# Segurança Ofensiva em Redes de Computadores

## OBJETIVO

Este curso tem como objetivo, apresentar os tipos de ameaças que existem na infraestrutura de serviços de uma empresa, quais são, e como funcionam a arquitetura dos ataques realizados por pessoas mal intencionadas. Muitas das vezes os danos causados por estas pessoas podem ser irreverssíveis, e em muitas das vezes levar uma empresa a falência. Pois a coisa mas valiosa que uma empresa possúi são as informações.

Visando proteger da melhor forma estas informações que a empresa possúi, este curso abordará de forma totalmente prática as técnicas, métodos, estratégias e ferramentas utilizadas pelos crackers para obter acesso indevido as informações da empresa; possibilitando assim que os profissionais de TI da empresa ajam de forma proativa e encontre as falhas dentro da infraestrutura, antes que um cracker o faça primeiro.

## PRÉ-REQUISITOS

Conhecimentos sobre redes de computadores e sobre o sistema operacional GNU/Linux

## METODOLOGIA

As aulas são compostas por módulos, onde será passado para os alunos todo o conhecimento teórico para a realização de exercícios práticos. Cada aluno terá um computador para realizar os exercícios, que será realizado em uma infraestrutura virtualizada.
O curso é totalmente presencial e disponibiliza o material virtual ou impresso.

## VANTAGENS TREINAR

- Grade curricular baseada na vivencia em programação;
- Aulas práticas;
- Instrutores com anos de experiência em docência.

**Carga Horária:** 40 horas (5 Dias / 10 Noites)

# CONTEÚDO PROGRAMÁTICO

Aula 1:
- Noções básicas de segurança
- Tipos de malwares
- Arquitetura de ataques

Aula 2:
- Busca de hosts ativos
- Enumeração de serviços dos hosts

Aula 3
- Descoberta de versão do sistema operacional e serviços
- Criação de documentação base para início dos testes

Aula 4:
- Busca por vulnerabilidades conhecidas
- Teste de penetração nos serviços internos da rede

Aula 5
- Validação de vulnerabilidades
- Escalada de privilégios

Aula 6:
- Busca de vulnerabilidades pela internet
- Busca de arquivos e informações sensiveis na internet

Aula 7
- Testes de vulnerabilidades de serviços publicados na internet
- Validação de vulnerabilidades

Aula 8:
- Boas práticas de segurança
- Gerência de riscos

Aula 9
- Produção de relatórios
- Plano contingência e continuidade de negócios

Aula 10:
- Escaneamento de vulnerabilidades em massa
- Validação de vulnerabilidades
- Exibição de gráficos de vulnerabilidades