Pentest: por que e como fazer?

Pentest: por que e como fazer?

Identificar as falhas de seu sistema de proteção é essencial para uma empresa manter a ***segurança*** de suas redes e informações - e é isso que o Pentest busca fazer. Também conhecido como Teste de Intrusão (Penetration Test), ele detecta minuciosamente as ***vulnerabilidades de um sistema*** de computador.

O Pentest simula um ataque que identifica os pontos fracos da defesa de um determinado sistema. Em outras palavras, é uma verdadeira simulação de uma invasão hacker, que explora as partes que poderiam ser aproveitadas de forma ágil.

Dessa forma, o processo também mostra as informações e dados que estão sujeitos a roubos, possibilitando que as corporações entendam quais aspectos precisam melhorar e onde reforçar a segurança. Tudo isso sendo feito a partir nicas realizadas por especialistas em segurança da informação.

Como funciona: as fases do Pentest

Para realizar o Pentest, em primeiro lugar, é necessário a ajuda de um profissional da área de segurança da informação. É ele que irá identificar os pontos de melhoria do sistema de proteção. Nesse caso, as empresas de consultoria são comumente contratadas para realizar os testes.

Posteriormente, a análise é feita em 6 fases detalhadas e cada uma delas possuem etapas e instruções distintas:

Reconhecimento e coleta de informações

Nessa primeira fase, o profissional que está realizando o Pentest - também chamado de pentester - faz o levantamento do máximo de informações possíveis sobre a empresa-alvo. Tais informações podem ser sobre o ramo de atuação, a existência de filiais, os serviços prestados, os endereços físicos e virtuais, entre outros dados.

Com tudo isso, o pentester consegue identificar a utilização de VPN (Virtual Private Network) e coletar os endereços dos ***servidores*** DNS (Domain Name Service).

Varredura ou mapeamento de rede

Depois de obter a informação de DNS, o especialista deve realizar o mapeamento da rede. Para isso, ele também irá fazer uma varredura do que está presente nela e no sistema.

Ao avançar no processo, é possível descobrir a topologia da rede, os servidores existentes, os sistemas operacionais usados, a quantidade de aparelhos na rede interna e o IP utilizado.

Enumeração de Serviços

Em seguida, depois da varredura, inicia a etapa de análise dos serviços que estão sendo executados e também das portas de acesso para o sistema.

꞉nção de acesso

Reunindo todas as informações anteriores, nessa fase, o profissional vai

explorar cada item e buscar pelas ***vulnerabilidades*** existentes. Para isso, ele utilizará técnicas específicas - de ***exploit*** e brute force - e também tentará encontrar quais informações poderiam ser obtidas pelos serviços que estão vulneráveis.

Exploração da vulnerabilidade

Nessa etapa, o pentester vai explorar as vulnerabilidades encontradas nas fases anteriores. Para isso, pode executar algum programa que recebe comandos remotamente ou mesmo ataques SQL.

Evidência e reporte

Depois de ter identificado e coletado as vulnerabilidades do sistema, um relatório será gerado expondo todos esses pontos vulneráveis, os ***erros de segurança*** e os aspectos que precisam de melhoria - como as más configurações e falhas de atualização do sistema.

Passando por essa etapa e contando com a ajuda da área de TI corporativo, finalmente, será possível corrigir os problemas.

Tipos de Pentest

O Pentest apresenta diferentes tipos que se distinguem pela suas formas de execução. São eles:

Pentest White Box

Esse é o tipo mais completo, porque avalia toda a infraestrutura da rede. Nele o profissional recebe, com antecedência, todas as informações sobre a estrutura de segurança da empresa.

Pentest Black Box

No Black Box, o pentester não recebe nenhuma informação da empresa-alvo - o trabalho é “feito às cegas”. Então, realiza-se todo o processo do zero. Esse é o ais fiel de pentest, porque funciona de forma muito semelhante a u leiro ataque malicioso.

Pentest Gray Box

Esse tipo de Pentest é feito partindo de informações mínimas e específicas da empresa. Sendo assim, trata-se de um meio termo entre o White e o Black Box.

Pentest interno

Nesse caso, o especialista faz o teste na rede interna da empresa. Assim, ele pode identificar os danos causados por funcionários insatisfeitos, por exemplo.

Pentest externo

O especialista, ao realizar o Pentest externo, irá explorar a tecnologia externa da empresa - como os servidores da DMZ. Nesse contexto, o método será realizado de forma remota, ou seja, fora da corporação.

Com todas essas opções, é preciso identificar qual é a mais apropriada para o contexto da sua empresa. E, com a ajuda de uma ***consultoria*** especializada, tomar essa decisão pode ser mais fácil.

Você pode obter esse serviço e garantir a máxima proteção contra invasões cibernéticas com a 4Infra Consultoria! ***Entre em contato*** com a nossa equipe e escolha a melhor opção para a sua corporação.

REDACAO4INFRA

17 de abril de 2020
Dicas

Próximos Artigos

← **Como usar a tecnologia para se proteger do coronavírus**

Boas práticas de governança de TI →