Cyber Security Internship

**Task 5 : Capture and Analyze Network Traffic Using Wireshark.**

**Objective:** Capture live network packets and identify basic protocols and traffic types.

**Tools:** Wireshark (free).

**Deliverables:** A packet capture (.pcap) file and a short report of protocols identified.

**1.Install Wireshark.**

* Installed Wireshark using command.
* sudo apt install Wireshark.

**2.Start capturing on your active network interface.**

Open Wireshark.

Look at the list of available interfaces and click on eth0.

Start capturing on the one with live traffic.

**3.Browse a website or ping a server to generate traffic.**

Use a command: ping google.com   
A screenshot of a computer screen

Description automatically generated

It starts pinging to google.com and starts capturing the data in Wireshark.

**4.Stop capture after a minute.**

After one minute stop the capture by clicking on the red square button on top of Wireshark.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**5.Filter captured packets by protocol (e.g., HTTP, DNS, TCP).**

DNS, ARP, ICMP, MDNS are the protocol filters found in captured packets.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**6.Identify at least 3 different protocols in the capture.**

In your capture, the common protocols:

* **DNS**: Used for resolving domain names.
* **MDNS**: **Local network name resolution** without needing a central DNS server.
* **ICMP**: Ping-related traffic.
* **ARP**: Address Resolution Protocol for local networks.

**7.Export the capture as a .pcap file.**

 Go to File > Export Specified Packets

 Save with .pcap extension.

I saved my file as “wireshark\_capture.pcap”.

**8.Summarize your findings and packet details.**

**Protocols Found:**

1. **DNS:**
   * Request to www.google.com
   * Response with IP address 192.168.136.2
2. **ICMP\_:**
   * ICMP echo request/reply pairs during ping
   * Request IP: 192.168.136.129 & Reply IP: 142.251.221.110
3. **ARP:**
   * Multiple ARP requests detected for local IP-to-MAC resolution.
4. **MDNS:**

* Responses with IP addresses and services offered
* Queries (standard or service discovery)