Pentest

O que é um Pentest (Teste de Invasão)

- Simula ataques hackers reais para encontrar falhas antes que sejam exploradas, ajudando a reforçar a segurança digital.

Diferença entre Análise de Vulnerabilidades e Pentest

- A análise encontra falhas sem explorá-las; o pentest testa até onde um invasor pode chegar. Ambos se completam na segurança da informação.

Fases de um Pentest

- Reconhecimento: coleta de informações sobre o alvo (IPs, domínios, estrutura).
- Varredura: uso de ferramentas para identificar falhas e serviços vulneráveis.
- Ganho de Acesso: exploração das vulnerabilidades encontradas.
- Manutenção de Acesso: verifica se é possível permanecer no sistema sem ser detectado.
- Limpeza de Rastros: geração de relatório e remoção de evidências do teste.

Importância da Ética e do Contrato (Escopo)

- Todo pentest deve ser autorizado e documentado em contrato, definindo limites e técnicas. Isso garante ética e segurança jurídica.

Tipos de Pentest

1. Black Box: o testador não tem informações do sistema; simula um ataque externo.
2. Grey Box: o testador tem algum conhecimento parcial, como um ex-funcionário.
3. White Box: o testador tem acesso completo e autorizado, simulando um ataque interno.

Esses níveis ajudam a avaliar diferentes cenários de risco.

📝 Agora escreva um resumo de tudo o que você entendeu aqui: