Assignment #4: Wireshark Lab and Performing DNS Spoofing to redirect target queries to our selected address DUE: March 6, 2020 at 11:59 pm Late Deadline: March 13, 2020 at 11:59 pm

IMPORTANT NOTE:

** DO NOT perform this experiment on the GSU network. You can either do it on your own Network at home or go to Langdale room 876 during TA's Office Hours to do it there. **

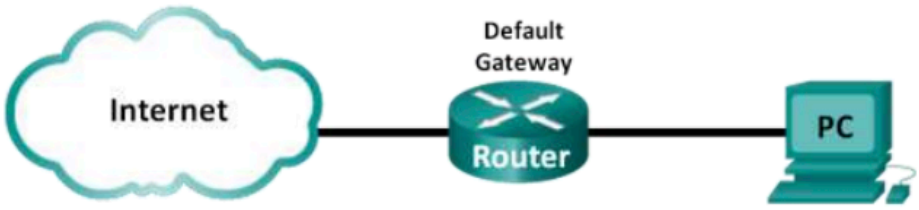
ASSIGNMENT DELIVERABLES:

- Screenshot of DNS filtered results in Wireshark
- Screenshot of Part 3 - step 2b of Wireshark assignment
- All tables and answers to questions of assignment part 1 filled out and placed in final assignment report
- Screenshot of active DNS_spoof plugin from Ettercap as shown in step 22
- Screenshot of successful spoof from Ettercap window as shown in step 25
- Screenshot of edited etter.dns file
- In one paragraph (200 -300 words) describe what DNS Poisoning is and how it works.
- Submit a single file with all the screen shots labeled and the paragraph summary.
- Submit file as "FirstName_LastName.docx"
- Honor and Grad Students: Look up a defense to DNS spoofing and write a 1-2 paragraph summary of what the defense is and how it works.

Part 1: Wireshark Assignment Instructions:

Lab - Using Wireshark to Examine a UDP DNS Capture

Topology



Objectives

Part 1: Record a PC's IP Configuration Information

Part 2: Use Wireshark to Capture DNS Queries and Responses

Part 3: Analyze Captured DNS or UDP Packets

Background / Scenario

If you have ever used the Internet, you have used the Domain Name System (DNS). DNS is a distributed network of servers that translates user-friendly domain names like www.google.com to an IP address. When you type a website URL into your browser, your PC performs a DNS query to the DNS server's IP address. Your PC's DNS server query and the DNS server's response make use of the User Datagram Protocol (UDP) as the transport layer protocol. UDP is connectionless and does not require a session setup as does TCP. DNS queries and responses are very small and do not require the overhead of TCP.

In this lab, you will communicate with a DNS server by sending a DNS query using the UDP transport protocol. You will use Wireshark to examine the DNS query and response exchanges with the name server.

Part 1: Record a PC's IP Configuration Information

In Part 1, you will use the terminal on your local PC to find and record the MAC and IP addresses of your PC's network interface card (NIC), the IP address of the specified default gateway, and the DNS server IP address specified for the PC. The information will be used in the following parts of this lab with packet analysis.

IP address	
MAC address	
Default gateway IP address	
DNS server IP address	

Part 2: Use Wireshark to Capture DNS Queries and Responses

In Part 2, you will set up Wireshark to capture DNS query and response packets to demonstrate the use of UDP transport protocol while communicating with a DNS server.

a. Click the Windows **Start** button and navigate to the Wireshark program.

   Note: If Wireshark is not yet installed, it can be downloaded at http://www.wireshark.org/download.html.

b. Select an interface for Wireshark for capturing packets. Use the **Interface List** to choose the interface that is associated with the recorded PC's IP and Media Access Control (MAC) addresses in Part 1.

c. After selecting the desired interface, click **Start** to capture the packets.

d. Open a web browser and type **www.google.com**. Press Enter to continue.

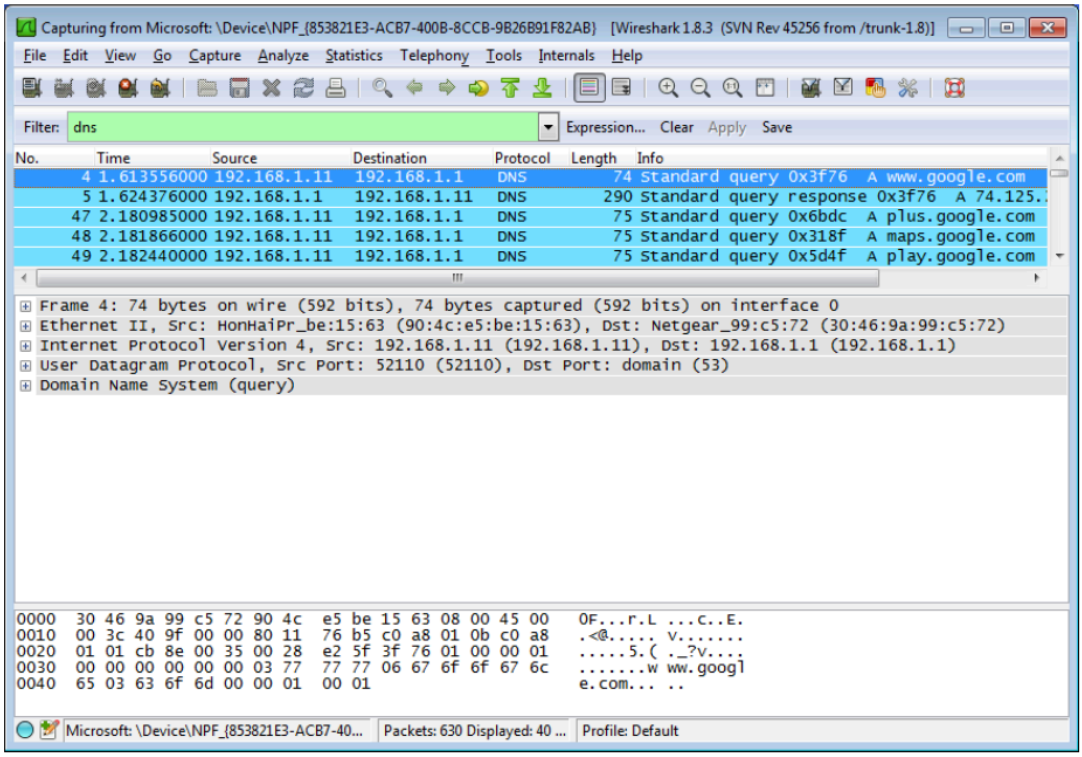
e. Click **Stop** to stop the Wireshark capture when you see Google's home page.

Part 3: Analyze Captured DNS or UDP Packets

In Part 3, you will examine the UDP packets that were generated when communicating with a DNS server for the IP addresses for www.google.com.

Step 1: Filter DNS packets.

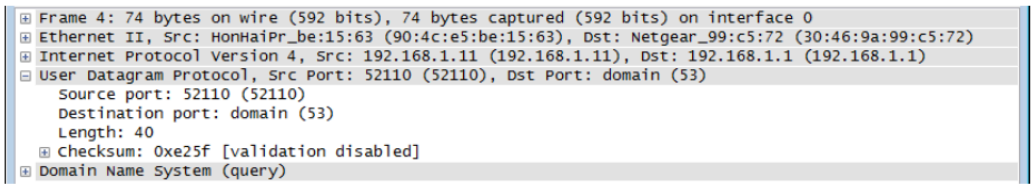
a. In the Wireshark main window, type **dns** in the entry area of the **Filter** toolbar. Click **Apply** or press Enter.



b. In the packet list pane (top section) of the main window, locate the packet that includes “standard query” and “A www.google.com”. See frame 4 as an example.

Step 2: Examine UDP segment using DNS query.

Examine UDP by using a DNS query for www.google.com as captured by Wireshark. In this example, Wireshark capture frame 4 in the packet list pane is selected for analysis. The protocols in this query are displayed in the packet details pane (middle section) of the main window. The protocol entries are highlighted in gray.



a. In the packet details pane, frame 4 had 74 bytes of data on the wire as displayed on the first line. This is the number of bytes to send a DNS query to a name server requesting the IP addresses of www.google.com.

b. The Ethernet II line displays the source and destination MAC addresses. The source MAC address is from your local PC because your local PC originated the DNS query. The destination MAC address is from the default gateway, because this is the last stop before this query exits the local network.

Is the source MAC address the same as recorded from Part 1 for the local PC? _____

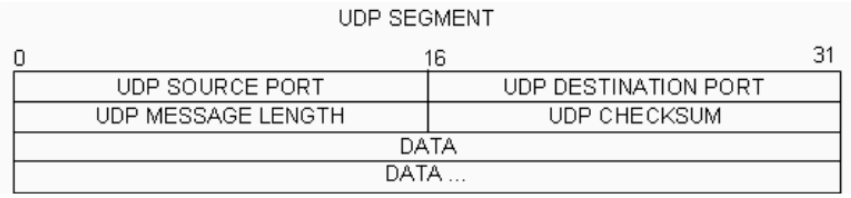
c. In the Internet Protocol Version 4 line, the IP packet Wireshark capture indicates that the source IP address of this DNS query is 192.168.1.11, and the destination IP address is 192.168.1.1. In this example, the destination address is the default gateway. The router is the default gateway in this network.

Can you pair up the IP and MAC addresses for the source and destination devices?

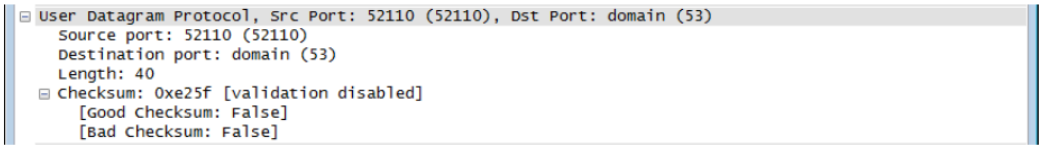
Device	IP Address	MAC Address
Local PC		
Default Gateway		

The IP packet and header encapsulates the UDP segment. The UDP segment contains the DNS query as the data.

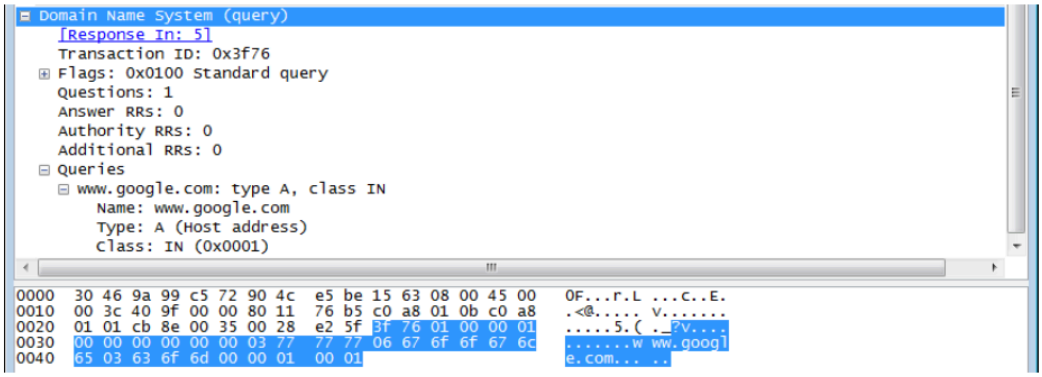
d. A UDP header only has four fields: source port, destination port, length, and checksum. Each field in UDP header is only 16 bits as depicted below.



Expand the User Datagram Protocol in the packet details pane by clicking the plus (+) sign. Notice that there are only four fields. The source port number in this example is 52110. The source port was randomly generated by the local PC using port numbers that are not reserved. The destination port is 53. Port 53 is a well-known port reserved for use with DNS. DNS servers listen on port 53 for DNS queries from clients.



In this example, the length of this UDP segment is 40 bytes. Out of 40 bytes, 8 bytes are used as header. The other 32 bytes are used by DNS query data. The 32 bytes of DNS query data is highlighted in the following illustration in the packet bytes pane (lower section) of the Wireshark main window.



The checksum is used to determine the integrity of the packet after it has traversed the Internet.

The UDP header has low overhead because UDP does not have fields that are associated with three-way handshake in TCP. Any data transfer reliability issues that occur must be handled by the application layer.

Record your Wireshark results in the table below:

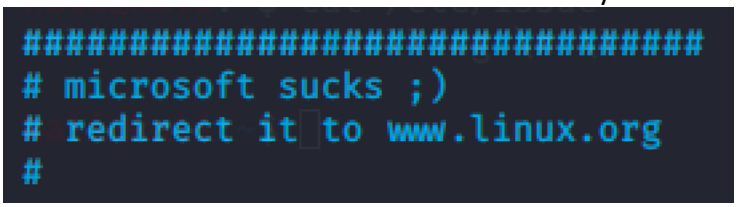
Frame Size	
Source MAC address	
Destination MAC address	
Source IP address	
Destination IP address	
Source Port	
Destination Port	

Is the source IP address the same as the local PC's IP address recorded in Part 1? _____

Is the destination IP address the same as the default gateway noted in Part 1? _____

Part 2: Ettercap Assignment Instructions:

1. Open a terminal in the kali VM and type in the command “ip a” and under the section “eth0” look for the IP address following the word inet. This IP address is your Virtual Machine’s IP address on your LAN connection.
2. Next, switch over to your physical computer and open your terminal and find its IP address on your LAN. Take note of this IP address.
3. Next, while still on your physical computer’s terminal, type in the command “netstat -rn” and under the section heading of “Internet:” look for destination of default. The gateway associated with that contains the IP address of your router. Take note of this IP address.
4. Next type the command “locate etter.dns”. This command will locate the file that contains all entries for DNS addresses which is used by Ettercap to resolve the domain name addresses.
5. Next type the following command “sudo nano /etc/ettercap/etter.dns”. This command will take you to the file mentioned above.
6. Once in the file scroll down to the section where it says:



7. Under this section you will see the mapping of Microsoft.com to a specific address.
8. You will change the associated IP addresses to another http website other than Microsoft.com.
9. First go back to your physical machine and type the command “nslookup mit.edu”. This command will return the DNS address associated with mit.edu. This attack with ettercap only works on http websites and not https websites, therefore the “redirection” has to be a http website like mit.edu. In reality you can use any http website but for this assignment please use mit.edu.
10. Now go back to the virtual machine and in the etter.dns file replace the IP addresses associated with Microsoft.com with the IP address of mit.edu. Your edit in the file should look SIMILAR (IP address might be different) to the image below:

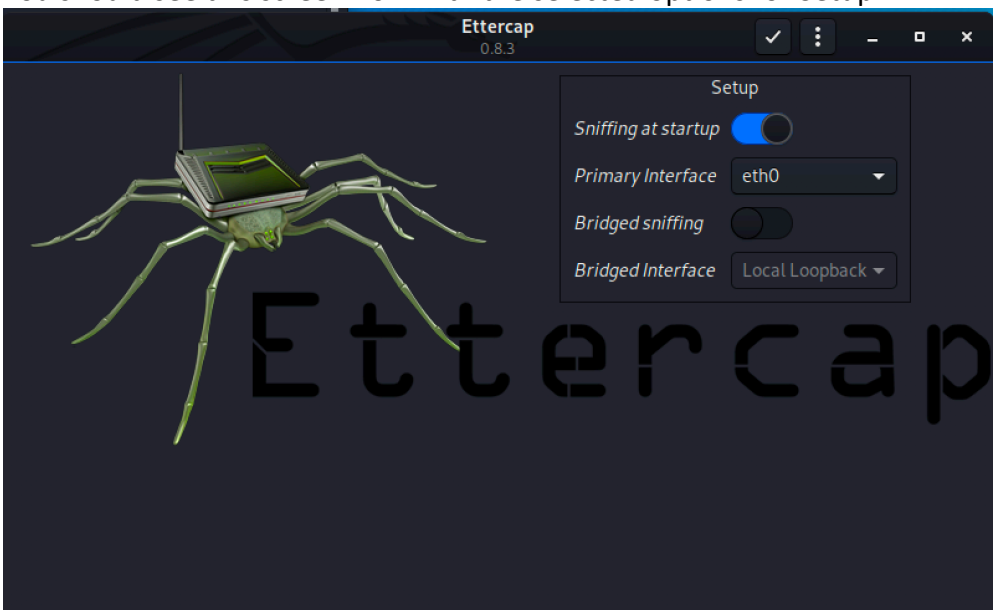
Note that the third entry for Microsoft has been removed.

    a. To get the IP address of mit.edu, do “nslookup mit.edu” on your terminal from your physical machine

11. Next save and close the file by doing the following operations.
    a. Hit ctr+X
    b. Hit Y
    c. Hit enter
12. Once the DNS address has been updated, enter the following command in the Kali Linux OS terminal:

a. sudo “ettercap -G”

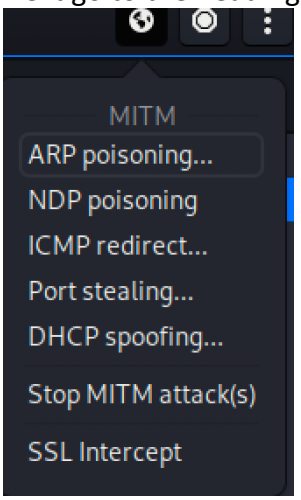
13. You should see this screen now with the selected options for Setup:



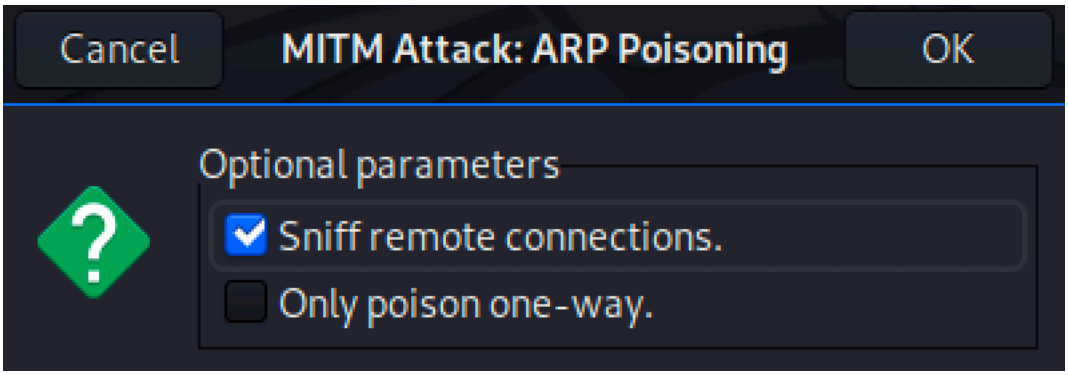
14. At this point, click the check mark button on the menu bar of Ettercap. You should see the following screen:

15. Now hit the green circled icon first and then the red circled icon. This will show you a list of connected hosts on your LAN.

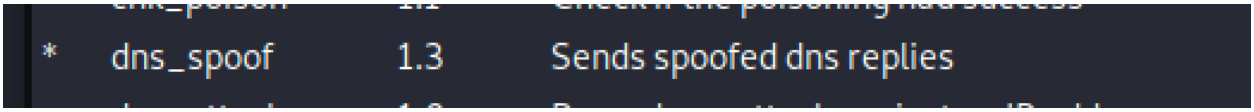
16. Click the IP address corresponding to your physical computer and hit the “Add to Target 1” button.
17. Click the IP address corresponding to your router address and hit the “Add to Target 2” button.
18. Next go to the heading called ARP poisoning as shown below:



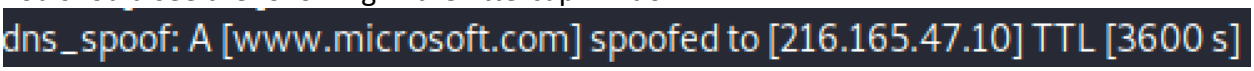
19. Make sure your settings are the same as below and then press “OK”:



20. Next hit the icon with 3 vertical dots and go to ‘Plugins’
21. Then go to ‘Manage plugins’
22. Next double click ‘dns_spoof’, you should now see a star appear next to the plugin like so:



23. Now you are all set and the system is ready to attack
24. Open an Incognito window and type in “microsoft.com”. You will first see a warning page but there should be an option for “proceed anyways” or something equivalent. Once you continue on you will be shown the nyu.edu website. If you open another window on the same incognito page and type in “microsfot.com” again you will be immediately redirected to nyu.edu.
25. You should see the following in the Ettercap window:



This indicates that the spoof worked.

26. That’s it. Go ahead and close the Ettercap window and then shutdown your Virtual Machine.