**What was the project is about**

This project, titled **“Network Analysis – Web Shell”**, focused on investigating a simulated cybersecurity incident from a **Blue Team Labs Online** challenge. The scenario involved a **SIEM alert for local-to-local port scanning**, where one internal system began probing another within the same network. Using tools like **Wireshark, Tcpdump, and Tshark**, the goal was to analyze the captured network traffic (PCAP file), detect malicious activity, and uncover evidence of a **web shell upload**. The project demonstrated practical network forensics skills—identifying scans, analyzing HTTP traffic, and correlating findings with SIEM data to understand how the attack unfolded.

**What has done in project**

The analysis began by extracting and unpacking the provided PCAP file (584 KB) using the password **btlo**, revealing the network capture for investigation. An initial triage was performed with **Tcpdump** and **Tshark** to quickly review packet details, identify communicating IP addresses, and determine active protocols. The capture was then examined in **Wireshark** using filters such as tcp.flags.syn==1 && tcp.flags.ack==0 to detect port scanning, http to isolate web traffic, and http.request.method == "POST" to pinpoint suspicious uploads. Next, all HTTP objects were exported via *File → Export Objects → HTTP* and inspected for potentially malicious scripts or code fragments (e.g., system(), eval(), cmd=), which could indicate a web shell. Finally, findings were correlated with the SIEM alert for “Local to Local Port Scanning” to build a clear incident timeline showing when the scan occurred, when malicious uploads happened, and which internal systems were impacted

**To explain how I do it**

I started by unpacking the PCAP file and using **Tcpdump** and **Tshark** for a quick overview of the network activity. Then, in **Wireshark**, I applied filters to detect port scans and suspicious HTTP POST requests. After exporting HTTP objects, I found potential web shell indicators like encoded scripts and command patterns. Finally, I matched these findings with the SIEM alert to build a clear timeline of the attack — showing how internal scanning led to a possible web shell upload

**Solved and results in BTLO chalenges**

In the “Network Analysis – Web Shell” challenge, the investigation revealed that the IP address 10.251.96.4 was responsible for conducting a TCP SYN port scan across the range 1–1024. Further reconnaissance was performed using Gobuster 3.0.1 and sqlmap 1.4.7 to identify potential vulnerabilities. The attacker exploited a PHP file named Editprofile.php to upload a malicious web shell called Dbfunctions.php. The shell used the cmd parameter to execute system commands, beginning with the command id. Finally, the attacker established a reverse shell connection on a specific port, gaining remote access to the compromised system.