

pesquisar



(https://prolinx.com.br/)

nkedi (http (http (http
s://w s://w s://w
n.co ww.f ww.in s://t ww.y
m/co aceb stagr witteroutu
npanr ook.co am.c .com be.co
y/pro om/ om/ /prol m/c
linxti /? Proli om/ /prol m/c
/? Proli om/ /prol m/c
origin nXTI/ proli inxti) /Prol
alSub nx/) inxti) inxti)
doma)
in-br)



Segurança (https://Prolinx.Com.Br/Category/Seguranca/)

PENTEST: CONHEÇA AS PRINCIPAIS METODOLOGIAS E PADRÕES



📅 26/01/2022(https://prolinx.com.br/2022/01/26/)

Tempo de leitura: 6 minutos



SUMÁRIO



- Pentest: o que é
- Pentest: metodologias



- Pentest: conheça os diferentes tipos
- Pentest: onde deve ser realizado
- Pentest: quando deve ser realizado
- Pentest: por que fazer?

Testes sistemáticos como o *Pentest* são cada vez mais buscados por gestores que desejam proteger ativos críticos antes da ocorrência de um incidente como invasão ou falha.

Para muitas empresas, a disponibilidade e a transparência das informações passaram a ser obrigatórias para que se mantenham competitivas. O mesmo vale para a garantia da integridade e confidencialidade de dados estratégicos.

Neste post, vamos te explicar o que é e **mostrar a importância do *Pentest*, ferramenta que simula situações de ataques ou falhas operacionais em sistemas ou bancos de dados** e mais.

Continue a leitura, confira as principais metodologias utilizadas para esse teste e entenda quando e por que realizá-lo!

PENTEST: O QUE É

Também chamado de teste de intrusão ou teste de invasão, o teste de penetração é um **processo de verificação e análise de vulnerabilidades em ambientes de rede**, sistemas ou aplicações de infraestrutura interna ou externa.

Trata-se de um teste que visa proteger informações críticas das empresas, identificando as vulnerabilidades dos seus sistemas e avaliando o impacto que elas têm sobre seu funcionamento geral.

Desta forma, ao realizar testes que simulam ataques reais que seriam feitos por *crackers*, o *Pentest* ajuda a prevenir essas invasões, melhorando a taxa de resposta aos riscos.

PENTEST: METODOLOGIAS

Como dissemos, o *Pentest* conta com ferramentas e processos que selecionam informações relevantes, auxiliando a identificar e mitigar os riscos aos dados críticos da organização.

Esse tipo de serviço já existe no mercado há algum tempo, mas a quantidade de metodologias relacionadas ao *Pentest* pode confundir até mesmo profissionais mais experientes na área da TI.

A variedade de opções desse tipo de serviço se deve ao fato de que **não existe uma metodologia única a ser aplicada em todos os tipos de organizações** e ambientes de rede.

Porém, ainda que não exista uma única forma de realizar os testes, **existem algumas metodologias que permitem resultados mais conclusivos e com menores chances de erros** de interpretação dos dados.

A seguir, confira as principais ferramentas utilizadas para a execução do *Pentest*.

OSSTMM - OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL

O Manual de Metodologia Aberta de Comprovação de Segurança (OSSTMM, Open



Source Security Testing Methodology Manual) é um manual de uma metodologia desenvolvida pelo ISECOM (Institute for Security Open Methodologies), uma organização colaborativa que realiza pesquisas na área de segurança da informação.

Trata-se de um documento completo, composto por dicas de dezenas de especialistas internacionais e muito utilizado em auditorias de Segurança da Informação e sistemas web, pois descreve as fases que se deve seguir para executar qualquer auditoria. Abrange todas as áreas da segurança da informação.

Como a metodologia utiliza o conceito de "open source", está em constante evolução.

Essa metodologia pode ser aplicada a qualquer tipo de organização, de todos os tamanhos e em diversos setores de atuação. Para tanto, realiza-se o *Pentest* de acordo com as necessidades da organização e do conhecimento prévio dos ativos que serão analisados.

OWASP - OPEN WEB APPLICATION SECURITY PROJECT

O OWASP (Projeto Aberto de Segurança em Aplicações Web) também é uma instituição sem fins lucrativos composta por profissionais das áreas de tecnologia e Segurança da Informação e **tem o objetivo de promover melhorias no desenvolvimento de sistemas**.

Um dos projetos de maior destaque da OWASP, que tem se tornado referência para desenvolvedores e analistas de segurança, é o OWASP Top 10. É um projeto que **informa sobre as principais vulnerabilidades em aplicações web**.

O OWASP tem alguns princípios para a execução dos *Pentests*. Veja:

- Não acreditar em milagres, é preciso ser realista;
- Ter pensamento estratégico;
- Realizar testes regularmente;
- Entender o escopo dos sistemas;
- Desenvolver a mentalidade correta;
- Estender os objetivos das análises;
- Utilizar as ferramentas corretas;
- Ficar atento aos detalhes;
- Documentar os resultados.

NIST CYBERSECURITY FRAMEWORK

Essa metodologia para o *Pentest* foi desenvolvida pelo Instituto Nacional de Padrões e Tecnologia (NIST – National Institute Standards and Technology), um órgão do governo dos Estados Unidos que promove a competitividade e a inovação industrial no país.

Na área de tecnologia e Segurança da Informação, **o NIST conta com regras para a realização de testes de segurança e ações preventivas**. Entre as técnicas indicadas pelo instituto para a realização do teste de penetração, existem algumas etapas:

- Execução dos testes de segurança;
- Revisão das técnicas utilizadas;
- Identificação do alvo a ser analisado;
- Elaboração de técnicas de validação;
- Planejamento das avaliações de segurança;
- Execução das avaliações;
- Atividades pós-teste.

PTES - PENETRATION TESTING EXECUTION STANDARD

Essa é uma das metodologias mais recentes para a realização de *Pentests* e que **tem como objetivo se tornar uma norma-padrão para a execução deste tipo de serviço**.

O PTES (Padrão de Execução de Teste de Penetração) divide os testes nas seguintes etapas:



etapas:

- Predefinição;
- Coleta de Inteligência;
- Modelagem de ameaças;
- Análise de vulnerabilidade;
- Exploração;
- Publicar exploração;
- Relatório.

ISSAF - INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK

Disponibilizada pelo OISSG (Open Information Systems Security Group), essa metodologia é a mais extensa do mercado. Suas fases estratégicas englobam o **planejamento e a preparação do Pentest, a avaliação em si, os relatórios e a limpeza.**

A metodologia ISSAF pode ser aplicada em quatro áreas distintas dos sistemas de uma empresa: segurança de rede, e host, de aplicação e de banco de dados.

PENTEST: CONHEÇA OS DIFERENTES TIPOS

Existem ainda tipos diferentes da ferramenta, conforme elencamos abaixo. Confira:

- **Blackbox:**
 - Não há conhecimento prévio da infraestrutura de rede e da arquitetura das aplicações;
 - Mais utilizada devido a produção de um cenário real.
- **Graybox:**
 - Acesso ou validação de informações e/ou utilização de credenciais legítimas, visando a validação das permissões de acesso e autorização estão em conformidade com as necessidades de negócio.
- **Whitebox:**
 - Todas as informações da infraestrutura de rede e da arquitetura da aplicação são fornecidas;
 - Geralmente esta abordagem realiza a análise e revisão de segurança do código fonte da aplicação desenvolvida/testada.

PENTEST: ONDE DEVE SER REALIZADO

Ao contratar um Pentest, o cliente e o prestador de serviço devem **saber quais são os fatores que serão avaliados.**

Enquanto algumas empresas precisam apenas da análise de uma aplicação web, outras necessitam de uma varredura em toda a rede: servidores, firewalls e conexões wireless.

Por isso, é preciso compreender quais os ativos que necessitam desse tipo de avaliação. Do contrário, você pode encontrar orçamentos com valores discrepantes e incompatíveis com sua demanda.

PENTEST: QUANDO DEVE SER REALIZADO

Seja qual for a metodologia escolhida, é importante **realizar o Pentest de forma frequente, em intervalos programados** ou quando ocorrerem mudanças no ambiente da rede.

Afinal, com as constantes atualizações de recursos e soluções, é importante se adiantar aos riscos, eliminar as vulnerabilidades e realizar a adaptação aos novos modos de uso dos sistemas.

Ainda, é preciso ficar atento às ameaças de pessoas mal-intencionadas que encontram



brechas para obter vantagens sobre as operações.

PENTEST: POR QUE FAZER?

Se ao longo deste artigo você ainda não se convenceu da importância do *Pentest*, trouxemos alguns dados estatísticos sobre o assunto que podem ajudar.

De acordo com o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br), **somente em 2020 foram registrados 665.079 alertas** (<https://cert.br/stats/incidentes/2020-jan-dec/tipos-ataque.html>).

Desse total, a maior parte das notificações estava relacionada a tentativas de exploração de vulnerabilidade e a disseminação de *worms*.


Ainda, ataques a servidores web, fraudes e invasões a equipamentos também foram registrados. **Esses dados mostram que as empresas devem estar preparadas para os riscos** de exploração dos ambientes de suas redes.

Para reduzir esses riscos, é fundamental adotar testes de segurança que comprovem a proteção dos ativos. Portanto, **a execução de *Pentests* de forma preventiva pode poupar sua empresa** de muitos transtornos e gastos desnecessários.

Como vimos, existem diversos tipos de metodologias para a execução de *Pentests*, todas com a finalidade de identificar os gargalos e garantir melhor taxa de resposta aos riscos.

Em outros conteúdos, daremos mais detalhes sobre cada uma das metodologias do *Pentest*. Acompanhe para não perder!

Este conteúdo foi útil? Conheça o serviço de Análise, Gestão de Vulnerabilidades e Pentest da Prolinx (<https://prolinx.com.br/seguranca-informacao/analise-vulnerabilidade/>)!

 WhatsApp

 LinkedIn

 Facebook

 Twitter

PROLINX

Moderna e atenta às tendências do mercado mundial de
Tecnologia, Segurança, Inovação e Nuvem.

ÚLTIMOS POSTS

