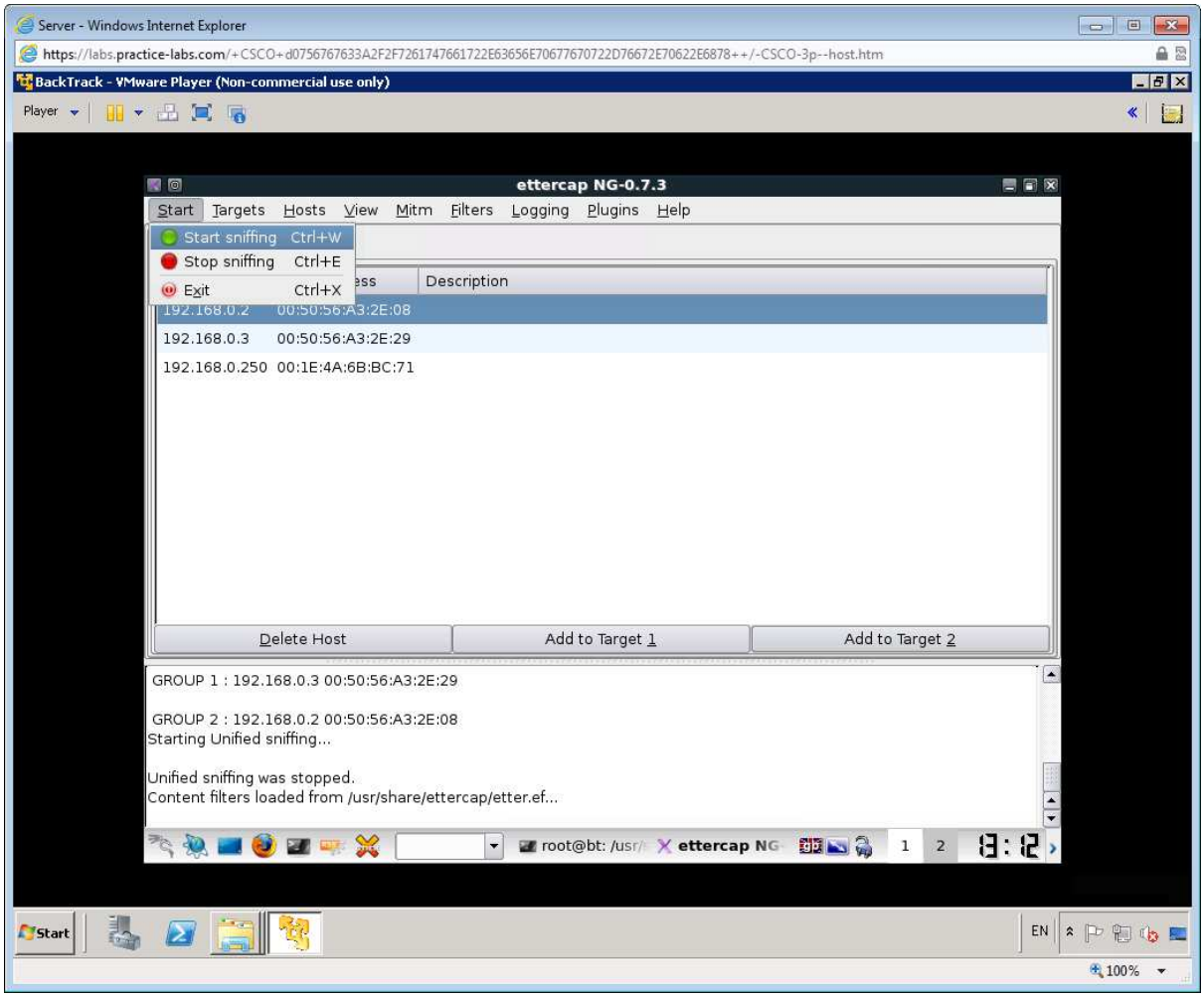
etterfilter etter.filter -o etter.ef



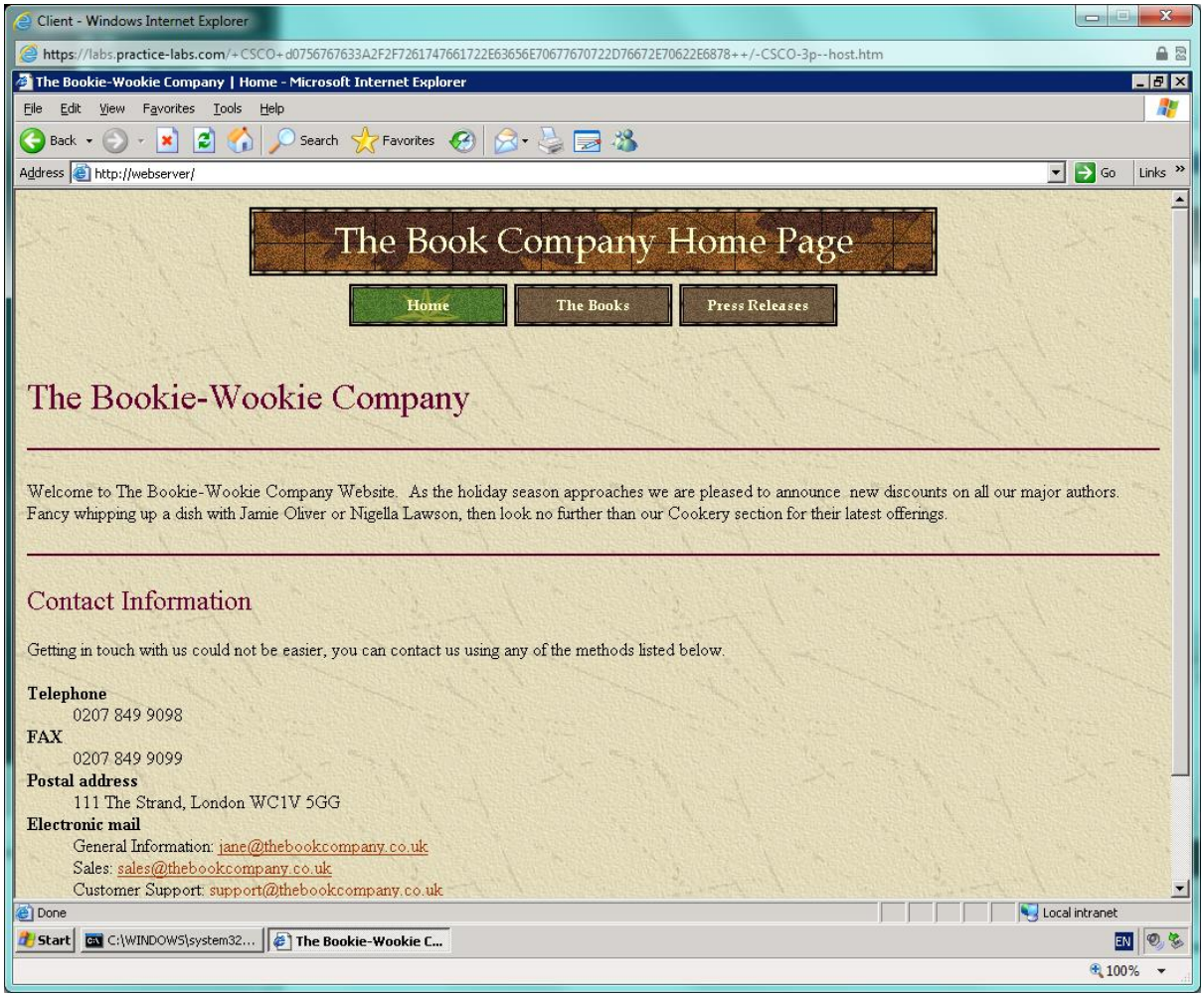
Switch back to Ettercap and select **Filters > Load a filter**. Select the **etter.ef** file and click OK.



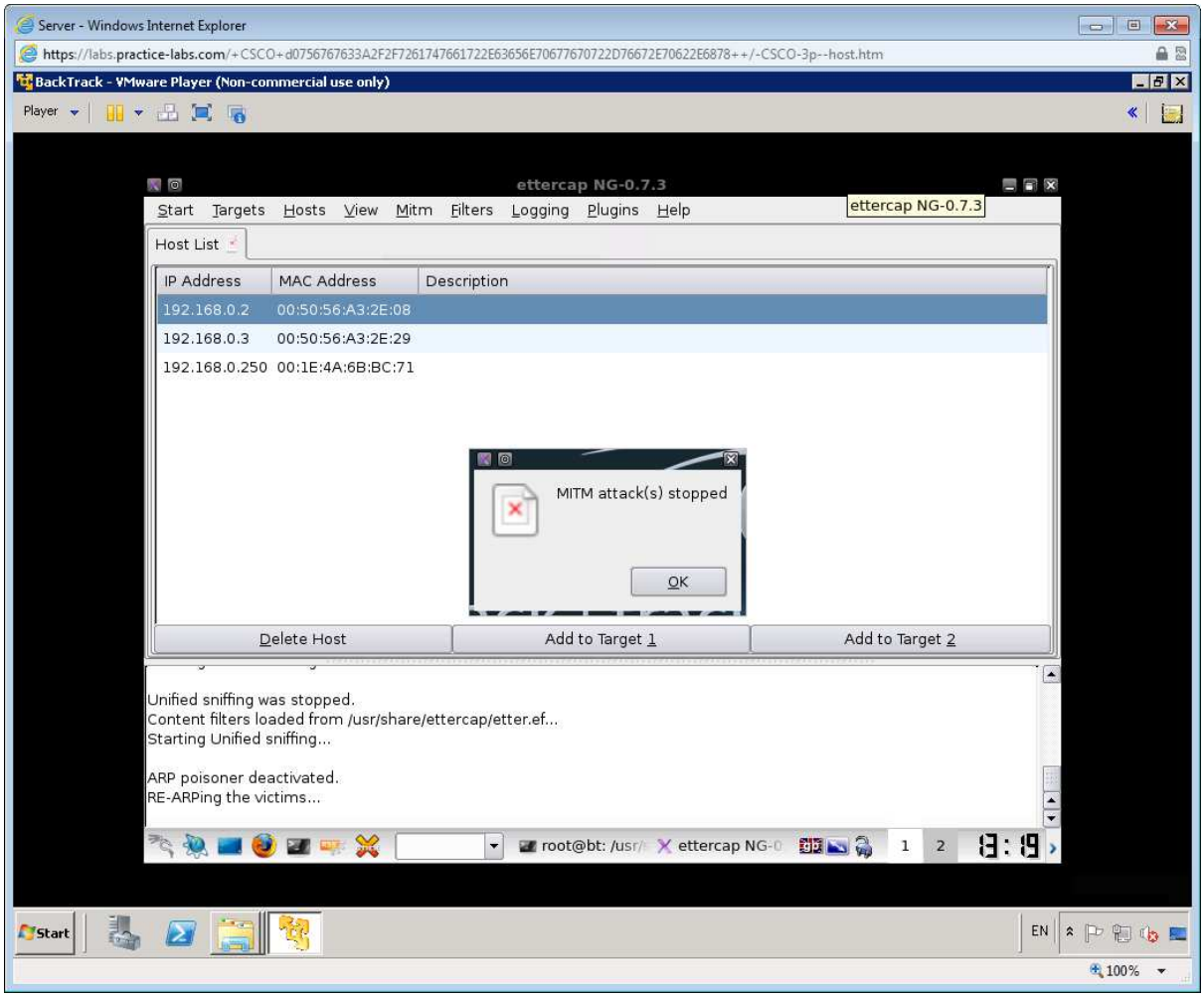
Start **Arp poisoning** and then **start sniffing.**



Switch back to the CLIENT workstation, open Internet Explorer, and load http ://webserver again (or press Ctrl+F5 to refresh the page). You should see a vandalized page which has change the heading from The Book Company to The Bookie-Wookie Company.



Switch over to BACKTRACK and in Ettercap, select **Filters > Stop filtering** then **Mitm > Stop Mitm attack(s)**.



Close Ettercap.

Switch to CLIENT and run **arp -a** - the ARP cache should have been restored.

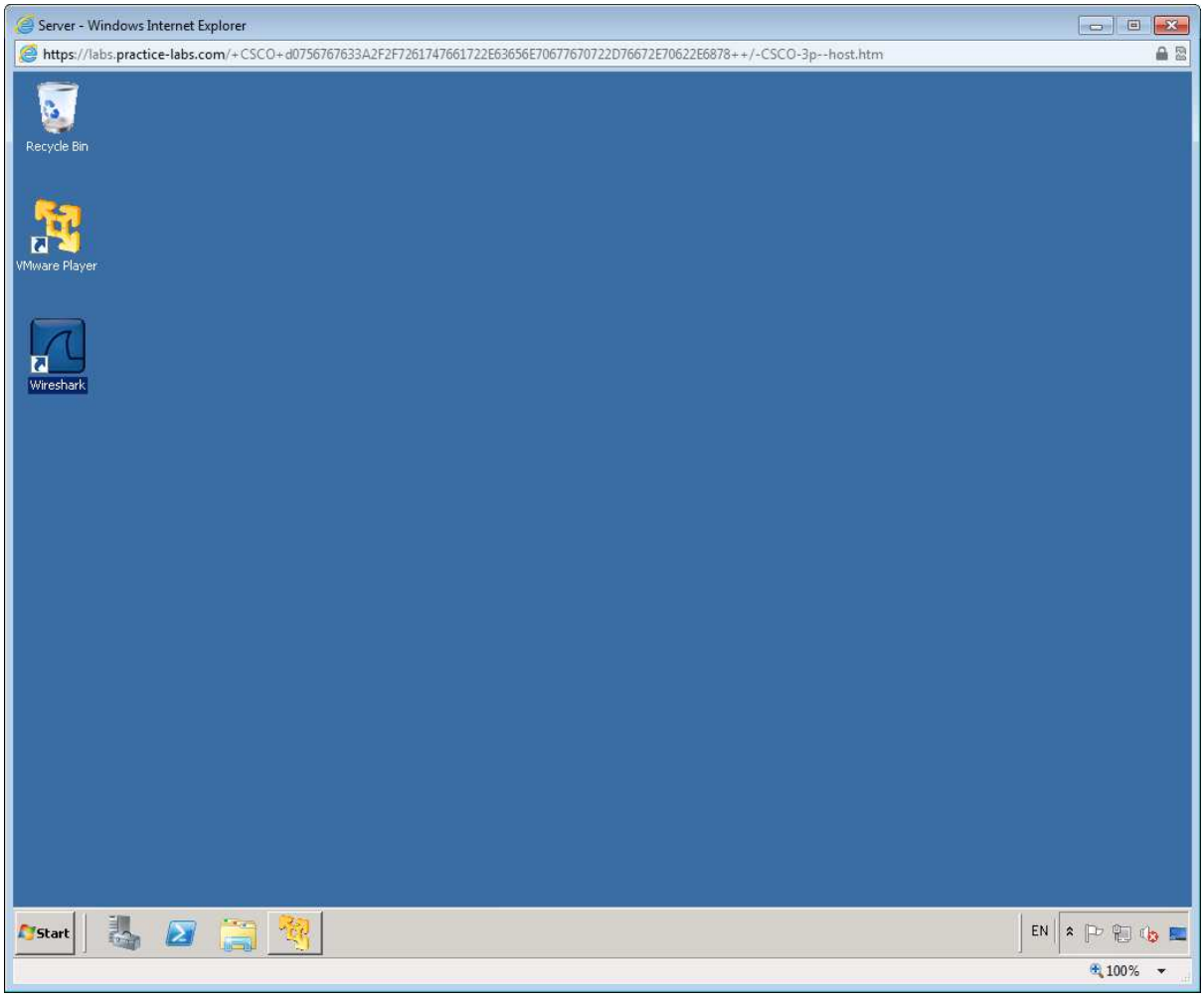
Continue to the next exercise in order to learn more about Denial of service attacks.

Exercise 4 - Denial of Service

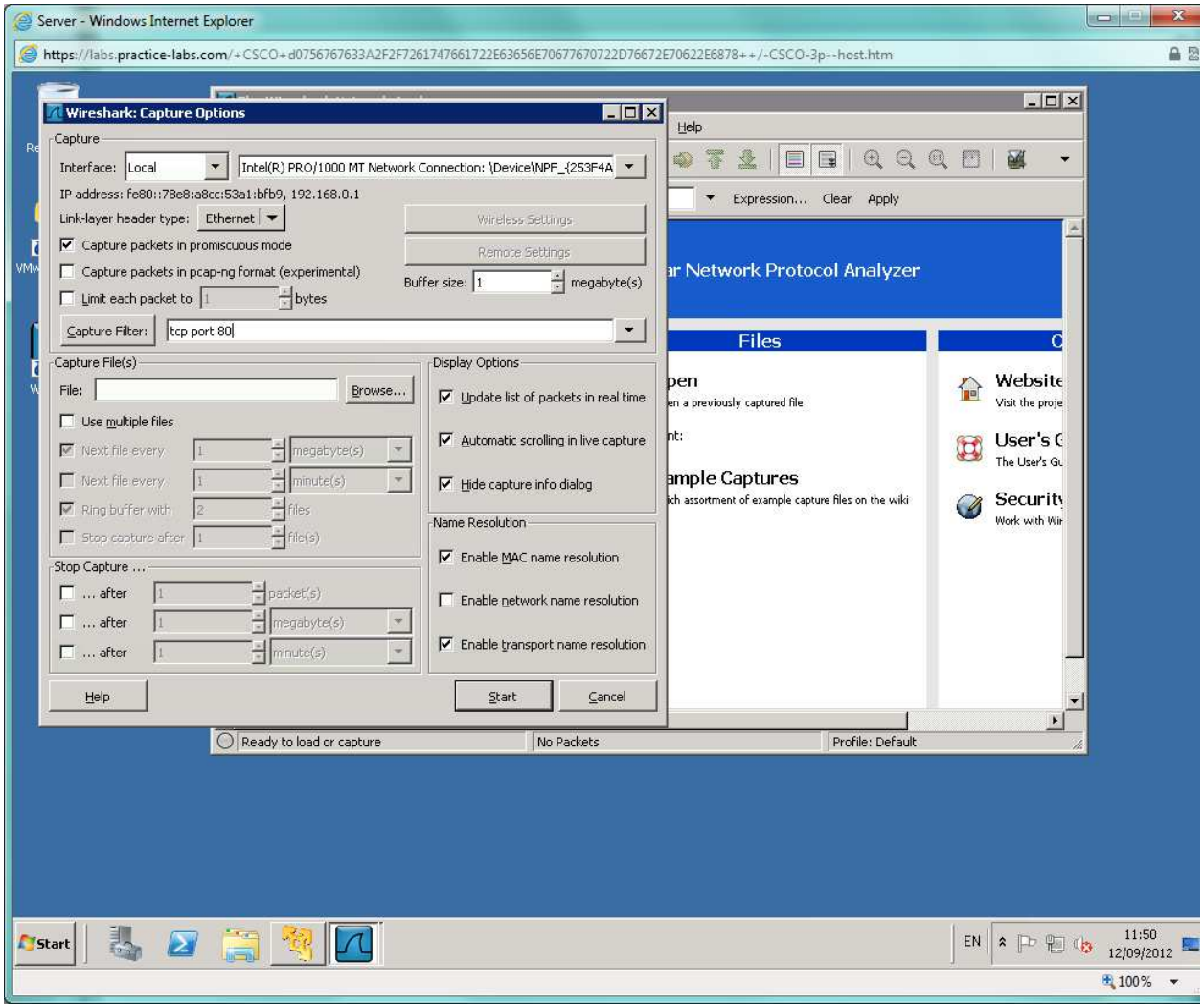
The last major class of attack is Denial of Service (DoS). There are any number of ways to prevent a server from responding to clients. We could have used Ettercap to simply discard any packets from client or server for instance.

Flood type attacks really depend on overwhelming the victim system with superior bandwidth, which itself depends on compromising thousands or even millions of "zombie" PCs in a "botnet". This exercise just illustrates how simple it is to craft the sort of malformed packets that can be used to try to flood a server.

On the SERVER, start Wireshark using the icon located on the Desktop.



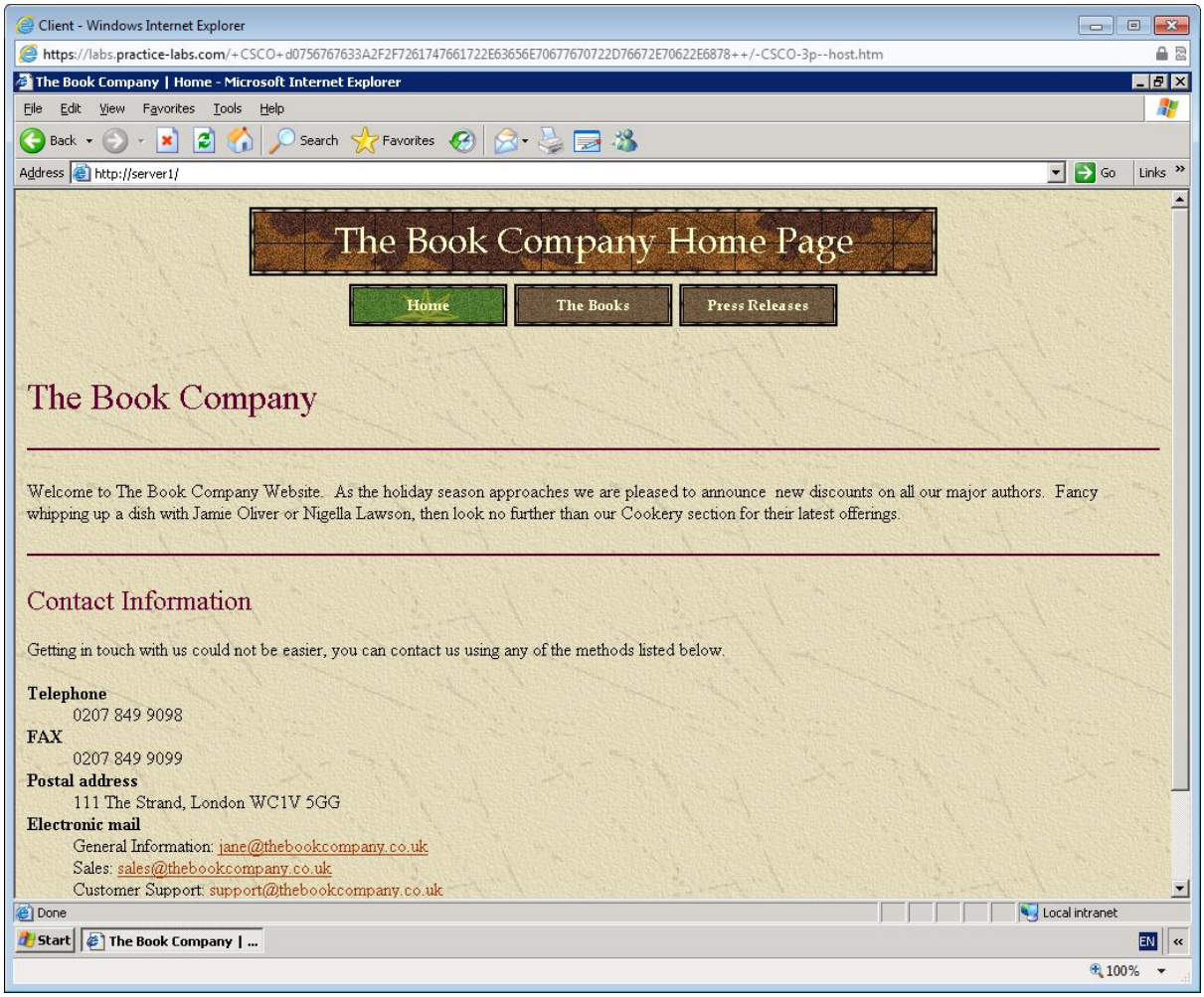
Open the **Capture Options** dialog. In the "Filter options" box, enter **tcp port 80** then start the capture.



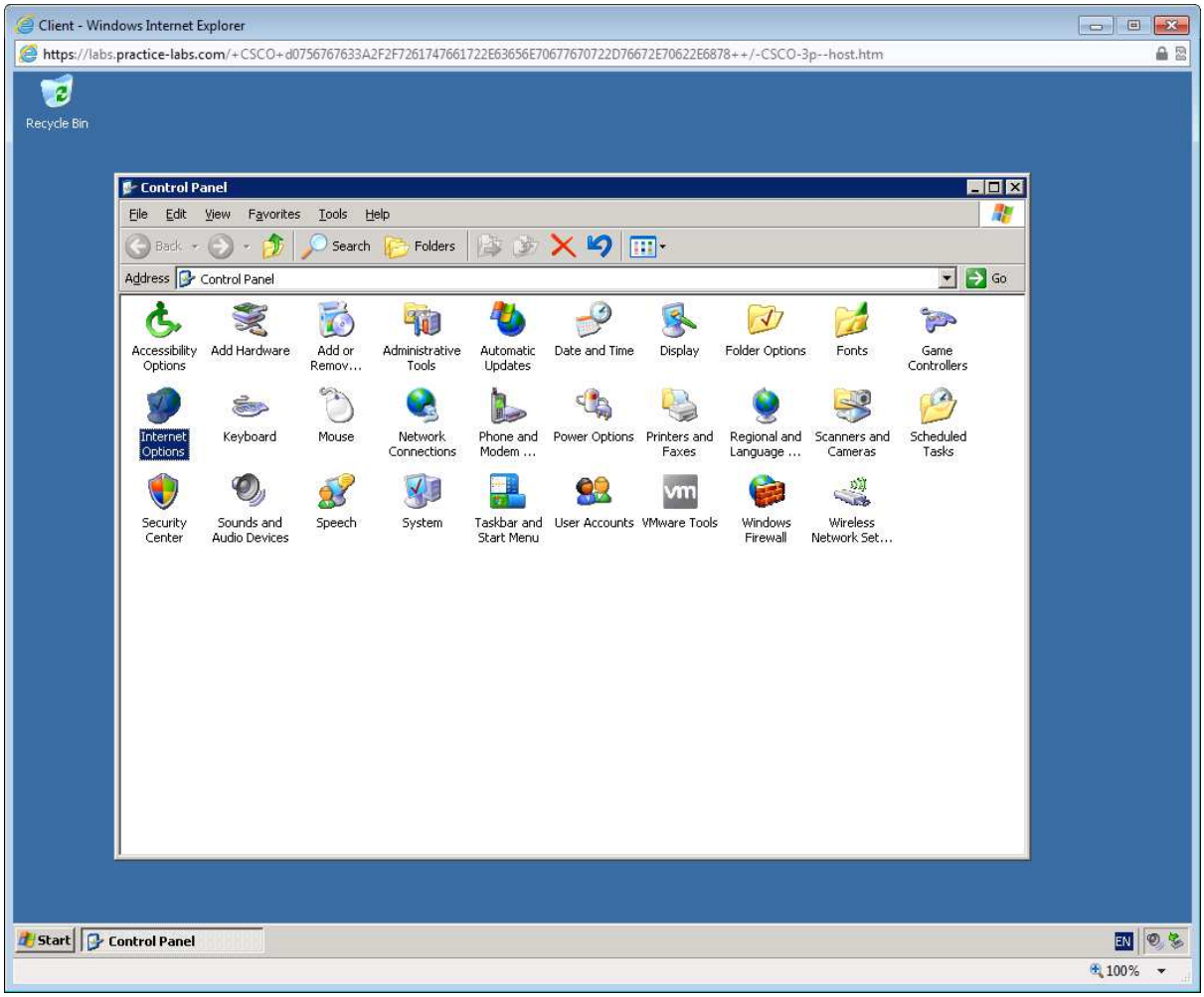
From the CLIENT workstation, open Internet Explorer type the following url into the address bar:

http://server1

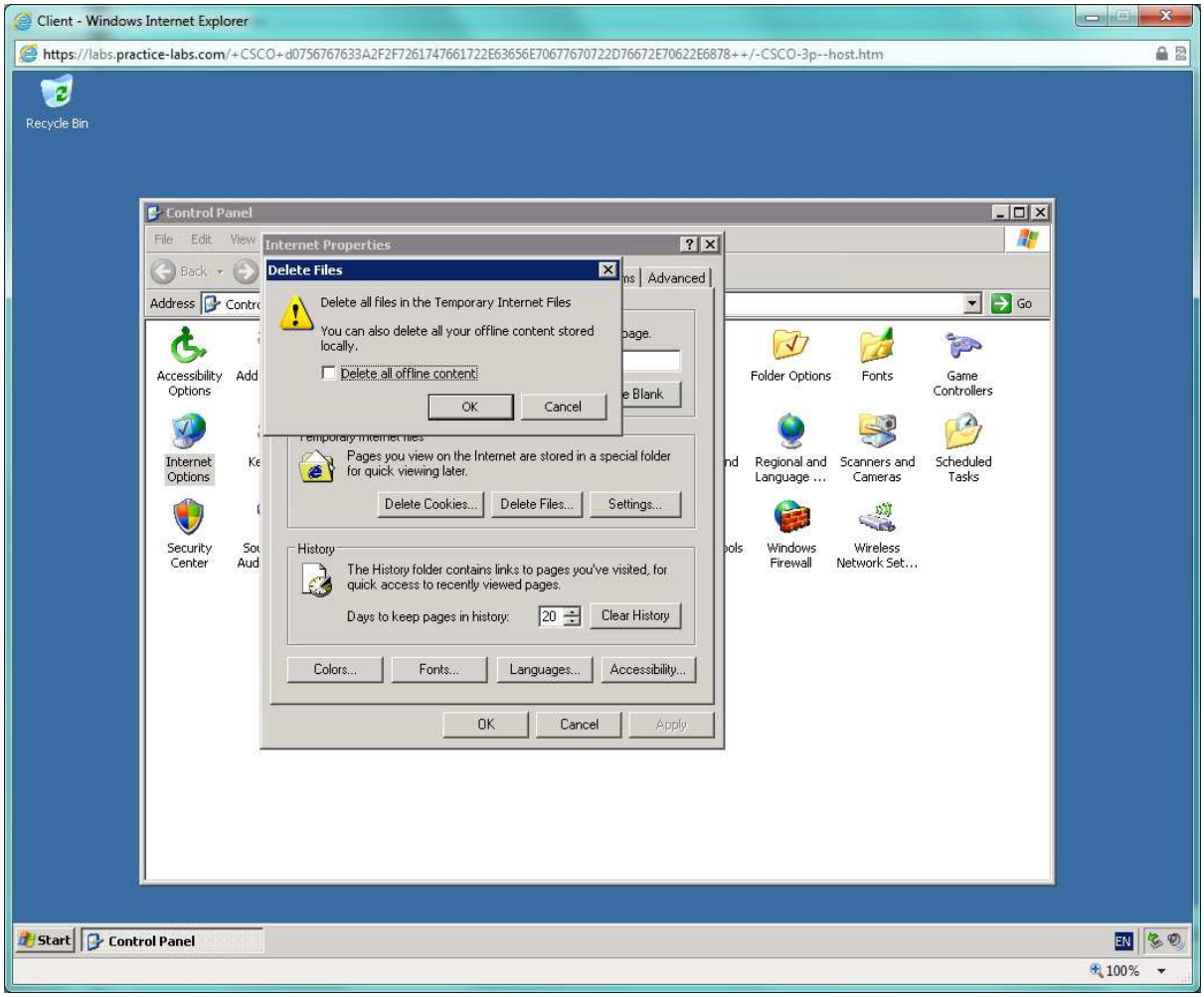
Navigate around the webpages making a mental note of how quick they are to load (there should be no noticeable delay).



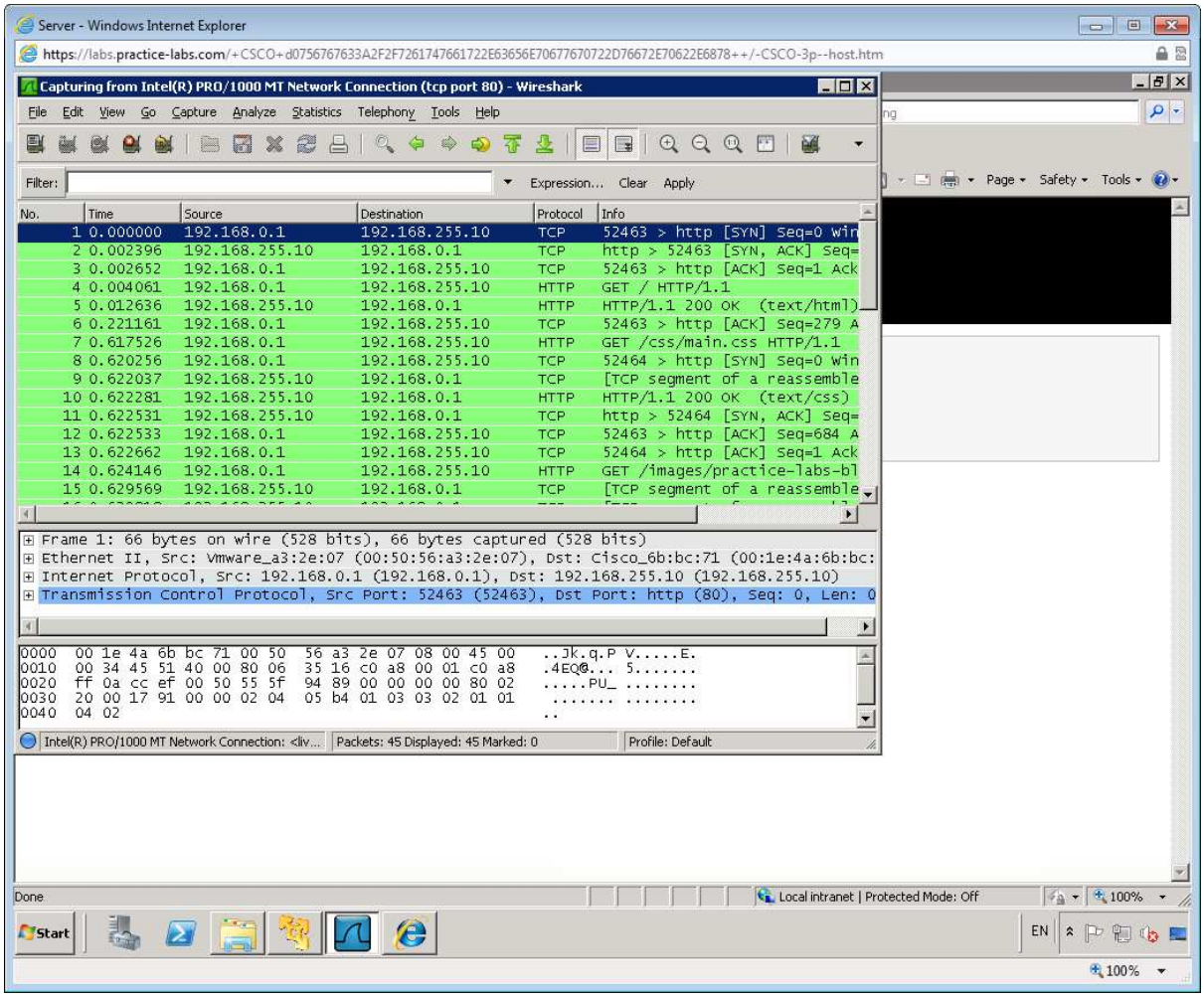
Close the Internet Explorer then open the **Internet Options** applet in **Control Panel**.



Under "Temporary Internet files", click **Delete Files** then click OK to both dialogs.

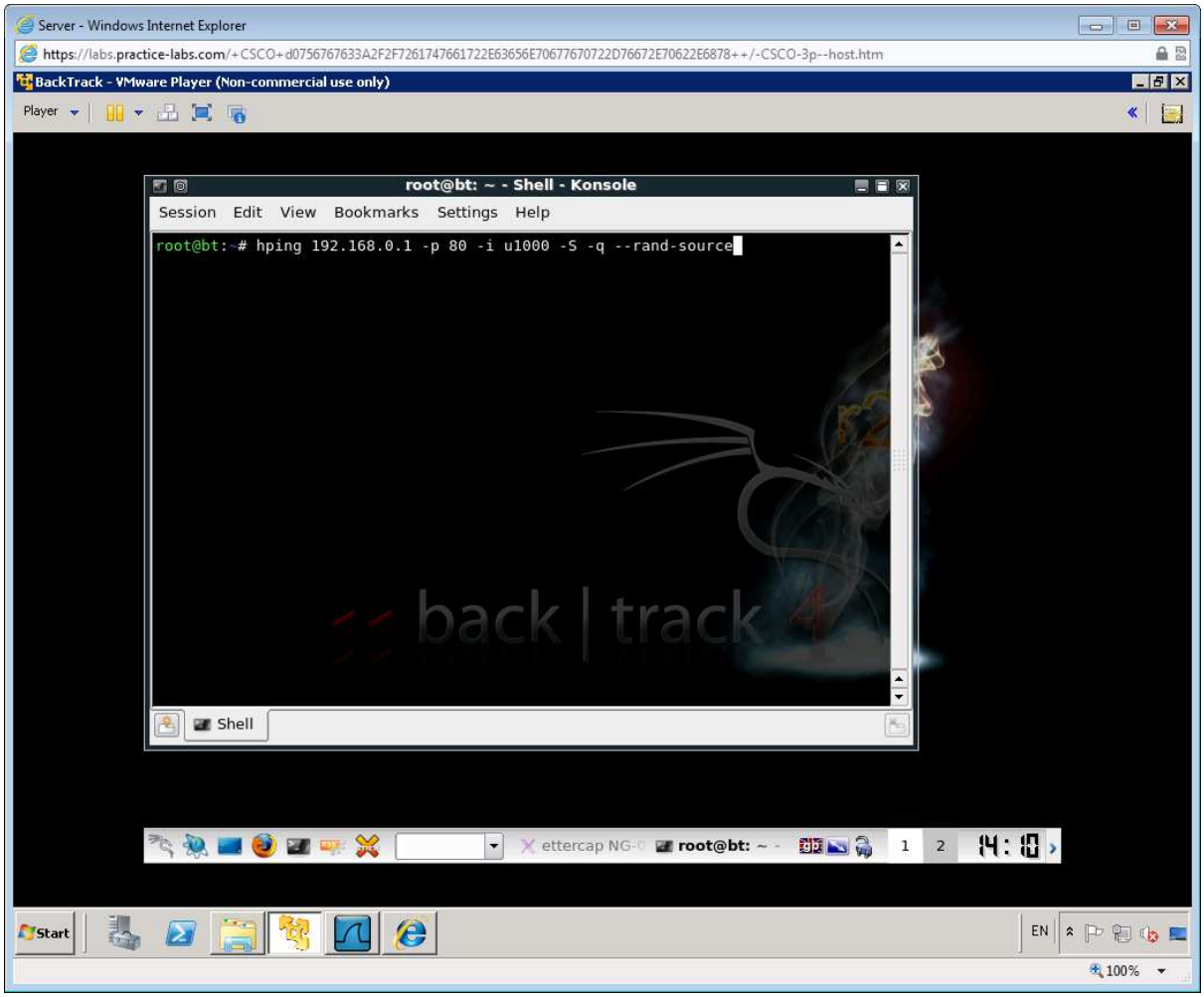


Switch to the SERVER and review the details in WireShark, note the **SYN > SYN/ACK > ACK** sequence in the first three packets. The remainder of the capture shows the CLIENT workstation retrieving the page using HTTP.



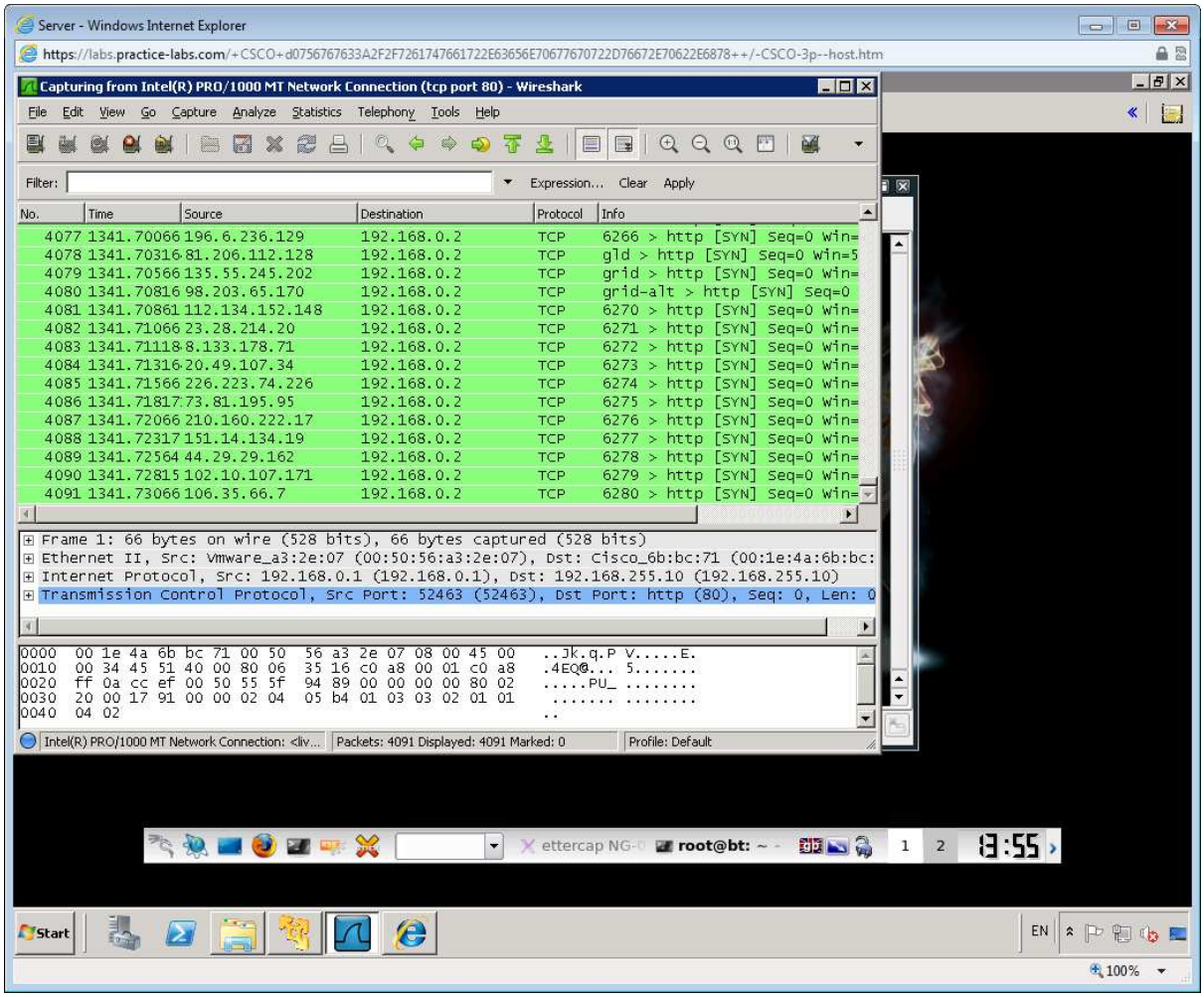
On the BACKTRACK, click in the console window then run the following command (remember that it is case sensitive and ignore the line break - type the whole command then press **Enter**):

hping 192.168.0.1 -p 80 -i u1000 -S -q --rand-source



hping crafts "SYN" packets from random spoofed IP addresses and sends them out at very short intervals.

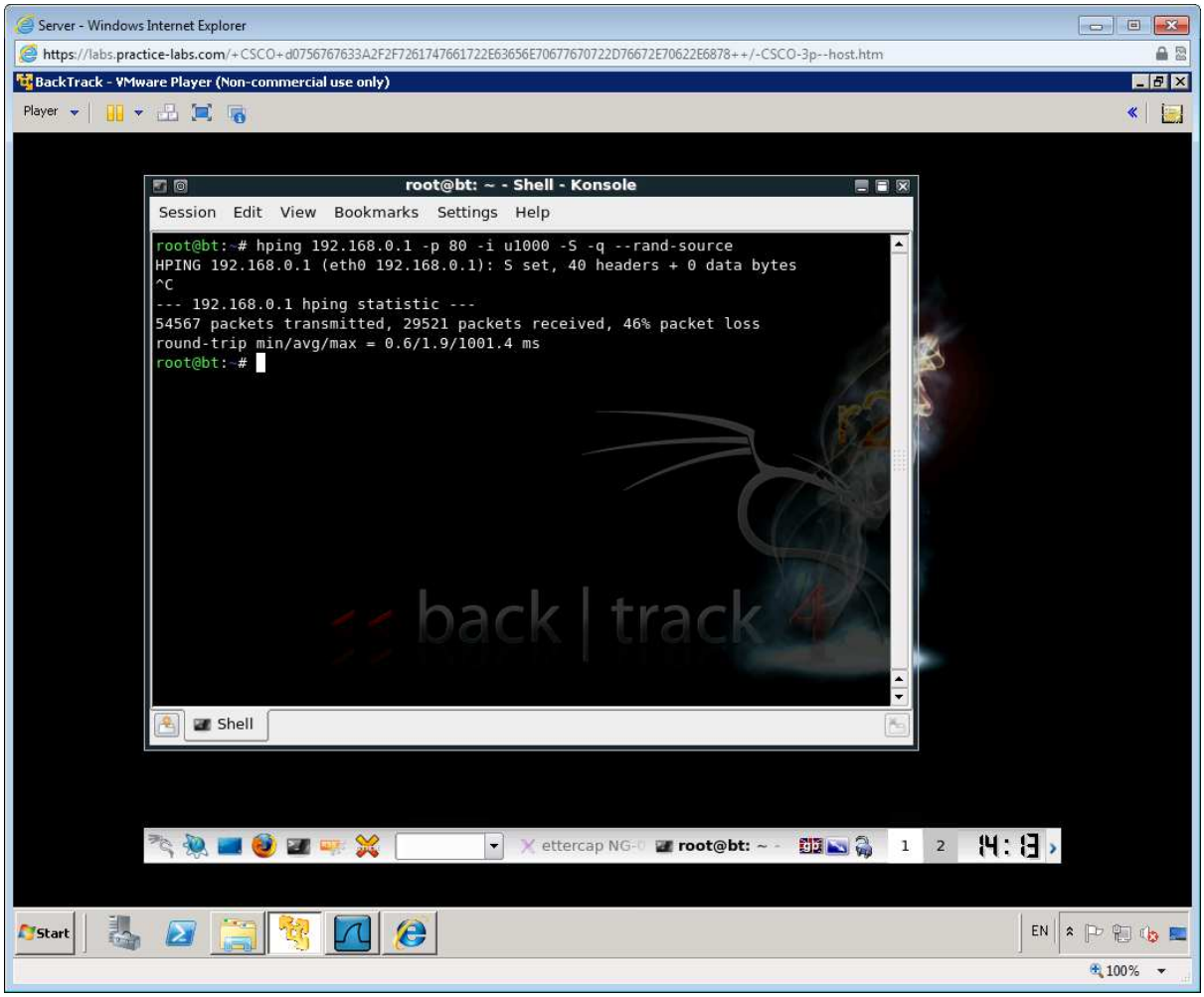
Note the flood of packets captured by Wireshark on SERVER.



On the CLIENT workstation, open IE and browse to the same webpage you did previously (http ://server1) you will notice it takes longer to load.

Clearly you would need a lot more bandwidth to overwhelm the server completely.

Switch to the BACKTRACK Server and halt **hping** using the **Ctrl+C** key combo.



After completing these exercises you should have a better understanding of network vulnerabilities. Go through the exercises again changing some additional parameters to view different results.

Summary

In this lab you completed the following practical tasks:

- Network Footprinting
- Packet Sniffing
- MitM with ARP Spoofing
- Denial of Service

Also Try

Using your lab infrastructure you can attempt the following topics at your own pace.