Sistemas Defensivos

Revisto em Junho, 2023

Duração do curso

3 dias.

Programa do Curso

➢ Dia 1: Firewalls e Conceitos Básicos

• Sessão 1: Introdução às Firewalls
o Conceito de firewall e sua importância na segurança de rede.
o Tipos de firewalls: stateful, stateless, de próxima geração.
o Papel da firewall na detecção e prevenção de intrusões.

• Sessão 2: Configuração de Firewall com pfSense
o Introdução ao pfSense como uma solução de firewall open-source.
o Instalação e configuração inicial do pfSense.
o Configuração de interfaces de rede.
o Criação de regras de firewall básicas.~

• Sessão 3: Criação de Redes para Teste da Firewall
o Projeto de redes de teste para simulação de cenários de firewall.
o Configuração de redes virtuais para testes.
o Implementação de regras de firewall em cenários de teste.

➢ **Dia 2: Sistemas de Detecção de Intrusão (IDS)**

• Sessão 4: Introdução aos IDS

o Conceito de IDS e sua importância na detecção de intrusões.

o Tipos de IDS: baseados em assinatura, baseados em comportamento.

o Detecção de anomalias e padrões.

• Sessão 5: Configuração de IDS

o Seleção de um IDS apropriado para as necessidades da organização.

o Instalação e configuração de um IDS open-source (por exemplo, Snort

ou Suricata).

o Configuração de regras de detecção de intrusões.

o Análise de logs e alertas gerados pelo IDS.

➢ **Dia 3: Sistemas de Prevenção de Intrusão (IPS)**

• Sessão 6: Introdução aos IPS

o Conceito de IPS e sua importância na prevenção de intrusões.

o Diferenças entre IDS e IPS.

o Técnicas de prevenção de intrusões.

• Sessão 7: Configuração de IPS

o Seleção de um IPS apropriado para as necessidades da organização.

o Instalação e configuração de um IPS open-source (por exemplo, Snort

como IPS).

o Configuração de regras de prevenção de intrusões.

o Testes práticos de prevenção de intrusões em cenários de teste.

• Sessão 8: Exercícios Práticos e Conclusão

o Exercícios práticos que envolvem a configuração de regras de firewall, detecção de intrusões e prevenção de intrusões em cenários de teste.

o Discussão de melhores práticas em detecção e prevenção de intrusões.

o Encerramento do curso com uma revisão das principais conclusões e recomendações