Pós-Graduação Lato Sensu
Curso de Especialização em Redes De Computadores

Serviços de Segurança em Redes

Prof. Dr. **Lucas Dias Hiera Sampaio**

LABORATÓRIO 1

As partes não podem ser compiladas integralmente.
Para uso exclusivo do curso de Pós Graduação da Universidade.

UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CAMPUS CORNÉLIO PROCÓPIO

LAB 1
Comunicação Criptografada

Enunciado da Atividade

Nesta atividade o estudante utilizará o software **Wireshark, Python e uma IDE de desenvolvimento.** O objetivo desta atividade é efetuar a criptografia do programa base chatp2p (disponível junto a este PDF) utilizando o algoritmo AESGCM conforme documentação disponível em Documentação Biblioteca Cryptography.

O estudante deverá entregar um documento em PDF com:

- **Código do script Client.py alterado utilizando a biblioteca sugerida e o algoritmo AESGCM para criptografar e descriptografar as mensagens (utilizar chave e nonce fixo).**
- **Captura de tela do Wireshark demonstrando com pelo menos 4 mensagens (2 em cada cliente) que as informações estão de fato criptografadas (Usar CTRL+ALT+SHIFT+T).**

O código e as figuras que comprovem a atividade devem estar legíveis.

ATENÇÃO: USE A VIDEOAULA APENAS COMO GUIA. TRABALHOS IGUAIS A VIDEOAULA RECEBERÃO NOTA ZERO. VERIFIQUE QUE O ALGORITMO DE CRIPTOGRAFIA É DIFERENTE DO DA VIDEOAULA.

Entrega

Salvar o documento no formato **PDF**.
Utilize seu nome e sobrenome no nome de arquivo:
Nome_Sobrenome_LAB_01.pdf

Submeta no ambiente de ensino.
Não deixar a tarefa em **Modo Rascunho**. Enviar **Tarefa por Definitivo**.

Observação

A porta na qual o Socket do Server.py está ativo é a 50250.