WIRESHARK & SNIFFING ATTACKS

28th Sep 2022

OVERVIEW

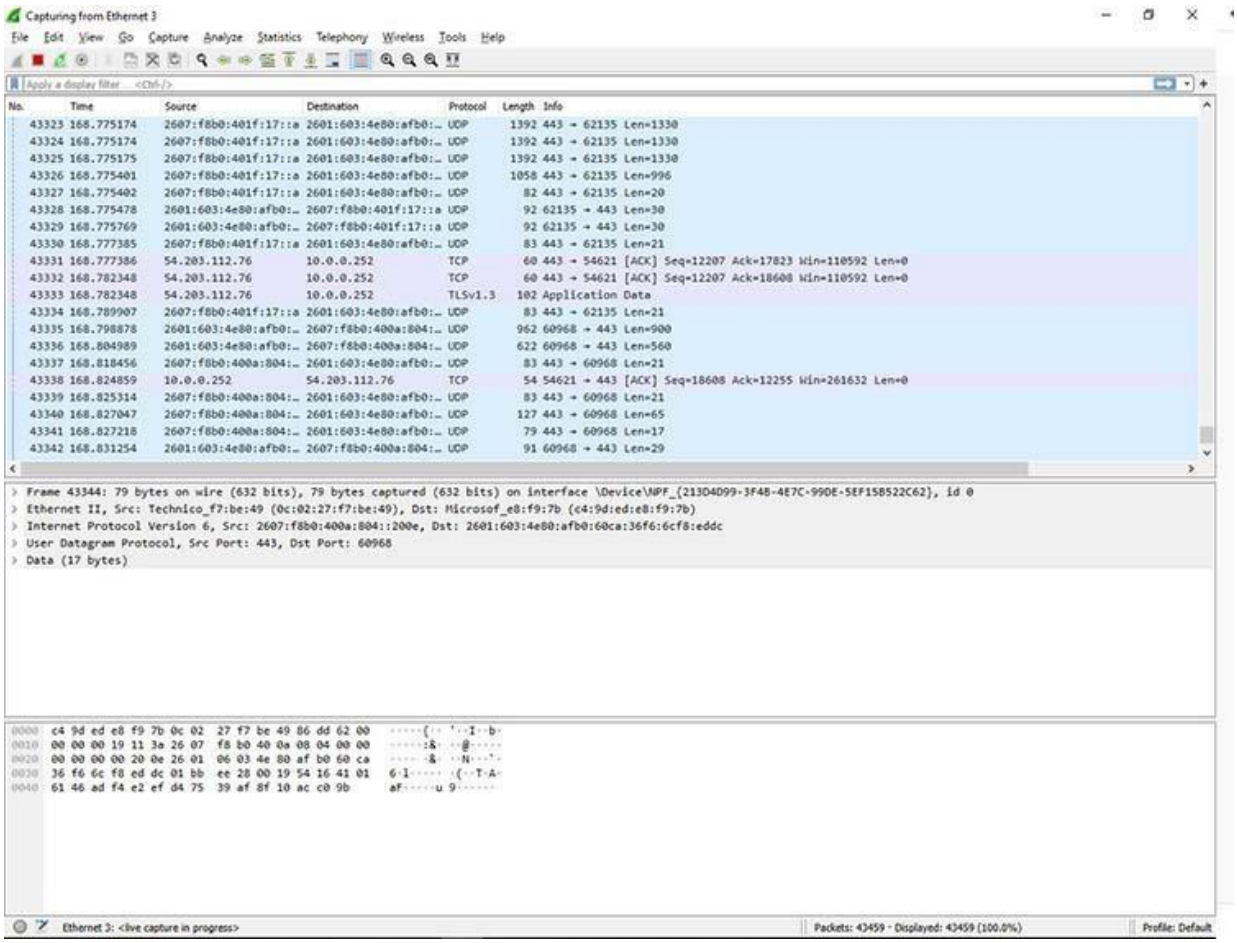
Wireshark is a network protocol analyser or an application that captures packets from a network connection, such as from your computer to your home office or the internet. A packet is a name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. **Packet Capture:** Wireshark listens to a network connection in real-time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.

2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.

3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.



How to Install Wireshark on Linux

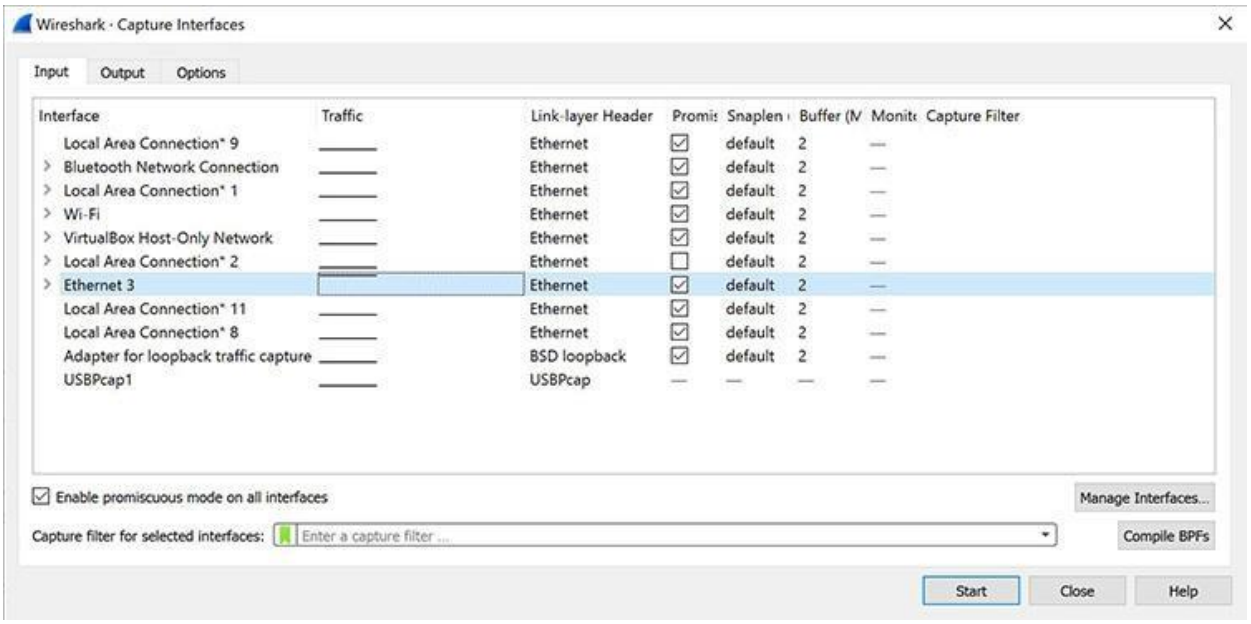
- If you have a Linux system, you'd install Wireshark using the following sequence (notice that you'll need to have root permissions):
- $ sudo apt-get install wireshark
- $ sudo dpkg-reconfigure wireshark-common
- $ sudo usermod -a -G wireshark $USER
- $ newgrp wireshark
- Once you have completed the above steps, you then log out and log back in, and then start Wireshark:
- $ wireshark &

How to Capture Packets Using Wireshark

Once you've installed Wireshark, you can start grabbing network traffic. But remember: To capture any packets, you need to have proper permissions on your computer to put Wireshark into promiscuous mode.

- In a Windows system, this usually means you have administrator access.
- In a Linux system, it usually means that you have root access.

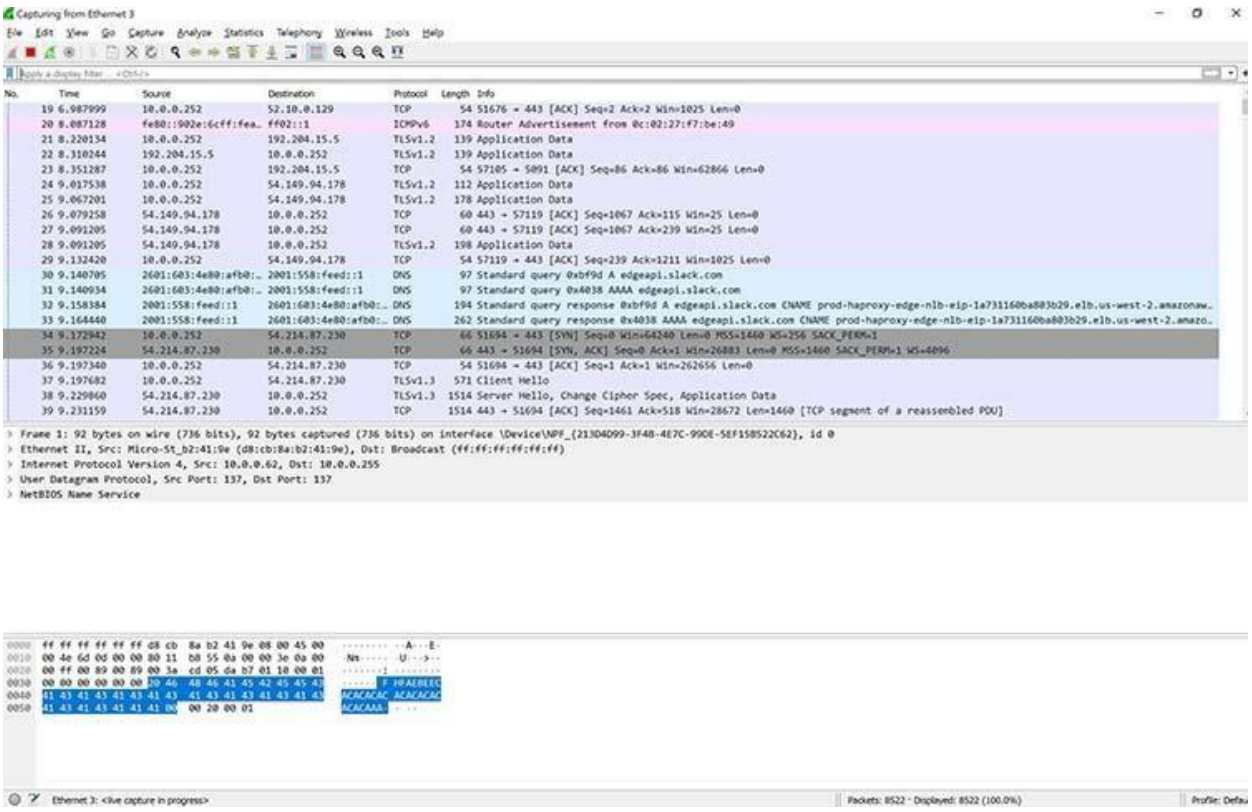
As long as you have the right permissions, you have several options to start thecapture. Perhaps the best is to select Capture >> Options from the main window. This will bring up the Capture Interfaces window, as shown below.



This window will list all available interfaces. In this case, Wireshark provides several to choose from.

For this example, we'll select the Ethernet 3 interface, which is the most active interface. Wireshark visualizes the traffic by showing a moving line, which represents the packets on the network.

Once the network interface is selected, you simply click the Start button to begin your capture. As the capture begins, it's possible to view the packets that appear on the screen.



Once you have captured all the packets that you want, simply click the red, square button at the top. Now you have a static packet capture to investigate.

How Can We Capture Credentials And Other INFO?

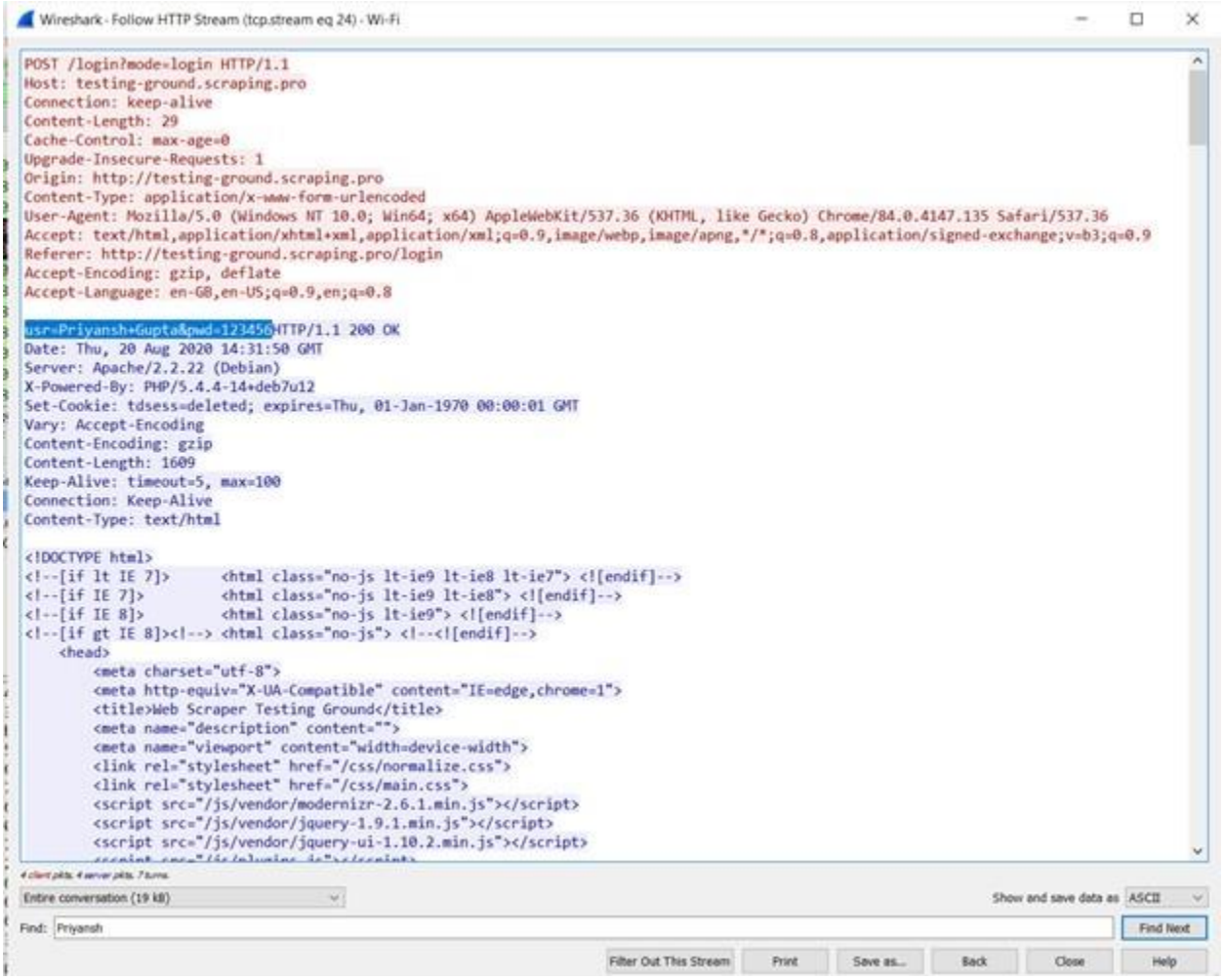
Generally, In A Vulnerable Web App, The Protocol Use Is A Simple HTTP (Not HTTPS) Or An HTTPS GET Method. These Protocols Send Data From One End To The Other Without Applying Any Type Of Encryption Or Other Methods To Hide Data In A Simple Plain Text. Now All Of This Data Is Bound To Exit From A Choke Point In A Network. When An Attacker Monitors Traffic Of This Choke Point, And When He Sniffs The Packets, He Can Easily See All The Relevant Info Via A Network Monitoring Tool Like Wireshark.

We Will Now Try To Capture Credentials Using Wireshark.

1) Capturing Passwords in Insecure Web Apps Using Wireshark:

- Start Wireshark, Select Appropriate Network Adapter (Wi-Fi) In Our Case
- Now Click On The Small Shark Icon At the Top Left Of The Screen To Start Capturing The Packets.
- Now Open The Web Browser And Visit Any Insecure Site.
- Enter Credential Info To Login.
- Now Stop Capturing The Packets.
- Now In Wireshark, Go To Edit->Find Packet

- Select Packet Type To Packet Details And Type To String.
- Search For The Phrase ‘Pwd’ Or ‘Pass’ Or ‘Password’.
- Right Click On The Found Packet And Click Follow Ipv4 Stream.
- You Can Now Analyze And See The Username And Password You Entered.



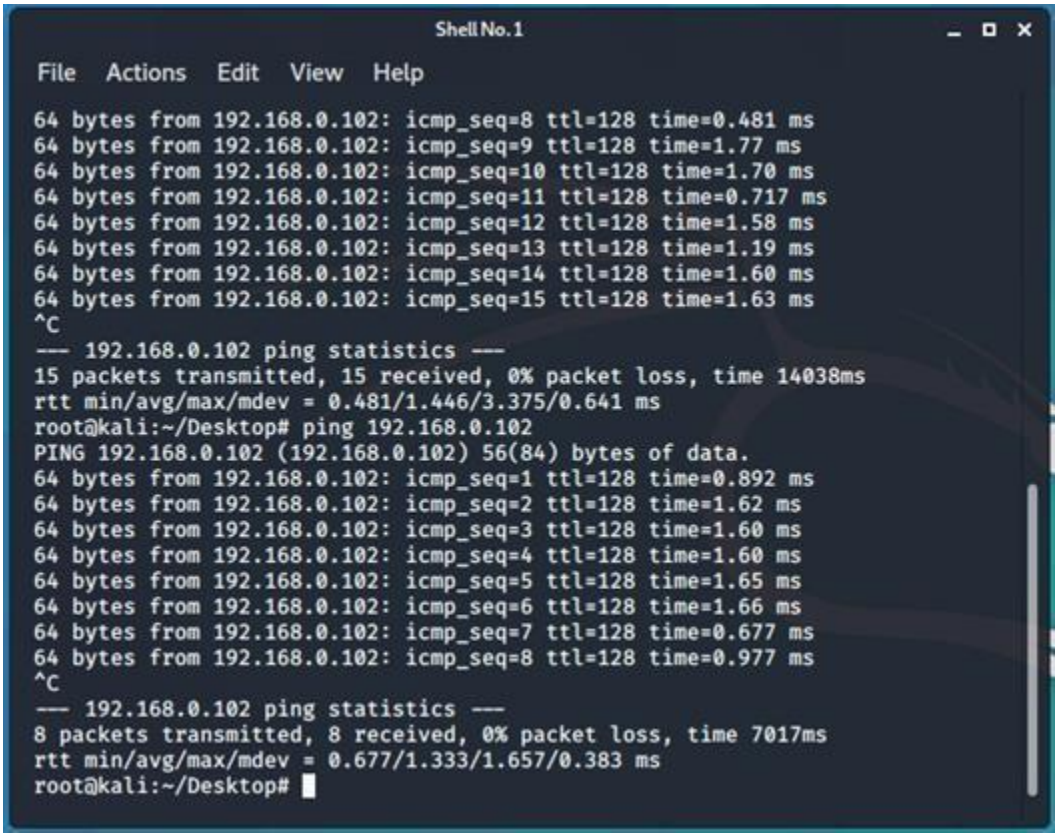
As Seen In The Above Screenshot, The First Line Mentions The Request Method And The Protocol Used. It States That A POST Method With An HTTP Protocol Was Make To The Server, Which Sent The Credentials In A Plain Text Instead of In An Encrypt Format.

Capturing OS Info And Packet Details While Pinging :

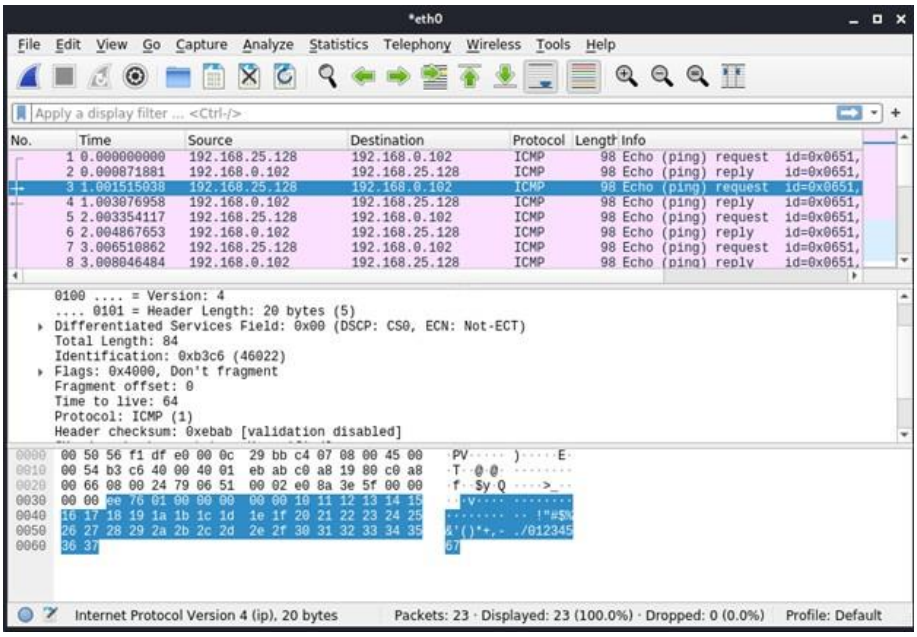
We Can Also Use Wireshark To Capture Different Packets Having Different Protocols Other Than HTTP Or HTTPS. For Instance, We Will Now Capture Traffic Generated Via A “PING” Command While Pinging PC A To PC B. The Ping Command Uses The ICMP Protocol.

- Start Kali Linux VM.
- Then, Start Wireshark In Kali Linux.
- Start Capturing The Packets By Selecting the Appropriate Network Adapter And By Clicking The Shark Icon At TheTop Left Of The Screen.

- Open Terminal And Type “Ping Ipaddress_of_windows_machine” To Ping The Windows Machine From Kali Linux.



- Now Stop Capturing The Packets.
- Open A Packet Having Protocol As ICMP(Request). This Is The Request Packet Sent From Kali Linux To Windows. Analyze The Packet And Lookout For Header Details And Time To Live (TTL). It Should Be 64 To Ensure A Linux Machine.



- Do The Above Step To The ICMP(Reply) Packet. This Is The Reply Packet From Windows. Lookout And Analyze For Time To Live Value(TTL). It Should Be 128 To Ensure That It Is A Windows Machine.