

Lab - Network Sniffing with Wireshark

Objectives

In this lab, you will use the Linux utility **tcpdump** to capture and save network traffic. You will then use Wireshark to investigate the traffic capture.

- Prepare the host to capture network traffic.
- Capture and save network traffic.
- View and Analyze the Packet capture.

Background / Scenario

Wireshark is a network packet capture utility that can be used by network administrators to troubleshoot network problems. It can also be used to eavesdrop on network communications to passively collect information about users and services. Wireshark is considered a passive tool because it does not create traffic on the network.

Required Resources

- Kali VM customized for Ethical Hacker course
- Internet access

Instructions

Part 1: Prepare the Host to Capture Network Traffic.

Step 1: Start the virtual machine and log in.

- a. Start the Kali workstation virtual machine. Use the following user credentials:

Username: **kali**

Password: **kali**

- b. Start a terminal session by clicking on the terminal icon on the menu bar.

Step 2: Verify the environment.

- a. Verify the user directory that will be used to store the captured traffic. To display the current directory, use the **pwd** command to display the full path to the current working directory.

```
└─(kali@Kali)-[~]
```

```
└─$ pwd
```

Record the directory location.

Answer Area

```
<!----><!---->
```

- b. Determine the IP address of the Kali Ethernet interface using the **ifconfig** command. The ethernet interface is usually named **eth0**.

```
(kali㉿kali)-[~]  
└─$ ifconfig
```

Record the IP address and MAC address of the Ethernet network interface. This will be the source address for packets originating on the Kali machine.

Answer Area

<!--><!-->

- c. Determine the default gateway assigned to the Kali host using the **ip route** command.

```
(kali㉿kali)-[~]  
└─$ ip route
```

Record the IP address of the default gateway. The default gateway responds to ARP requests for destination IP address located off the source network.

Answer Area

<!--><!-->

Note: The IP address of the default gateway must be on the same IP subnet as the Ethernet interface address.

- d. Determine the address of the configured default DNS server by displaying the contents of the **/etc/resolv.conf** file. You can view the file using the **cat <file name>** command.

```
$ cat /etc/resolv.conf
```

Record the IP address of the configured default DNS server. The DNS server IP address will be the destination address of standard query packets and the source address for DNS reply packets.

Answer Area

<!--><!-->

Part 2: Capture and Save Network Traffic.

In this part, you will use **tcpdump** from the CLI to capture traffic. You will use command options to save the traffic to a packet capture (pcap) file. These records can then be analyzed using different applications that read pcap files, including Wireshark.

Step 1: Open a terminal and start tcpdump.

- a. Open a terminal application and enter the command **ifconfig**.

```
└─(kali㉿Kali)-[~]
```

```
└─$ ifconfig
```

- b. In the **ifconfig** output, find the interface name that corresponds to the Ethernet adapter (usually eth0). Right click the interface name and select **Copy Selection**.
- c. Enter the **sudo tcpdump** command as shown. Replace the **<interface>** text with the interface name that you copied in the previous step. This command requires root user access, so enter **kali** as the password if prompted.

```
└─(kali㉿Kali)-[~]
```

```
└─$ sudo tcpdump -i eth0 -s 0 -w packetdump.pcap
```

The **-i** command option allows you to specify the interface. If not specified, the tcpdump will capture all traffic on all interfaces.

The **-s** command option specifies the length of the snapshot for each packet. Setting this option to 0 sets it to the default of 262144.

The **-w** command option is used to write the result of the **tcpdump** command to a file. Adding the extension **.pcap** ensures that operating systems and applications will be able to read the file. All recorded traffic will be printed to the file **packetdump.pcap** in the home directory of the user.

Step 2: Generate network traffic using a web browser

- a. To capture an HTTP request and reply, open a web browser in Kali desktop. Navigate to **Google.com**. Do not login or search.
- b. Open a second tab in the browser, enter **skillsforall.com** on the launch bar. Once the page appears, click the user icon at the top right of the page. Log in with your Skills for All login information.
- c. Return to the terminal window that is running the **tcpdump** utility and enter **CTRL-C** to complete the packet capture.
- d. The tcpdump utility saved the output to a file named **packetdump.pcap**. This file should be saved in the default home directory. Verify that the file exists in the directory using the **ls** command.

```
└─(kali㉿Kali)-[~]
```

```
└─$ ls packetdump.pcap
```

```
packetdump.pcap
```

Part 3: View and Analyze the Packet capture.

In this part, you will use Wireshark to analyze the packet capture file that you created in Part 2 of this lab.

Step 1: Open the Wireshark application to view the packet capture.

- a. Use Wireshark to view the captured packets. Launch the graphical Wireshark application by typing **wireshark** at the CLI prompt.

```
└─(kali㉿Kali)-[~]
```

```
└─$ wireshark
```

The Wireshark application should open in a different window. Expand the Wireshark window to full screen.

- b. Use the **File -> Open** menu option and enter **packetdump.pcap** in the File Name field. Click **Open**. A screen should open displaying the contents of the **packetdump.pcap** file.

Step 2: Analyze DNS traffic.

When you type a website URL into your browser, your PC performs a DNS query to the DNS server's IP address. Observing DNS queries and responses provides the names (URLs) and IP addresses of sites a user visits. Knowing websites that are commonly visited by users can be valuable when formulating social engineering attacks.

- a. Filter the captured traffic to only display DNS queries and responses. Enter **dns** in the Filter Field on the Wireshark main screen. You will notice that in addition to the **Skills for All** website that you requested, other DNS lookups are shown. These correspond to links contained within the Skills For All and Google homepages.

What are some of the websites that are listed in the DNS Standard queries?

Answer Area

<!--><!-->

- b. Click the search icon and search for the **skillsforall.com** hostname. Select **String** in the dropdown box and enter **skillsforall** in the search box.
- c. Select the first Standard query for the **skillsforall.com** website. Expand the query details pane below the packet list to view the contents of the query packet.
- d. Expand the **Ethernet II** information to display the Layer 2 header data contained in the packet. The source MAC address is the MAC of the sending device interface, in this case the Kali VM, and the destination MAC address is the MAC of the default gateway since the DNS server is not on the same Layer 2 network.

Does the source MAC address match the address that you recorded in Part 1?

Answer Area

<!--><!-->

- e. Expand the **Domain Name System (query)** section to see the details of what is being sent to the DNS server. It also indicates the line that contains the reply packet that was received in response to the query. Double-click the link to the response. The details of the Standard query response packet are shown.

What IP addresses are associated with the URL **skillsforall.com**?

Answer Area

<!--><!-->

- f. Close Wireshark to return to the CLI prompt.

Step 3: Analyze an HTTP Session

In this step, you will capture and analyze a web request and response. You will use Wireshark to capture the traffic and to analyze the messages exchanged between the web server and the client. The website server is a VM server running in a Docker container on the Kali Linux host.

- a. Use **ifconfig** to determine which interface on the Kali Linux VM is configured in the 10.6.6.0/24 network.

```
└─(kali㉿kali)-[~]
```

```
└─$ ifconfig
```

What is the name of the interface connected to the 10.6.6.0/24 network?

Answer Area

```
<!--><!-->
```

What is the IP address assigned to that interface?

Answer Area

```
<!--><!-->
```

- b. Open Wireshark by typing **wireshark** at the command prompt. Wireshark will open in a new window, expand the window to full screen. At the center of the main Wireshark screen there will be a list of interface names to choose to capture traffic. Double click the interface name that matches the interface name you discovered in step 2a.
- c. Open a browser window and enter the IP address 10.6.6.13 on the launch bar. A login screen for the DVWA web server appears. Enter **admin** as the username and **password** as the password.

Username: **admin**

Password: **password**

- d. When the main DVWA page appears, click the **Instructions** button at the top of the menu on the left side of the screen. When the instructions page appears close the browser window.
- e. Return to the Wireshark window. Stop the capture using the **red square icon** on the menu bar. The web server DVWA is using HTTP, not HTTPS. Use the **search icon** to find the string **POST** in the captured packets. POST messages transfer form data from the client to the server, in this case the login information.
- f. Double click the first POST packet to view the detail in a separate window. Expand the section titled **HTML Form URL Encoded**:

What information is contained in this section?

Answer Area

```
<!--><!-->
```

- g. Cookies are used for various purposes. Most frequently, they are used to save information about a user's session. Cookies can be hijacked and used in session hijacking attacks. The initial cookie for a session is sent from the web server to the client with the **Set-Cookie** value in a HTTP response. Use the search icon to find the string **302 Found** in the packet pane. Double click the first packet that was found and expand the **Hypertext Transport Protocol** section.

What value is being set in the cookie being sent from the web server to the Kali client?

Answer Area

<!--><!-->

- h. Examine the next **GET** packet being sent from the Kali client browser after receiving the cookie information. Expand the **Hypertext Transfer Protocol** section. Look for the Cookie values being sent in the packet.

Does the PHPSESSID being sent back to the server in the GET request the same as the one sent from server in the earlier reply?

Answer Area

<!--><!-->

- i. Close Wireshark. You will have the option to save the .pcap file containing the capture or to quit without saving. The .pcap file will be saved in the current working directory unless otherwise specified.

Reflection Questions

1. In this lab, you had the opportunity to become familiar with capturing packets in both the tcpdump utility and the Wireshark application. What are the benefits of using packet capture utilities when performing passive reconnaissance on a potential target?

Answer Area

<!--><!-->

2. What pieces of information can be gathered using packet captures?

Answer Area

<!--><!-->