

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.
-

Hardening em Segurança Cibernética

- **Práticas Comuns:**
- **Desativação de serviços e portas não utilizados:**
 - Desative serviços e portas que não são necessários para minimizar os pontos de ataque.
 - **Exemplo:** Desativar o serviço de telnet se não estiver em uso.
- **Implementação de políticas de senhas fortes:**
 - Implemente senhas complexas e altere-as regularmente.
 - **Exemplo:** Exigir senhas com pelo menos 12 caracteres, incluindo números, letras maiúsculas e minúsculas, e símbolos.
- **Instalação de software antivírus:**
 - Use software antivírus atualizado para detectar e remover malwares.
 - **Exemplo:** Instalar e atualizar regularmente o Windows Defender.
- **Treinamento de usuários:**
 - Eduque os usuários sobre práticas de segurança.
 - **Exemplo:** Realizar treinamentos periódicos sobre como identificar e-mails de phishing.




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.
-

OWASP Top 10 e Vulnerabilidades

- **Principais Vulnerabilidades:**
- **Injection:**
 - Ataques que envolvem a inserção de código malicioso em uma aplicação.
 - **Exemplo:** SQL Injection, onde o atacante pode executar comandos SQL maliciosos.
- **Cross-Site Scripting (XSS):**
 - Inserção de scripts maliciosos em páginas web.
 - **Exemplo:** Inserir JavaScript malicioso em um campo de entrada que é exibido aos outros usuários.
- **Broken Authentication:**
 - Vulnerabilidades que permitem a invasão de contas.
 - **Exemplo:** Sessões que não expiram corretamente.
 - **Mitigações:**
- **Uso de prepared statements:**
 - Previne SQL Injection usando consultas parametrizadas.
- **Validação de entrada do usuário:**
 - Verifique e sanitize todas as entradas de 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.
-

Plano de Recuperação de Desastres (DRP)

- **Componentes Essenciais:**
- **Testes periódicos:**
 - Realizar testes regulares para garantir que o plano funcione.
 - **Exemplo:** Simular um desastre e seguir o plano de recuperação.
- **Backup de dados:**
 - Manter backups atualizados e armazenados em locais seguros.
 - **Exemplo:** Realizar backups diários e armazená-los em um local remoto.
- **Comunicação efetiva:**
 - Ter um plano de comunicação claro para informar todos os envolvidos.
 - **Exemplo:** Criar uma lista de contatos de emergência.



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.
-

Ataques de Phishing

- **Características:**
- **E-mails que parecem legítimos:**
 - Mensagens que imitam comunicações oficiais.
 - **Exemplo:** E-mails que parecem ser do banco solicitando atualização de senha.
- **Links para sites falsos:**
 - Redirecionam para sites que coletam informações pessoais.
 - **Exemplo:** Site falso que imita a página de login do banco.
 - **Prevenção:**
- **Verificação de remetentes:**
 - Confirme a legitimidade do remetente antes de clicar em links.
- **Educação dos usuários:**
 - Treine os usuários para reconhecer sinais de phishing.
 - **Exemplo:** Não clicar em links suspeitos e verificar URLs.



Varredura de Vulnerabilidades

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

Varredura de Vulnerabilidades

- **Ferramentas Comuns:**
- **Nessus:**
 - Ferramenta de varredura de vulnerabilidades que identifica falhas de segurança.
- **OpenVAS:**
 - Outra ferramenta popular para varredura de vulnerabilidades.
- **Exemplos Práticos:**
- **Demonstração de uma varredura de vulnerabilidade:**
 - Mostrar como configurar e executar uma varredura com Nessus.
 - Analisar os resultados e discutir as correções recomendadas.



Gerenciamento de Patches e HotFixes

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

Gerenciamento de Patches e HotFixes

- **Processo:**
- **Aplicar atualizações de segurança regularmente:**
 - Mantenha todos os sistemas atualizados.
- **Monitorar e gerenciar patches:**
 - Use ferramentas de gerenciamento de patches para aplicar e monitorar atualizações.
 - **Exemplo:** Utilizar WSUS (Windows Server Update Services) para gerenciamento de 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.
-

Análise de Riscos e Avaliação de Custos

- **Componentes:**
- **Identificação de ativos:**
 - Listar e avaliar todos os ativos importantes.
- **Avaliação de ameaças e vulnerabilidades:**
 - Determinar quais ameaças podem afetar os ativos.
- **Determinação do equilíbrio entre custo e benefício:**
 - Avaliar o custo das medidas de segurança versus o potencial impacto das ameaças.
 - **Exemplo:** Analisar o custo de um antivírus em comparação com o custo de uma infecção por malware.



Segurança de Protocolos

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

Segurança de Protocolos

- **Vulnerabilidades Comuns:**
- **Falta de criptografia no TCP/IP:**
 - Transmissão de dados sem criptografia pode ser interceptada.
- **Boas Práticas:**
- **Uso de HTTPS e SSH:**
 - Garantir que as comunicações sejam criptografadas.
 - **Exemplo:** Usar HTTPS para proteger a transmissão de dados em sites.
- **Implementação de SSL/TLS:**
 - Criptografar dados durante a transmissão para evitar interceptações.
 - **Exemplo:** Configurar SSL/TLS em servidores web.



Sessão de Perguntas e Respostas

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