Information Security

Assignment #1

Getting your hands dirty

Purpose:

The purpose of this assignment is to become familiar with some of the available tools that can be used for network analysis. These tools aid in understanding what happening in the Transport, Network and link level of the machine.

Environment and tools

All commands are for linux machines

Handing in format:

- **Please answer the following questions**
- Answer should be handed as a word or text document.
- In each section you will be asked question and your results needs to be documented.
- If you are asked to save a capture file please save it under the following format QX-section-myid.pcapng, is some cases the extension will be pcapng, this is also fine. (example **Q1-UnderstandingWireShark-111122123.pcapng)**
- Results need to be handed in also. Please zip the files and explain in the main document what each one is.

Answers:

- Should not be too long and informative (I can find the same information online also)
- Should not be too short (yes, I know you figure that I can complete the answers for you but let's assume this is not true)
- Answers should be short, full, to the point and address the question presented.

Not enough information? Need more information on a certain command? **Google it!**

Documentation:

- No printscreens!!!
- Attach text files or any required format properly labeled.
- Remember an entire encyclopedia in text format is 4 mb while 1 printscreen in BMP format is 1.2 mb.

1. **Understanding WireShark**

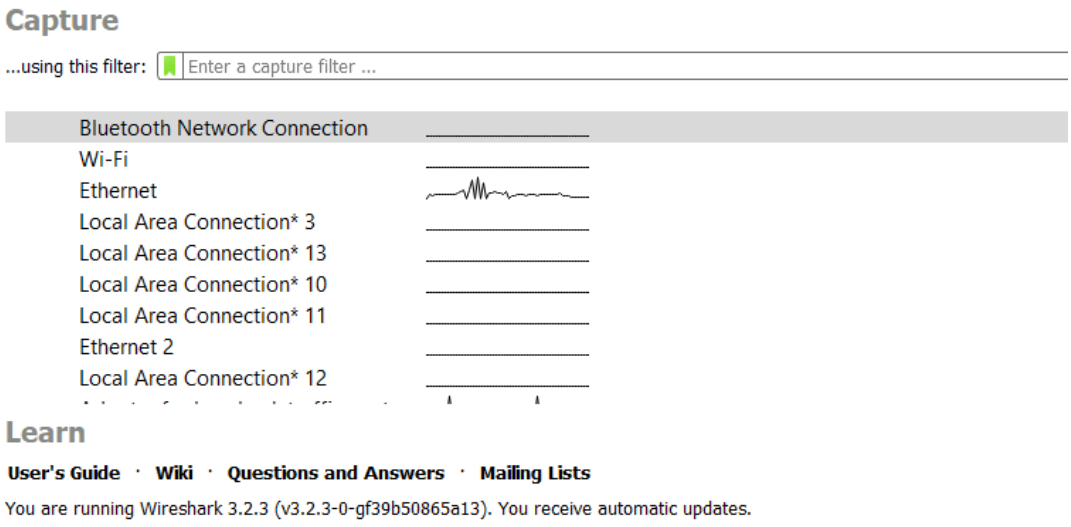
- Download and install Wireshark (it is already installed in the lab) (http://www.wireshark.org/)
- Observe that after installation WinPcap has been installed on the machine

When installing Wireshark on windows, WinPcap (or Npcap) is also installed, why is it needed?

Run wireshark

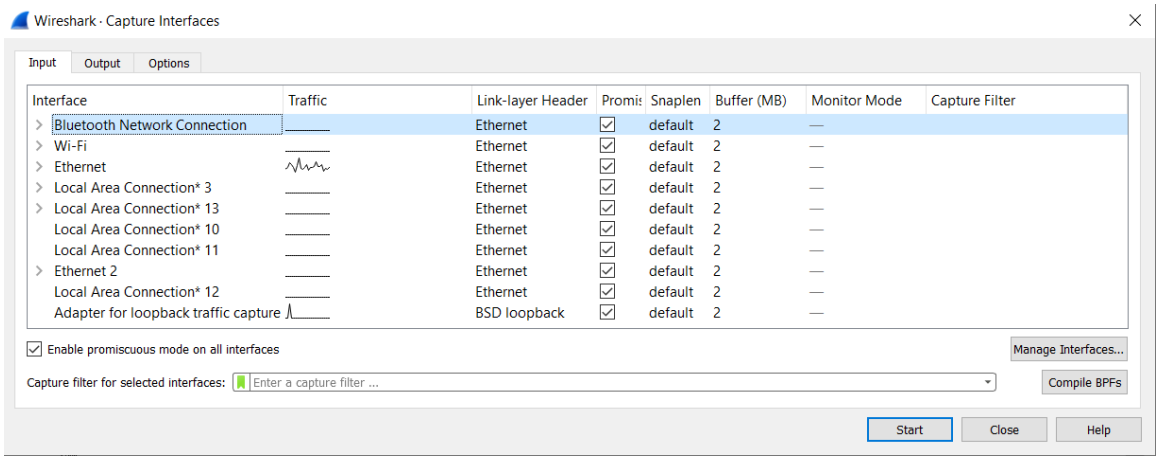
Start a simple traffic capture:

After WireShark is open you will see a "Capture" title with the networking interfaces. Near each of them you will see the traffic graph.



For example, in this picture, we can see that there is traffic only through the Ethernet interface.

You can also see this list with more information if you click on the "capture" tab and then "Options".



In the capture options:

- **Interface:** choose the correct interface. If you are using a notebook computer, it usually has at list two interfaces (LAN and wireless NIC). In the lab you should choose the 'ethx' interface. You can see what interfaces are active.
- **Capture packets in promiscuous mode:** make sure it is unchecked if you are using a wireless connection.
- **Capture Filter: Make sure it is empty**
- **Leave all other options the same and start the capture.**
- **Press Start**

Now you will see packets that come in and go out of this interface.

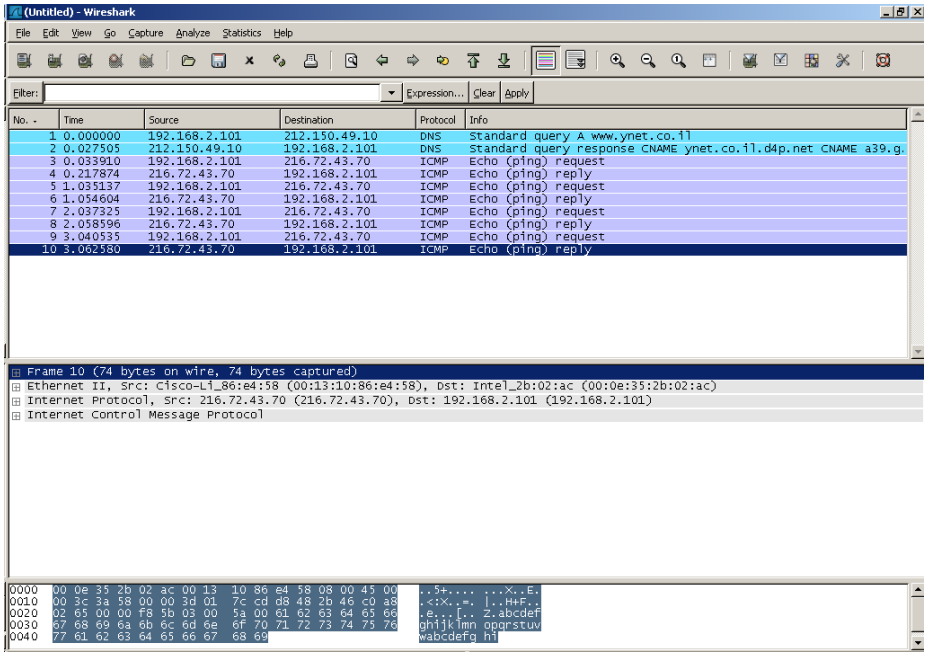
- Open the terminal (cmd for windows)
- Input the following command :

ping www.ynet.co.il

After the command is executed, the following should appear or something very similar.

```
C:\Documents and Settings\Administrator>ping www.ynet.co.il

Pinging a39.g.akamai.net [216.72.43.79] with 32 bytes of data:

Reply from 216.72.43.79: bytes=32 time=39ms TTL=61
Reply from 216.72.43.79: bytes=32 time=20ms TTL=61
Reply from 216.72.43.79: bytes=32 time=22ms TTL=61
Reply from 216.72.43.79: bytes=32 time=20ms TTL=61

Ping statistics for 216.72.43.79:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 39ms, Average = 25ms

C:\Documents and Settings\Administrator>_
```

You should click on stop in wireshark (red square at the left-top of the windows) and see the capture



a. Is your capture the same as the print screen above or do you have extra packets captured? Is so, what are they? List the protocols you see.
b. Filter the capture as much as you can so only (or almost only) the ping packets will appear.
   Hint: find the IP address of ynet, you can find it either by searching for the ynet DNS packets or from the ping command. Then filter traffic by that IP address.
c. Save the capture and label it
   Q1-UnderstandingWireShark-myID.jpcapng
   Attach it to your assignment hand-in zip

Congratulations you have completed your first network capture.

2. ARP

ARP Displays and modifies entries in the Address Resolution Protocol (ARP) cache, which contains one or more tables that are used to store IP addresses and their resolved Ethernet or Token Ring physical addresses.

- **ARP requests to a real address not in cache.**
    - **Start WireShark and start a capture. Set a filter so only the arp packets will appear.**
    - **Open a terminal and type sudo to be root, or run cmd as administrator for windows**
        i. View the ARP cache (arp /a for windows or see man arp for linux)
    - Delete the ARP cache (arp /d)
    - Ping another machine in your network
    - Observe the ARP packages in WireShark.
    - Observe the MAC addressed in the Ethernet headers of the captured packets. Pay attention to the following fields.
        i. The destination MAC address of the ARP Request packets.
        ii. The Type field in the Ethernet headers of ARP packets and the ARP opcode value.
    - View the ARP cache again. Note that the cache is refreshed/deleted in around 2 minutes.
    - Save the capture and label it: **Q2-arp-realaddress-myID.jpcapng** Attach it to your assignment hand-in zip

Use the capture to answer the following questions

a. What is the destination MAC address of an ARP Request packet? What does this mean?
b. Shortly explain the process in which ARP acquires the MAC address for IP address. Base your answer upon the capture.

- **ARP requests to an unknown host.**

Observe what happens when and ARP request is sent to an address which has no host

- **Start WireShark and start a capture with a new filter.**
- Start a telnet session to un-existing address in your network (e.g. 192.168.5.200).
- Observe the time interval and the frequency with which your PC transmits ARP Request packets. Repeat the experiment a number of times to discover the pattern.
- Save the capture and label it: **Q2-arp-unknownaddress-myID.jpcapng** Attach it to your assignment hand-in zip

Use the capture to answer the following questions

a. Describe the time interval between each ARP Request packet issued by your PC.
b. Why are ARP Request's packets not transmitted (i.e. not encapsulated) as IP packets? Explain your answer

3. **Netstat**

Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols).

Try different usages of the command in man netstat (try netstat -help on windows to see all options):

a. Display information on the network interfaces
b. Display the content of the IP routing table
c. Display information on TCP and UDP ports that are currently in use
d. Display the statistics of various networking protocols

Output the commands and results to a text file name **netstat-myid.txt**. Attach it to your assignment hand-in zip

a. What are the network's interfaces of your PC?
b. How many IP datagram's, ICMP messages, UDP datagram's, and TCP segments has your machine transmitted and received since it was last rebooted?
c. Show your machine's routing table. What do the columns in this table mean?

4. Ifconfig/ipconfig

Ifconfig displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings

Try out these commands. Some may require a reboot

Understanding DNS:

- ping www.cnn.com (or any site)
- **Start WireShark and start a capture**
- ping www.cnn.com (note that the host name mapping is in the DNS cache)
- search for "cnn" in your packets
- flush the DNS cache (windows: **ipconfig /flushdns,** linux: /etc/rc.d/init.d/nscd restart)
- ping www.cnn.com
- stop the capture
- search for "cnn" again in your packets
- Save the capture and label it:
  Q4-Ipconfig-myID.jpcapng
  Attach it to your assignment hand-in zip

a) Which packets did you see in the second time you searched for "cnn" that were not there is the first search?
b) What sequence of packets is required when the network layer must go to the DNS to resolve a name?
c) How does your machine know what IP address should be used to ask for that name?