

Segurança cibernética

Revisão para a Prova de Segurança Cibernética



Revisar os principais conceitos de segurança cibernética.



Preparar os alunos para a prova com exemplos práticos.



Responder dúvidas e reforçar o entendimento.



Hardening em Segurança Cibernética

- **Definição:**

- Hardening é o processo de fortalecer a segurança de um sistema, reduzindo suas vulnerabilidades.


- **Práticas Comuns:**

- Desativação de serviços e portas não utilizados.
 - Implementação de políticas de senhas fortes.
 - Instalação de software antivírus.
 - Treinamento de usuários.
-



OWASP Top 10 e Vulnerabilidades

- **O que é OWASP Top 10:**
 - Uma lista das 10 vulnerabilidades mais críticas em aplicações web.
 - **Principais Vulnerabilidades:**
 - Injection.
 - Cross-Site Scripting (XSS).
 - Broken Authentication.
 - **Mitigações:**
 - Uso de prepared statements.
 - Validação de entrada do usuário.
-



Plano de Recuperação de Desastres (DRP)

- **Definição:**
 - DRP é um conjunto de políticas e procedimentos para recuperar sistemas após um desastre.
 - **Componentes Essenciais:**
 - Testes periódicos.
 - Backup de dados.
 - Comunicação efetiva durante a recuperação.
-



Ataques de Phishing

- **Definição:**
 - Phishing é uma tentativa de obter informações sensíveis enviando e-mails fraudulentos.
 - **Características:**
 - E-mails que parecem legítimos.
 - Links para sites falsos.
 - **Prevenção:**
 - Verificação de remetentes.
 - Educação dos usuários.
-



Varredura de Vulnerabilidades

- **Definição:**
 - Processo automatizado para identificar vulnerabilidades conhecidas.
 - **Ferramentas Comuns:**
 - Nessus.
 - OpenVAS.
 - **Exemplos Práticos:**
 - Demonstração de uma varredura de vulnerabilidade.
-



Gerenciamento de Patches e HotFixes

- **Definições:**
 - Patches: Atualizações que corrigem vulnerabilidades.
 - HotFixes: Correções emergenciais.
 - **Processo:**
 - Aplicar atualizações de segurança regularmente.
 - Monitorar e gerenciar patches.
-



Análise de Riscos e Avaliação de Custos

- **Definição:**
 - Processo de identificar, avaliar e priorizar riscos.
 - **Componentes:**
 - Identificação de ativos.
 - Avaliação de ameaças e vulnerabilidades.
 - Determinação do equilíbrio entre custo e benefício.
-



Segurança de Protocolos

- **Vulnerabilidades Comuns:**
 - Falta de criptografia no TCP/IP.
 - **Boas Práticas:**
 - Uso de HTTPS e SSH.
 - Implementação de SSL/TLS.
-



Sessão de Perguntas e Respostas

- **Discussão Aberta:**
 - Responder perguntas dos alunos.
 - Revisar pontos específicos conforme necessário.
-