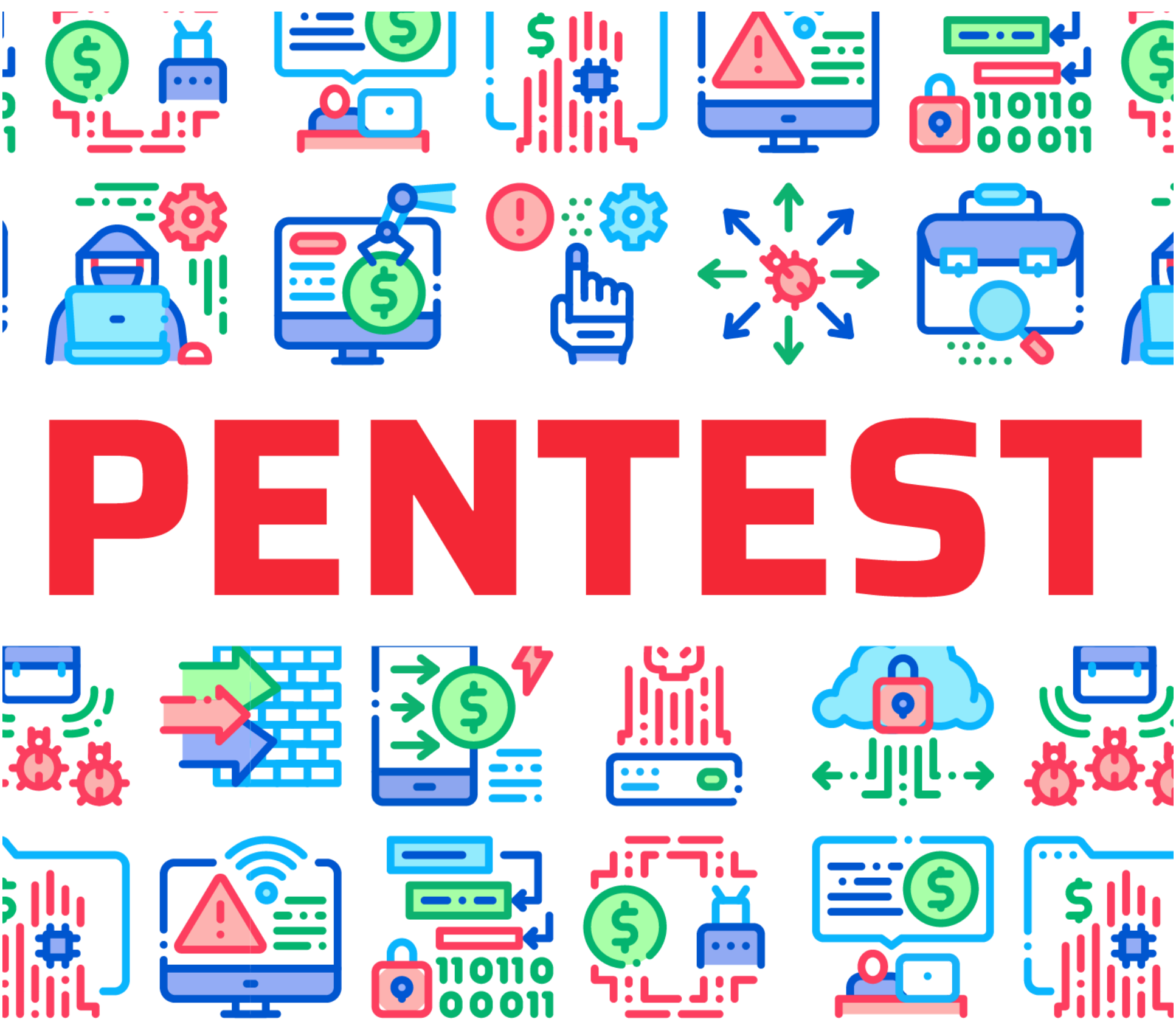
Artigos

Como otimizar o pentest e os testes de invasão em 5 etapas



Tempo de leitura: 5 minutos

Como **otimizar o pentest e os testes de invasão** diante de ameaças cada vez mais sofisticadas e aumento de ciberataques?

Essa é a questão-chave para os especialistas em TI e SI que desejam aprimorar sua gestão de vulnerabilidades e garantir a efetividade dos controles de segurança da informação no mundo real.

Afinal, um sistema só está realmente seguro e em conformidade com os padrões legais se incluir defesas contra um **hacker qualificado** e motivado — daí a importância de conduzir testes de segurança contínuos.

Por isso, vamos entender como otimizar o pentest e os testes de invasão em um **processo ágil e rastreável**, seguindo as principais metodologias e padrões internacionais.

Leia até o fim para garantir a eficiência dos seus testes.

Como otimizar o pentest e os testes de invasão

Saber como otimizar o pentest e os testes de invasão é essencial para **identificar e corrigir** as vulnerabilidades dos sistemas de forma efetiva — e evitar que um hacker encontre essas brechas primeiro.

Essas **simulações de ciberataques** são realizadas por especialistas em TI e SI para explorar vulnerabilidades no ambiente, colocando à prova suas medidas e soluções de segurança da informação.

Enquanto as auditorias apenas verificam a existência dos controles e suas configurações, esses testes de segurança comprovam a efetividade das suas defesas contra um hacker com alto nível de **conhecimento e motivação**.

E não faltam cibercriminosos motivados: no Brasil, foram **15 bilhões** de tentativas de ataque cibernético em um único trimestre de 2019, segundo dados da Fortinet publicados na Tecmundo.

Além disso, **85% dos brasileiros** já foram vítimas de ataques cibernéticos, 76% estão preocupados com roubo de identidade e 69% temem os vírus e hackers, segundo a pesquisa Unisys Índice de Segurança 2019.

Para proteger sua infraestrutura dessas ameaças, é preciso otimizar o pentest e os testes de invasão seguindo rigorosamente as metodologias e padrões, em um processo **contínuo e rastreável**.

Padrões e metodologias do pentests e testes de invasão

Para entender como otimizar o pentest e os testes de invasão, é fundamental conhecer as **metodologias e padrões internacionais** que orientam a validação dos pontos de falha.

Essas referências são importantes para embasar o processo em convenções reconhecidas no mundo todo e assinadas por profissionais de segurança, garantindo a identificação de todas as vulnerabilidades — além de promover uma análise mais **rápida e assertiva**.

Conheça as metodologias e padrões mais utilizados.

NIST SP 800-115

O NIST SP 800-115 é um **guia técnico** para testes e avaliações em segurança da informação publicado pelo National Institute of Standards and Technology dos EUA.

O documento apresenta recomendações práticas e procedimentos para execução de **análise de vulnerabilidades** em aplicações e redes, auditoria de conformidade, entre outros serviços.

É utilizado como referência para ações preventivas de segurança, permitindo a identificação e a mitigação de vulnerabilidade

OWASP Testing Guide

O OWASP Testing Guide é um guia colaborativo mantido pela **comunidade** de profissionais de segurança The Open Web Application Security Project (OWASP).

O documento já está em sua **quarta versão** e descreve em detalhes as boas práticas, técnicas e ferramentas necessárias para executar testes de segurança em aplicações web, baseado na experiência de centenas de especialistas em TI e SI ao redor do

logy Manual (OSSTM 3) é uma **metodologia científica** para avaliações de Segurança *Sec*).

testes de segurança de diversos níveis, considera qualquer tipo de auditoria, incluindo ades estáticas e dinâmicas e **hacking ético**, além de estar em conformidade com o NIST,

O Information Systems Security Assessment Framework (ISSAF) é um **framework** desenvolvido pelo Open Information Systems Security Group (OISSG).

Seu objetivo é integrar ferramentas de gestão e controles de segurança, avaliar os processos e políticas de segurança da informação e buscar **conformidade** com padrões e normas regulatórias voltados para infraestrutura de TI.

Como otimizar o pentest e testes de invasão em 5 etapas

Se você quer saber como otimizar o pentest e testes de invasão, precisa enxergá-los como parte de um **processo mais amplo** de gestão de vulnerabilidades.

Ou seja: a identificação de vulnerabilidades é apenas o primeiro passo, e seus testes de segurança precisam seguir padrões e métodos racionais para cumprirem seu objetivo.

Acompanhe as **etapas essenciais** para conduzir os testes.

1. Planejamento e reconhecimento

A primeira etapa do pentest e dos testes de invasão é dedicada ao **planejamento e reconhecimento**.

Aqui, você deverá definir o escopo dos testes, objetivos, logística, expectativas, implicações legais e sistemas-alvo, além de escolher qual **tipo de teste** será mais adequado — por exemplo, um Blackbox, GreyBox ou WhiteBox.

Além disso, é o momento de fazer a **coleta de OSINT** (Open Source Intelligence, ou inteligência de fonte aberta), que consiste em uma pesquisa por fontes de informações públicas realizada por meio de motores de busca.

2. Escaneamento de vulnerabilidades

O próximo passo de como otimizar o pentest e testes de invasão é utilizar o **scanner de vulnerabilidades** para mapear as brechas de segurança do sistema.

Depois de identificadas, as vulnerabilidades devem ser **classificadas** de acordo com seu risco aos ativos da empresa — e as ameaças também devem ser listadas.

3. Exploração das vulnerabilidades

Com o mapa das vulnerabilidades, você pode começar a **explorar as brechas** usando táticas como cross-site scripting, injeção de SQL, backdoors, engenharia social, etc.

Nessa etapa dos pentests e testes de invasão, o objetivo é roubar dados, escalar privilégios e interceptar o tráfego para entender o nível de efetividade dos controles de segurança.

Além de invadir o sistema, também é importante testar se a vulnerabilidade pode ser usada para uma **permanência mais longa** que pode levar a um acesso mais profundo do cibercriminoso.

4. Análise de risco e recomendações

Ao término dos testes de invasão, é preciso fazer uma **análise aprofundada** dos resultados, compilando as vulnerabilidades exploradas, métodos utilizados, dados sensíveis acessados e tempo de permanência do pentester no sistema sem detecção.

Essas informações devem ser documentadas em um relatório e compartilhadas com as áreas envolvidas, junto com as recomendações para **correções das falhas** encontradas.

va do investimento

pentest e testes de invasão ao **acompanhar de perto** a correção das vulnerabilidades, com

orizados de acordo com os riscos que representam para os ativos da empresa.

ém será essencial para **justificar os investimentos** em SI e provar o valor dos testes de a segurança da informação.

imizar o pentest e os testes de invasão

O segredo de como otimizar o pentest e os testes de invasão é ter uma **ferramenta de gestão** que facilite o encaminhamento de correções e acompanhamento, compilação de indicadores e automatização dos processos.

Em vez de utilizar planilhas **desconexas e desatualizadas**, que precisam ser preenchidas manualmente e não têm rastreabilidade, você pode optar por uma plataforma de gestão integrada de segurança da informação e conformidade como a GAT.

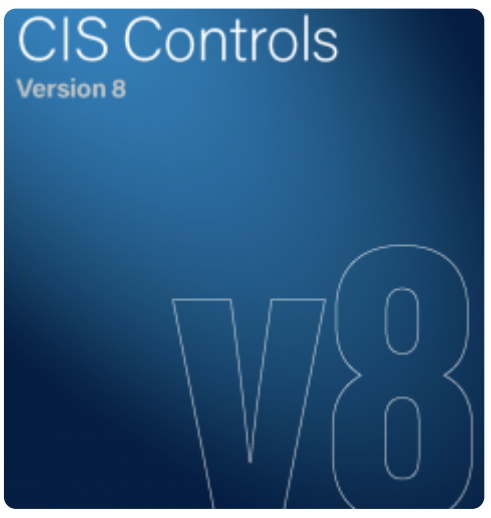
Com GAT você otimiza processos de gestão de Segurança da Informação, centraliza os relatórios de vulnerabilidades e mantém sua base sempre atualizada — além de contar com indicadores personalizáveis, regras customizadas e comunicação colaborativa. Assim, você saberá como otimizar o pentest e os testes de invasão em um processo **estruturado, rastreável e integrado** de gestão de vulnerabilidades. Solicite sua demonstração para entender melhor como GAT pode revolucionar seu processo de Pentest.

share:

Você também pode curtir isso:

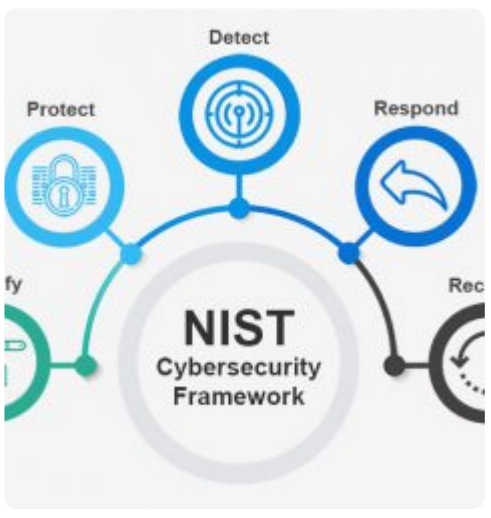
Gerenciamento da Superfície de Ataque

Tempo de leitura: 7 minutos



Implementação do CIS Controls V8

Tempo de leitura: 13 minutos



Implementação do NIST Cybersecurity Framework

Tempo de leitura: 12 minutos

Postagens Recentes

GAT InfoSec no pódio do Top 100 Startups

10/11/2022