Cybersecurity Training Diary – Day 4

Date: 27/06/25
Day: 4th Day
Topic Covered: Wireshark in detail, TCP Handshaking Protocol, Email Breach Check Task

---

Session Overview:

On the fourth day of our cybersecurity training, the session began with an in-depth explanation of **Wireshark**, a powerful network protocol analyzer. Sir explained how Wireshark can be used to monitor, capture, and analyze real-time network traffic, which is essential for identifying suspicious activities, performance issues, and security threats in a network.

1. Understanding Wireshark:

Sir first demonstrated how to install and set up Wireshark on our systems. After launching the tool, he explained the interface – especially the **capture interfaces**, **packet list pane**, **packet details pane**, and **packet bytes pane**.

Key points covered:

- How to start and stop a capture session.
- Filtering packets using filter expressions like http, tcp, ip.addr == 192.168.1.1, etc.
- How to inspect individual packets to see headers and payloads.
- Importance of using Wireshark **ethically** and only on authorized networks.

He also mentioned that Wireshark is commonly used by cybersecurity professionals to detect attacks like **man-in-the-middle attacks**, **unauthorized traffic**, or **data leakage**.

---

2. TCP Handshaking Protocol:

After the Wireshark session, we were introduced to the **TCP 3-way Handshake** protocol which is the foundation of a secure and reliable connection in networks.

Sir explained:

- The steps involved in TCP handshaking:
    1. **SYN** – The client sends a connection request.
    2. **SYN-ACK** – The server acknowledges and responds.
    3. **ACK** – The client acknowledges the server's response.
- We observed this process using Wireshark by applying the filter: tcp.handshake.

- Importance of the 3-way handshake in ensuring **connection establishment**, **packet order**, and **error checking**.

This helped us correlate how low-level networking concepts are captured and analyzed in tools like Wireshark.

---

3. Practical Task: Checking for Email Data Breaches

In the final part of the session, we were given a **practical task** to check whether our email addresses have been involved in any known data breaches.

Steps we followed:

1. Sir guided us to use online services like **Have I Been Pwned** (https://haveibeenpwned.com).
2. We entered our email addresses to check if they were found in any leaked data dumps.
3. If our email had been exposed, the site listed the **names of the breaches**, **what data was exposed** (e.g., passwords, phone numbers), and **recommendations** like changing passwords or enabling 2FA.

This task helped us understand the **real-world impact of cyber breaches** and the importance of **personal cybersecurity hygiene**.

What I Learned Today:

- How to capture and analyze network packets using Wireshark.
- The working of TCP Handshaking Protocol and its role in network communication.
- How to verify if my personal data has been exposed online due to data breaches.
- The importance of regularly monitoring digital exposure and securing personal credentials.

Reflection:

Today's session was highly interactive and practical. The live demonstration of Wireshark and the exercise of checking email data breaches provided me with hands-on experience in network analysis and cybersecurity awareness. I look forward to more such practical activities in the upcoming sessions.