**Undergraduate Program in Information Assurance Engineering**

**IA-201: Introduction to Information Assurance**

Lab 8 – Packets – Packet Capturing

**Lab Objective:**

The objective of this lab is to introduce students to Wireshark and packet capturing. The students will be able to use Wireshark to capture packets on a network. Students will also be introduced to what network packets are.

**Laboratory Deliverable:**

1. Screenshot of Wireshark session with successful capture.
2. Pcap of your lab session.

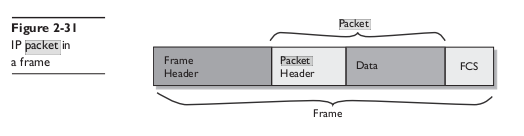
**Materials:**

1. Backtrack 4 Virtual Machine
2. Metasploitable Virtual Machine

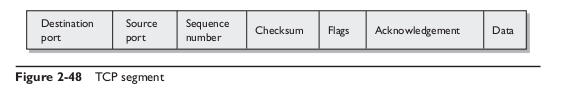
**Background:**

A network packet is a container containing data that is sent between networked computers. Packets can use different protocols and their data will differ. A frame is the container for a packet and allows for the packet to be sent from one device to another.

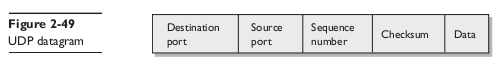
The following is an IP packet and its frame.



The data within the IP packet is called the TCP segment. It looks like the following:



The data within an IP packet could also be a UDP datagram. It looks like the following:



**Instructions:**

1. Open your Backtrack VM and make sure it’s network settings are set to Custom VMnet3. Then edit the /etc/network/interfaces file to look like:

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet static

address 192.168.100.201

netmask 255.255.255.0

network 192.168.100.0

1. Now we need to restart the networking. On your Backtrack VM, execute:

$ /etc/init.d/networking restart

1. Now we need to open Metasploitable VM and make sure it’s networking settings are set to Custom VMnet3. Then edit the /etc/network/interfaces file to look like (remember to edit the file using root privileges):

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet static

address 192.168.100.202

netmask 255.255.255.0

network 192.168.100.0

1. Now we need to restart the networking. On your Backtrack VM, execute:

$ sudo /etc/init.d/networking restart

1. We need to open Wireshark. On Backtrack, open Applications->Privilege Escalation->All->Wireshark.
2. To begin capturing the network data, click Capture->Interfaces…. Click “Start” on the device called “eth0”. Confirm the IP address says “192.168.100.201”.
3. What we want to do now is populate our network capture by actively using the network. On Backtrack VM, execute:

$ ping –c 3 192.168.100.202

This sends 3 packets to the specified address.

1. On Backtrack VM, execute:

$ wget 192.168.100.202

1. On Backtrack, VM, execute:

$ ssh [msfadmin@192.168.100.202](mailto:msfadmin@192.168.100.202)

Login with the password “msfadmin”, then execute some command in the ssh terminal. Then logout by executing:

$ exit

1. In Backtrack, open the web browser and go to the url: <http://192.168.100.202/twiki/bin/view/Main/WebHome>
2. In the search form, enter your name.
3. Go to the url: <http://192.168.100.202/twiki/bin/view/TWiki/TWikiRegistration>

Register a user. This will give us a frame with a bunch of user provided data.

1. While you are in the TWiki website, navigate around the site to generate more frames.
2. In Backtrack VM, execute:

$ arping –c 3 192.168.100.202

1. In Backtrack VM, execute:

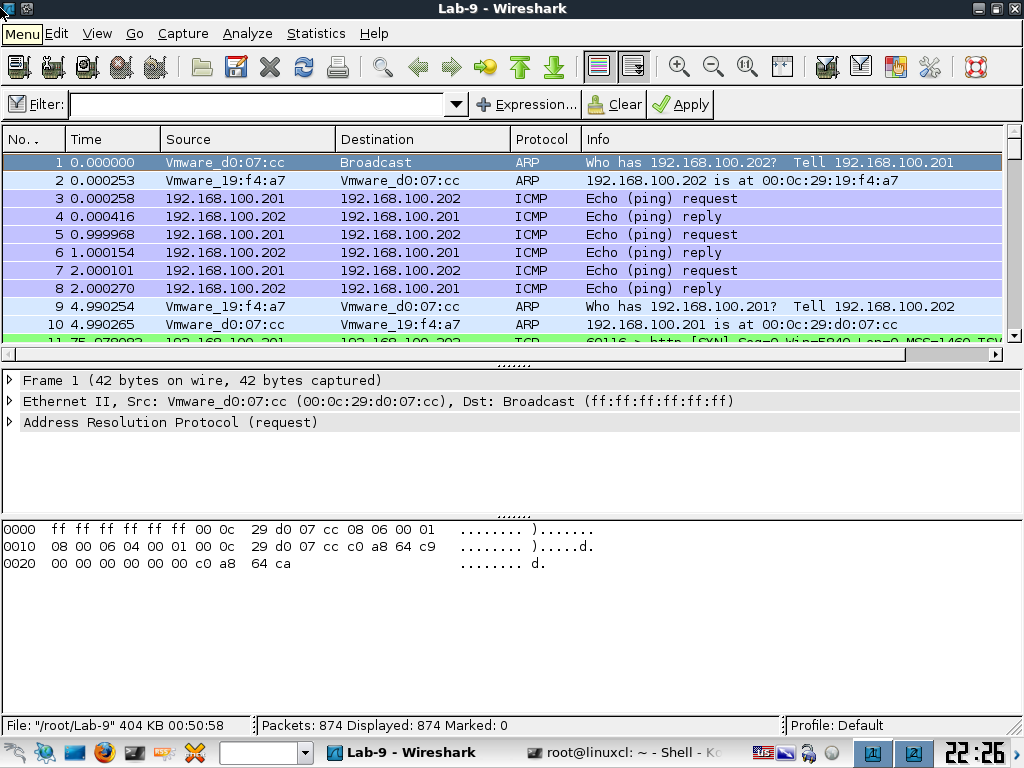
$ ftp 192.168.100.202

Login with “msfadmin” with the password “msfadmin”. To logout, execute:

$ exit

1. To stop capturing, click Capture->Stop.

Take a screenshot of your Wireshark session.



The top window is the Packet List which lists out all of the packet frames that have been captured.

The middle window is the Packet Details which breaks down the packet frame into a format that we can quickly navigate and understand what the frame says.

The bottom window is the Packet Bytes which is the actual data the frame is made up of.

1. Navigate through these windows and click different packet frames. Get used to the interface.
2. Save the capture by clicking File->Save As… and save the file as whatever you’d like. Try backing up the file somewhere. If you have to, change your networking settings to NAT and change your /etc/network/interfaces file to look like:

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet dhcp

And restart the networking by:

$ /etc/init.d/networking restart

Now that you are connected to the internet, send the file you saved to your email or save to some other online storage. We will be using this file next week.

==END==

**Questions:**

1. What is Wireshark? Wireshark is a software used to capture packets of data on the internet
2. What is a packet frame? A container for a packet which allows the packet to be sent and received
3. What is a packet? It contains data that is sent between networked computers
4. What is TCP? It is inside a IP packet, and it shows if there are any flags and if there is acknowledgement between the two computers as well as other basic information
5. What is UDP? It is inside the IP packet, and it shows the: destination port, source port, sequence number, checksum, and data
6. What is ICMP? Packets that are created when you ping other hosts
7. What is a pcap? An application programming interface for capturing network packets

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement** | **Points Allowed** | **Points Actual** | **Comments** |
|  |  |  |  |
| **Title page** | **5** |  |  |
| **Screen shots** | **5** |  |  |
| **Questions** | **10** |  |  |
| **Conclusion** | **5** |  |  |
|  |  |  |  |
| **Extra Credit** |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Total Points** | **25** |  |  |