MAJOR – SEP

Name – Anjali Kuamri

Email – anjalirajwar101@gmail.com

College Name – BIT Sindri

Cyber Security Major Project

7. Use Wireshark tool to identify the traffic inspect and see the content flowing in website while you are accessing any http website to login.

A sniffer is a piece of software that captures network traffic and performs network analysis, traffic analysis, protocol analysis, sniffing, packet analysis, and so on.

A network analyzer is a combination of hardware and software tools that can detect, decode, and manipulate traffic on the network. Network administrators use network analyzers to troubleshoot networking issues, but many hackers use them to gather vital information.

The following list contains some common analyzers:

- Wireshark
- Ettercap®
- Dsniff®
- Tcpdump
- Etherpeak®
- Cain and Abel®

Wireshark is a packet sniffer and analysis tool. It captures network traffic on the local network and stores that data for offline analysis. Wireshark captures network traffic from Ethernet, Bluetooth, Wireless (IEEE.802.11), Token Ring, Frame Relay connections, and more.

Open a terminal and type the following command to install Wireshark:

sudo apt update

sudo apt install wireshark

Type the following command to open Wireshark:

sudo wireshark

Wireshark may display an error as you have opened it as superuser. Ignore it as now and press ‘OK’ to continue.

Check “enp0s3” interface and uncheck all other interfaces, then press ‘OK’.

Start packet capturing by clicking “Capture” → “Start” button.
Wireshark will start capturing network packets and display a table.
Browse one or more websites.
After a while (15 to 20 seconds), stop capturing (“Capture” → “Stop”).

You can now observe few things. There are several packets captured by your system. Each packet associates with a protocol. Few of them are as follows:

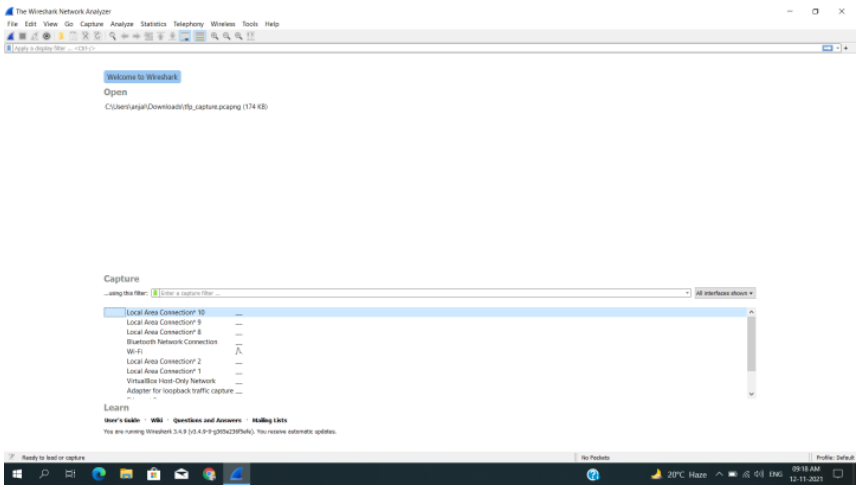
i. DNS – Domain Name System

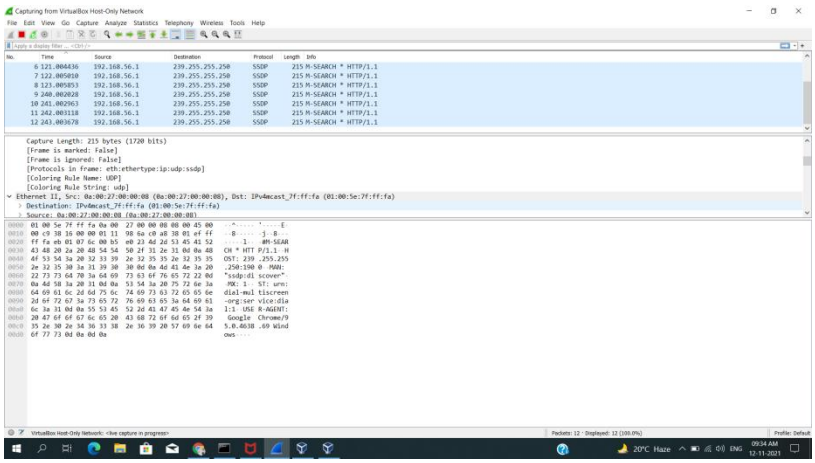
ii. TCP – Transmission Control Protocol

iii. HTTP – Hypertext Transfer Protocol

iv. TLSv1.2 – Transport Layer Security Version 1.2

v. OCSP – Online Certificate Status Protocol





Protecting Yourself From Packet Sniffers

1. Aside from refraining from using public networks,
2. encryption is your best bet for protecting yourself from potential packet sniffers.
3. Using HTTPS, the secure version of HTTP will prevent packet sniffers from seeing the traffic on the websites you are visiting.
4. One effective way to protect yourself from packet sniffers is to tunnel your connectivity a virtual private network, or a VPN.

Thank You···