**Lab 4 Write-Up**

**Wireshark**

Submitted by:

Joao Berardo

Paarth

Date: June, 3 2017

**LAB STEPS AND PROCEDURES**

1. **Lab Setup**
2. We opened Virtual Box and started the virtual Windows server with no problems.
3. **Configuring and testing Wireshark**
4. Executed with no problems.
5. There are 2 network interfaces. Ethernet and USBPcap1.
6. IP address of the network interface showing activity: 192.168.14.246.
   1. We couldn’t find that option.
   2. We couldn’t find that option.
   3. We did not see any transmit or receive error.
   4. Approximate ratio of directed vs. broadcast packets: 13/3 directed/broadcast.
7. **Enabling/Disabling Promiscuous Mode**

We successfully switched the promiscuous mode on for the network interface that we were capturing data.

1. **Observing PING**
2. Closed all browsers.
3. Prepared PING command but didn’t executed yet.
4. Capture option selected on Wireshark.
5. Started capturing.
6. Executed PING command.
   * In the first message, the protocol used was ARP and our computer (192.168.14.246) sent a message to the broadcast address asking the MAC Address of the default gateway (192.168.14.1).

Then, we can see a DNS request for googla.ca sent from our computer (192.168.14.1) to the primary DNS server (10.65.0.100).

The last messages were from the PING command that we issued. They were all ICMP echo messages, and we can see request and reply messages.

* + We recognizes the protocols ARP, DNS and ICMP. The ping command uses the ICMP protocol.
  + The first message is a request, and then a reply message is sent back. In the request message, the source IP is from our computer (192.168.14.246) and the destination IP is 2.168.14.1 (default gateway). The reply message has the opposite source/destination.
  + MAC Address of our computer: 08:00:27:64:3D:FA

MAC Address from default gateway: 00:1E:E5:6C:A0:92.

1. We started another capture.
2. We pinged google.ca.
3. The protocol before the ICMP was DNS protocol. We used the name of the host in the PING command, so in order to get the host IP address, we needed to request its IP from a DNS server. The DNS server used was our primary DNS server (10.65.0.100).
4. We started another capture.
5. We did try to ping a non-existent host two times.
6. As expected, we couldn’t ping a host that doesn’t exist. We sent a request to our primary DNS server (10.65.0.100) and receive the following response:
   * No such name A <non-existent-host>
7. **Observing Ethernet**
8. We opened Firefox and cleared all cache.
9. We started a Wireshark capture.
10. In Firefox, we accessed [www.microsoft.com](http://www.microsoft.com).
11. After using Firefox, we stopped the capture.
12. We used a filter and located the HTTP GET message.
13. HTTP message -> TCP segment ->IP Datagram -> Ethernet frame
14. We examined the contents of the Ethernet frame.
    1. MAC Address of our computer: 08:00:27:64:3D:FA.
    2. Destination MAC Address: 00:1E:25:6C:A0:92. The device is a cisco router. Probably, the Microsoft server is behind the Cisco router or firewall, so we can’t see the MAC Address of the server.
    3. It has our MAC Address. The response is sent to us because we requested it. In fact, the response goes to Langara’s router, and then to our computer (with some other devices in between). Because we are inside Langara’s network, its router knows our MAC Address so it can send back our HTTP GET message.
    4. Destination MAC Address is 00:1E:25:6C:A0:92 and it is a Cisco device.
15. First, we need to know the IP address of the destination, in that case microsoft.com. In order to achieve that, we request its name to our primary DNS server. If the DNS server doesn’t have it in cache, it request to another server, until some root server that has the answer can send the response to our DNS server and then back to us. With the IP address, our computer sends a message to the destination host (Microsoft) and if the server is up we receive a response. After that, we send the HTTP GET message and the server returns an HTTP OK and then start to send the webpage that we requested.
16. **Observing DHCP**
17. IPv4 is set to DHCP.
18. We opened the command prompt and prepared the command ipconfig /release.
19. We started capturing from Wireshark.
20. We started capturing from Wireshark.
21. We entered the ipconfig /release command.
22. After the release, we used the ipconfig /renew command.
23. We stopped the capture.
24. In the DHCP Release message the source device was our computer and the destination was the default gateway.

In the DHCP lease, the “discover” and “request” messages have the following source and destination addresses:

Source: 0.0.0.0

Destination: 255.255.255.255

The destination address (255.255.255.255) is a broadcast address, so the DHCP server can broadcast its message to every host on the local network.

IP Address lease time: 86400 seconds (1 day).

Length: 4 bytes.

DHCP uses UDP.