The Evil Eye

Devashish Gosain

Deadline: April 1, 2025 (23 59hrs)

1 Description

There has been a sudden rise in Tor traffic in the country "Juniper". The state of Juniper has thus initiated a project called "Evil Eye" to detect Tor traffic. You, the citizen of Juniper, have been hired as a senior trainer in this project, and your first job is to develop a proof-of-concept (PoC) Tor detector.

1.1 Objectives 1

Your task is to develop a Wireshark plugin that analyzes traffic to detect whether a client uses the Tor network. The plugin should identify Tor-related packets and display an appropriate label in Wireshark's packet list view.

Requirements:

1. Plugin Development (Points: 10):
   - Implement the plugin using **Lua** language (preferred) or **C**.
   - Use Wireshark 3.x or later, prefer using the latest version.
   - The plugin must be able to analyze **both** live traffic and saved PCAP files.
2. Detection Mechanism (Points: 20):
   - The plugin should determine whether the system running Wireshark is actively using Tor.
   - It should analyze packet flows and detect characteristics of Tor-related network activity.
   - Detection logic should be efficient to minimize false positives.
3. Wireshark Integration (Points: 10):
   - Add a custom column to the Wireshark packet list pane that displays Tor! for suspected Tor-related packets.
   - The plugin should dynamically update this column when Tor traffic is detected.
   - Apply color rules to highlight detected packets for better visibility.

1.2 Submission Guidelines (10 points):

- Submit your Lua script (or C source files) along with a README explaining installation and usage.
- Include a sample PCAP file demonstrating detection.
- Provide a brief report (1–2 pages max.) explaining your approach and key implementation details.