11-Session Hijacking

PLEASE use prebuilt labs

Victim Data: direct interaction Need 2-6 computers online that have the services running and vulnerable

Advanced: Build a data file / artifact that is actionable by the contract holder. There are no instructions for this task. You must figure everything out.
Advanced: capture encrypted packets, using decryption process from capture discussion

Attacker Data: Kali/ Parrot

Objective

Perform session hijacking:

- Hijack a session by intercepting traffic between server and client
- Steal a user session ID by intercepting traffic
- Detect session hijacking attacks

Overview of Session Hijacking

Session hijacking can be either active or passive

Lab Tasks

Ethical hackers or penetration testers use numerous tools and techniques to perform session hijacking on the target systems. Recommended labs that will assist you in learning various session hijacking techniques include:

1. Perform session hijacking
   1.1. Hijack a session using WIN:Zed Attack Proxy (ZAP)
   1.2. Intercept HTTP traffic using bettercap
2. Detect session hijacking
   2.1. Detect session hijacking using Wireshark*

*Indicates capture