Pentest ou Testes de Invasão: O que é e quais são as etapas?

Os Testes de Intrusão, Penetração ou Pentests podem auxiliar e muito na hora de investigação, correção de vulnerabilidades e melhorias de segurança para todo ambiente de tecnologia da informação. Mas você sabe como ele efetivamente ocorre, qual o real processo, etapas e benefícios dessa solução? Confere com a gente em nossa matéria ;)

Para melhorar a segurança digital e confiabilidade de todo o setor de tecnologia e da empresa como um todo, é de extrema importância que haja **direcionamento e indicadores ou um plano para seguir**, de maneira assertiva e com objetivos claros para que recursos e tempo

Pesquisar...

Postagens acerca de:

Backup Firewall
Lei Geral de Proteção de Dados
lgpd
Monitoramento de Redes
Proteção de dados
Ransomware
red team
Resposta a incidentes
Security Operations Center
Segurança da Informação
Segurança de dados
Segurança de redes
Segurança Digital
SIEM SOC

Pentest e Hacker Ético

Em um artigo que publicamos em nosso blog falamos do Hacker Ético e como ele é importante para analisar todo o ambiente de T.I – através de um assessment/cyber scan – e explorar as falhas encontradas através dos testes de intrusão – pentests – **se quiser saber mais sobre o Hacker Ético, uma abordagem do Red Team, clique aqui.**

O que não falamos no texto anterior foi todo o processo do Pentest, além de como as etapas seguem mesmo após a finalização dos testes de intrusão, mas segue com a gente que vamos explicar com detalhes esse processo.

Porque o Pentest é importante na segurança de T.I

Visibilidade, exploração e correção, é para isso que o Pentest serve. A documentação de erros e falhas encontradas em um ambiente pode ser extensa. Sem o direcionamento da análise de vulnerabilidades e a exploração dos pontos críticos encontrados através dessa análise, a correção pode ser muito onerosa além de haver desperdício de recursos.

Por isso um Pentest é de extrema importância para o ambiente de tecnologia da empresa, **medindo a maturidade** não somente através das ferramentas de segurança implementadas contra intrusão, vazamento e perda de dados, mas de todos os endpoints a servidores e

O Pentester ou desenvolvedor recebe algumas informações do ambiente, ferramentas de armazenamento de dados, redes e até as aplicações de segurança. Além disso, pode **ter conhecimento de toda** a topologia da rede, IPs, senhas, níveis de usuários e logins. Por ser um teste amplo e com mais chances de encontrar falhas e brechas, é o mais requisitado entre as empresas, inclusive pelos clientes atendidos pela Softwall.

Black Box

Nessa modalidade, o Pentester ou desenvolvedor não recebe **nenhum tipo de informação do ambiente** ou ferramentas aplicadas, aqui, tudo é obtido “na raça”, é um modelo de teste de intrusão que se aproxima de uma situação real, mas pode deixar algumas ferramentas críticas fora da análise.

PENTEST PARA O SEU AMBIENTE DE TI

Fases do Pentest ou Teste de Intrusão

1 – Planejamento e Pré-acordo

Aqui as empresas, tanto a contratante quanto a contratada, fazem o acordo do que será testado, por quais meios, qual modalidade da análise e testes e quais serão os objetivos que deverão ser alcançados. Aqui também é feito o termo

aplicações de segurança e dados e tudo que compõe o ambiente físico e digital da empresa.

3 – Pentests/Testes de Intrusão

A partir dos pontos identificados e a classificação da criticidade de cada indicador, é possível então fazer um pentest mais direcionado e assertivo com o respaldo do assessment do ambiente – item 2. É possível explorar cada item de forma isolada, seja por um “exploit” conhecido na ferramenta ou até um “brute force”, dependendo do ativo ou aplicação que está sendo analisada ou explorada.

4 – Análise de Código e Aplicações

Aplicações, sejam elas de algum sistema de uso diário ou algum software de manipulação de dados e informações vitais de uma empresa, podem ser analisadas até mesmo em tempo real para verificar as possíveis falhas de segurança que podem conter nessas aplicações, sejam elas sistemas financeiros, e-commerces, aplicações de produtividade, colaboração ou qualquer outra usada na organização.

5 – Documentação e reporte

Após identificar e explorar falhas e brechas, classificar os pontos críticos, realizar os testes pertinentes, coletar evidências dessas falhas encontradas, a equipe deve gerar um relatório reportando os itens encontrados na rede da empresa e aplicações, apontando erros como má configuração, aplicações conflitantes, problemas com autenticação insegura, mesa e tela limpa, ambiente de

Depois de todo esse processo, ainda, como uma última fase pode ser estudado um reteste do ambiente ou aplicação que foram abordados no primeiro teste, assim, é **possível verificar se a empresa que contratou a solução fez sua "lição de casa"** ou se a equipe contratada também tomou as ações corretivas necessárias para que todas as brechas encontradas fossem fechadas – ou solucionadas.

Esse reteste geralmente é feito após um período acordado entre as empresas, que varia em torno de 2-6 meses, dependendo das falhas e brechas encontradas.

Red Team e Pentests

Apesar dos testes serem reais, dentro do ambiente real da empresa, eles não causam dano à organização, no entanto, ele é de extrema importância justamente pela intenção da equipe de pentest: eles não querem prejudicar o ambiente de T.I, roubar dados ou causar danos ou roubar dados, mas sim expor os pontos de melhorias justamente para prevenir crimes digitais e vazamento de dados.

Os Testes de Intrusão/Pentests fazem parte da estratégia de Red Team da Softwall, que utilizam de técnicas como o **Hacker Ético**, **Pentest** e **Forense Digital**. Conte com a gente para a melhoria da segurança do seu ambiente, nossa