# Etapas de um Pentest



As etapas de um ***pentest*** são fases de preparação, planejamento e execução**.** Antes de iniciar um ***pentest***, é necessário que o cliente esteja a par de todo o processo para que não haja nenhuma falha de comunicação entre as partes. É necessário conhecer os objetivos do negócio do cliente no que diz respeito ao teste de invasão: se esse é o primeiro teste de invasão, o que o levou a procurar esse serviço? Quais as exposições que ele mais teme? Existe algum dispositivo frágil com o qual deveremos ter cuidado ao efetuar os testes?

## 1. Preparação

Nessa fase é necessário decidir o **escopo** do teste de invasão: quais endereços de IP serão incluídos nos testes e quais não serão, quais tipos de ações o cliente permitirá que sejam realizados durante o teste, permissões para desativar potencialmente determinado serviço, limitar a avaliação a simplesmente uma análise de vulnerabilidades, etc. O cliente pode solicitar que os testes sejam realizados somente em determinados dias e durante horários específicos.

## 2. Coleta de Informações

Nesta fase será analisada livremente as fontes de informações disponíveis, um processo conhecido como coleta de ***OSINT*** (Open Source Intelligence (https://pt.wikipedia.org/wiki/OSINT), ou dados de fontes abertas). Essa pesquisa é realizada através de motores de busca, como o Google, Bing e Yahoo, redes sociais e demais fontes de informações públicas como registro de domínio.

## 3. Mapeamento de Rede

O DNS (Domain Name System, ou sistema de nomes de domínio) é um sistema de gerenciamento de nomes hierárquico e distribuído para computadores, serviços ou qualquer recurso conectado à Internet ou em uma rede privada. Através do DNS é possível descobrir a topologia da rede, endereços de IP e a quantidade de computadores na rede interna.

## 4. Enumeração de Serviços

Utilizando ferramentas específicas, uma varredura de portas abertas é realizada nas máquinas descobertas e nos IPs informados com o fim de descobrir quais sistemas estão presentes na Internet ou na rede interna, bem como quais ***softwares*** estão sendo executados.

## 5. Análise de Vulnerabilidades

Tendo conhecimento das portas, softwares instalados e sistemas ativos, é iniciado o processo de análise de vulnerabilidades utilizando ***scanners*** e banco de dados de vulnerabilidades no auxílio em detectar falhas nos ativos do cliente que possam a vir, através da execução de ***exploits*** (códigos específicos para exploração de falhas), permitir o acesso à rede e computadores.

## 6. Exploração de Falhas

Esta é a fase onde executamos os ***exploits*** nas vulnerabilidades detectadas na fase anterior, como por exemplo: acessar remotamente uma máquina sem a necessidade de autenticação através de login e senha ou por meio de tentativas de autenticação com senhas padrão em determinados sistemas.

## 7. Pós-Exploração de Falhas

Nesta fase são reunidas informações sobre o sistema invadido, busca por arquivos relevantes ao teste de invasão, a criação de ***backdoors*** para posteriores acessos ao sistema, ampliar a exploração da rede ganhando assim acesso à demais máquinas / sistemas que não estavam visíveis na tentativa inicial de escaneamento da rede.

***Tipos de Pentest → (http://www.auzac.com.br/testes-de-invasao/tipos-de-pentest/)***