

# TESTE DE INVASÃO

## O que e como testar?

Além das várias modalidades de teste de invasão, você também conta com uma grande diversidade de alvos para testar contra os mais avançados métodos do cybercrime. Veja a seguir em quais elementos você pode validar sua estratégia de proteção:



### Ambiente externo

Criação de simulações de ataques reais para avaliar o ambiente externo em sua totalidade, buscando vulnerabilidades que permitam acesso não autorizado.



### Segurança interna

Uso de abordagem do tipo BlackBox ou GrayBox para avaliar a segurança interna da rede, buscando eventuais inconsistências nas permissões de acesso.



### ATMs

Verificação dos controles de segurança de caixas eletrônicos com foco no usuário e no ambiente interno do equipamento para avaliar seu nível de exposição.



### Redes sem fio

Criação de simulações de ataques reais contra redes sem fio com o objetivo de identificar vulnerabilidades que possam ser exploradas pelos usuários.



### Aplicações web, apps mobile e APIs

Validação da estratégia de segurança de todos os elementos que compõem aplicações web e apps mobile e APIs.



### Pessoas

Verificação do nível de conscientização dos usuários para verificar se eles estão preparados para proteger a confidencialidade e a integridade dos recursos.



### Rede corporativa

Teste de verificação da quantidade e do tipo de tráfego suportado por uma infraestrutura remota para minimizar o impacto de um ataque de negação de serviço distribuído (DDoS).



### Cloud computing

Testes que levam em consideração características do modelo IaaS ou SaaS para identificar falhas de segurança no compartilhamento de sistemas em cloud.



### Servidores

Manipulação de solicitações para comprometer a segurança de serviços web.

## Como testar?

Independente do que você for testar, o principal objetivo do teste de invasão é obter acesso restrito ou irrestrito a sistemas de informação, para isso, podem ser feitos usando três diferentes abordagens:



### Blackbox

Trata-se de um teste cego, em que não há necessidade de contar com conhecimento prévio do ambiente de TI ou credenciais de acesso a sistemas e aplicações. Basta fornecer o domínio a ser avaliado ou o acesso a um ponto da rede



### Greybox

A empresa fornece apenas as credenciais de um operador ou um terceiro. Com isso o teste será executado para descobrir o que aquele perfil de usuário pode acessar dentro da empresa.



### Whitebox

A equipe de pentests recebe todas as informações sobre a topologia da rede e também conta com credenciais de acesso a sistemas e aplicações para avaliar vulnerabilidades em todo o ambiente.

A IBLISS conta com uma equipe de profissionais com alto nível de expertise que se mantém atualizada de todas as metodologias e usa como referências padrões de mercado. Todos os resultados são entregues no GAT, que se mantém à disposição da equipe todo o detalhamento técnico das vulnerabilidades, recomendações específicas para correção, suporte e indicadores de segurança.

