TLS Security Incident

Problem Description

Transport Layer security (TLS) is a security protocol, supporting application layer protocols such as HTTP, FTP, and SMTP with confidentiality, authenticity, and data integrity. However, TLS could allow a man-in-the-middle attacker to redirect TLS traffic to a different TLS service on another IP address and/or port. The article “ALPACA: Application Layer Protocol Confusion - Analyzing and Mitigating Cracks in TLS Authentication" explains the attack in detail. It provides attack scenarios at https://github.com/RUB-NDS/alpaca-code/tree/master/testlab.

Task

1. Understand how the attack could happen.
2. Replicate the attack in a virtual machine, e.g., VirtualBox, with the code provided at https://github.com/RUB-NDS/alpaca-code/tree/master/testlab.
3. Explain your findings in a report (less than two pages).

Relates to Objectives

1.2, 2.7, 2.8, 2.9, 3.1, 3.5, 4.1, 4.2, 4.4, 4.7, 4.8

(Group)