
Instituto Infnet

# Segurança Da Informação

FABIANO GISBERT

# Teste de Penetração (Pen Test)

# Teste de Penetração (Pen Test)

Instituto Infnet

## Conceito

É uma prática de segurança que envolve testes autorizados e simulados em sistemas de TI para identificar e explorar vulnerabilidades. O objetivo é avaliar a segurança do sistema, encontrar falhas e indicar recomendações para mitigação antes que atacantes mal-intencionados possam explorá-las.

O teste de penetração faz parte de uma estratégia holística de segurança de um ambiente de TI.

# Teste de Penetração (Pen Test)

Instituto Infnet

## Tipos de Testes

- Invasão de perímetro (verficar firewall e gateways)
- Invasão de aplicações e Banco de dados (verificação de inserção de códigos)
- Invasão de Rede Sem fio (ativação de spots)
- Análise em dispositivos Byod (Verificação de vulnerabilidades)
- Testes de DoS (Verficar como se comporta o sistema numa tentativa de ataque)
- Invasão por Engenharia Social (Testes de Email, Phishing, Penetração física a empresa)

# Teste de Penetração (Pen Test)

Instituto Infnet

## Técnicas de Testes

- Invasão de perímetro (verficar firewall e gateways)
- Invasão de aplicações e Banco de dados (verificação de inserção de códigos)
- Invasão de Rede Sem fio (ativação de spots)
- Análise em dispositivos Byod (Verificação de vulnerabilidades)
- Testes de DoS (Verficar como se comporta o sistema numa tentativa de ataque)
- Invasão por Engenharia Social (Testes de Email, Phishing, Penetração física a empresa)

# Teste de Penetração (Pen Test)

Instituto Infnet

## Técnicas de Testes

- **Black Box**: O testador não tem conhecimento prévio sobre a infraestrutura do alvo. Simula um ataque externo.
- **Gray Box:** O testador tem algum conhecimento sobre a infraestrutura do alvo, como credenciais de usuário ou detalhes da rede interna. Simula um ataque de um usuário interno ou um invasor que já conseguiu acesso parcial ao sistema.
- **White Box:** O testador tem total conhecimento sobre a infraestrutura do alvo, incluindo código-fonte, diagramas de rede, e credenciais de acesso. Simula um ataque com conhecimento interno profundo, como um desenvolvedor ou administrador de sistemas.

# Teste de Penetração (Pen Test)

Instituto Infnet

## Roteiro de Testes – Black Box

### 1) Reconhecimento

•Coleta de informações públicas sobre o alvo (whois, DNS, etc.).
•Varredura de portas e serviços com Nmap.
•Enumeração de serviços web e de rede.

### 2) Varredura

•Identificação de vulnerabilidades com ferramentas como Nmap e Nikto.
•Exploração de vulnerabilidades comuns.

# Teste de Penetração (Pen Test)

Instituto Infnet

## Roteiro de Testes – Black Box

**3) Exploração (Exploit)**

•Tentativas de exploração de falhas encontradas.
•Acesso inicial ao sistema.

**4)Pós-Exploração**

•Coleta de informações do sistema comprometido.
•Escalonamento de privilégios.

**5) Relatório**

•Documentação das vulnerabilidades encontradas.
•Recomendação de medidas corretivas.

# Teste de Penetração (Pen Test)

Instituto Infnet

## Roteiro de Testes – Grey Box

**1) Reconhecimento**

•Coleta de informações sobre a rede interna (sub-redes, dispositivos, etc.).
•Varredura de portas e serviços com Nmap, incluindo varredura interna.

**2) Varredura**

•Identificação de vulnerabilidades específicas com Nessus.
•Teste de configuração de serviços (SSH, SMB, etc.).

**3) Exploração**

•Testes de vulnerabilidades de autenticação.
•Exploração de falhas encontradas e acesso ao sistema

# Teste de Penetração (Pen Test)

## Roteiro de Testes – Grey Box

**4) Pós-Exploração**

- Movimentação lateral dentro da rede (busca de compartilhamentos vulneráveis).
- Coleta de informações sensíveis
- Escalonamento de privilégios.

**5) Relatório**

- Documentação das vulnerabilidades encontradas.
- Recomendação de medidas corretivas.

# Teste de Penetração (Pen Test)

Instituto Infnet

## Roteiro de Testes – White Box

**1) Reconhecimento**

•Análise detalhada do código-fonte (se disponível).
•Revisão das configurações de segurança da rede e dos sistemas.

**2) Varredura**

•Varredura de vulnerabilidades com ferramentas específicas (SonarQube, Fortify).
•Testes de penetração em APIs e serviços internos.
•Verificação das redes virtualizadas

# Teste de Penetração (Pen Test)

Instituto Infnet

## Roteiro de Testes – White Box

**3) Exploração**

•Exploração de vulnerabilidades lógicas e de negócios.
•Testes de falhas de autenticação e autorização.

**4) Pós-Exploração**

- Simulação de ataques avançados com conhecimento interno.
- Avaliação da resposta a incidentes.

**5) Relatório**

- Documentação das vulnerabilidades encontradas.
- Recomendação de medidas corretivas.

# Teste de Penetração (Pen Test)

Instituto Infnet

## Montagem do Relatório Final

**1) Introdução**

•Objetivo do teste de penetração.
•Escopo e limitações.
•Metodologia utilizada.

**2) Resumo Executivo**

•Visão geral das descobertas.
•Principais vulnerabilidades encontradas.
•Impacto potencial e riscos associados.

# Teste de Penetração (Pen Test)

Instituto Infnet

## Montagem do Relatório Final

### 3) Detalhamento Técnico

•Descrição detalhada de cada vulnerabilidade encontrada.
•Evidências (capturas de tela, logs, etc.).
•Metodologia de exploração utilizada.

### 4) Análise de Riscos

•Potencial ameaça ao negócio de cada vulnerabilidade.
•Probabilidade de exploração por terceiros.
•Matriz Probabilidade x Impacto.

# Teste de Penetração (Pen Test)

Instituto Infnet

## Montagem do Relatório Final

**5) Recomendações**

•Medidas corretivas para cada vulnerabilidade.
•Sugestões de melhorias para a segurança geral do sistema.

**6) Conclusão**

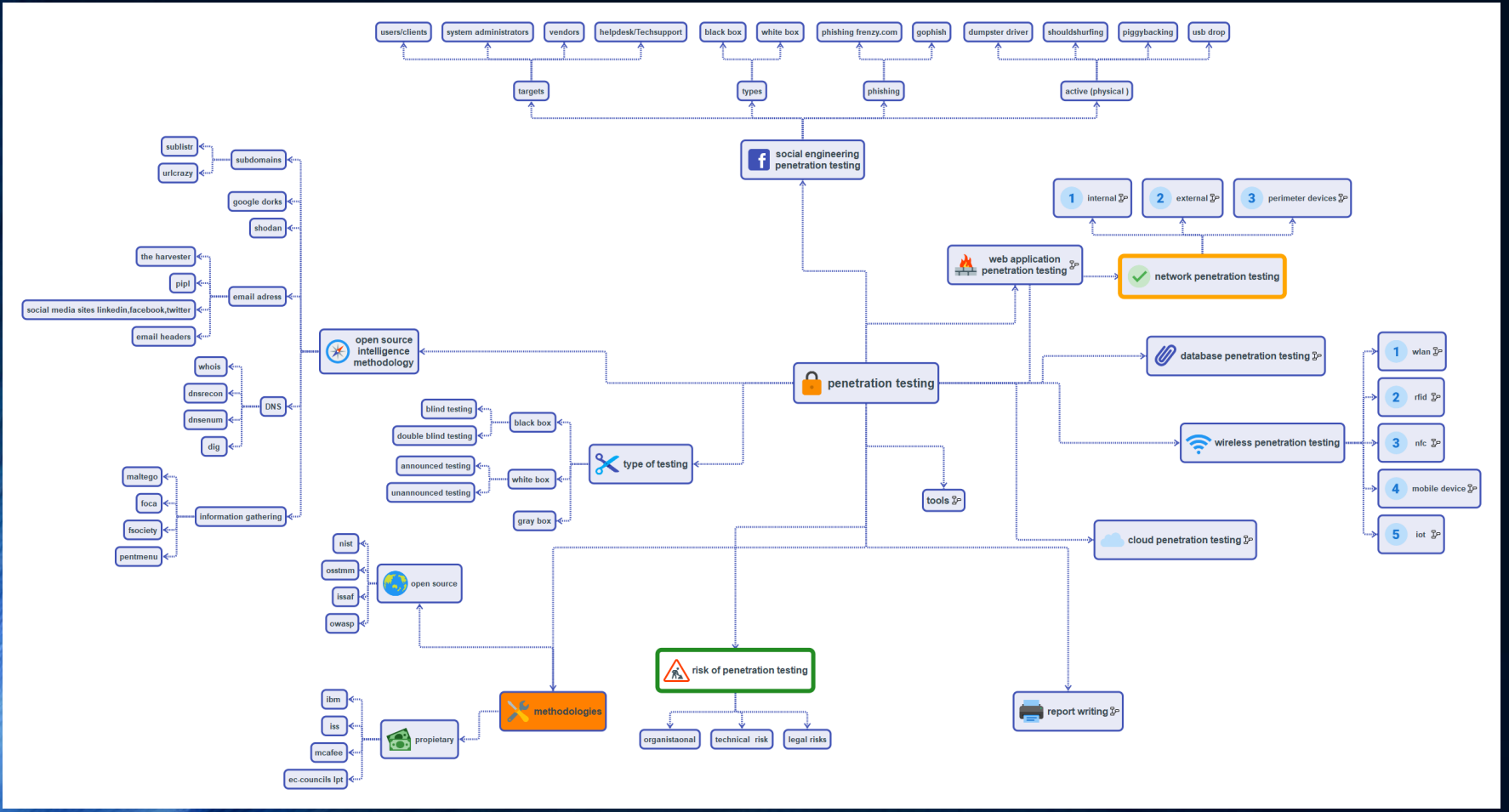
•Resumo dos resultados.
•Próximos passos sugeridos.

**7) Anexos**

•Detalhes adicionais, scripts utilizados, e referências.

# Teste de Penetração (Pen Test)

## Mapa Mental (exemplo)




https://github.com/5bhuv4n35h/pentestmindmap/blob/master/README.md

# FIM