Laboratory Exercise – Introduction to Wireshark

1. Overview

In this lesson, the student will be introduced to Wireshark, a very useful tool that covers a very important network forensics concept – reading and understanding networking traffic. Wireshark (software known as a packet analyzer) allows you to view pieces of data (called packets) in real-time as they go in and out of a system and can be saved as packet capture (pcap or cap) files. In this exercise, the student will be analyzing packet capture files as well as capturing live network traffic in real-time.

2. Resources required

This exercise requires a local Kali Linux Virtual Machine running on a computer (laptop) or a Kali Linux VM running in the Cyber Range.

[Note to instructors: This lab exercise requires an account on the Cyber Range if you intend to use a Cyber Range Kali Linux VM. To sign up for an account, please visit our Sign-Up page. Your students will also require Cyber Range accounts; this will be explained upon course setup.]

3. Initial Setup

From you Cyber Range course, select the **Kali Desktop** or the **Cyber Basics** environment. Click “start” to start your environment and “join” to get to your Linux desktop.

4. Tasks

Task 4.1: Getting familiar with Wireshark by observing live capture

What is Wireshark and why should you care? Wireshark is a powerful analysis tool that allows you to not only capture network and device packets, but to analyze them too. To recap from lesson 5, a packet is a fragment of data that is sent over a network from one machine to another. This data usually includes a *source port*, *source IP* address, *destination por*t, *destination IP*, and other data that we will see in this lab.

Wireshark allows a user to analyze the traffic traveling in and out of the machine, which can serve many uses. These include, but are not limited to:

- Troubleshooting network connections.
- Filtering data between two hosts to see a single network “conversation.”
- Comparing all “conversations” to discover bad actors or “bandwidth hogs.”
  NOTE: *The endpoint using the most bandwidth is known as the “top talker.”*
- Filtering captured data to analyze specific protocols and ports being used.
- Analyzing specific statistics about the traffic coming in and out of the system.

© 2023 Virginia Cyber Range. Created by Thomas Weeks. (CC BY-NC-SA 4.0)

How do we use Wireshark? Let's take a look at this application. Open Wireshark either by clicking on the "Kali" menu on the upper-left corner of the desktop, then begin to type "wireshark" in the search bar and select the "wireshark" application (see figure 1 below).

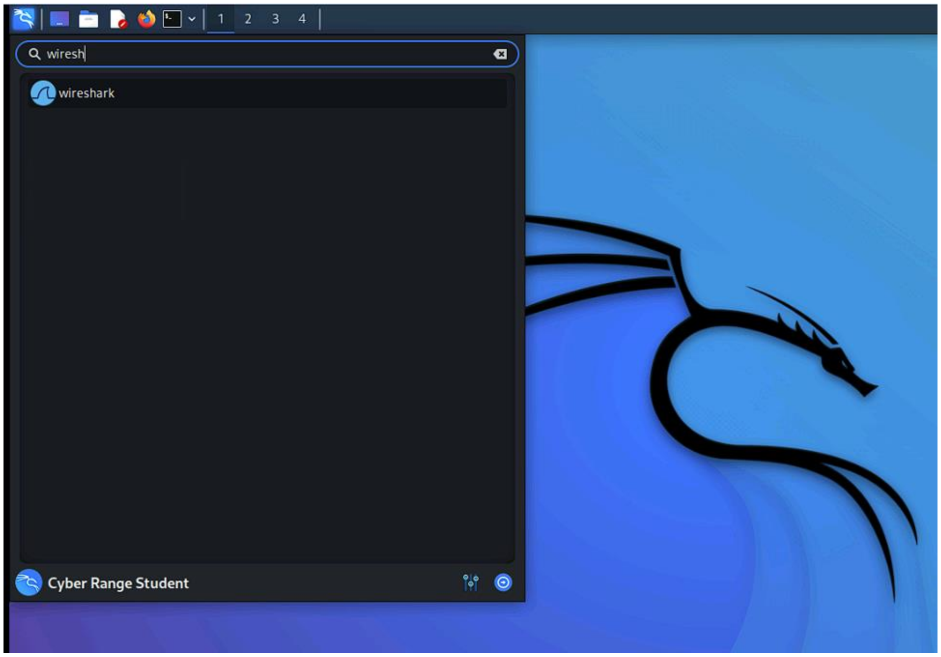
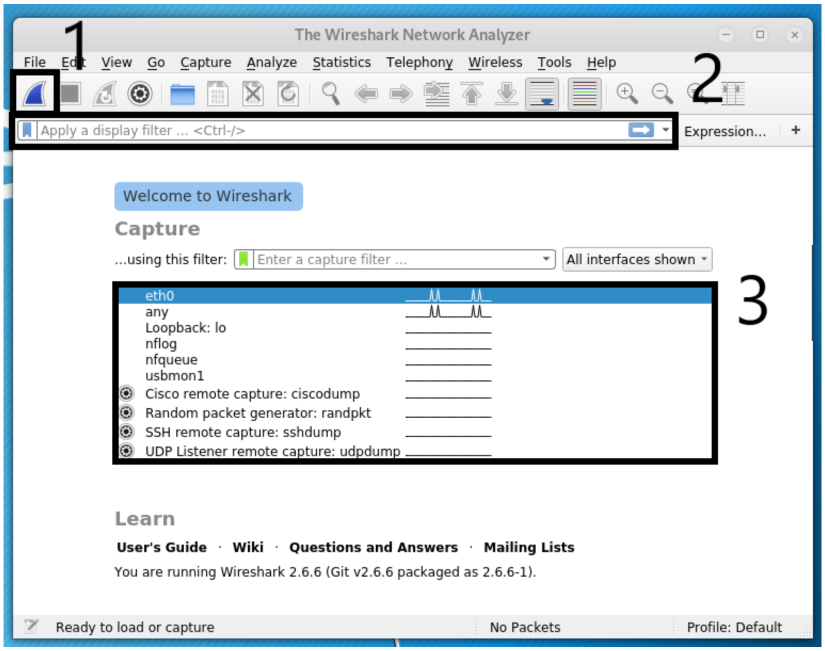


Figure 1. Start Wireshark using the Kali menu. When asked for a password, enter "student".

Taking a closer look at the Wireshark user interface, let's explore how it's laid out.


The Wireshark Network Analyzer
1
2
3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

eth0
any
Loopback: lo
nflog
nfqueue
usbmon1
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump

You are running Wireshark 2.6.6 (Git v2.6.6 packaged as 2.6.6-1).

Ready to load or capture | No Packets | Profile: Default

Figure 2 - The Wireshark opening user interface.

© 2023 Virginia Cyber Range. Created by Thomas Weeks. (CC BY-NC-SA 4.0)

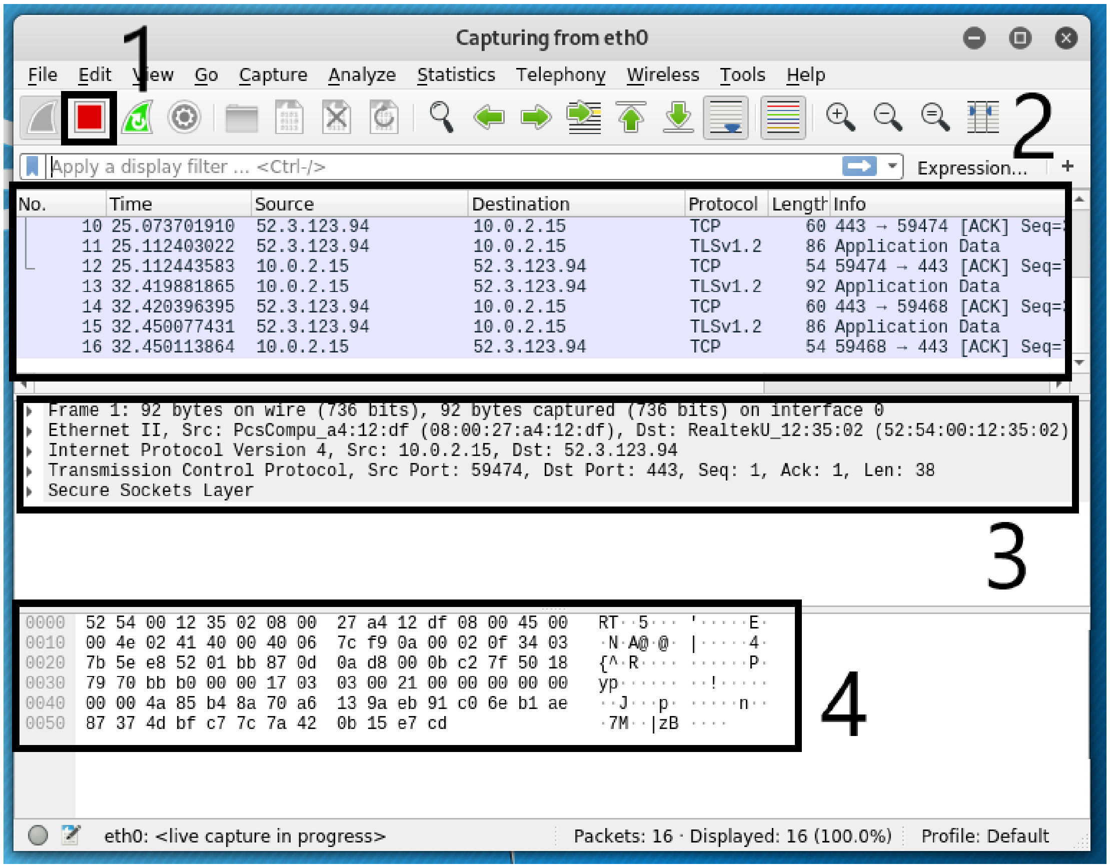
From Figure 3 above, let's breakdown some of the important Wireshark features outlined by the three numbered boxes:

1. **Start Capturing Packets:** This is the button to start a live packet capture. This will capture network traffic going in and out of your system in real-time. We will demo this later in the lab.
2. **Filter String Field:** This field allows the user to apply filters to the traffic captured. This can be done by certain text, a protocol, a port, etc.. We will look at applying filters later.
3. **Live Packet Devices:** This is a list of the network interfaces from which we can capture traffic.

So, if we wish to look traffic for the eth0 network interface, highlight the "eth0" interfaces (shown above *highlighted in blue in Box #3*) and press the start button (Box #1) or double-click the "eth0." After doing so, the live packet capture will record all packet data traversing the host running Wireshark.

> ***WARNING:*** *Capturing or recording live packet traffic takes up a very large amount of memory. Be mindful of this and never just leave a Wireshark capture running. Doing so for just a few minutes, can fill up Gigabytes of system memory or fill up your disk when trying to save. Both of these situations can make your system unstable or crash Wireshark. Stop Wireshark by hitting the button in Box #1 as shown below in Figure 4.*

Now we will take a look at some important packet data capture Wireshark features outlined by the four numbered boxes below in Figure 4.



```
No.    Time          Source         Destination    Protocol  Length Info
    10 25.073701910  52.3.123.94    10.0.2.15      TCP         60 443 → 59474 [ACK] Seq=
    11 25.112403022  52.3.123.94    10.0.2.15      TLSv1.2     86 Application Data
    12 25.112443583  10.0.2.15      52.3.123.94    TCP         54 59474 → 443 [ACK] Seq=
    13 32.419881865  10.0.2.15      52.3.123.94    TLSv1.2     92 Application Data
    14 32.420396395  52.3.123.94    10.0.2.15      TCP         60 443 → 59468 [ACK] Seq=
    15 32.450077431  52.3.123.94    10.0.2.15      TLSv1.2     86 Application Data
    16 32.450113864  10.0.2.15      52.3.123.94    TCP         54 59468 → 443 [ACK] Seq=
```

```
▸ Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_a4:12:df (08:00:27:a4:12:df), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 52.3.123.94
▸ Transmission Control Protocol, Src Port: 59474, Dst Port: 443, Seq: 1, Ack: 1, Len: 38
▸ Secure Sockets Layer
```

```
0000  52 54 00 12 35 02 08 00  27 a4 12 df 08 00 45 00   RT··5···  '·····E·
0010  00 4e 02 41 40 00 40 06  7c f9 0a 00 02 0f 34 03   ·N·A@·@·  |·····4·
0020  7b 5e e8 52 01 bb 87 0d  0a d8 00 0b c2 7f 50 18   {^·R····  ······P·
0030  79 70 bb b0 00 00 17 03  03 00 21 00 00 00 00 00   yp······  ··!·····
0040  00 00 4a 85 b4 8a 70 a6  13 9a eb 91 c0 6e b1 ae   ··J···p·  ·····n··
0050  87 37 4d bf c7 7c 7a 42  0b 15 e7 cd               ·7M··|zB  ····
```

eth0: <live capture in progress>   Packets: 16 · Displayed: 16 (100.0%)   Profile: Default

Figure 3 The three main capture inspection frames in Wireshark

© 2023 Virginia Cyber Range. Created by Thomas Weeks. (CC BY-NC-SA 4.0)

1. **Stop Capture Button:** This button stops the current capture. Once you click this, you can analyze the data and then save it as a .pcap file (a file containing captured packet data) for further analysis or exporting.

   > ***NOTE:** Once you capture data, you can save it by simply opening **File / Save** and giving it a file name. By default, it will save the newer file format called .pcapng, but you can also save in the more classic .pcap format as well as a couple dozen other network capture formats.*

2. **Packet List Pane:** This displays the captured data packets. It shows the Source IP, Destination IP, Protocol, etc. of each packet captured.

3. **Packet Details Pane:** This displays the data structure contained within the selected packet from the Packet List Pane (in Box #2). In the details pane, you can clearly see the Layer-1 through Layer-3 TCP/IP encapsulated data structures. From the top, the Layer-1 frame & Ethernet data, wrapped in a Layer-2 IP datagram, in turn wrapped in a Layer-3 TCP transport session or connection.

4. **Packet Bytes Pane:** This displays the raw data of the highlighted packet (in Box #2) in its most basic or "canonical" hexadecimal + ASCII formats — the lowest level, most basic, binary data, represented in both hex (machine) and ASCII (human) readable formats side-by-side.

Now that we understand how Wireshark is used to capture data and then export it to a file as pcap file, let's take a look at a few pcap files, interpret the data in them, and see what we can learn!

Task 4.2: Analyzing pcap files:

Let's first download several .pcap files for analysis from the Wireshark website.

On your Cyber Range Kali Linux system, open a terminal window and type the following (or open the web browser and browse to the page below):

```
$ firefox https://wiki.wireshark.org/SampleCaptures
```

Scroll down to find and download (Save File) the following files:

Under heading of General / Unsorted
- dhcp.pcap
- dns.cap

Under heading of Viruses and worms
- slammer.pcap

Close any previously opened Wireshark sessions, and then at the terminal, input the following commands:

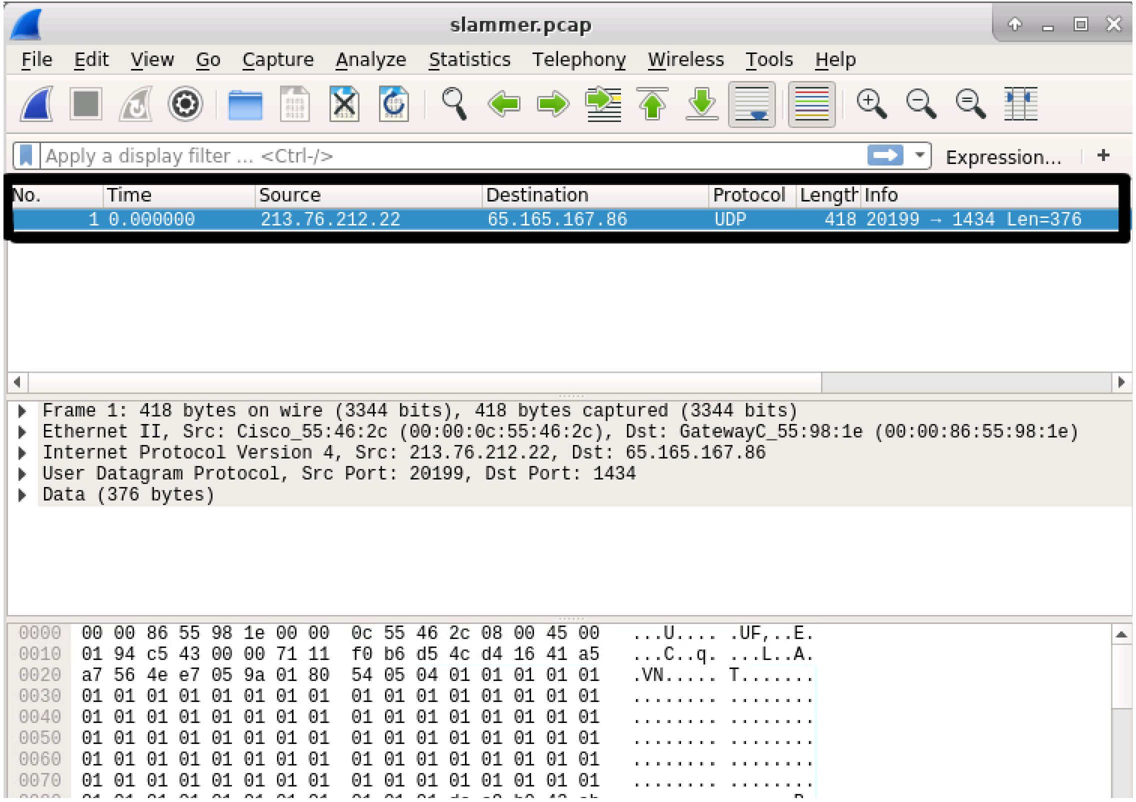
```
$ cd ~/Downloads
$ ls -lah *cap
```

© 2023 Virginia Cyber Range. Created by Thomas Weeks. (CC BY-NC-SA 4.0)

```
-rw-r--r-- 1 student student 1.4K Jan 30 21:46 dhcp.pcap
-rw-r--r-- 1 student student 4.3K Jan 30 21:47 dns.cap
-rw-r--r-- 1 student student  458 Jan 30 21:47 slammer.pcap
$ wireshark slammer.pcap
```

This **slammer.pcap** packet capture we're opening contains a single packet; it's used for simplicity's sake. Looking at the top packet in the Packet List Pane in Figure 5, let's see what information we can gather.

Figure 5



slammer.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time       Source          Destination     Protocol Length Info
    1 0.000000   213.76.212.22   65.165.167.86   UDP         418 20199 → 1434 Len=376
```

```
▸ Frame 1: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits)
▸ Ethernet II, Src: Cisco_55:46:2c (00:00:0c:55:46:2c), Dst: GatewayC_55:98:1e (00:00:86:55:98:1e)
▸ Internet Protocol Version 4, Src: 213.76.212.22, Dst: 65.165.167.86
▸ User Datagram Protocol, Src Port: 20199, Dst Port: 1434
▸ Data (376 bytes)
```

```
0000  00 00 86 55 98 1e 00 00  0c 55 46 2c 08 00 45 00   ...U.... .UF,..E.
0010  01 94 c5 43 00 00 71 11  f0 b6 d5 4c d4 16 41 a5   ...C..q. ...L..A.
0020  a7 56 4e e7 05 9a 01 80  54 05 04 01 01 01 01 01   .VN..... T.......
0030  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01   ........ ........
0040  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01   ........ ........
0050  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01   ........ ........
0060  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01   ........ ........
0070  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01   ........ ........
```

If you view the top window, this pane lists all of the packets in the capture (in this case, a single packet), as well as other basic information about the packets. The table below explains what each field means.

Field Name	Description
No.	The packet number; this goes incrementally in order by which packets reach the machine or leave the machine first.
Time	This is the time from the first packet capture to the selected one; if it is the first packet, the time is 0.0.
Source	The IP address of the machine the packet originated from.
Destination	The IP address of the intended recipient of the packet.
Protocol	The networking protocol used to send this packet. In Wireshark, if we desire we can filter captured data based on specific protocols. Recall from lesson 5 (Intro to Networking) where we introduced and elaborated on TCP and UDP. Here, we are seeing a real-world application of what we learned in the "Intro to Networking Lab" where we had discussed protocols and their uses. Specifically, this data is Network Layer traffic and we can see this packet is using the UDP protocol.
Length	The data length/size of the packet.
Info	Details about the packet; may be helpful or contain little value.

© 2023 Virginia Cyber Range. Created by Thomas Weeks. (CC BY-NC-SA 4.0)

The Packet Details pane allows you to drill down into the details of the packet highlighted up in the Packet List Pane.

In the packet in Figure 5 from the file **slammer.pcap**, use the Packet Details Pane to drill down into the details of this single highlighted packet and answer the questions below.

Question 4.2.1: What is the *source port* of the packet in question?

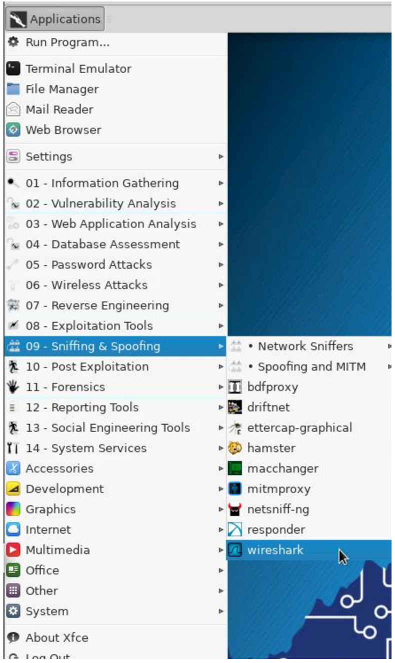
Question 4.2.2: What is the *destination port* of the packet in question?

Task 4.3: Analyzing DNS Packets

DNS (Domain Name System) is a network service that runs over TCP/UDP port 53 and translates human readable domain names (www.example.com) into IP Addresses (10.234.123.45). For example, when you enter www.facebook.com into your web browser, your computer or network provider's DNS service translates this human readable FQDN (fully qualified domain name) into an IP Address so the browser can use it to retrieve or "*GET*" the website.

Why is name-to-IP address-resolution even needed? As you know, all data within computers (e.g., memory addresses, binary machine code, IP addresses, etc.) are all ultimately interpreted using numbers and binary data. These forms of data are not as easily interpreted by humans as are words. It is easier for us to remember "kali.example.com" rather than an IP address. Imagine if every website you wish to visit, you would have to remember some IP address such as 10.43.233.78. Instead, we remember domains and URLs, and DNS translates these into their respective IP addresses for the computer host to translate and interpret.

Figure 6



DIG-IN: *To see how DNS works, open a terminal in your Kali Linux VM on the Cyber Range and look up the DNS record to translate google.com into its IP address by typing the DNS lookup command:*

```
   host google.com
```

This will resolve (or translate) the domain google.com to one or more IPv4 addresses (called A records), IPv6 addresses (called AAAA records), and also provide the known email servers that handle email traffic for that domain (called MX records). This type of DNS resolution happens every time you visit a website, click on a link, or send an email.

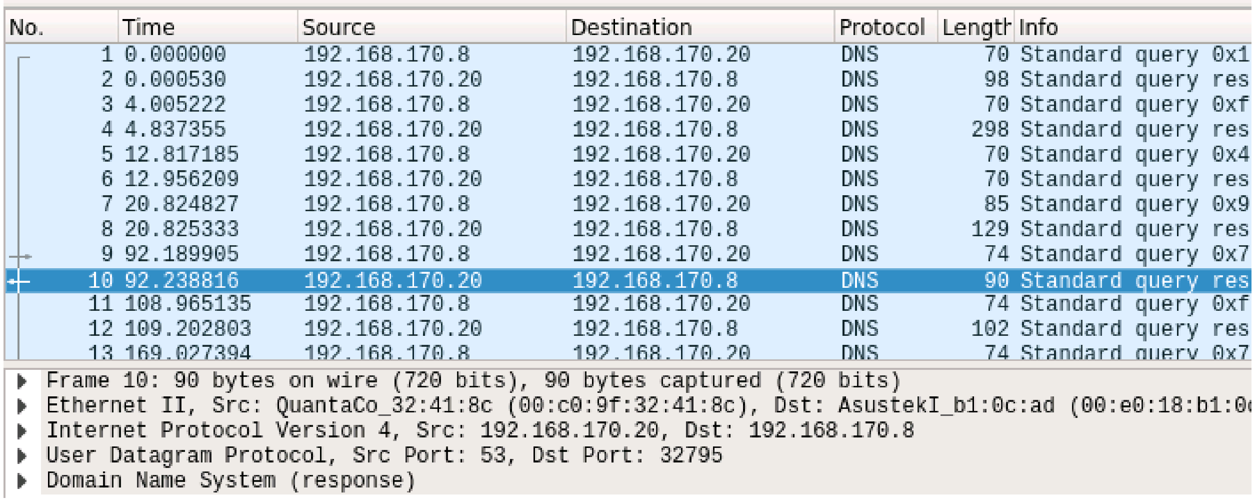
Exit and close down any other running Wireshark instances and either start a new Wireshark instance from the Kali UI (upper left) by clicking on **Applications / 09 – Sniffing & Spoofing / Wireshark** (See Figure 6 on the left.). Once Wireshark starts, open the dns.cap file by selecting Wireshark's **File / Open Ctrl+O**.

If you prefer starting applications from the command line, instead of using the desktop UI, try opening the dns.cap like this:

```
$ cd Downloads
$ wireshark dns.cap &
```

*__NOTE:__ Ending a command with **&** puts the process in the background. This allows you to continue to use the terminal and your hands never have to leave the keyboard.*

Right away, you'll notice this DNS capture (dns.cap) has many more packets than the last one. See Figure 7 below. In the Packet List pane, select the 10th packet (No. 10) and explore some of the content in the Packet Details pane:



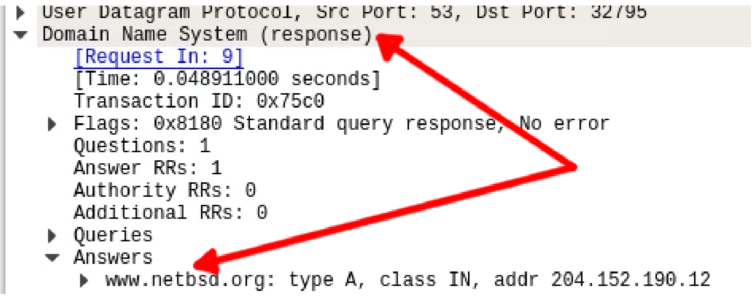
```
No.       Time           Source           Destination      Protocol  Lengtł Info
       1 0.000000       192.168.170.8    192.168.170.20   DNS          70 Standard query 0x1
       2 0.000530       192.168.170.20   192.168.170.8    DNS          98 Standard query res
       3 4.005222       192.168.170.8    192.168.170.20   DNS          70 Standard query 0xf
       4 4.837355       192.168.170.20   192.168.170.8    DNS         298 Standard query res
       5 12.817185      192.168.170.8    192.168.170.20   DNS          70 Standard query 0x4
       6 12.956209      192.168.170.20   192.168.170.8    DNS          70 Standard query res
       7 20.824827      192.168.170.8    192.168.170.20   DNS          85 Standard query 0x9
       8 20.825333      192.168.170.20   192.168.170.8    DNS         129 Standard query res
       9 92.189905      192.168.170.8    192.168.170.20   DNS          74 Standard query 0x7
      10 92.238816      192.168.170.20   192.168.170.8    DNS          90 Standard query res
      11 108.965135     192.168.170.8    192.168.170.20   DNS          74 Standard query 0xf
      12 109.202803     192.168.170.20   192.168.170.8    DNS         102 Standard query res
      13 169.027394     192.168.170.8    192.168.170.20   DNS          74 Standard query 0x7
▶ Frame 10: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
▶ Ethernet II, Src: QuantaCo_32:41:8c (00:c0:9f:32:41:8c), Dst: AsustekI_b1:0c:ad (00:e0:18:b1:0c
▶ Internet Protocol Version 4, Src: 192.168.170.20, Dst: 192.168.170.8
▶ User Datagram Protocol, Src Port: 53, Dst Port: 32795
▶ Domain Name System (response)
```

Figure 7 Exploring the details of packet #10

In the Packet Details pane, we are able to examine much more of the packet's internal details. Let's examine the DNS information for packet no. 10. See Figure 8 below.

Expanding the **Domain Name System (response)** and then the **Answers** tabs, you will notice the IP response for the domain www.netbsd.org. This means that a query was made for the domain www.netbsd.org and the IP address was successfully retrieved.

Figure 8 Looking at the DNS response



```
▶ User Datagram Protocol, Src Port: 53, Dst Port: 32795
▼ Domain Name System (response)
    [Request In: 9]
    [Time: 0.048911000 seconds]
    Transaction ID: 0x75c0
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▶ Queries
  ▼ Answers
    ▶ www.netbsd.org: type A, class IN, addr 204.152.190.12
```

Question 4.3.1: In Packet No. 28, what is the Source Port of the UDP data? (Hint: What does UDP stand for?)

Question 4.3.2: In Packet No. 5, what URL was queried for DNS information?

Task 4.4: Analyzing DHCP

Previously, we discussed what IP addresses are and what role they play in a network. Now we are going to discuss how a device gets configured with an IP address on the network.

© 2023 Virginia Cyber Range. Created by Thomas Weeks. (CC BY-NC-SA 4.0)

There are two methods for a system getting an IP address:

1. **Static IPs –** Some devices allow you to manually set an IP address in the network settings of the device. This requires a user to log into their device, configure the IP address to match the LAN settings, and save the IP address for future sessions. Static IP addresses are suitable for devices that you want to have constant (unchanging) IP settings such as a printer, a web server, or a file server. Generically speaking, static IP addresses are mostly used on servers and infrastructure devices that should not (or cannot) change IPs.

2. **Dynamic IPs –** Devices can also have IPs automatically assigned via *DHCP* (dynamic host configuration protocol), which automatically assigns IP addresses from dynamic IP address pools, pre-configured by the network administrators to allow devices (mostly human client hosts). DHCP-assigned IPs tend to be less prone to human error as they are automatically assigned when a device connects to a LAN (local area network). DHCP-based IP configurations are much more common on LANs than static IPs, and are used almost exclusively on WiFi networks.

Let's take a closer look at what DHCP traffic looks like on a local network.

Close down any Wireshark instances. Launch Wireshark and open the downloaded dhcp.pcap file by typing the following in a terminal:

```
$ cd ~/Downloads
$ wireshark dhcp.pcap &
```

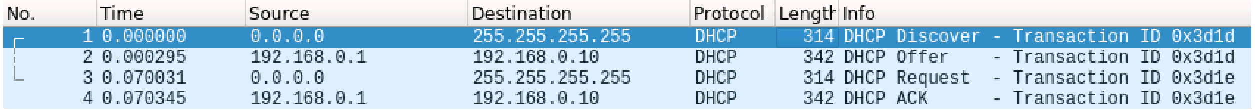
NOTE: *The* ***`cd ~/`*** *part of this command sets your working directory to your home path /home/$USER. So, by typing* ***`cd ~/Downloads`*** *in a terminal on the Cyber Range Kali VM, you will land in the /home/student/Downloads directory.*

Looking at the four packets from this capture (dhcp.pcap) as shown in Figure 9, they clearly illustrate how DHCP works. When a device like your computer is connected to a network, it interacts with the DHCP server in the following way:

Packet-1. DHCP Discover – Client broadcasts a discovery request to all devices on the network in an attempt to reach a DHCP server.
Packet-2. DHCP Offer – An IP lease is offered to the client by the DHCP server.
Packet-3. DHCP Request – The client then requests an IP lease from the server.
Packet-4. DHCP ACK(knowledge) – Lastly the server acknowledges an IP lease.

Now the device has been assigned a leased IP address.

Figure 9 The DHCP client & server packet exchange showing how an IP address is assigned via DHCP.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	314	DHCP Discover - Transaction ID 0x3d1d
2	0.000295	192.168.0.1	192.168.0.10	DHCP	342	DHCP Offer - Transaction ID 0x3d1d
3	0.070031	0.0.0.0	255.255.255.255	DHCP	314	DHCP Request - Transaction ID 0x3d1e
4	0.070345	192.168.0.1	192.168.0.10	DHCP	342	DHCP ACK - Transaction ID 0x3d1e

As you will see, the 4-step process that assigns the dynamic IP address to the device is listed in the four packets in Wireshark. Analyze the four packets in this packet capture and answer the questions below.

© 2023 Virginia Cyber Range. Created by Thomas Weeks. (CC BY-NC-SA 4.0)

Question 4.4.1: After looking at the packets, what are the 4 phases of a DHCP request?

Question 4.4.2: Out of the two transport protocols (TCP or UDP), which is used for DHCP? Why do you think this is?

Question 4.4.3: What incoming server port does DHCP rely on to receive requests?   (Hint: Look at the Packet Details Pane.)

End of Lab Questions:

1. From our slammer.pcap file, what is the destination IP of the packet?

2. What is DNS?

3. What port does DNS listen on?

4. Who is the DHCP Discover sent to? Who is the intended recipient?

5. References

None.

[This portion of the lab is provided for instructors that will be using this lab and associated material in their class.]

[**Note to instructors**: This exercise makes use of resources provided in the Cyber Range. It is a single Kali Linux virtual machine, or you can choose to have the students complete this exercise with a VirtualBox Kali Linux Virtual Machine on their computer (laptop).

Answers to in-task questions:

4.2.1 – 20199
4.2.2 – 1434
4.3.1 – 1707
4.3.2 – google.com

© 2023 Virginia Cyber Range. Created by Thomas Weeks. (CC BY-NC-SA 4.0)

4.4.1 – DHCP Discover(client), DHCP Offer(server), DHCP Lease Request(client), DHCP Lease ACK(server)
4.4.2 – DHCP uses UDP as its transport layer. First, UDP is used because TCP cannot establish a connection (three-way handshake) without a configured destination IP address. Second, since DHCP is only used via LAN broadcasts, UDP packets are 100% local (not routed) and thus should be very reliable and also are logical to use in this application.
4.4.3 – UDP port 67

Answers to End of Lab Questions:

1. 65.165.167.86
2. Domain Name System – A networking protocol that translates human domain names (www.example.com) to IP addresses (understood by browsers).
3. 53
4. It is broadcasted and sent to all devices, but is intended for the DHCP server.]

KSAs Addressed
From: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Knowledge:

- **K0001:** Knowledge of computer networking concepts and protocols, and network security methodologies.
- **K0010:** Knowledge of communication methods, principles, and concepts that support the network infrastructure.
- **K0034:** Knowledge of network services and protocols interactions that provide network communications.
- **K0088:** Knowledge of systems administration concepts.
- **K0129:** Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep).
- **K0174:** Knowledge of networking protocols.
- **K0301:** Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
- **K0555:** Knowledge of TCP/IP networking protocols.

Skills:

- **S0046:** Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
- **S0156:** Skill in performing packet-level analysis.
- **S0199:** Skill in creating and extracting important information from packet captures.
- **S0275:** Skill in server administration.

Abilities: None.

Knowledge Units (KUs) Addressed:
From: https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf
(you may need to accept an invalid iag.gov SSL certificate to reach this PDF)

- Basic Networking (BNW)
- Network Defense (NDF)

© 2023 Virginia Cyber Range. Created by Thomas Weeks. (CC BY-NC-SA 4.0)