

# Intercepting and Interpreting Network Traffic with Packet Sniffing Tools

## Scenario

In this activity, you will use Wireshark and tcpdump to capture network traffic and display relevant information on the local network. Interpreting the output from such captures is useful for security assessments.

## Objectives

This activity is designed to test your understanding of and ability to apply content examples in the following CompTIA Security+ objective:

- 4.1 Given a scenario, use the appropriate tool to assess organizational security.

## Lab

- Kali VM
- MS1 VM
- LX1 VM
- pfSense VM

## Task 1

### Sniff network traffic

Use the Kali Linux virtual machine to capture some network traffic and identify the main features of the Wireshark network analyzer. You'll assume that Kali has been able to obtain some sort of network tap, which has been simulated for you already by configuring port mirroring on the virtual switch.

1. Select the **Kali** VM and log on with the user **kali** and **Pa\$\$w0rd** as the password.
2. From the desktop, select the **Wireshark** application.

**TIP:** Maximize the window to make Wireshark easier to work with.

3. In the **Capture filter** box, type **ip**.

**TIP:** The **ip** filter captures IPv4 traffic, not IPv6 traffic.

4. Under **Capture**, select the **eth0** adapter.

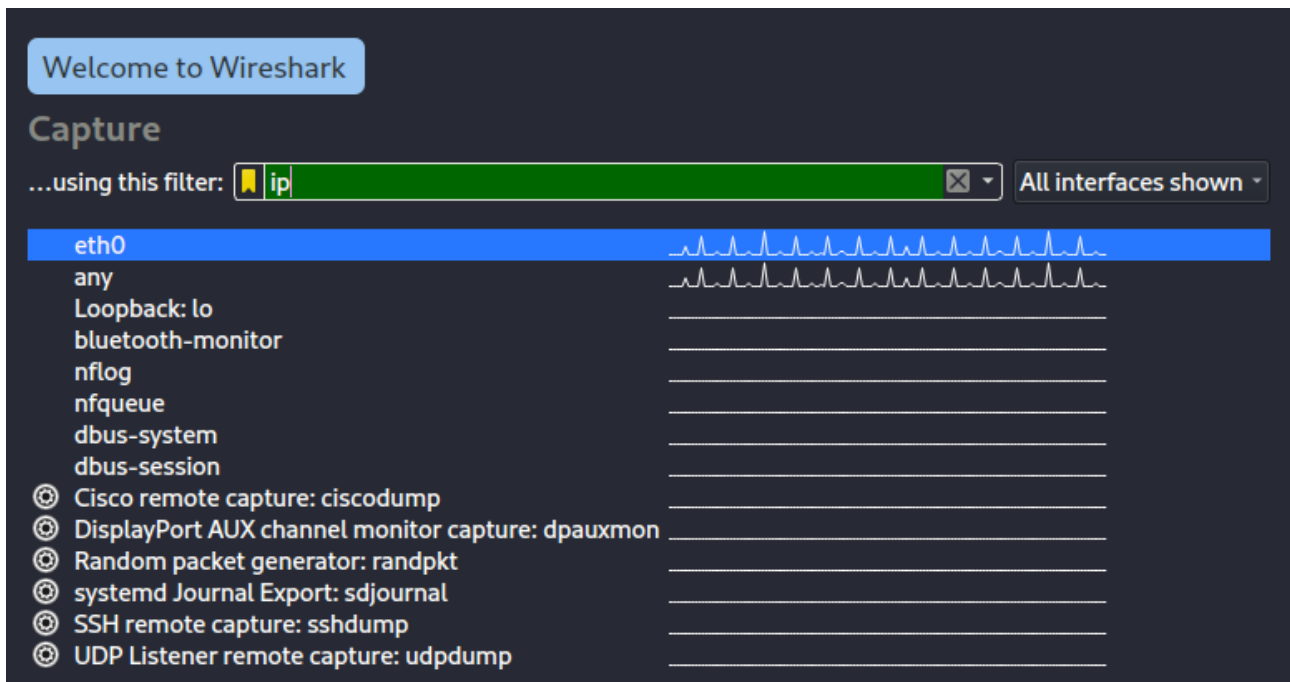


Figure 1.1 – Wireshark Welcome window.

**NOTE:** There are two types of filters: **capture filters** restricts which frames the sniffer records while **display filters** (but does not discard) what has been recorded. The syntax of capture and display filters is different, and capture filters are more basic.

5. Start the capture by selecting the blue **Start capturing packets** button in the upper left corner or the Wireshark interface.

6. On the **Kali** VM, launch **Firefox** from the menu, and the type in the address bar:

`http://192.168.1.2`

7. As soon as the web page is displayed in Firefox, switch back to the Wireshark application.

**NOTE:** In this task, you are capturing packets on the **Kali** VM and connecting to the **MS1** web server from the same **Kali** VM.

**TIP:** Capturing traffic on a client computer as it is attempting to connect to a destination computer might be useful in both security and networking troubleshooting scenarios.

8. Select the **Stop** button on the toolbar to end the live capture.

9. Select any **DNS** frame (they are color-coded as light blue) from the top panel, and then observe the frame contents displayed in the middle panel.

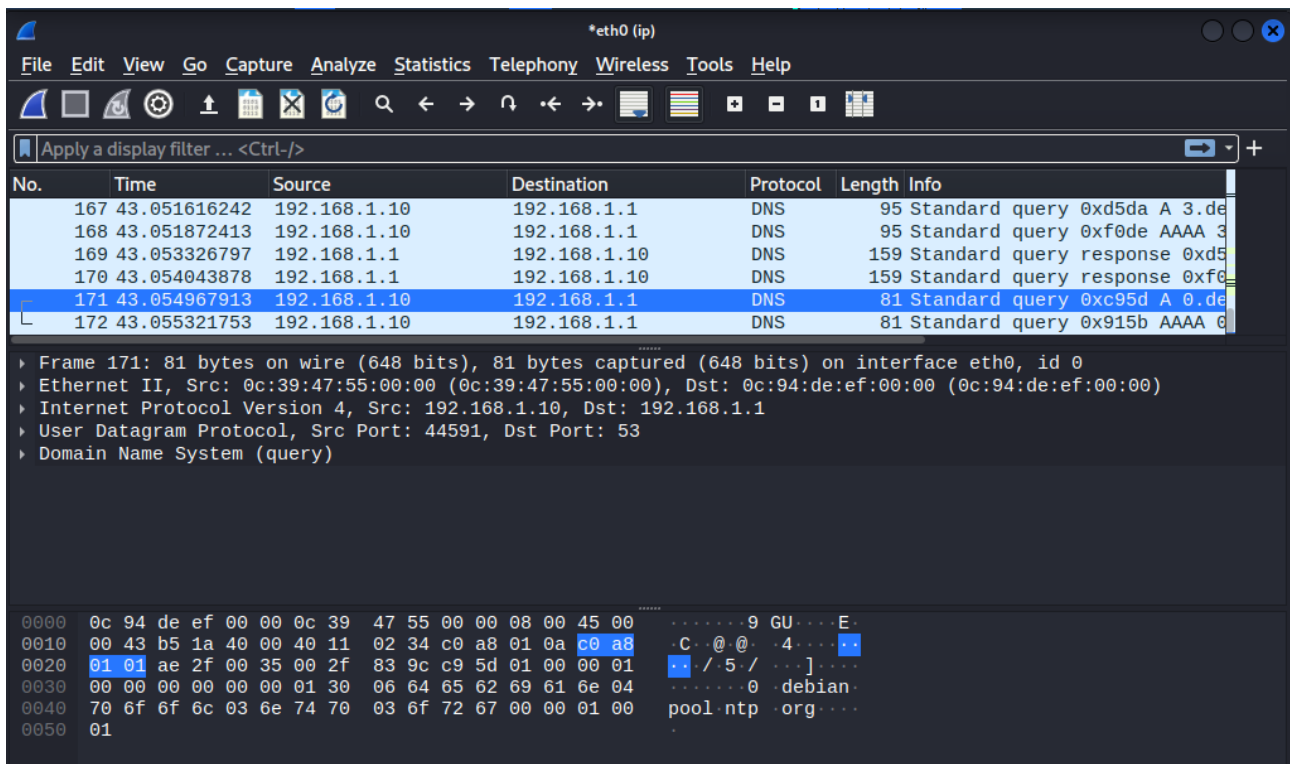


Figure 1.2 – Wireshark capture.

Wireshark splits out the successive headers and payloads to decode each protocol.

- **Frame:** this shows information about the bytes captured.
- **Ethernet II:** this shows the frame type (data link layer/layer 2) and the source and destination MAC addresses.
- **Internet Protocol Version 4:** this is the IPv4 datagram, notably showing the source and destination IP (layer 3) addresses. Note there's also a GeoIP function in this section, but as these are private addresses, they cannot be resolved to a particular regional registry or ISP.
- **User Datagram Protocol:** layer 4 (transport) uses either UDP or TCP. The most significant fields here are the source and destination ports. UDP port 53 is the “well known” DNS server port.
- **Domain Name System:** this is the application protocol. Depending on which frame you selected, you may be looking at a query or a response.

**NOTE:** Observe how this window in Wireshark reflects the layers of the TCP/IP stack (though it is inverted). Ethernet II displays physical (MAC) address information, Layer 3 shows logical addressing (IP) and layer 4 shows application layer source and destination ports. The application layer contains protocol-specific headers and the data payload (DNS in this example).

10. Select the **TCP** frame that opens the connection to the web server (the first frame that is colored green), and then examine the contents of the middle panel.

Be sure to note both the source and destination port numbers.

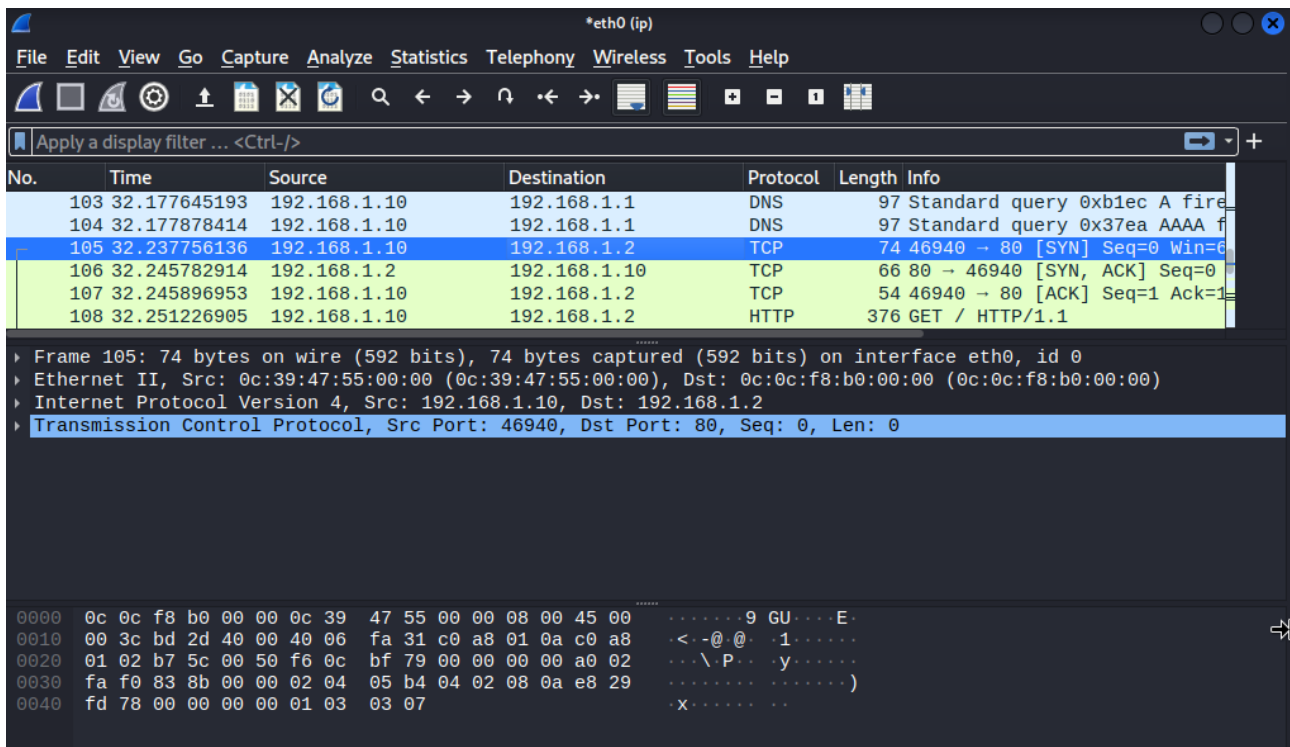


Figure 1.3 – Wireshark capture displaying the first TCP packet.

11. Close or minimize **Wireshark**.

## Task 2

### Use tcpdump to intercept HTTP network traffic

The **tcpdump** program is another protocol analyzer (packet sniffer). In this activity, you will use **tcpdump** to intercept HTTP traffic.

1. Switch to the **MS1** VM, select **CTRL+ALT+Delete**, and then sign in as **CONSOTO\Administrator** with **Pa\$\$w0rd** as the password.

**NOTE:** The MS1 VM is hosting a default web site that will be used as part of the packet interception activity.

2. From **Server Manager**, select **Tools > Internet Information Services (IIS) Manager**.

3. Expand the **MS1** and **Sites** nodes to display the **Default Web Site** node.

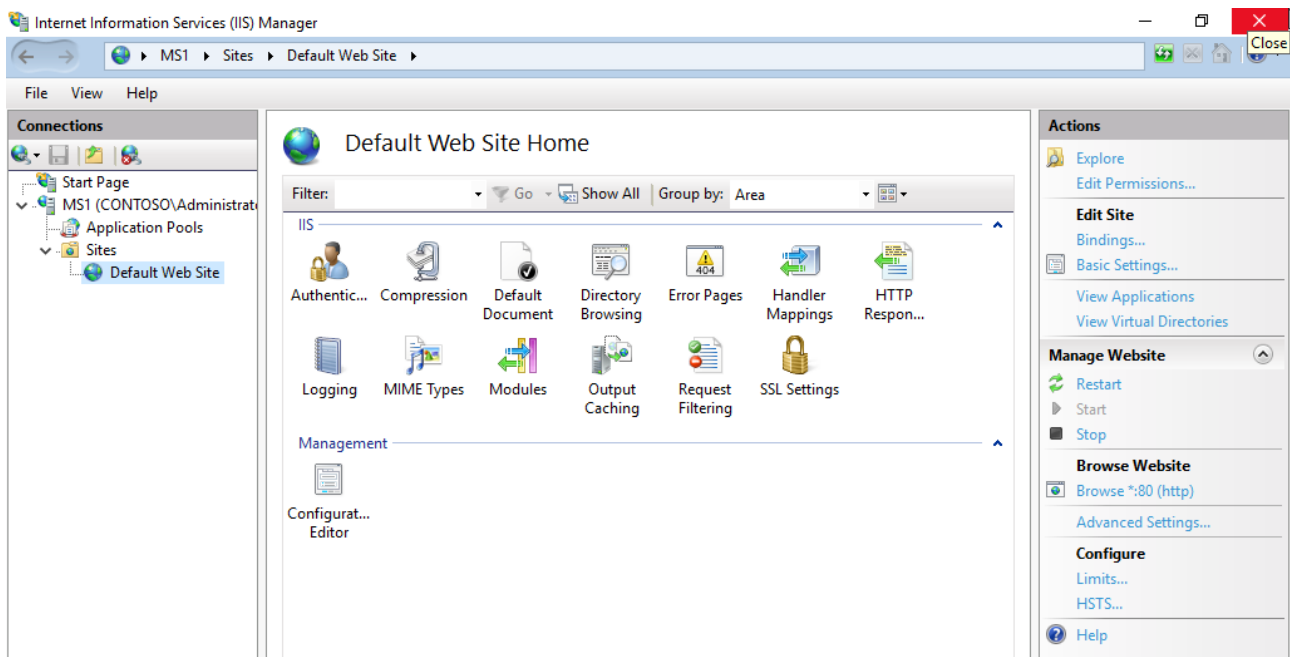


Figure 2.1 – Internet Information Services (IIS) Manager.

4. Double-click the **Authentication** applet in the Default Web Site Home pane.
5. Select **Anonymous Authentication**, and then from the **Actions** pane on the right, select **Disable**.
6. Select **Basic Authentication**, and then from the **Actions** pane on the right select **Enable**.

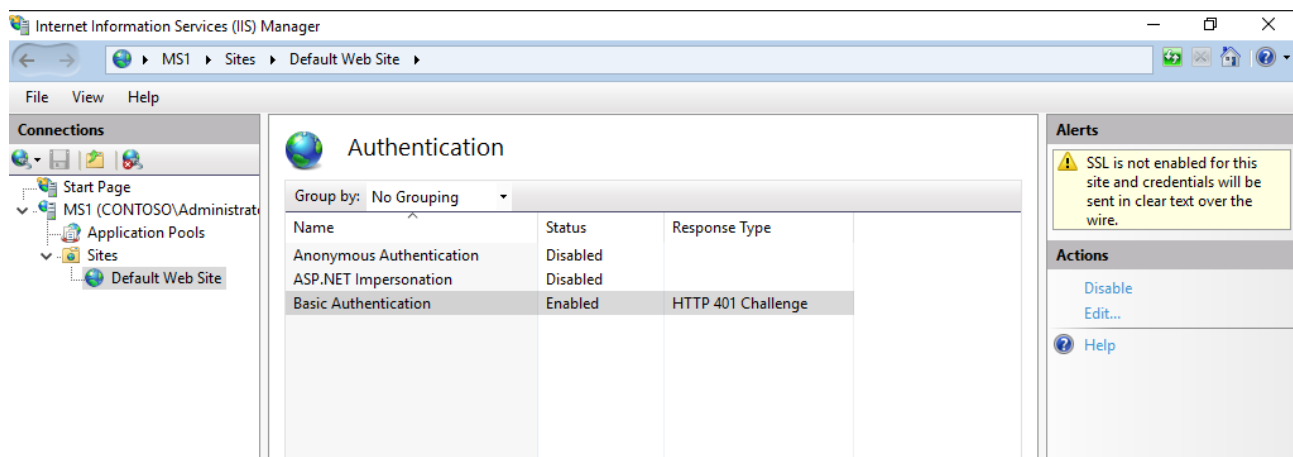


Figure 2.2 – IIS Manager enabling Basic Authentication.

**NOTE:** The alert about the lack of SSL and cleartext credentials, but ignore it for the purposes of this activity.

7. Switch to the **Kali** VM, and then confirm that you are signed in. If necessary, log on with the credentials **kali** and **Pa\$\$w0rd**.
8. From the menu at the top of the desktop, open the **Terminal**.
9. Run the following command to begin intercepting MS1 **HTTP** network traffic by using **tcpdump**:

```
sudo tcpdump -vv dst 192.168.1.2 and port www -w www.pcap
```

```
(kali㉿kali)-[~]  
$ sudo tcpdump -vv dst 192.168.1.2 and port www -w www.pcap  
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
Got 0
```

Figure 2.3 – The tcpdump command.

**TIP:** You will not see captured frames in the Terminal output. The -w switch directs output to a capture file.

10. From the top menu, start **Firefox**, and then connect to the website hosted at **http://192.168.1.2**

11. You will be prompted to enter the following name and password (if not, press **F5** to refresh the page).

```
CONTOSO\Administrator  
Pa$$w0rd
```

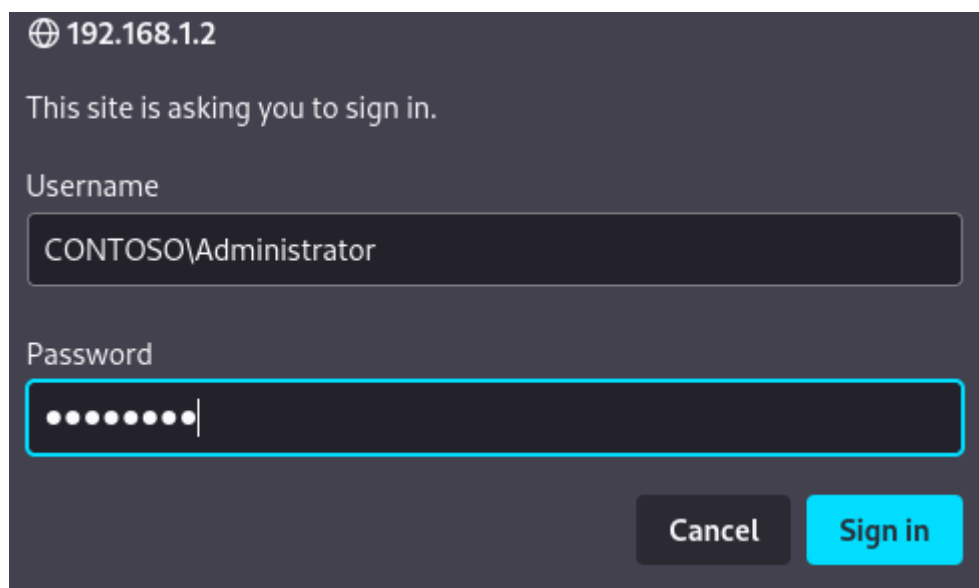


Figure 2.4 – Typing the administrator credentials for authentication.

12. Switch to the **Terminal** window and then select the **CTRL+C** to stop the tcpdump capture.

13. Switch to the Wireshark application, if you closed the program, launch it again from the desktop. Select the **File** menu, and then select **Open**.

14. Select the **www.pcap** file from the kali user's home directory, and then select **Open**. If prompted, select **Continue without saving** to discard the previous Wireshark scan and open this file.

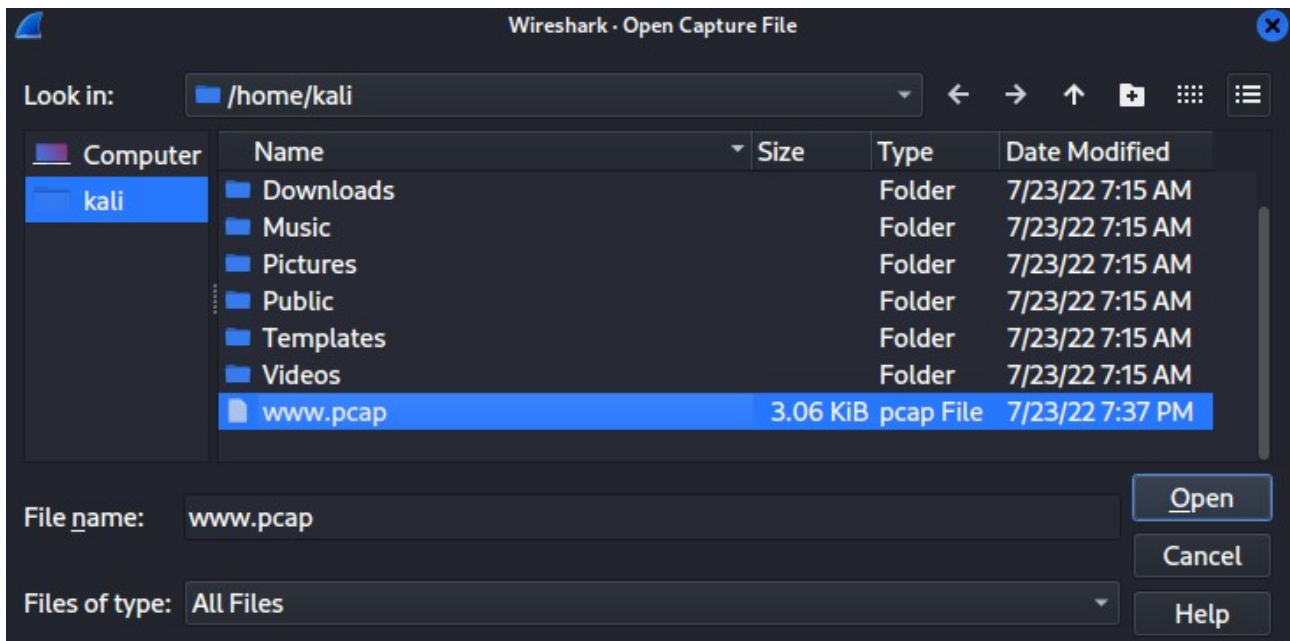


Figure 2.5 – Opening the tcpdump capture www.pcap file with Wireshark.

**NOTE:** tcpdump files are not stored in a human-readable format. Applications such as Wireshark can be used to display their contents.

15. Select one of the **GET** HTTP messages from the top panel in Wireshark. With the **GET** message selected, in the middle panel, expand the **Hypertext Transfer Protocol**, and then expand **Authorization**.

**TIP:** If you had to refresh the page, select one of the GET frames in the second block of HTTP requests to see the authorization header.

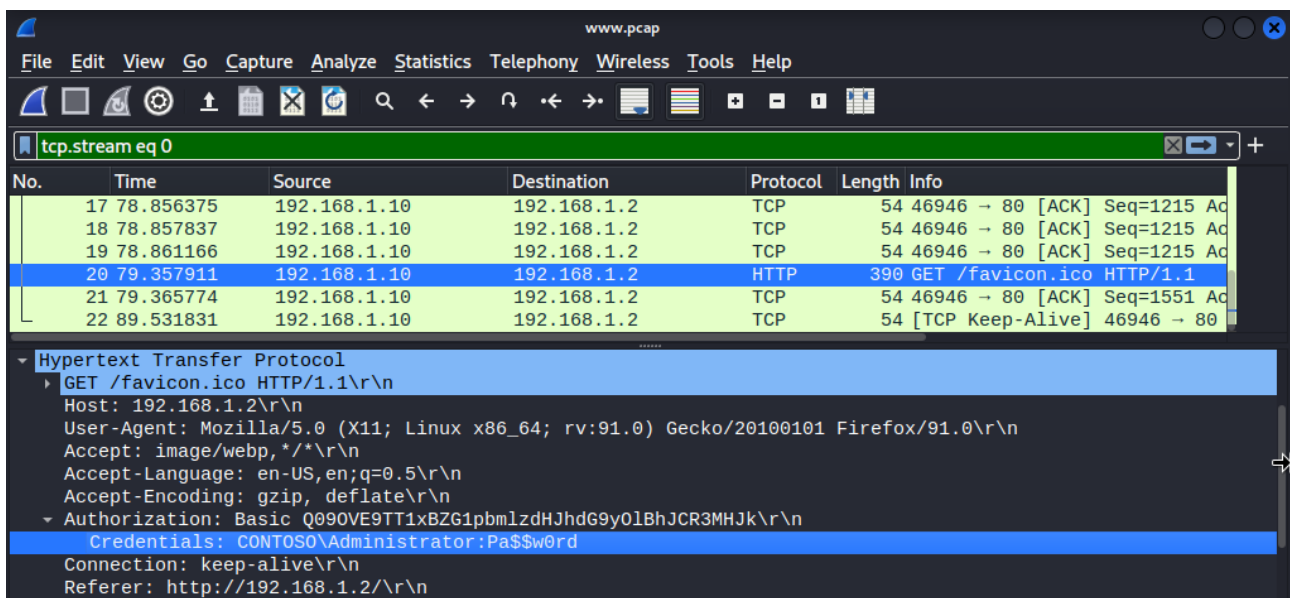


Figure 2.6 – Wireshark showing authentication information.

**NOTE:** HTTP packets are unencrypted and therefore vulnerable to packet sniffing.

16. Close the **Wireshark** application.



## Task 3

### Use tcpdump to intercept SSH network traffic

You will use **tcpdump** to intercept SSH network traffic and attempt to display contents of the traffic. You will use an SSH connection to the 192.168.1.8 IP address. This address is assigned to the **LX1** VM, which runs the CentOS 7 Linux Distribution.

1. On the **Kali** VM, run the following command to begin intercepting SSH network traffic by using tcpdump.

```
sudo tcpdump -vv dst 192.168.1.8 and port ssh -w ssh.pcap
```



```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo tcpdump -vv dst 192.168.1.8 and port ssh -w ssh.pcap
[sudo] password for kali:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
Got 0
```

Figure 3.1 – The tcpdump command capturing ssh traffic.

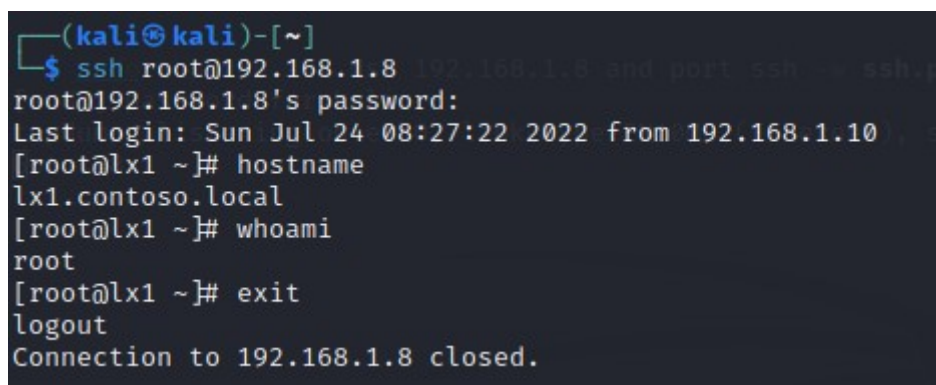
2. Open a second **Terminal** window and then run the following command:

```
ssh root@192.168.1.8
```

3. Enter **yes** to confirm the connection attempt if prompted, and then enter **Pa\$\$w0rd** and the password.

4. Run the **hostname** and **whoami** commands to confirm you are the **root** user on the **LX1** remote system.

5. Run the **exit** command to disconnect from the remote system.



```
(kali㉿kali)-[~]
$ ssh root@192.168.1.8 192.168.1.8 and port ssh -w ssh.pcap
root@192.168.1.8's password:
Last login: Sun Jul 24 08:27:22 2022 from 192.168.1.10
[root@lx1 ~]# hostname
lx1.contoso.local
[root@lx1 ~]# whoami
root
[root@lx1 ~]# exit
logout
Connection to 192.168.1.8 closed.
```

Figure 3.2 – The ssh command authenticating to LX1.

6. Switch to the **Terminal** window hosting **tcpdump** and then press **CTRL+C** to stop the capture.



7. Switch to the **Wireshark** application. If you closed the program, launch it again from the desktop.

8. Select the **File** menu, and then open the **ssh.pcap** file from the kali user's home directory.

This is the same task you did before with the **www.pcap** file.

9. Spend a few minutes browsing the captured SSH information.

Specifically, do you find any authentication credentials? Also notice details such as the source and destination port numbers, etc. Were you able to read information about the root user, such as the password?