APRESENTAÇÃO DO CURSO

- **CENTRO PAULA SOUZA**
  - **Faculdade de Tecnologia São Caetano do Sul**
    - **Curso: Tecnologia em Segurança da Informação**
    - **Disciplina: Criptografia**
    - **Professor: Everson Denis**

OBJETIVOS

- **Ementa;**
- **Avaliação;**
- **Cronograma;**
- **Seminários.**

EMENTA

- Necessidade de segurança;
- Conceitos básicos de segurança (confidencialidade, integridade e disponibilidade);
- Conceitos de criptografia;
- Criptografia simétrica e assimétrica (OpenSSL);
- Assinaturas digitais, autoridades certificadoras, funções de hash, distribuição de chaves, certificados digitais (OpenSSL);
- PGP, uso do GPG (Windows e Linux);
- Análise de Protocolos (Wireshark);
- Análise de Vulnerabilidades;
- Proposta de Segurança usando Criptografia.

AVALIAÇÃO

- Nota P1 – questionários e tarefas, seminário – 50% da nota.
  - Questionários e tarefas (20%)
  - Seminário 1 (20%)
  - Prova (60%)
- Nota P2 - Atividades, questionários, tarefas, seminários – 50% da nota.
  - Tarefas e Trabalho Final (60%)
  - Seminário 2 (40%)
- Nota P3 – Prova

CRONOGRAMA

- Apresentação do curso, necessidade de segurança.
- Conceitos matemáticos, histórico da criptografia (Sistemas monoalfabéticos e polialfabéticos, dispositivos criptográficos, criptoanálise).
- Criptografia de chaves privadas (DES).
- Criptografia de chaves públicas (RSA).
- Autenticação, Funções de Hash, salting, HMAC.
- Algoritmos Assimétricos, Assinatura Digital e Certificado Digital.
- Atividades, trabalhos.
- Seminário 1.
- Prova P1.

CRONOGRAMA

- Criptografia de Dados, Hash, Assinatura Digital usando OpenSSL
- GPG e PGP - Aplicações com Windows e Linux
- Análise de protocolos com Wireshark.
- Análise de Vulnerabilidades.
- Proposta de Segurança usando Criptografia (HTTPS e SSH).
- Atividades e trabalhos.
- Seminário 2.

SEMINÁRIOS

- **Primeiro seminário (Temas):**
  - Algoritmo AES (demonstração);
  - Criptoanálise com Kali (Linux, Windows, wordlists, senhas) com demonstração);
  - Segurança em IoT (ataque e defesa);
  - Vulnerabilidades em algoritmos de hash (md5, sha1) com demonstração;
  - Esteganografia (demonstração);
  - Forense Computacional (demonstração);
  - Aplicações com Criptografia usando CTF (Capture the Flag) – (demonstração prática com desafios quiz - OverTheWire: Wargames, PicoCTF, entre outros).

SEMINÁRIOS

- **Segundo seminário (Temas):**
  - Web Hacking: Explorando serviços, Burp, OWASP 10 (ataque e defesa - demonstração);
  - Engenharia Social: explorando serviços, criando páginas falsas (ataque e defesa - demonstração);
  - Desenvolvimento de Exploits (buffer overflow, análise de código) com demonstração;
  - Aplicações de segurança com Python;
  - Segurança na Nuvem (ataque e defesa);
  - WiFi Hacking: Principais Vulnerabilidades (ataque e defesa com demonstração);
  - Aplicações com Criptografia usando CTF (Capture the Flag) – (ataque/defesa, Tryhackme, Hackthebox, entre outros).

SEMINÁRIOS

- **Apresentação dos seminários:**
  - Duração da apresentação (Power Point): de 20 à 30 minutos;
  - Entregar apresentação em pdf (email);
  - Tópicos abordados na apresentação:
    - Breve histórico;
    - Comparação com outros sistemas operacionais, implementações e tecnologias;
    - Operação e funcionamento do sistema;
    - Cenários, aplicações e demonstrações (quando necessário);
    - Previsões futuras;
    - Conclusão.

SEMINÁRIOS (DIURNO)

- **Apresentação dos seminários (Avaliação):**
  - Avaliação por outros grupos e retorno do professor;
  - Tópicos a serem avaliados (performance individual e em grupo, trabalho em equipe, pertinência com o tema apresentado, pontos fortes e de melhoria nos seminários)
  - Compartilhamento de arquivos e apresentações
- Datas:
  - Seminário 1: 17/09/2024
  - Seminário 2: 26/11/2024

SEMINÁRIOS (NOTURNO)

- **Apresentação dos seminários (Avaliação):**
  - Avaliação por outros grupos e retorno do professor;
  - Tópicos a serem avaliados (performance individual e em grupo, trabalho em equipe, pertinência com o tema apresentado, pontos fortes e de melhoria nos seminários)
  - Compartilhamento de arquivos e apresentações
- Datas:
  - Seminário 1: 19/09/2024
  - Seminário 2: 28/11/2024