LOGIX ACADEMY

Lab: Wireshark Credentials Breach

Purpose

In this lab, we are going to demonstrate how **Wireshark** can be used to conduct effective forensic investigation in case of credentials breach.

Pre-Requisite

Before you can start the lab, you need to run the lab script which will setup everything. Open the **Labs** folder on Desktop then right-click and "Open Terminal Here". Or open a terminal and cd to Desktop/Labs folder, then issue the command:

```
sudo ./main_script.sh
```

Select **Wireshark Introduction Lab** option from the lab menu.

Scenario

Your organization has been alerted that a sensitive file, `credentials.txt`, hosted on an internal **nginx web server**, has been found **leaked on the dark web**.

The file contains login credentials and API tokens used by internal tools. A **pcapng network capture** (`credentials-breach.pcapng`) from the company's monitoring system has been handed over to you to conduct forensic investigation. Please open the file `/home/kali/Desktop/Labs/credentials-breach.pcapng` in Wireshark.

Challenge

You are part of the incident response team, and your job is to **analyse the capture using Wireshark** to:

1. **Identify how the credentials were accessed**
2. **Determine whether they were exfiltrated**
3. **Provide undeniable proof** that the credentials were indeed leaked

---

🔍 Your Tasks

☑ 1. Find out who accessed the credentials

- Which IP accessed the internal nginx server?
- What protocol and port were used?

☑ 2. Identify if and how the credentials were exfiltrated

- Was there an outbound DNS resolution to an external system?
- What was the remote host name and resolved IP?

☑ 3. Prove that the actual credentials were leaked

Wireshark captures only have value if you can prove what was inside. Your task is to:

- Reconstruct the data sent over the TCP stream
- Take a **screenshot of the payload** showing the contents of `credentials.txt`
- Make sure the credentials are **visible in plain text** (not encrypted)

(Solution in next lecture)