4·Linux Open Software Specialists™

CERTIFICADO

Certificate

Gilberto Aprigio

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.

21 de novembro de 2023



RODOLFO GOBBI

DIRETOR GERAL

Para validar a autenticidade deste certificado acesse aia.4linux.com.br/admin/tool/certificate/ e digite o código: 1462983641GA

Ementa de Curso

Gilberto Aprigio

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.
21 de novembro de 2023

A autenticidade deste documento pode ser verificado em aia.4linux.com.br/admin/tool/certificate/ digitando o código 1462983641GA

Conteúdo Programático

Compreender o que é PenTest

- Choque de realidade
- Hacker X Ethical Hacker
- Tipos de pentesters
- Hacking Phases
- Tipos de Ataques
- Como se preparar para as Certificações CEH e Exin

Reconnaissance / Footprinting

- Conceitos Gerais
- Web Footprinting
- Google Hacking
- Contra-Medidas

Varreduras

- Overview Scanning
- Tipos de Scanning (full, half, xmas, fin, null, udp)
- Técnicas de evasão de IDS
- Banner Grabbing
- Scan de Vulnerabilidades
- Enumeração

System Hacking

- Network Scanning
- Enumeration
- Exploiting (1st Method: file Upload)
- Exploiting (2nd Method: LFI & CSRF)
- Exploiting (3rd Method: SQL Injection)
- Exploiting (4th Method: RFI)
- Exploiting (5th Method: Authenticated File Upload)

Malware Threads

- Conceitos sobre Malware
- Ignorar AV com modelos Metaploit e binários personalizados
- Veil-Evasion – Gerando payloads indetectáveis

Sniffing

- Conceitos Gerais de Sniffing
- MAC Attacks
- DHCP Attacks
- ARP Poisoning
- Spoofing Attacks
- DNS Poisoning
- Sniffing Tools/Contramedidas

Engenharia Social

- Conceitos Gerais
- Trabalhando com Java Applet e browser exploits
- Conhecendo Tabnabbing
- Conhecendo Web Jacking
- Conhecendo Credential Harvesting

DoS/DDoS

- DoS Attack Penetration Testing (Part 1)
- DoS Attack Penetration Testing (Part 2)
- Botnets
- Ferramentas DoS/DDoS
- Contramedidas

Brute Force

- Criando Dicionários
- JTR, Hydra, Meduza
- Brute force em Web Servers
- Brute force em cenários reais

Web Server Hacking Concepts

- Injeção e Quebra de Autenticação
- Exposição de Dados Sensíveis e Entidades Externas de XML (XXE)
- Quebra de Controle de Acessos e Configurações de Segurança Incorretas

- Cross-Site Scripting (XSS) e Desserialização Insegura
- Utilização de Componentes Vulneráveis e Registo e Monitorização Insuficiente
- Configurando Web Application Pentest Lab usando Docker

Web Server Hacking Attacks

- Exploração Manual SQL Injection Step by Step
- XSS Exploitation
- XXE (XML external entity) injection
- Remote & Local File Include (RFI & LFI)
- Web Challenge

Metasploit Framework

- Metasploit – Conceitos Gerais
- Network Scan, Exploiting Port 21 FTP (Hydra), VSFTPD 2.3.4, Port 22 SSH, Bruteforce Port 22 SSH (RSA Method)
- Exploiting port 23 TELNET (Credential Capture), TELNET (Bruteforce), Port 25 SMTP User Enumeration, Port 80 (PHP), Port 139 & 445 (Samba)
- Exploiting Port 8080 (Java), Port 5432 (PostgreSQL), Port 6667 (UnrealIRCD), Port 36255, Remote Login Exploitation
- Remote Shell Exploitation, Exploiting Port 8787, Bindshell, Exploiting Port 5900 (VNC)
- Access Port 2121 (ProFTPD), Exploiting Port 8180 (Apache Tomcat), Privilege Escalation via NFS, Exploiting Port 3306 (MySQL)
- Armitage