



# Teste de Intrusão

**Penetration Testing interno e externo em infraestrutura de rede e sistemas.**

## Parceiros Tecnológicos:

### **McAfee**

Maiores informações sobre a McAfee® e seus produtos podem ser encontradas em:

[www.McAfee.com/br](http://www.McAfee.com/br)



Maiores informações sobre a Check Point® e seus produtos podem ser encontradas em:

[www.checkpoint.com](http://www.checkpoint.com)



Maiores informações sobre a SonicWALL e seus produtos podem ser encontradas em:

[www.sonicwall.com](http://www.sonicwall.com)



Maiores informações sobre a VM Ware® e seus produtos podem ser encontradas em:

[www.vmware.com](http://www.vmware.com)

Uma empresa não saberá se está segura se não testar o seu ambiente computacional. O Penetration Testing, ou teste de intrusão permite conhecer os passos de um atacante potencial (hacker, cracker, etc.) e descobrir se seria possível que o mesmo obtivesse sucesso em seus ataques.

Com o teste de intrusão é possível conhecer as vulnerabilidades do ambiente, sistemas, infraestrutura (firewalls, wi-fi, roteadores, etc) e pessoas (engenharia social).

É importante saber ainda que parte dos acessos não autorizados a informações ocorrem como consequência de falhas humanas (ex: senhas fracas, revelação de informações sigilosas), todos os dias surgem novas vulnerabilidades, e por isso um sistema nunca será 100% seguro.

## **Escopo Inicial**

Será realizada a auditoria conhecida como grey-box, onde o auditor conhece parte da estrutura do cliente, e o cliente conhece as atividades a serem realizadas pelo auditor.

No início do projeto será realizada uma reunião inicial, para obtenção de informações iniciais sobre a estrutura do cliente, e a definição dos alvos a serem testados pelo auditor. É importante que o cliente já tenha definido quais os equipamentos a serem testados nesta primeira reunião.

Os testes serão realizados em duas etapas, sendo elas:

## **Testes de Intrusão Externos**

Serão realizados ataques externos nos endereços de IP informados pela Empresa Contratante, de forma a explorar possíveis vulnerabilidades nos serviços disponíveis.

Esses ataques serão compostos pelas seguintes atividades:

- Obtenção de informações básicas

## Metodologia

Baseada nas normas ISO 27001, OSSTMM e CSD/NIST para testes de intrusão, a metodologia pode ser consolidada nos seguintes domínios principais:

- Planejamento
- Coleta de informações
- Mapeamento de Rede (LAN/WAN)
- Identificação de vulnerabilidades
- Intrusão
- Escalação de Privilégio
- Relatório

**OSSTMM:** O *Open Source Security Testing Methodology Manual* é uma metodologia aberta para realização de testes de segurança. O OSSTMM foca em detalhes técnicos para a realização de testes e na medição dos resultados.

**CSD/NIST:** Divisão de Segurança Computacional do Instituto Nacional de Padrões e Tecnologia (EUA).

**ISO 27001:** Norma que define Sistema de Gestão de Segurança da Informação, e recomenda objetivos de controle e controles para minimizar riscos de segurança.

- Fingerprinting (descoberta de informações sobre a estrutura e serviços)
- Descoberta de vulnerabilidades
- Servidores
  - DNS
  - Web
  - FTP
  - POP / SMTP / IMAP
  - VPN / SSH / Terminal Services / Metaframe
  - Regras do firewall
- Tentativa de acesso a roteadores
- Tentativa de acesso a bancos de dados
- Captura de senhas
- Testes de intrusão em sistemas web disponíveis externamente

Ataques que puderem resultar em negação de serviço ou qualquer outro tipo de parada em servidores serão agendados previamente com os administradores dos sistemas, com possibilidade de execução em final de semana ou no horário que a Empresa Contratante sugerir.

Opta-se por realizar ataques intrusivos (que podem causar invasão real ou negação de serviço) por se tratarem de testes onde o auditor age da mesma forma que um possível atacante agiria em caso de situação real de intrusão.

Com base nos resultados a Empresa Contratante conhecerá suas fragilidades e poderá criar os controles de segurança necessários para minimizar o risco de invasão.

Será verificada a existência de vulnerabilidades em access-points (redes sem fio) que possam ser acessadas externa ou internamente na sede da Empresa Contratante.

## Testes de Intrusão Internos

Serão testados servidores, estações e outros equipamentos da estrutura da rede com o objetivo de obter acesso a informações controladas.

Serão testados todos os roteadores e switches gerenciáveis da empresa.

Serão realizados testes de intrusão em aplicações web disponíveis na rede interna.

Serão realizados testes de segurança nos servidores de banco de dados e dispositivos mobile.

Ataques de *man in the middle* (ARP Spoofing, captura de informações trafegando na rede) e tentativas de burlar firewall e proxy para a saída de informações também serão executados.

Além do conhecimento dos auditores serão utilizadas normas de controles de segurança do DoD (Departamento de Defesa dos EUA) e NIST (National Institute of Standards and Technology), e diversas ferramentas com os objetivos listados abaixo:

- Port Scanners (varredura de portas)
- Avaliação de vulnerabilidades
- Testes de intrusão de rede
- Quebra de senhas
- Análise de protocolos
- Spoofing (o atacante faz-se passar por uma máquina autorizada)

- Obtenção de pacotes de rede

## **Pré-Requisitos**

No início do projeto serão solicitadas as seguintes informações:

- Diagrama da rede do cliente
- Endereços IPv4 dos equipamentos a serem testados

Essas informações são imprescindíveis para o início do trabalho.

## **Produto Final (Delivery)**

Como produto final será apresentado à Empresa Contratante o relatório de auditoria com os testes realizados, vulnerabilidades encontradas e recomendações de melhoria.

A estrutura do relatório irá se assemelhar à seguinte:

- Sumário executivo
- Escopo
- Sumário técnico dos ataques
- Fragilidades/vulnerabilidades encontradas
- Recomendações
- Anexos