Tipos de Pentest

Existem vários tipos de ***pentest***, dentre os quais mais comuns são:

White Box

Todas as informações do cliente sobre a rede, servidores, banco de dados e sistemas que estão inclusos no escopo do teste de invasão, e demais informações de acesso aos mesmos, são fornecidas para que possam ser realizados testes extensivos e com mais abrangência.

Testes White Box mais conhecidos são aqueles realizados para analisar aplicações web, onde a configuração do servidor e o próprio código-fonte são analisados abertamente em busca de falhas de segurança que possam comprometer o serviço.

Black Box

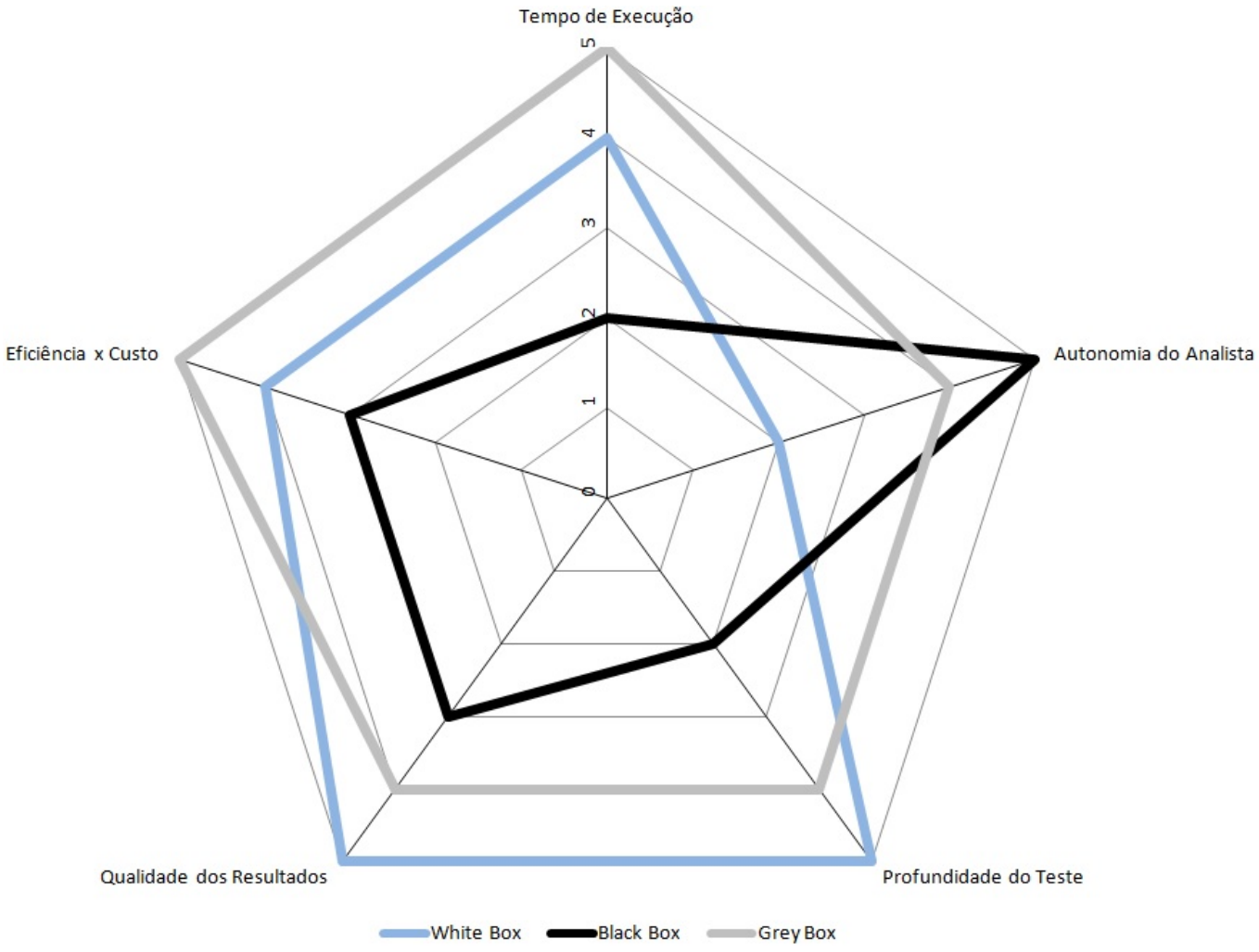
É o tipo de análise mais próximo de uma ataque externo, pois nenhuma informação vinda do cliente é fornecida ao analista de teste.

Sendo assim, todo e qualquer tipo de informação para a realização de um teste Black Box é adquirida através de técnicas específicas de hacking sobre os serviços disponíveis do alvo, identificando assim as vulnerabilidades e os possíveis danos causados por um ataque mal intencionado.

Grey Box

Esse tipo de análise pode ser considerado um mix dos anteriores, pois o analista de teste recebe alguma informação do cliente, como: dados da infraestrutura da rede ou acesso à determinado serviço web.

Um bom exemplo de teste Grey Box são aqueles direcionados para analisar possíveis falhas de segurança em uma aplicação vinda através de um usuário credenciado, como níveis de permissões de acesso e alterações não autorizadas.



Relatório Gerenciais e Técnicos → (http://www.auzac.com.br/testes-de-invasao/relatorios-gerenciais-e-tecnicos/)

Saiba Mais

- Testes de Invasão (https://www.auzac.com.br/testes-de-invasao/)
- Etapas de um Pentest (https://www.auzac.com.br/testes-de-invasao/etapas-de-um-pentest/)