4·Linux Open Software Specialists™

CERTIFICADO

Certificate

Orleans Samai Avelar De Oliveira

Concluiu seus estudos no curso **507 - Pen Test: Técnicas de Intrusão em Redes Corporativas - AC** ministrado pela empresa 4Linux e cumprindo a carga horária de 40 horas.

3 de maio de 2025

RODOLFO GOBBI

DIRETOR GERAL

Para validar a autenticidade deste certificado acesse aia.4linux.com.br/admin/tool/certificate/ e digite o código: 8135015420OA

Ementa de Curso

Orleans Samai Avelar De Oliveira
Concluiu seus estudos no curso **507 - Pen Test: Técnicas de Intrusão em Redes Corporativas - AC** ministrado pela empresa 4Linux e cumprindo a carga horária de 40 horas.
3 de maio de 2025

A autenticidade deste documento pode ser verificado em aia.4linux.com.br/admin/tool/certificate/ digitando o código 8135015420OA

Aula 1: Introdução ao Pentest e Metodologias

- Micro Aula 1.1: O que é um Pentest?
- Micro Aula 1.2: Tipos de Pentest
- Micro Aula 1.3: Metodologias de Pentest
- Micro Aula 1.4: Fases de um Pentest
- Micro Aula 1.5: Ferramentas e Recursos Iniciais

Aula 2: Coleta de Informações e Reconhecimento

- Micro Aula 2.1: Footprinting e Fingerprinting - Conceitos Gerais
- Micro Aula 2.2: Busca de Informações Públicas - Footprinting Passivo
- Micro Aula 2.3: Frameworks e Metodologias - OSINT e SpiderFoot
- Micro Aula 2.4: Identificação de Alvos e Tecnologias - Shodan e Censys
- Micro Aula 2.5: Enumeração de Subdomínios e Serviços - Footprinting Ativo
- Micro Aula 2.6 Ferramenta de automação em reconaissance - AutoRecon

Aula 3: Escaneamento e Enumeração

- Micro Aula 3.1: Network Scanning usando NMAP
- Micro Aula 3.2: Descoberta de Hosts
- Micro Aula 3.3: Scan de Vulnerabilidades
- Micro Aula 3.4: Varredura Nmap com parâmetros de tempo
- Micro Aula 3.5: Varredura de Ping
- Micro Aula 3.6: Password Cracking
- Micro Aula 3.7: Nmap: Output Format Scan
- Micro Aula 3.8: Active Directory Enumeration: RPCClient

- Micro Aula 3.9: Assessment de Vulnerabilidades em Serviços de Rede (Nessus, OpenVas)

Aula 4: Spoofing e Sniffing

- Micro Aula 4.1: Ataques de Spoofing/Sniffing: ARP Poisoning/MITM
- Micro Aula 4.2: Ataques de E-mail Spoofing
- Micro Aula 4.3: MitM (Man-in-the-Middle) e Ferramentas(Responder)
- Micro Aula 4.4: Ataques de SMS Spoofing

Aula 5: Técnicas envolvendo Forca Bruta

- Micro Aula 5.1: Criando Dicionários
- Micro Aula 5.2: Password Guessing - JTR, Hydra, Meduza
- Micro Aula 5.3: Password Cracking - Crackmapexec
- Micro Aula 5.4: Password Spraying
- Micro Aula 5.5: Brute force em aplicacoes WEB

Aula 6: Exploração de Vulnerabilidades Web

- Micro Aula 6.1: Owasp Top 10
- Micro Aula 6.2: SQL Injection na cláusula WHERE permitindo a recuperação de dados ocultos
- Micro Aula 6.3: Vulnerabilidade CSRF sem defesas
- Micro Aula 6.4: Vulnerabilidade CORS com reflexão básica de origem
- Micro Aula 6.5: Directory traversal
- Micro Aula 6.6: HTTP Basic Authentication Brute Force
- Micro Aula 6.7: Execute remote code (RCE)
- Micro Aula 6.8: Configuração do Lab de Pentest Web usando Docker

Aula 7: Privilege Scalation Linux e Windows

- Micro Aula 7.1: Escalada de Privilégios
- Micro Aula 7.2: Linux Privilege Escalation: LD_Preload
- Micro Aula 7.3: Linux Privilege Escalation: Wget
- Micro Aula 7.4: Windows Privilege Escalation: Scheduled Task/Job (T1573.005)
- Micro Aula 7.5: Automatizando a escalação de Privilegios Linux e Windows

Aula 8: Pós-Exploração e Movimento Lateral

- Micro Aula 8.1: Pós-Exploração com WMIC e Comandos de Sistema
- Micro Aula 8.2: Hacking com o Empire - Agente de Pós-Exploração PowerShell
- Micro Aula 8.3: Uso do Módulo Mimikatz no PowerShell Empire
- Micro Aula 8.4: Pós-Exploração com LaZagne
- Micro Aula 8.5: Pós-Exploração com SilentTrinity - Recuperação de Senhas e Controle de Comando e Controle
- Micro Aula 8.5: Movimentação Lateral e Ataque ‘Pass the Hash’ - Explorando Acessos com Hashes

Aula 9: Engenharia Social e Testes de Phishing

- Micro Aula 9.1: Psicologia por Trás da Engenharia Social
- Micro Aula 9.2: Ferramentas de Engenharia Social (SET)
- Micro Aula 9.3: Gophish: Configurando uma campanha de phishing

- Micro Aula 9.4: Gophish: Realizando uma campanha de phishing
- Micro Aula 9.5: USB Rubber Ducky - Conceitos
- Micro Aula 9.6: USB Rubber Ducky - Trabalhando com Scripts
- Micro Aula 9.7: USB Rubber Ducky - Obtendo Shell reverso

Aula 10: Análise de Malware e Exploração de Clientes

- Micro Aula 10.1: Malware Conceitos e Exemplos (Linux/Windows) - Parte I
- Micro Aula 10.2: Malware Conceitos e Exemplos (Linux/Windows) - Parte II
- Micro Aula 10.3: Process Herpaderping (Mitre:T1055)
- Micro Aula 10.4: HTML Smuggling (T1027.006)
- Micro Aula 10.5: Escrevendo Ransomnwares
- Micro Aula 10.6: Criando Payloads indetectáveis com Veil-Evasion

Aula 11: Exploração de Vulnerabilidades Wireless

- Wireless Penetration Testing: SSID Discovery
- Wireless Penetration Testing: PMKID Attack
- Wireless Penetration Testing: Airgeddon
- Wireless Penetration Testing: Airgeddon - Evil Twin
- Wireless Penetration Testing: Fluxion
- Wireless Penetration Testing: Bettercap
- Wireless Penetration Testing: Wifite

Aula 12: Avaliação de Segurança em Aplicações Móveis

- Micro Aula 12.1: Conceitos sobre Pentest Mobile - Owasp TOP 10 mobile
- Micro Aula 12.2: Passo-a-passo de como construir um laboratorio Pentest - Android
- Micro Aula 12.3: Explorando vulnerabilidades comuns no Android: registro inseguro, credenciais codificadas, armazenamento de dados inseguro e problemas de validação de entrada.
- Micro Aula 12.4: Despejando a memória do aplicativo Android com o Fridump

Aula 13: Técnicas Avançadas de Exploração

- Micro Aula 13.1: Enumeração Avançada em AD com BloodHound
- Micro Aula 13.2: Metasploit - **Noções básicas de Metasploit Framework**
- Micro Aula 13.3: Metasploit - **Comandos básicos do Metasploit Framework**
- Micro Aula 13.4: Metasploit - **A penetration test walkthrough**
- Micro Aula 13.5: Metasploit - **Tarefas de pós-exploração com Metasploit & Meterpreter**
- Micro Aula 13.6: Metasploit - **Criando payloads personalizadas com msfvenom**
- Micro Aula 13.7: BufferOverflow - **O que é o Buffer Overflow?**
- Micro Aula 13.8: BufferOverflow - **Ataque de Overflow do Buffer do Windows**
- Micro Aula 13.9: BufferOverflow - **Descoberta Offset e Controle EIP**
- Micro Aula 13.10: BufferOverflow - **Encontrando Caracteres Ruins**
- MicroAula 13.11: BufferOverflow - Shell Reverse Shellcode Generation
- Micro Aula 13.12: Propostas e Relatórios