Plano de Aulas - Segurança da Informação

40 aulas de 50 minutos | 20 dias letivos | 2 aulas por dia

DIA 1 - Introdução e Reconhecimento

Aula 1: Introdução à Segurança da Informação

- **Prática**: Instalação e configuração do ambiente de laboratório (Kali Linux, VirtualBox)
- Configuração de máquinas virtuais vulneráveis (Metasploitable, DVWA)
- Apresentação das ferramentas que serão utilizadas durante o curso

Aula 2: Reconhecimento e Coleta de Informações

- **Prática**: Técnicas de OSINT (Open Source Intelligence)
- Uso de ferramentas: Maltego, theHarvester, Shodan
- Análise de metadados em documentos e imagens

DIA 2 - Scanning e Enumeração

Aula 3: Network Scanning

- **Prática**: Uso do Nmap para descoberta de hosts e serviços
- Técnicas de port scanning e identificação de sistemas operacionais
- Interpretação de resultados e evasão de detecção

Aula 4: Enumeração de Serviços

- **Prática**: Enumeração de serviços comuns (HTTP, SSH, FTP, SMB)
- Uso de ferramentas: enum4linux, nikto, dirb/gobuster
- Identificação de vulnerabilidades através da enumeração

DIA 3 - Vulnerabilidades Web I

Aula 5: SQL Injection - Conceitos

- **Prática**: Identificação e exploração manual de SQL Injection
- Teste em aplicações vulneráveis (DVWA, SQLi-labs)
- Diferentes tipos de SQL Injection (Error-based, Blind, Time-based)

Aula 6: SQL Injection - Ferramentas

- **Prática**: Uso do SQLmap para automatizar ataques
- Extração de dados, bypass de autenticação
- Técnicas de mitigação e prevenção

DIA 4 - Vulnerabilidades Web II

Aula 7: Cross-Site Scripting (XSS)

- **Prática**: Identificação e exploração de XSS (Stored, Reflected, DOM)
- Criação de payloads maliciosos
- Uso do BeEF Framework para exploração

Aula 8: Cross-Site Request Forgery (CSRF)

- **Prática**: Demonstração de ataques CSRF
- Criação de exploits e bypass de tokens
- Implementação de proteções anti-CSRF

DIA 5 - Vulnerabilidades Web III

Aula 9: Local File Inclusion (LFI) e Remote File Inclusion (RFI)

- **Prática**: Exploração de inclusões de arquivos
- Log poisoning e RCE através de LFI
- Directory traversal e bypass de filtros

Aula 10: Command Injection

- **Prática**: Identificação e exploração de command injection
- Bypass de filtros e obtenção de shell reverso
- Análise de código vulnerável

DIA 6 - Engenharia Social e Phishing

Aula 11: Engenharia Social

- **Prática**: Criação de campanhas de phishing com Gophish
- Técnicas de social engineering e pretexting
- Análise de vetores de ataque psicológicos

Aula 12: Criação de Payloads Maliciosos

- **Prática**: Uso do SET (Social Engineering Toolkit)
- Criação de documentos maliciosos com macros
- Bypass de antivírus com encoders

DIA 7 - Wireless Security

Aula 13: Segurança em Redes Wi-Fi I

- **Prática**: Auditoria de redes wireless com Aircrack-ng
- Captura de handshakes WPA/WPA2
- Ataques de desautenticação

Aula 14: Segurança em Redes Wi-Fi II

- **Prática**: Evil Twin e ataques de AP falso
- Captura de credenciais com Captive Portal
- WPS attacks com Reaver

DIA 8 - Criptografia Prática I

Aula 15: Criptografia Simétrica

- **Prática**: Implementação de algoritmos de criptografia (AES, DES)
- Modos de operação (CBC, ECB, CTR)
- Quebra de cifras fracas com ferramentas

Aula 16: Criptografia Assimétrica

- **Prática**: Geração de chaves RSA/ECC
- Assinatura digital e verificação
- Ataques contra implementações fracas de RSA

DIA 9 - Criptografia Prática II

Aula 17: Hash Functions e Password Cracking

- **Prática**: Uso do Hashcat e John the Ripper
- Rainbow tables e ataques de dicionário
- Análise de diferentes algoritmos de hash

Aula 18: Certificados Digitais e PKI

- **Prática**: Criação de CA própria com OpenSSL
- Geração e validação de certificados
- Análise de certificados SSL/TLS com ferramentas

DIA 10 - SSL/TLS e Comunicação Segura

Aula 19: Análise de Protocolos SSL/TLS

- **Prática**: Uso do SSLyze e testssl.sh
- Identificação de vulnerabilidades (Heartbleed, POODLE, BEAST)
- Configuração segura de servidores web

Aula 20: Man-in-the-Middle Attacks

- **Prática**: Implementação de ataques MITM com Ettercap
- SSL stripping e bypass de HTTPS
- Uso do Burp Suite como proxy interceptador

DIA 11 - Segurança em Redes I

Aula 21: Análise de Tráfego de Rede

- **Prática**: Uso do Wireshark para análise de pacotes
- Identificação de protocolos inseguros
- Detecção de anomalias e ataques em captures

Aula 22: ARP Spoofing e Network Attacks

- **Prática**: Ataques ARP spoofing com Ettercap/Bettercap
- DHCP spoofing e DNS spoofing
- Mitigações através de configurações de switch

DIA 12 - Segurança em Redes II

Aula 23: Firewall e Evasão

- **Prática**: Configuração de iptables/pfSense
- Técnicas de evasão de firewall com Nmap
- Análise de logs e detecção de tentativas de bypass

Aula 24: VPN e Túneis Seguros

- **Prática**: Configuração de OpenVPN e WireGuard
- Análise de segurança de implementações VPN
- Detecção de vazamentos de DNS/IP

DIA 13 - Exploração de Vulnerabilidades I

Aula 25: Buffer Overflow - Conceitos

- **Prática**: Exploração básica de buffer overflow
- Análise de binários com GDB/Immunity Debugger
- Identificação de vulnerabilidades em código C

Aula 26: Buffer Overflow - Exploração

- **Prática**: Criação de shellcode e exploits
- Bypass de proteções (ASLR, DEP, Stack Canaries)
- Uso do Metasploit para exploração automatizada

DIA 14 - Exploração de Vulnerabilidades II

Aula 27: Metasploit Framework

- **Prática**: Uso avançado do Metasploit
- Criação de payloads customizados
- Post-exploitation e persistence

Aula 28: Privilege Escalation - Linux

- **Prática**: Técnicas de escalação de privilégios no Linux
- Exploração de SUIDfiles, kernel exploits
- Uso de ferramentas automatizadas (LinEnum, linux-exploit-suggester)

DIA 15 - Exploração de Vulnerabilidades III

Aula 29: Privilege Escalation - Windows

- **Prática**: Escalação de privilégios no Windows
- Exploração de serviços mal configurados
- PowerShell para post-exploitation

Aula 30: Active Directory Attacks

- **Prática**: Ataques contra Active Directory
- Kerberoasting e ASREPRoasting
- Golden Ticket e Silver Ticket attacks

DIA 16 - Segurança em Programação I

Aula 31: Code Review e Static Analysis

- **Prática**: Análise de código com ferramentas (SonarQube, Bandit)
- Identificação de vulnerabilidades em código fonte
- Revisão manual de código vulnerable

Aula 32: Dynamic Analysis e Fuzzing

- **Prática**: Fuzzing de aplicações com AFL/libFuzzer
- Análise dinâmica com Valgrind
- Descoberta de crashes e vulnerabilidades

DIA 17 - Segurança em Programação II

Aula 33: Secure Coding Practices - Web

- **Prática**: Implementação de validações seguras
- Prevenção de OWASP Top 10
- Uso de frameworks seguros e bibliotecas

Aula 34: API Security

- **Prática**: Teste de segurança em APIs REST
- Uso do Postman/Burp Suite para testes
- Implementação de autenticação e autorização seguras

DIA 18 - Mobile Security

Aula 35: Android Security

- **Prática**: Análise de aplicativos Android com jadx/apktool
- Bypass de certificados SSL em apps
- Hooking com Frida para análise dinâmica

Aula 36: iOS Security Basics

- **Prática**: Análise básica de aplicativos iOS
- Jailbreak e ferramentas de análise
- Bypass de proteções de aplicativos

DIA 19 - Forense Digital e Incident Response

Aula 37: Digital Forensics

- **Prática**: Análise forense com Autopsy/Sleuth Kit
- Recuperação de dados apagados
- Análise de logs e evidências digitais

Aula 38: Malware Analysis

- **Prática**: Análise básica de malware em ambiente controlado
- Uso de ferramentas como VirusTotal, Cuckoo Sandbox
- Identificação de IoCs (Indicators of Compromise)

DIA 20 - Projeto Final e Defesa

Aula 39: Penetration Testing Completo

- **Prática**: Execução de pentest completo em ambiente controlado
- Documentação de vulnerabilidades encontradas
- Criação de relatório técnico

Aula 40: Apresentação de Projetos e Defesa

- **Prática**: Apresentação dos projetos finais
- Simulação de resposta a incidentes
- Discussão de casos reais e lições aprendidas

Recursos Necessários para o Laboratório

Software

- Kali Linux (máquina virtual)
- Máquinas vulneráveis: Metasploitable, DVWA, VulnHub VMs
- Burp Suite Professional (ou Community)
- Wireshark
- VirtualBox/VMware

Hardware

- Computadores com pelo menos 8GB RAM
- Adaptadores Wi-Fi com suporte a modo monitor
- Roteadores para testes de segurança wireless

Ambiente

- Rede isolada para testes
- Servidor para hospedar aplicações vulneráveis
- Projector para demonstrações