

Plano de Aulas - Segurança da Informação

40 aulas de 50 minutos | 20 dias letivos | 2 aulas por dia *Adaptado para laboratório offline e trabalho em equipes*

DIA 1 - Fundamentos da Segurança da Informação

Aula 1: Conceitos Fundamentais de Segurança

- **Teoria:** Tríade CIA (Confidencialidade, Integridade, Disponibilidade)
- Princípios de autenticação, autorização e auditoria
- Conceitos de risco, ameaça, vulnerabilidade e impacto
- Tipos de atacantes e motivações

Aula 2: Configuração do Ambiente de Laboratório

- **Prática Offline:** Instalação em equipes (2-3 alunos por notebook)
 - Download e configuração de VirtualBox
 - Instalação do Kali Linux e máquinas vulneráveis offline
 - Configuração de rede interna entre VMs (NAT/Host-only)
-

DIA 2 - Criptografia: Fundamentos Teóricos

Aula 3: Introdução à Criptografia

- **Teoria:** História e evolução da criptografia
- Diferença entre criptografia simétrica e assimétrica
- Conceitos de chave, algoritmo, plaintext e ciphertext
- Princípios de Kerckhoffs e segurança computacional

Aula 4: Criptografia Simétrica - Prática Básica

- **Prática Offline:** Implementação de cifras clássicas (César, Vigenère)
 - Uso do OpenSSL para AES (arquivos locais)
 - Comparação visual de diferentes modos (ECB vs CBC)
 - Exercícios com arquivos de texto em VMs
-

DIA 3 - Criptografia Assimétrica

Aula 5: Algoritmos de Criptografia Assimétrica

- **Teoria:** RSA, ECC, Diffie-Hellman
- Matemática básica (conceito de números primos)
- Problema da distribuição de chaves resolvido
- Assinatura digital e não-repúdio

Aula 6: Implementação de RSA

- **Prática Offline:** Geração de chaves RSA com OpenSSL
 - Criptografia e descriptografia de arquivos locais
 - Demonstração de assinatura digital em documentos
 - Exercícios matemáticos simples de RSA manual
-

DIA 4 - Integridade e Funções Hash

Aula 7: Funções Hash e Integridade

- **Teoria:** Propriedades das funções hash (MD5, SHA-1, SHA-256)
- Detecção de modificações e verificação de integridade
- Ataques de colisão (demonstração teórica)
- HMAC e autenticação de mensagens

Aula 8: Quebra de Senhas Offline

- **Prática Offline:** Uso do Hashcat e John the Ripper
 - Criação de wordlists customizadas
 - Ataques contra hashes pré-calculados (arquivo local)
 - Rainbow tables - conceito e demonstração com arquivos pequenos
-

DIA 5 - Mecanismos de Autenticação

Aula 9: Sistemas de Autenticação

- **Teoria:** Fatores de autenticação (algo que você sabe/tem/é)
- Autenticação multifator (2FA/MFA) - tipos e implementações
- Protocolos de autenticação (Kerberos, LDAP, RADIUS)
- Single Sign-On (SSO) e federação de identidades

Aula 10: Simulação de Autenticação

- **Prática Offline:** Análise de tokens JWT (decodificação manual)
 - Simulação de 2FA com aplicativos offline (Google Authenticator)
 - Exercícios de criação de senhas seguras
 - Demonstração de password managers
-

DIA 6 - PKI e Certificados Digitais

Aula 11: Infraestrutura de Chaves Públicas (PKI)

- **Teoria:** Componentes de uma PKI (CA, RA, repositório)
- Ciclo de vida de certificados digitais
- Cadeia de confiança e validação de certificados
- Revogação de certificados (CRL, OCSP)

Aula 12: Criação de PKI Local

- **Prática Offline:** Criação de CA própria com OpenSSL (offline)
 - Geração de certificados para uso interno
 - Importação de certificados no navegador (VMs)
 - Análise da estrutura de certificados existentes
-

DIA 7 - SSL/TLS e Comunicação Segura

Aula 13: Protocolo SSL/TLS

- **Teoria:** Handshake SSL/TLS detalhado
- Cipher suites e negociação de algoritmos
- Evolução do protocolo (SSL 2.0/3.0, TLS 1.0-1.3)
- Perfect Forward Secrecy e proteções modernas

Aula 14: Análise de Certificados SSL

- **Prática Offline:** Configuração de Apache com SSL (VMs internas)
- Análise de certificados com navegador
- Simulação de certificados auto-assinados vs válidos
- Uso do OpenSSL para análise de certificados salvos

DIA 8 - Não-Repúdio e Assinatura Digital

Aula 15: Assinatura Digital e Não-Repúdio

- **Teoria:** Diferença entre assinatura manuscrita e digital
- Processo de geração e verificação de assinaturas
- Timestamping e carimbo de tempo
- Aspectos legais do não-repúdio

Aula 16: Prática de Assinatura Digital

- **Prática Offline:** Assinatura de documentos com LibreOffice
 - Criação e verificação de assinaturas com GnuPG
 - Análise de PDFs assinados digitalmente
 - Simulação de cenários de não-repúdio
-

DIA 9 - Vulnerabilidades Web: Ambiente Controlado

Aula 17: OWASP Top 10 - Fundamentos

- **Teoria:** Principais vulnerabilidades web
- Injeções (SQL, NoSQL, LDAP, OS Command)
- Cross-Site Scripting (XSS) - tipos e impactos
- Broken Authentication e Session Management

Aula 18: Configuração de Aplicações Vulneráveis

- **Prática Offline:** Instalação do DVWA em VMs
 - Configuração de WebGoat (aplicação Java vulnerável)
 - Setup de Mutillidae em ambiente local
 - Primeiro contato com Burp Suite (modo offline)
-

DIA 10 - SQL Injection em Ambiente Controlado

Aula 19: SQL Injection - Teoria Detalhada

- **Teoria:** Anatomia de uma injeção SQL
- Tipos: Union-based, Error-based, Blind, Time-based
- Técnicas de bypass de filtros
- Impactos e cenários reais

Aula 20: SQL Injection - Prática Local

- **Prática Offline:** Exploração manual em DVWA
 - Uso do SQLmap contra aplicações locais
 - Criação de payloads customizados
 - Extração de dados de bancos locais (MySQL/SQLite)
-

DIA 11 - XSS e CSRF em Laboratório

Aula 21: XSS e CSRF - Conceitos Avançados

- **Teoria:** Anatomia de ataques XSS (Stored, Reflected, DOM)
- Cross-Site Request Forgery - mecânica do ataque
- Content Security Policy (CSP) como defesa
- Same-Origin Policy e suas limitações

Aula 22: Exploração de XSS Local

- **Prática Offline:** Exploração de XSS em aplicações locais
 - Criação de payloads JavaScript maliciosos
 - Simulação de roubo de cookies (ambiente controlado)
 - Demonstração de ataques CSRF simples
-

DIA 12 - Análise de Código e Programação Segura

Aula 23: Princípios de Desenvolvimento Seguro

- **Teoria:** Secure Development Lifecycle (SDL)
- Threat modeling básico
- Princípios de validação de entrada
- Defense in depth aplicado ao código

Aula 24: Code Review Prático

- **Prática Offline:** Análise manual de código PHP/Python vulnerável
 - Uso de ferramentas estáticas (SonarQube Community offline)
 - Exercícios de correção de vulnerabilidades
 - Implementação de validações seguras
-

DIA 13 - Criptoanálise e Quebra de Cifras

Aula 25: Criptoanálise - Fundamentos

- **Teoria:** Tipos de ataques criptográficos
- Análise de frequência e padrões
- Ataques de força bruta - complexidade computacional
- Pontos fracos em implementações

Aula 26: Quebra de Cifras Clássicas

- **Prática Offline:** Quebra manual de cifras César e Vigenère
 - Análise de frequência em textos criptografados
 - Uso de ferramentas simples (CyberChef offline)
 - Exercícios com cifras de substituição
-

DIA 14 - Forense Digital Básica

Aula 27: Introdução à Forense Digital

- **Teoria:** Metodologia forense e cadeia de custódia
- Tipos de evidência digital
- Ferramentas forenses e processo de investigação
- Aspectos legais e éticos

Aula 28: Análise Forense Prática

- **Prática Offline:** Uso do Autopsy em imagens de disco
 - Recuperação de arquivos deletados
 - Análise de metadados com ExifTool
 - Investigação de logs do sistema (arquivos locais)
-

DIA 15 - Esteganografia e Ocultação de Dados

Aula 29: Esteganografia - Conceitos

- **Teoria:** História da esteganografia
- Diferença entre criptografia e esteganografia
- Técnicas modernas de ocultação de dados
- Detecção de conteúdo oculto (estegoanálise)

Aula 30: Prática de Esteganografia

- **Prática Offline:** Ocultação de dados em imagens (steghide)
 - Análise de imagens suspeitas
 - Uso do Stegsolve para detectar conteúdo oculto
 - Exercícios com áudio e vídeo (arquivos locais)
-

DIA 16 - Malware e Análise Estática

Aula 31: Classificação e Comportamento de Malware

- **Teoria:** Tipos de malware (vírus, worms, trojans, ransomware)
- Técnicas de infecção e propagação
- Métodos de evasão de antivírus
- Análise comportamental vs estática

Aula 32: Análise Estática de Malware

- **Prática Offline:** Análise de samples inofensivos
 - Uso do VirusTotal offline (análise de hashes)
 - Strings, hexdump e análise básica de PE
 - Sandbox caseiro com VMs isoladas
-

DIA 17 - Segurança de Sistemas Operacionais

Aula 33: Hardening de Sistemas

- **Teoria:** Princípios de hardening Linux/Windows
- Configurações de segurança essenciais
- Gerenciamento de usuários e permissões
- Auditoria e monitoramento de sistemas

Aula 34: Configuração Segura Prática

- **Prática Offline:** Hardening de VMs Linux/Windows
 - Configuração de firewalls locais (iptables/Windows Firewall)
 - Auditoria de configurações com scripts
 - Implementação de políticas de senha
-

DIA 18 - Engenharia Social e Aspectos Humanos

Aula 35: Psicologia da Segurança

- **Teoria:** Fatores humanos na segurança
- Princípios psicológicos explorados
- Tipos de ataques de engenharia social
- Conscientização e treinamento

Aula 36: Simulação de Engenharia Social

- **Prática Offline:** Role-playing de cenários
 - Criação de emails de phishing (análise, não envio)
 - Análise de sites de phishing salvos localmente
 - Exercícios de conscientização em equipe
-

DIA 19 - Backup e Recuperação de Dados

Aula 37: Estratégias de Backup e Continuidade

- **Teoria:** Tipos de backup (completo, incremental, diferencial)
- RPO e RTO - métricas de recuperação
- Planos de continuidade de negócios
- Proteção contra ransomware

Aula 38: Implementação de Backup

- **Prática Offline:** Configuração de backups automáticos
 - Teste de restauração de dados
 - Simulação de recuperação após "ataque"
 - Criação de scripts de backup
-

DIA 20 - Projeto Integrador e Apresentações

Aula 39: Desenvolvimento do Projeto Final

- **Prática:** Cada equipe desenvolve um projeto prático:
 - Auditoria de segurança de aplicação local
 - Implementação de solução criptográfica
 - Análise forense de cenário simulado
 - Hardening completo de sistema

Aula 40: Apresentações e Discussões






- **Apresentações:** Cada equipe apresenta seu projeto
 - Discussão de casos reais e lições aprendidas
 - Avaliação peer-to-peer entre equipes
 - Planejamento de estudos futuros
-

Estratégias para Equipes Compartilhadas

Organização das Equipes

- **2-3 alunos por notebook** (quem tem + quem não tem)
- **Rotação de funções:** operador, observador, documentador
- **Divisão de tarefas:** cada membro fica responsável por uma parte

Atividades Offline Viáveis

-  **VMs isoladas** (não precisam de internet)
-  **Aplicações vulneráveis locais** (DVWA, WebGoat)
-  **Ferramentas criptográficas** (OpenSSL, GnuPG)
-  **Análise de arquivos** (malware inofensivo, images forenses)
-  **Simulações** (role-playing, cenários)

Material Pré-preparado

- **USBs com softwares** para instalação offline
- **VMs pré-configuradas** para distribuir
- **Datasets** de hashes, imagens forenses, samples
- **Documentos** para exercícios práticos

Metodologia de Avaliação Adaptada

- **40%** - Relatórios de equipe (todos assinam)
- **25%** - Prova individual teórica
- **20%** - Projeto final em equipe
- **15%** - Participação e peer review

Recursos Necessários

Por Equipe (2-3 alunos)

- 1 notebook com 4GB+ RAM
- VirtualBox instalado
- 50GB espaço livre em disco
- Pendrives para distribuição de material

Preparação do Professor

- VMs pré-configuradas (Kali + aplicações vulneráveis)
- Datasets offline (wordlists, hashes, samples)
- Material impresso para backup
- Roteiros detalhados por equipe