Trabalho em Grupo sobre Protocolo SSL

Entregável (Relatório PDF): Documento PDF com o seguinte conteúdo

1. **Parte Teórica**
   - 1.1. Explique a pilha de protocolos SSL e os respectivos serviços (inclua figuras para explicar o protocolo e mensagens):
     - 1.1.1. SSL Record Protocol
     - 1.1.2. SSL Alert Protocol
     - 1.1.3. SSL Change Cipher Spec Protocol
     - 1.1.4. SSL Handshake Protocol
   - 1.2. O que é uma conexão SSL?
     - 1.2.1. Explique cada um dos parâmetros que definem uma conexão SSL.
   - 1.3. O que é uma sessão SSL?
     - 1.3.1. Explique cada um dos parâmetros que definem uma sessão SSL.
   - 1.4. Quais são as diferenças entre o protocolo SSL e o TLS?
   - 1.5. Quais são os ataque conhecidos contra o SSL/TLS? Desses ataques, escolha dois ataques e os explique. Procure verificar na prática como realizar o ataque;
   - 1.6. Como o SSL/TLS lida com o Ataque do Homem no Meio (Man in the Middle Attack)?
2. **Parte Prática**
   - 2.1. Usando uma implementação do SSL[1], mostre exemplos de uso do SSL
   - 2.2. Você deve criar um site seguro usando SSL/TLS
   - 2.3. Utilize um servidor Web como o Apache (ou outro servidor, justificando sua escolha)
   - 2.4. Crie uma Autoridade Certificadora[2] e emita:
     - 2.4.1. um certificado SSL para servidor
     - 2.4.2. um certificado Cliente SSL
   - 2.5. Mostre a conexão SSL funcionado através de um acesso de um navegador Web qualquer
   - 2.6. Mostre como usar o certificado cliente SSL para autenticação do usuário

Apresentação

Os alunos serão chamados para a apresentação e defesa do trabalho: Avaliação da parte teórica será feita através de perguntas escritas individuais sem consulta que devem ser respondidas baseadas no trabalho realizado. A avaliação da parte prática será feita pelo grupo em data e hora a ser definida.

Bibliografia

[1] William Stallings. 2010. Cryptography and Network Security: Principles and Practice (5th ed.). Prentice Hall Press, Upper Saddle River, NJ, USA.

[1] Uma excelente opção é usar os comandos SSL do OpenSSL para estalever conexões SSL e poder monitorar e capturar mensagens.

[2] Você pode usar o OpenSSL para criar uma AC e depois emitir certificados. Basicamente você deverá gerar um certificado autoassinado que será a AC Raiz. Depois use a chave dessa AC Raiz para assinar certificados finais: neste caso, gere dois certificados, um SSL para o servidor e outro cliente que será usado no cliente.

Definição dos Grupos, Cronograma e Avaliação

1) A tabela abaixo define o participantes de cada grupo e o dia da defesa da parte prática do trabalho em grupo.

Grupo	**Aluno**	Dia	Hora
1	Léo Vieira Peres Lucas Pereira Zarbato	18/11	16:20 - 16:50
2	Igor Henrique Grajefe Feitosa Thiago Senhorinha Rose	18/11	16:50 - 17:20
3	Bruno Martins Crocomo Rafael de Lucena Valle	18/11	17:20 - 17:50
4	Luiz Henrique Américo Salazar Nathan Frois Pereira Paiva	20/11	16:00 - 16:30
5	André Azevedo Vargas Paulo César Pereira Júnior	20/11	16:30 - 17:00
6	Alisson Granemann Abreu Pedro Henrique Pereira Martins	20/11	17:00 - 17:30
7	Diego Fretta Goncalves Rafael Pires Moser	20/11	17:30 - 18:00
8	Fernando Burigo Texeira Luiz Philipi Machado da Silva	25/11	16:20 - 16:50
9	Arthur Machado Branco Júlio César Fernandes Neto	25/11	16:50 - 17:20
10	Lucas Madalozzo Seifert Thaísa Cardoso Lacerda	25/11	17:20 - 17:50

2) A avalição da parte teórica será no dia 27/11, na Sala CTC 101 em horário de aula. Os alunos deverão individualmente responder um questionário de perguntas sobre o SSL/TLS.

3) O relatório final em PDF deverá ser entregue via Moodle até o **dia 26/11.**