

E-book: Cibersegurança Natty ou Not?

Perguntas e Respostas Geradas por IA

1. O que é engenharia social em cibersegurança?

Engenharia social é uma técnica utilizada por atacantes para manipular pessoas e obter informações confidenciais, como senhas ou dados bancários. Em vez de explorar falhas técnicas, o atacante explora o fator humano, convencendo a vítima a fornecer acesso ou informações sensíveis.

2. Como funciona um ataque de phishing?

Phishing é um ataque em que o criminoso se passa por uma entidade confiável, geralmente por e-mail, para enganar a vítima e levá-la a fornecer dados pessoais, clicar em links maliciosos ou baixar arquivos infectados. A prevenção envolve atenção a remetentes desconhecidos e verificação de links antes de clicar.

3. O que é um exploit?

Um exploit é um código ou técnica que explora uma vulnerabilidade em um sistema, software ou rede, permitindo que o atacante execute ações não autorizadas, como obter acesso privilegiado ou comprometer dados.

4. Por que o Linux é popular entre profissionais de segurança?

O Linux é popular devido à sua flexibilidade, código aberto, grande variedade de ferramentas de segurança e personalização. Ele permite que profissionais de segurança realizem auditorias, testes de penetração e análises forenses de forma eficiente.

5. Como proteger sistemas contra ataques comuns?

Algumas práticas essenciais incluem: manter sistemas atualizados, usar autenticação forte, realizar backups regulares, treinar usuários sobre ameaças e monitorar logs de segurança. A defesa em camadas é fundamental para reduzir riscos.

Essas respostas foram geradas por um pipeline de IA local, utilizando apenas o conteúdo dos PDFs

técnicos presentes na pasta do projeto.

LabDIONattyOrNot @falvojr @dio_makethechange