40

**CSIS2270 - Lab #9 (Final Lab)**

***Packet Capturing and Analysis Using Wireshark on Virtual Machines***

**Name: Leandro Miranda Fahur Machado Student No.: 300326045**

**Due: Saturday, April 10th, 11:59 PM**

**Introduction:** Packet capturing and protocol analysis tool can be used to help us better understand how two devices communicate with each other. In this lab, we will be using the software tool ***Wireshark*** to capture messages sent from and received by your computer, and display the content of various protocol fields of each message. By capturing the packets, you can examine the process used by Address Resolution Protocol, and see how FTP uses TCP to move user data across the network.

**Objectives:**

1. To gain a good understanding of the packet capturing tool ***Wireshark***.
2. To gain experience in using protocol capturing and analysis tool for analyzing network traffic.
3. To understand the operations of ARP, TCP and FTP protocols.
4. To get familiar with PDU’s encapsulation between different protocol layers.

**Equipment Required:**

1. Two VMs (VM1 Win 10 and VM1C Win 10 from previous labs) connected through a virtual network
2. Wireshark installation program.

**NOTE: You are required to download the Wireshark Installer (64-bit) for Windows from** [***http://www.wireshark.org***](http://www.wireshark.org) **,** (or get it from the instructor’s Blackboard page)

**Introduction to Wireshark**

Figure 1 shows the structure of a **packet sniffe**r which can be used to capture messages sent from or received by your computer. It is composed mainly of two parts: the packet capture library and the packet analyzer. The packet capture library stores a copy of every layer 2 frame that is sent from or received by the computer. Since your computer is connected to an Ethernet network, all higher layer protocol data units (PDUs) are hence encapsulated within the Ethernet frames.



The packet analyzer is used to display the contents of all the fields within the Ethernet frames. It is capable of identifying the various protocols’ fields and structures; hence, it can identify the IP datagram within an Ethernet frame, the TCP PDU within the IP, and the higher layer application data within TCP.

We will be using a free packet sniffer, ***Wireshark***, for this lab. You can download a copy of Wireshark from http://www.wireshark.org, and you can get a user’s guide and other documents from https://www.wireshark.org/docs/.

1. **Network Setup [\_\_\_\_\_/4]**
2. Start VirtualBox manager on your computer (the host)
3. Start both VM1 Win 10 and VM1C Win 10. For this lab we will refer to the virtual machine VM1 Win 10 as virtual PC A and to virtual machine VM1C Win 10 as virtual PC B.
4. Through the setting of each VM, make sure that both of them are connected to the same virtual adapter (Host-Only Ethernet Adapter) which you have created earlier.
5. What is the ip address of virtual PC A? **192.168.56.101**

What is the ip address of virtual PC B? **192.168.56.102**

1. Make sure that the Fire Wall is off on both virtual PCs
2. Test the connectivity between the two virtual PCs.  
   What is the command used for testing connectivity? **Ping**
3. **Wireshark installation [\_\_\_\_\_/4]**
4. Copy the WireShark installation file to the desktop of each virtual PC
5. Run the installation file.
6. Take the default settings during installation. Note that ***Npcap/WinPcap*** will also need to be installed.
7. Run Wireshark on virtual PC A when installation is completed.
8. An ***Interface List*** will be shown on the first screen giving you a list of network interfaces (adapters) on your virtual PC A. Select the Ethernet interface(adapter) that your virtual PC is connected to, which will be used by Wireshark to capture the packets.
9. Click the *blue**shark fin* icon on the top left to start packet capture, and a screen will be displayed showing information about the packets being captured. Stop packet capturing by clicking the Stop button on the command menu.



1. **Using Wireshark to study ARP requests and replies [\_\_\_\_\_/16]**

Since all messages exchange between any two devices on an Ethernet network will be encapsulated in Ethernet frames, it is necessary for the devices to determine each other’s physical address before messages can be exchanged. Knowing the destination’s IP address, a device can find out the corresponding MAC address by use of the Address Resolution Protocol (ARP). We will use Wireshark to capture the packets exchanges between the two PCs to gain a better understanding of ARP.

What is the physical address (MAC address) of the Ethernet interface on virtual PC A?  
 **08:00:27:E9:64:7B**

What is the physical address (MAC address) of the Ethernet interface on virtual PC B?  
 **08:00:AC:E9:D4:70**

Do the following on virtual PC A.

1. Open a ***cmd*** window and run it as administrator.
2. Use the command ***arp –a*** to examine the contents of the ARP table on the virtual PC A.
3. Start Wireshark and select the Ethernet interface, but DO NOT start packet capturing yet.
4. In the ***cmd*** window, use ***arp –d*** to delete all entries in the ARP table. Use ***arp –a*** to re-examine the ARP table and ensure that it is empty.
5. Start packet capturing on Wireshark on virtual PC A.
6. Ping virtual PC B from virtual PC A.
7. Stop packet capturing on Wireshark on virtual PC A.
8. By examining the packets captured as outlined in the next two steps, you should see some ***arp*** packets followed by some ***icmp*** packets.
9. Examine the ***arp*** packets captured.
   1. Type ***arp*** in the filter box and press Enter. Only arp packets should now be displayed.
   2. Select the first packet listed.

* What is the source address in the Ethernet frame? **192.168.56.101**
* What is the destination address in the Ethernet frame? **192.168.56.102**
* From the ARP PDU:
  + What is the Opcode? **Request**
  + What is the Sender MAC address? **08:00:AC:E9:D4:70**
  + What is the Sender IP address? **192.168.56.102**
  + What is the Target MAC address? **08:00:27:E9:64:7B**
  + What is the Target IP address? **192.168.56.101**
  1. Select the second packet listed.
* What is the source address in the Ethernet frame?
* What is the destination address in the Ethernet frame?
* From the ARP PDU:
  + What is the Opcode? **Reply**
  + What is the Sender MAC address? **08:00:27:E9:64:7B**
  + What is the Sender IP address? **192.168.56.101**
  + What is the Target MAC address? **08:00:AC:E9:D4:70**
  + What is the Target IP address? **192.168.56.102**

1. Examine the ***ICMP*** packets.
2. ICMP is the protocol used by the ***ping*** command for sending an ***echo request*** message to the remote device, and for the remote device to return a corresponding response ***echo reply*** message back.
3. Type ***icmp*** in the filter box and press Enter. Only icmp packets should now be displayed.

* How many Echo request/reply message pairs are there?
* What are the source and destination MAC addresses of the first ***Echo request*** message?

**Source: 08:00:27:E9:64:7B**

**Destination: 08:00:AC:E9:D4:70**

* What are the source and destination IP addresses of the first ***Echo requ***est message?

**Source: 192.168.56.101**

**Destination: 192.168.56.102**

* What are the source and destination IP addresses of the first ***Echo reply*** message?

**Source: 192.168.56.102**

**Destination: 192.168.56.101**

* For the Echo request message, what is the value of ***Type*** in the ICMP PDU? **8**
* For the Echo reply message, what is the value of ***Type*** in the ICMP PDU? **0**
* The Round Trip Time (RTT) is calculated by subtracting the time when the ***request*** was sent from the time when the ***reply*** was received. Determine the RTT for the first Echo request/reply pair. (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark *View* pull down menu, then select Time *Display Format*, then select *Time-of-day*.) **07:21:11 ,426030**
* Examine the ICMP field of the first reply message. What is the ***Response*** time shown? **0.279572 ms.**

1. **Using Wireshark to study FTP session [\_\_\_\_\_/16]**

**Refer to the lab work from lab#8**

1. Ensure that the ftp server has been setup and started on virtual PC A (the FTP server).
2. Test from virtual PC B that the ftp server on virtual PC A is working.
3. Use the file ***test.txt*** saved already on virtual **PC B** (the FTP client)in the folder C:\users\public
4. Open the ***cmd*** on the virtual PC A (the FTP server) and change the directory to C:\users\public  
   then use ***dir*** command to check that *test.txt* file still there (from previous lab9). Now you have to delete it using the command c:\users\public > ***erase*** *test.txt* so that it will not exist on this computer any more.
5. In the cmd window of virtual PC B, use *arp –d* to delete all entries in the ARP table.  
    Use *arp –a* to re-examine the arp table and see it is empty.  
     
   **STEPS 6-11 MUST BE DONE WITHOUT INTERRUPTION**
6. Start packet capturing using ***Wireshark*** on virtual PC B.
7. Open ftp session on virtual PC B using the user name ***anonymous*** with no password.
8. Use ***dir*** to double check that test.txt is not exist there
9. Transfer the file ***test.txt*** from virtual PC B (the client) to virtual PC A (the FTP server) using the command: ftp> ***put*** *test.txt*.
10. End the ftp session by typing ***quit***.
11. Stop packet capturing on Wireshark on virtual PC B.
12. Examine the packets captured and you should see some ***arp*** packets followed by some ***tcp*** and ***ftp*** packets.
13. Type tcp in the filter box and press Enter. Only ***tcp*** and ***ftp*** (which runs on top of tcp) packets will be displayed.
14. Examine the three ***tcp*** packets captured BEFORE the first FTP message.

* For the first TCP message, which Flag is set in TCP? **S**
* For the second TCP message, which Flags are set in TCP? **A-S**
* For the third TCP message, which Flag is set in TCP? **A**
  + The above is known as three-way handshake that is used by TCP to set up a connection between two devices before data exchange.

1. Examine the FTP messages exchanged between the server and the client. Note that the server sent ***Response*** messages to the client, whereas the client sent ***Request*** messages to the server.
2. After client user logged in and before the transfer of the file, can you see there is another three-way handshake that TCP used to establish another connection between the two devices? **YES**

What are the packet numbers of these TCP messages shown on the first column?

The second TCP connection is used by ftp for data transfer whereas the first TCP connection is for ftp control data.

1. Examine the packet that sent your file to the server (FTP-DATA).

* How many bytes of data were sent (TCP payload)?
* Can you see the content of the file in the packet? **YES**

1. Observe the TCP packets with the FIN flag set. The FIN TCP packets are exchanged between the two devices to close a connection.
   * How many TCP packets are there with FIN flag set?

* The first two were sent after the file transfer to close the data connection. What was the FTP operation that caused the last two FIN packets to be sent? **Closing data connection (226) , Transfer Complete.**

1. Close the WireShark programs on both virtual PCs

Finish all the steps and answer all the questions then save the lab report file as instructed in the submission instructions below.

**You have finished all labs. You should switch the firewall back on on your PC.**

**Lab Submission instructions:**

1. Save your report file as yourFirstnameLastname\_Lab9.docx.  
    (example: RupaManabala\_Lab9.docx)
2. Send the file to your instructor no later 11:59 pm of Saturday, April 10th, 2021 via Blackboard only (do not send labs by email please. Any lab submitted by email will be ignored).
3. Late submissions will not be marked and the student will lose the mark of that lab.
4. Students who don’t save lab files with proper names as indicated in 1,2,3 above, will lose 50% of the lab’s mark.