17.1.7 Lab - Exploring DNS Traffic

This lab has been updated for use on NETLAB+.
www.netdevgroup.com

Objectives

Part 1: Explore DNS Query Traffic

Part 2: Explore DNS Response Traffic

Background / Scenario

Wireshark is an open source packet capture and analysis tool. Wireshark gives a detailed breakdown of the network protocol stack. Wireshark allows you to filter traffic for network troubleshooting, investigate security issues, and analyze network protocols. Because Wireshark allows you to view the packet details, it can be used as a reconnaissance tool for an attacker.

In this lab, you will install Wireshark and use Wireshark to filter for DNS packets and view the details of both DNS query and response packets.

Instructions

Part 1: Explore DNS Query Traffic

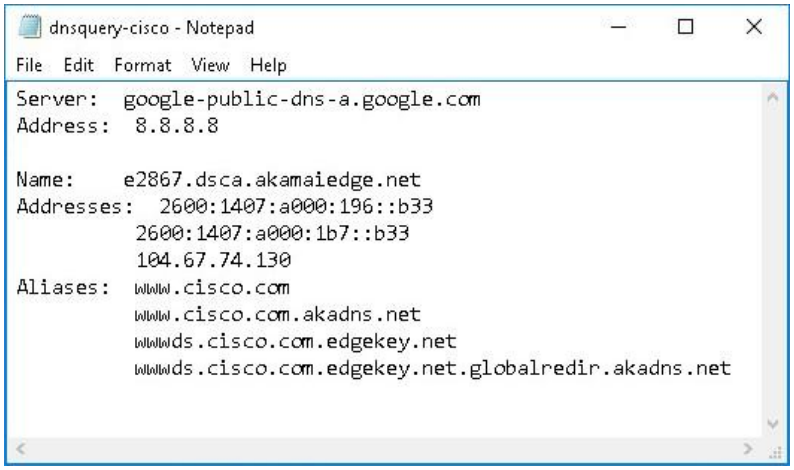
a. Access the **WinClient** machine. Unlock the machine by clicking on the drop-down arrow for that specific machine's tab and select **Send CTRL+ALT+DEL**.

b. Login as the `CyberOpsUser` using `cyberops` as the password.

c. On the *Desktop*, navigate to the **Toolbox** folder and open the **dns_query_files** folder.

d. Open the **dnsquery-cisco.txt** file.

e. Notice the *DNS* query information from the www.cisco.com domain.



f. Minimize the **Notepad** application and change focus to the **Toolbox** folder.

g. Launch the **Wireshark** application. Navigate to **File > Open** and open the **dnstrafficcisco.pcap** file from the **pcaps** folder in the *Toolbox* folder.

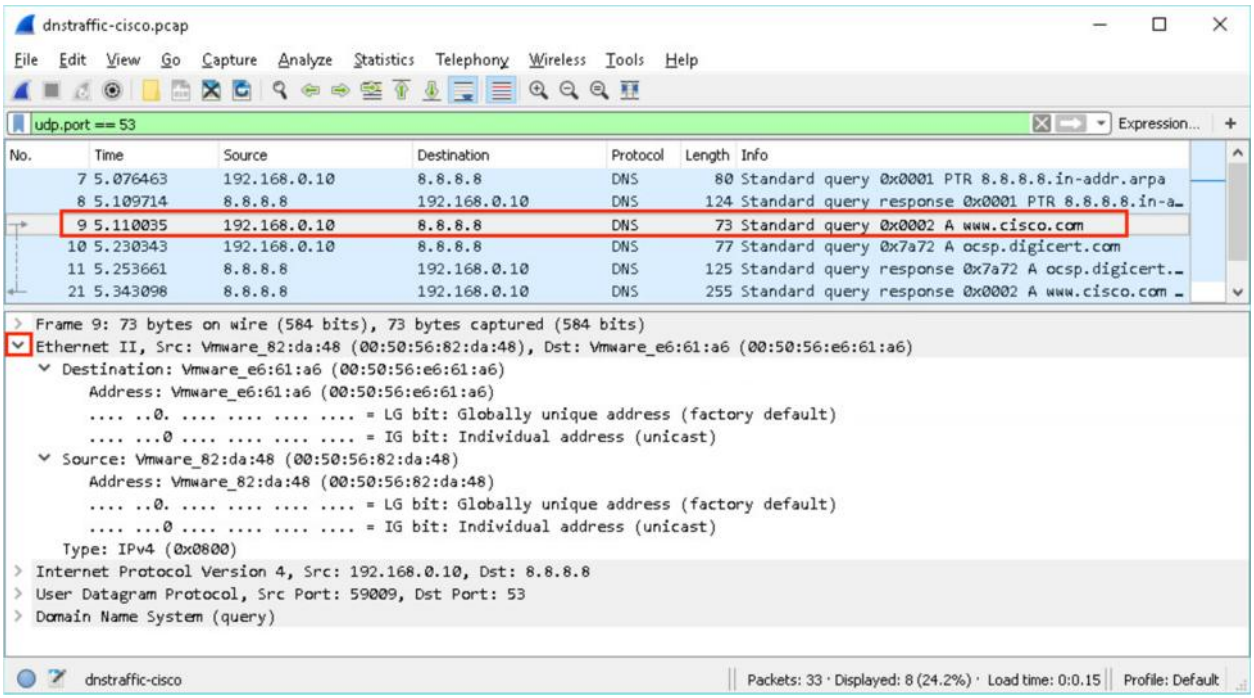
h. Observe the traffic captured in the Wireshark Packet List pane. Enter **udp.port == 53** in the filter box and click the arrow (or press enter) to display only DNS packets.

Note: The provided screenshots are just examples. Your output maybe slightly different.

i. Select the DNS packet that contains **Standard query** and **A www.cisco.com** in the Info column.

j. In the Packet Details pane, notice this packet has Ethernet II, Internet Protocol Version 4, User Datagram Protocol and Domain Name System (query).

k. Expand **Ethernet II** to view the details. Observe the source and destination fields.



What are the source and destination MAC addresses? Which network interfaces are these MAC addresses associated with?

_____

_____

l. Expand **Internet Protocol Version 4**. Observe the source and destination IPv4 addresses.

```
Internet Protocol Version 4, Src: 192.168.0.10, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 59
    Identification: 0x7ad9 (31449)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xef16 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.10
    Destination: 8.8.8.8
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

What are the source and destination IP addresses? Which network interfaces are these IP addresses associated with?

_____

_____

m. Expand the **User Datagram Protocol**. Observe the source and destination ports.

```
User Datagram Protocol, Src Port: 59009, Dst Port: 53
    Source Port: 59009
    Destination Port: 53
    Length: 39
    Checksum: 0x851f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
```

What are the source and destination ports? What is the default DNS port number?

_____

_____

n. Determine the IP and MAC address of the PC.

1) Start a Windows command prompt, enter **ipconfig /all** to record the MAC and IP addresses of the PC.

Compare the MAC and IP addresses in the Wireshark results to the IP and MAC addresses. What is your observation?

_____

_____

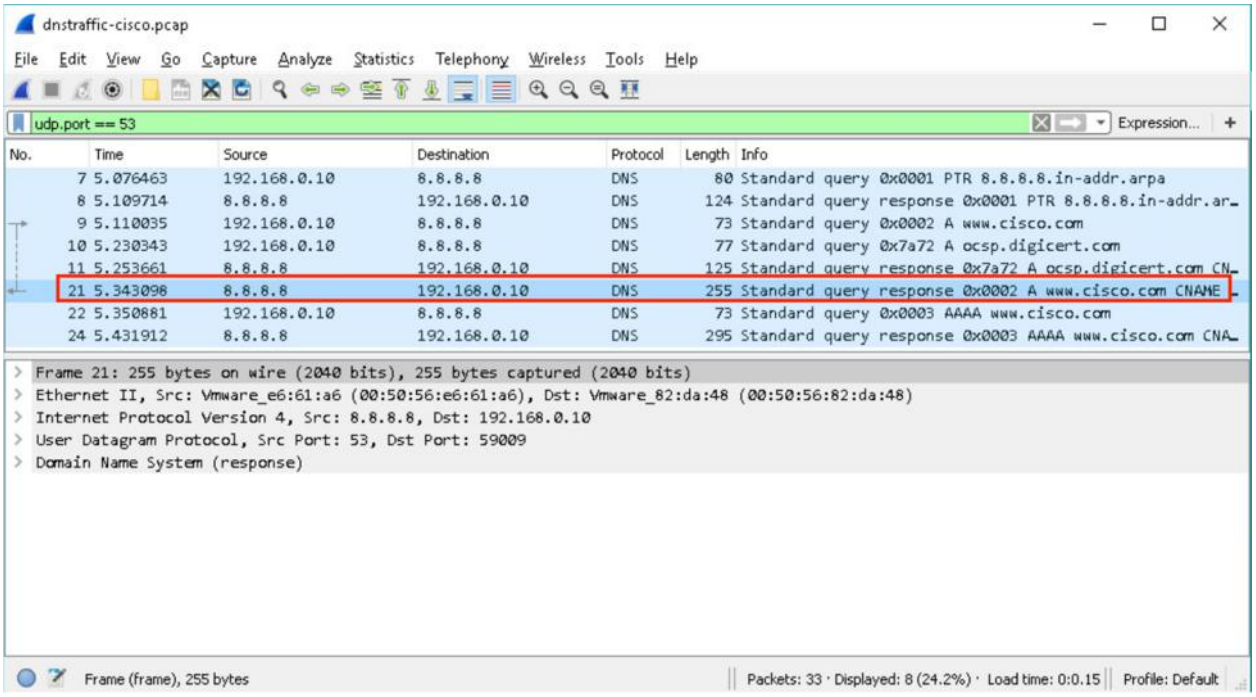
o. Expand **Domain Name System (query**) in the Packet Details pane. Then expand the **Flags** and **Queries**.

p. Observe the results. The flag is set to do the query recursively to query for the IP address to www.cisco.com.

```
Domain Name System (query)
    [Response In: 21]
    Transaction ID: 0x0002
  Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.cisco.com: type A, class IN
        Name: www.cisco.com
        [Name Length: 13]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Part 2: Explore DNS Response Traffic

a. Select the corresponding response DNS packet has **Standard query response** and **A www.cisco.com** in the Info column.



What are the source and destination MAC and IP addresses and port numbers? How do they compare to the addresses in the DNS query packets?

_____

_____

b. Expand **Domain Name System (response)**. Then expand the **Flags**, **Queries**, and **Answers**.

c. Observe the results.
Can the DNS server do recursive queries?

_____

```
Domain Name System (response)
    [Request In: 9]
    [Time: 0.233063000 seconds]
    Transaction ID: 0x0002
  Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.cisco.com: type A, class IN
        Name: www.cisco.com
        [Name Length: 13]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  Answers
    www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
    www.cisco.com.akadns.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net
    wwwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwwds.cisco.com.edgekey.net.globalredir.akadns.net
    wwwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e2867.dsca.akamaiedge.net
    e2867.dsca.akamaiedge.net: type A, class IN, addr 104.67.74.130
```

d. Observe the CNAME and A records in the Answers details.

Reflection

1. From the Wireshark results, what else can you learn about the network when you remove the filter?

_____

2. How can an attacker use Wireshark to compromise your network security?

_____

_____