



Introdução a Testes de Segurança



Você Sabia?

+612%

Tentativas de fraudes digitais em serviços financeiros

+135%

Fraudes na indústria de games

R\$ 2.7 bilhões

Estimativa de prejuízo com fraudes financeiras



+223.000.000

Brasileiros com dados vazados (fotos, endereços, documentos e renda)

+1.566%

Pessoas se passando por outras

12:00 às 00:00

Horário com maior incidência de golpes.

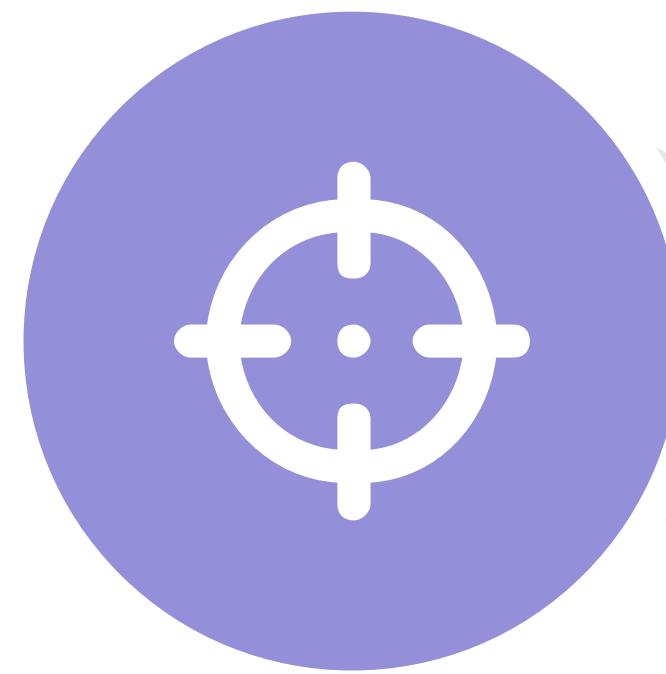


Principais Tipos de Ataque

- ✓ **Cavalo de Tróia:** Malware que opera com “autorização” do usuário.
- ✓ **Força Bruta:** Furto de senhas através de diversas tentativas de combinações de usuário e senha.
- ✓ **Phishing:** Geralmente aplicado via e-mail, usuários são enganados para revelarem informações sigilosas.
- ✓ **DDoS (Distributed Denial of Service):** Ataque de negação de serviços que sobrecarrega as atividades computacionais, provocando lentidão e tornando o sistema sob ataque indisponível.
- ✓ **Port Scanning:** Usa malwares que fazem uma busca pelo servidor na tentativa de encontrar alguma vulnerabilidade.
- ✓ **Ransomware:** “Sequestrador Virtual” que bloqueia o acesso a todos os dados, liberados mediante pagamento por criptomoeda.
- ✓ **Engenharia Social:** Induzir usuários desavisados a compartilhar dados pessoais (utilizados para identificar senhas de acesso), infectar seus computadores com malware ou abrir links para sites infectados.



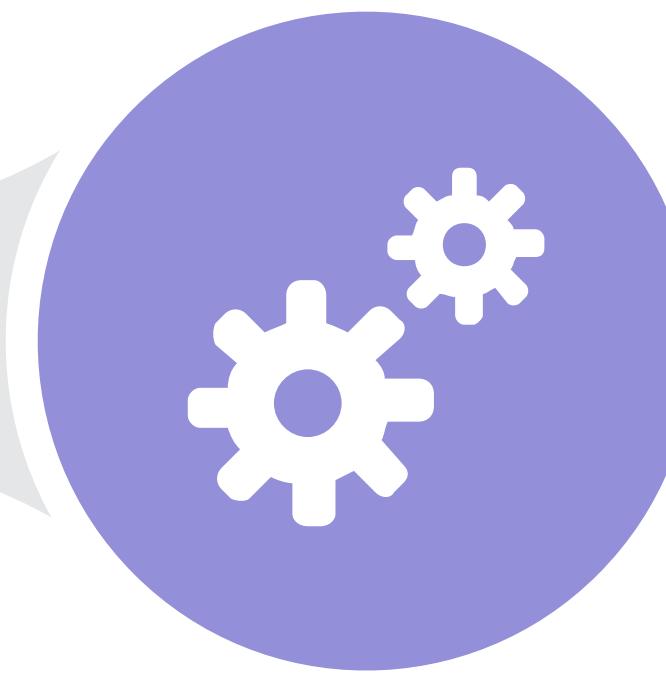
Testes de Segurança



É um tipo de Teste de Software **não funcional**, que busca identificar vulnerabilidades em um sistema para evitar ataques maliciosos de intrusos.



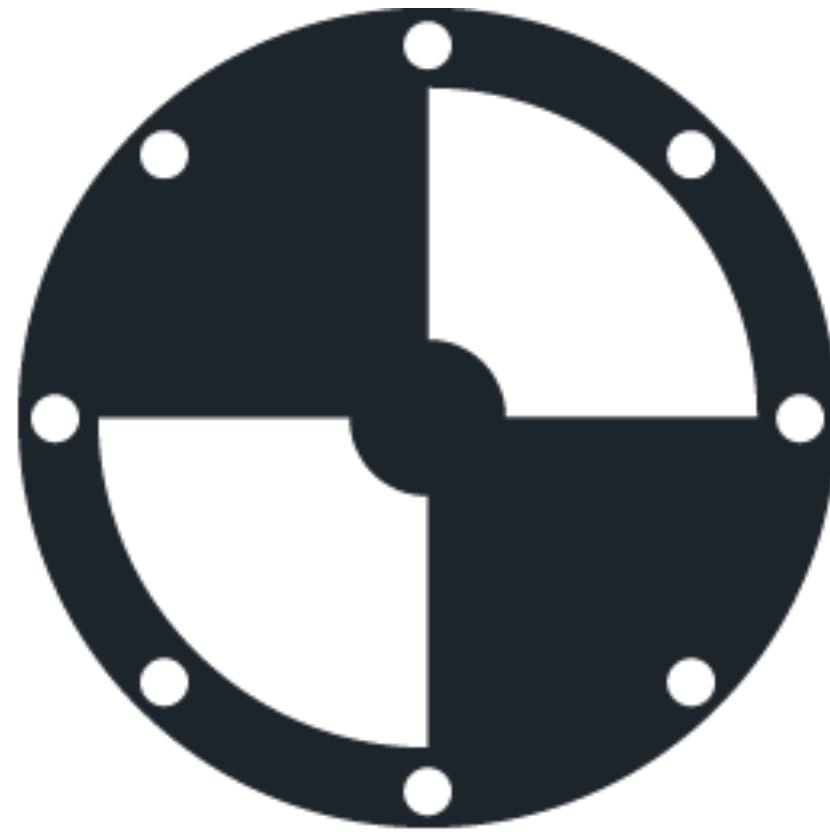
Busca as lacunas e fraquezas possíveis do sistema de software que podem resultar em vazamentos de dados e invasão.



Parte do ciclo de desenvolvimento de um software, especialmente em ambientes ágeis que implementam a cultura DevSecOps

Como se preparar?

Blue Team



Time que aprimora a defesa: Avalia a segurança de rede e identifica possíveis vulnerabilidades. Seu foco é em detecção de ameaças e resposta de incidentes, ou seja, seu principal objetivo é aplicar estratégias de defesa e manter a segurança dos sistemas e aplicações.

Red Team



Time de ataque: Tem como função a realização de testes de penetração. Imita ataques do mundo real, fazendo uso de todas as etapas e habilidades que um invasor usaria para, assim, identificar falhas e ameaças à segurança.





Princípios de Testes de Segurança

DISPONIBILIDADE

Garantia de que um serviço ou sistema está funcional e disponível e está fazendo o que se espera.

INTEGRIDADE

Garantia de que os dados ou resultados são consistentes e precisos em todas as plataformas.

AUTENTICAÇÃO

Consiste em confirmar a identidade de uma pessoa / sistema, tentando acessar um recurso protegido em outro sistema.

AUTORIZAÇÃO

É o processo de definir as funções que um cliente* tem permissão para realizar ações em um recurso protegido residente em um servidor.

CONFIDENCIALIDADE

É um processo de segurança que protege os dados do mundo externo por meio de criptografia / hash etc.

NÃO REPÚDIO

Garantia de que uma mensagem transmitida foi enviada e recebida pela pessoa que afirma ter enviado e recebido a mensagem.



Estratégias

VARREDURA DE VULNERABILIDADE

Feito por meio de ferramentas de software automatizadas para varrer um sistema contra vulnerabilidades conhecidas.

VARREDURA DE SEGURANÇA

Identificação de fraquezas da rede e do sistema por meio de ferramentas manuais e automatizadas e fornece soluções para reduzir esses riscos.

TESTE DE PENETRAÇÃO

Análise de um determinado sistema / serviço / aplicativo para verificar possíveis vulnerabilidades por meio da simulação de uma tentativa de hacking.

AVALIAÇÃO DE RISCO

Análise de riscos de segurança e classificação dos mesmos em Baixo, Médio e Alto. Este teste recomenda controles e medidas para reduzir o risco.

AUDITORIA DE SEGURANÇA

Inspeção interna de Aplicativos / Sistemas / Serviços para incidentes de violação de segurança.

HACKER ÉTICO

Hackear os sistemas de software de uma empresa com a intenção de expor falhas de segurança no sistema



Tipos de Análise

DAST Dynamic Application Security Testing



Examina uma aplicação em tempo de execução para encontrar vulnerabilidades que um invasor potencial pode explorar.

SAST Static Application Security Testing



Examina o código em busca de falhas e pontos fracos de software, como injeção de SQL, XML, JSON, registro e monitoramento insuficientes.



Plano de Testes

- ✓ **Descrição do seu objetivo e alvos**
- ✓ **Massa de dados de teste utilizados para reproduzir os "ataques"**
- ✓ **Ferramentas de teste necessárias para executar os testes**
- ✓ **Análise dos resultados e criação de caso de testes com o vetor de ataque (passo a passo detalhado para reproduzir como o ataque ocorreu)**



Mantenha-se atualizado!

- ✓ Painel de Incidentes Cibernéticos 2022: https://www.securityreport.com.br/email/InfoSR2022_.html
- ✓ Relatório de Brechas Verizon: <https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/>
- ✓ Mapa de ataques FortiGuard: <https://www.fortiguard.com/threat-research/map>
- ✓ Mapa de ataques Kaspersky: <https://cybermap.kaspersky.com/>
- ✓ Mapa de ataques Sonic Wall: <https://attackmap.sonicwall.com/live-attack-map/>



Referências

- <https://newsroom.transunion.com.br/um-ano-apos-a-pandemia-tentativas-de-fraude-digital-aumentam-no-brasil-segundo-estudos-da-transunionq4/>
- <https://www.securityreport.com.br/destaques/cenario-de-ameacas-ciberneticas-e-critico-no-brasil/#.Yi33GhDMIZG>
- <https://backupgarantido.com.br/blog/tipos-de-ataque-hacker/>
- <https://blog.konduto.com/pt/2021/07/censo-da-fraude-2021-como-e-o-comportamento-do-fraudador-no-brasil/>
- <https://g1.globo.com/economia/noticia/2021/06/24/cresce-no-de-consumidores-vitimas-de-fraudes-financeiras-no-brasil-veja-ranking-das-mais-recorrentes.ghtml>
- <https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2021/07/06/tentativas-de-fraudes-digitais-em-servicos-financeiros-crescem-612percent-no-brasil-em-2021.ghtml>
- <https://medium.com/it-security-best-practices-methodologies-loopholes/security-testing-basics-that-you-should-know-999f02084dc3>



Introdução a Testes de Segurança

