****

**Visão**

Com a crescente demanda sobre Tecnologias, percebemos que muitas pessoas apesar de buscarem informações, não possuem fontes que queiram realmente passar o conhecimento da maneira como ela deve ser, livre e com embasamento técnico que permita ser aplicado e utilizado quando necessário, além de serem testados em sua criação, tornando esta informação útil e confiável.

**Missão**

O Laboratório foi criado com a intenção de buscar e disseminar o conhecimento de uma maneira clara e objetiva, de forma gratuita, auxiliando na evolução dos membros e da sociedade na qual estas informações são compartilhadas, buscando o crescimento de todos os envolvidos nesta criação de valores.



Caso você pense que com a leitura dos materiais da How2Security, você irá se tornar um Cracker capaz de invadir sistemas, se você espera encontrar aqui scripts infalíveis para invasão e, a partir deles, sair por aí invadindo computadores, essa não é a leitura indicada. Indicamos, sim a leitura do Código Penal (Lei 2.848/1940), principalmente a Lei Carolina Dickmann (Lei 12.737/2012), nos Artigos 154-A e 154-B.

*154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:*

*Pena – Detenção, de 3 meses a 1 ano, e multa*

Este material é um conjunto de informações compiladas de documentos e ferramentas do Mundo Underground testadas em ambiente de laboratório na nossa intranet. Desta forma, todo conhecimento aqui condensado é tangível, assim como as orientações das contramedidas.

Dessa forma, esperamos ter sido bem claros que, em momento algum, estamos com a pretensão de ensinar a você como se tornar um invasor. Estaremos sim, mostrando muitas das técnicas utilizadas pelos crackers e, em alguns casos, pelos scripts kiddies, para que você, como administrador de redes, seja capaz de identificá-las em tempo hábil para se defender, antes que alguém com desejos menos nobres ô faça por você.

Assim sendo, todo o conteúdo dessa literatura tem apenas o objetivo didático de informar e preparar os administradores de redes dos novos tempos. Em momento algum nos responsabilizamos pelo mau uso desse conhecimento ou por danos causados em seu equipamento ou de terceiros, assim como também não somos responsáveis pelos códigos e ferramentas aqui citados.

Sandro Melo

Adaptado por Wellington Silva aka Well

**ÍNDICE**

[0 – Pen-Test (Penetration Testing – Teste de Invasão) 4](#_Toc485568760)

[1 – Teste de Invasão vs Análise de Vulnerabilidade 4](#_Toc485568761)

[2 – Teste de Invasão em Aplicações Web 5](#_Toc485568762)

[3 – Metodologias Existentes 5](#_Toc485568763)

[4 – Tipos de Teste de Invasão 6](#_Toc485568764)

[4.1 – Black Box (Caixa Preta) 6](#_Toc485568765)

[4.2 – White Box (Caixa Branca) 6](#_Toc485568766)

[4.3 – Gray Box (Caixa Cinza) 7](#_Toc485568767)

[4.4 – Double Blind (DuploCego) 7](#_Toc485568768)

[5 – Escopo do Teste de Invasão 7](#_Toc485568769)

[6 – Escopos Devido a Compliance (Normas, Padrões) 9](#_Toc485568770)

[7 – Fases do Teste de Invasão 10](#_Toc485568771)

[7.1 – Reconnaissance (Reconhecimento) 12](#_Toc485568772)

[7.2 – Scanning (Varreduras) 12](#_Toc485568773)

[7.3 – Gaining Access (Ganhando Acesso) 13](#_Toc485568774)

[7.4 – Maintaining Access (Mantendo Acesso) 13](#_Toc485568775)

[7.5 – Covering Tracks (Limpando os Rastros) 14](#_Toc485568776)

[7.6 – Denial of Service (Recusa de Serviço – DoS/DDoS/RDDoS) 14](#_Toc485568777)

[8 – Categorias de Teste de Invasão 15](#_Toc485568778)

[8.1 – Server Side Attack (Ataque do Lado Servidor) 15](#_Toc485568779)

[8.2 – Client Side Attack (Ataque do Lado Cliente) 15](#_Toc485568780)

[8.3 – Inside Attack (Ataque Interno) 15](#_Toc485568781)

[8.4 – Outside Attack (Ataque Externo) 16](#_Toc485568782)

[9 – Tipos de Vetores de Ataque 16](#_Toc485568783)

[10 – Tipos de Hacking 17](#_Toc485568784)

[11 – Referências 18](#_Toc485568785)

# 0 – Pen-Test (Penetration Testing – Teste de Invasão)

Os **Testes de Invasão/Intrusão** (aka **TDI**) vão além de uma simples **Análise de Vulnerabilidades**, para identificar as vulnerabilidades e verificar se as vulnerabilidades são reais ou um falso positivo.

Um teste de invasão pode ser definido como o processo de identificação, enumeração, varredura e buscar explorar vulnerabilidades utilizando um conjunto de técnicas dentro de uma metodologia objetiva simulando de forma controlada o **modus operandi** de um potencial invasor e não se limitando somente a ataques lógicos, sendo possível e previamente definido no escopo até mesmo realizar testes de engenharia social em equipes estratégicas da organização, desta forma verificaria as vulnerabilidades reais que expõe os sistemas em risco e poder mensurar os riscos ao negócio.

Os testes de invasão mais eficazes são os que visam um sistema específico, com um objetivo bem definido. A possibilidade de sucesso e a qualidade do teste serão altíssimas. Enumerar um único sistema durante um teste de invasão direcionado revela mais sobre a real segurança, e também revela o tempo de resposta a incidentes que seu cliente tem.

Escolhendo cuidadosamente alvos valiosos, um teste de invasão poderá comprometer toda a infraestrutura de segurança associado ao risco de um alvo valioso.

É importante lembrar que todos testes de invasão estão limitados por três fatores: recursos empresariais, tempo acordado e habilidade técnica do profissional.

# 1 – Teste de Invasão vs Análise de Vulnerabilidade

É muito comum o erro de achar que o teste de segurança denominado Análise de Vulnerabilidade seria a mesma coisa de realizar um Teste de Invasão. É necessário enfatizar que o teste de segurança de análise de vulnerabilidade é o procedimento de identificar potenciais vulnerabilidades, normalmente executado a partir de um scanner customizado que busca correlacionar potenciais vulnerabilidade com registros de segurança em sites como o BID (http://www.securityfocus.com), CAN/CVE (http://www.mitre.org), OSDBV (http://www.osdbv.org) entre outros.

Dessa forma por não ser o objetivo explorar as possíveis falhas e sim gerar um relatório pontual que em muitos casos podem ainda conter Falsos Positivos**(1)** ou Falso Negativos**(2)**, não tendo por objetivo ganhar acesso, ou seja, verificar até onde uma vulnerabilidade é realmente uma ameaça.

Todavia o processo de teste de invasão é uma forma mais objetiva, que vai utilizar o teste de segurança e análise de vulnerabilidade como recurso. Mais buscará avaliar as vulnerabilidades identificadas, uma-a-uma, objetivando ter certeza até onde são falsos positivos ou reais possibilidades de ameaças.

1. Falso Positivo: é quando o pacote é notificado como intrusivo, mas na verdade é somente um falso alerta, alarme falso.
2. Falso Negativo: é quando um pacote passa sem ser notificado como intrusivo, mesmo que ele seja intrusivo, porém o pacote passa como um fluxo normal, na minha opinião os mais perigosos.

# 2 – Teste de Invasão em Aplicações Web

Aplicação Web é qualquer aplicativo que usa um **Browser Web** (Navegador Web) como cliente. As aplicações Web pode ser um simples fórum de discussão ou um aplicativo com múltiplos cálculos complexos.

As aplicações web são populares pela facilidade de uso e acesso, além do gerenciamento centralizado da aplicação Web que é utilizado por vários clientes.

As aplicações Web são o tipo de aplicação mais utilizado dentro de qualquer organização. Eles são o padrão para a maioria das aplicações baseadas na Internet. Se você olhar os Smartphones ou Tablets, você vai descobrir que a maioria das aplicações nesses dispositivos também são aplicações Web. Isso criou uma superfície muito ampla de novos ataques que exploram esses sistemas e um rico mercado para os profissionais de segurança da informação.

# 3 – Metodologias Existentes

Temos inúmeras metodologias relacionadas a pen-test. Podemos citar algumas das mais importantes aqui, tais como:

* OSSTMM (Open Source Security Testing Methodology Manual – Manual de Metodologuia de Testes de Segurança em Código Aberto);
* OWASP (Open Web Application Security Project – Projeto Aberto para Segurança em Aplicações Web);
* NIST 800-115 (National Institute of Standards and Tecnology – Instituto Nacional de Padrões e Tecnologia) e;
* PTES (Penetration Testing Execution Standard – Padrão de Execução de Teste de Intrusão).

O PTES tem sete fases distintas: interação pré-contrato, coleta de inteligência, modelagem de ameaças, análise das vulnerabilidades, exploração, pós-exploração e geração de relatórios. Existem duas fases no PTES que não existem no OSSTMM, mas que não deixam de existir de forma separada, que são interação pré-contrato que separamos em dois documentos ***0001 – Contrato de Pen-Test*** e ***0002 – NDA – Acordo de Confidencialidade***. A outra fase que separamos é a geração de relatórios que separamos em ***0003 – Relatório do Pen-Test***.

Cada contrato seguirá essas fases até certo ponto, mas um pen-test experiente vai passar de uma fase para a próxima tranquilamente e relativamente sem problemas.

O maior benefício do uso de uma metodologia é que ela permite que os pen-tester avaliem um ambiente de forma holística e consistente.

Porém apenas uma nos interessa que é a **OSSTMM (Open Source Security Testing Methodology Manual)**. A OSSTMM é uma metodologia originalmente desenvolvida por Peter Herzong da ISECOM, e que hoje conta com vários colaboradores espalhados pela Internet, uma vez que se trata de uma metodologia aberta.

Nessa metodologia as premissas para a realização dos testes são:

* O teste deve ser conduzido exaustivamente;
* O teste deve contemplar todos os itens necessários;
* O escopo do teste não deve ferir os direitos humanos;
* Os resultados devem ser quantificáveis;
* Os resultados devem ser consistentes;
* Os resultados devem conter apenas o que foi obtido com os testes.

Essas são as premissas de um teste de intrusão. Ainda em acordo com a **OSSTMM**, o resultado final deve conter os seguintes tópicos:

* Data Hora dos testes;
* Tempo de duração dos testes;
* Analistas e pessoas envolvidas;
* Tipos do teste;
* Escopo do teste;
* O resultado da enumeração;
* Margem de erro;
* Quantificação do risco;
* Qualquer tipo de erro ou anomalia desconhecida.

# 4 – Tipos de Teste de Invasão

Há basicamente 4 (quatro) tipos de teste de invasão. Esses tipos seguem passos lógicos para a realização dos testes.

O primeiro passo é identificar o status de início do projeto. O termo mais comum definido no estado inicial do projeto é **Black Box** (Caixa Preta), em seguida temos a **White Box** (Caixa Branca), também temos uma mistura entre branco e preto conhecido como **Gray Box** (Caixa Cinza). E o quarto tipo é o **Double Blind**.

## 4.1 – Black Box (Caixa Preta)

Assume que o pen-tester não tem nenhum conhecimento prévio do alvo, não conhece a rede, os processos da empresa, os serviços oferecidos. Iniciando um projeto de Black Box requer grande quantidade de dados de reconhecimento por parte do pen-tester. Este é o cenário mais real, pois um atacante malicioso passaria um longo período para fazer o reconhecimento sobre o alvo antes de lançar seu ataque.

Como profissionais de segurança, encontramos alguns problemas quando utilizamos a metodologia Black Box. Um deles é a falta de foco inicial, com base nisto e na familiaridade do pen-tester com o meio ambiente do alvo, pode ser difícil de estimar quanto tempo a fase de reconhecimento vai durar. Isso geralmente apresenta um problema de faturamento. Os clientes, na maioria dos casos, não estão dispostos a assinar um cheque em branco para o pen-tester gastar tempo e recursos ilimitados na fase de reconhecimento, no entanto, se você não gastar tempo suficiente no reconhecimento seu teste de invasão acabou antes mesmo de começar.

Também seria irrealista porque um atacante motivado, não terá o mesmo escopo, ou restrição de orçamento. Por isso, é recomendado fazer sempre um Gray Box.

Neste caso em vez de cobrar hora/homem o ideal é cobrar um preço fechado e nos próximos serem cobrado por hora/homem.

## 4.2 – White Box (Caixa Branca)

Assume que o pen-tester tem conhecimento íntimo sobre os sistemas que serão testados. Nesta metodologia os objetivos são claramente definidos e os resultados do relatório normalmente esperado. O pen-tester tem os detalhes do alvo, tais como informações sobre a rede, o tipo de sistema, processos da empresa e serviços oferecidos.

Teste White Box tipicamente são focados em um objetivo de negócio, tais como a necessidade de conformidade (**compliance**), em vez da avaliação genérica, e pode ser um teste mais curto, dependendo do ambiente alvo (um ou mais servidores, ou uma ou mais aplicações em um único servidor).

Como aqui reduzimos a coleta de informações, como o reconhecimento naturalmente tem menos custo para os serviços de teste de invasão.

## 4.3 – Gray Box (Caixa Cinza)

Aqui temos um equilíbrio ente o White e Black Box. O cliente concorda em fornecer algumas informações e deixa outras para serem descobertas durante os testes, permitindo que o pen-tester pule algumas partes do reconhecimento. O pen-tester tem alguns detalhes básicos sobre o alvo, como: endereçamento da rede ou do serviço alvo, uma conta de acesso a aplicação para validar as permissões, controle de sessões, etc.

Atacantes reais coletam muitas informações sobre um alvo antes de atacar (com exceção dos **script kiddies** ou indivíduos que fazem download de ferramentas de teste e simplesmente atacam), eles não escolhem vítimas aleatória. Os atacantes motivados tendem a interagir de alguma forma com seu alvo antes de tentar um ataque.

Gray Box é uma opção atraente para muitos profissionais de segurança que realizam os testes de invasão, porque imita abordagens do mundo real de ataque. Aqui o pen-tester se concentra muito mais nas vulnerabilidades em vez de reconhecimento.

## 4.4 – Double Blind (DuploCego)

Aqui temos uma situação para o pen-tester igual ao do Back Box, a grande diferença está na equipe de administradores do ambiente a ser testado, desconhecer que será realizado os testes. Desta forma, serão testa não apenas os ambientes, mais as pessoas que cuidam desse ambiente como os SysAdmins, equipe de segurança da informação e resposta a incidente. Esse é o tipo de teste mais realista, mas não tão eficiente e com um alto grau de impacto.

# 5 – Escopo do Teste de Invasão

O escopo do trabalho de Pen-Test define a forma como o serviço será iniciado e executado. Aqui devemos definir bem o escopo do teste de invasão para que possamos focar no reconhecimento do ambiente do cliente, definindo os limites, assim evitando coletas desnecessárias, saindo fora do escopo. Desta forma podemos evitar também atrasos no prazo definido em contrato.

Por outro lado, atacantes reais não têm limites, tais como tempo, financeiro, ético ou ferramentas utilizadas, que limitam o âmbito do teste de invasão, com isso, podendo não representar um cenário do mundo real.

Outra preocupação é referente aos horários que serão feitos os ataques, pois atacantes reais podem atacar a qualquer momento e provavelmente quando as pessoas menos esperam.

Para podemos atender da melhor forma o escopo do teste de invasão, devemos criar procedimentos bem definidos como os que seguem:

* **Definição dos Sistemas Alvos** 🡪 Isto especifica quais sistemas são alvos dos testes de invasão, incluindo a localização na rede, tipos de sistemas e uso comercial desses sistemas.
* **Prazos** 🡪 Quando os testes de invasão serão iniciados e finalizados atingindo as metas especificadas. A melhor prática é não limitar o escopo de tempo para o horário comercial. Por isso, questione se os testes serão feitos apenas em horário comercial, ou tem preferência por outros horários.
* **Metas** 🡪 Qual a metodologia que será usado, quais explorações não serão permitidas, qual é o risco associado com os métodos de testes permitidos, qual o impacto se as metas forem atingidas? Por exemplo, pode ser utilizado redes sociais? Engenharia social, se passando por funcionário? Ataques de negação de serviços poderão ser feitos? Podemos utilizar a vulnerabilidade em servidores para servir como repositório de scripts (Bot Net interna)? Alguns métodos de teste de invasão podem representar um risco.
* **Ferramentas e Softwares** 🡪 Quais as ferramentas e softwares que serão usados durante o teste de invasão. Isso é importante e um pouco controverso. Quando são utilizadas ferramentas comerciais isso não é problema, porém, muitos pen-testers criam suas próprias ferramentas, e com isso, estão entregando seus segredos para os clientes. Além disso, documentar os comandos utilizados para explorar a vulnerabilidades é uma boa prática, para que possa ser recriado o ataque e melhor entendido pelo cliente.
* **Partes Envolvidas** 🡪 Quem irá fazer os testes de invasão? Quem no lado cliente está ciente dos testes e pode responder em caso de indisponibilidade durante o teste (aqui é importante que seja alguém que não implique na segurança ou resposta a incidente)? Os sistemas a serem testados estão todos dentro da infraestrutura do cliente ou envolve infraestrutura de terceiros? Quem responderá pelos serviços hospedados em terceiros?
* **Nível de Acesso Inicial 🡪** Qual o nível de acesso as informações no **Kick-Off** do pen-test? Os testes serão feitos pela Internet, ou na Intranet? O pen-tester terá um acesso inicial com usuário e senha na infraestrutura do cliente (por exemplo, em rede sem fio, ou no sistema a ser testado)? A metodologia usada será igual para todos os alvos, ou será uma metodologia para cada alvo?
* **Definição dos Serviços Alvo 🡪** Aqui definimos quais serão os serviços alvo do pen-test, por exemplo, em um servidor podemos ter mais de uma aplicação, porém os testes têm como alvo um dos sistemas, o teste pode ser direcionado para um sistema web de vendas, porém neste servidor temos uma aplicação utilizada pelo departamento de RH e esse não pode ser tocado. Isso nunca é bom, pois avaliar apenas uma aplicação em um ambiente que tenha mais aplicações sendo executada, pode gerar um falso negativo, pois o sistema de vendas pode não ser vulnerável, porém em conjunto com outras aplicações se torna vulnerável, gerando um ataque combinado.
* **Definindo Áreas de Operação Críticas 🡪** Definir sistemas críticos que não pode ser tocado pelo pen-tester, podendo causar um impacto aos negócios do cliente e trazendo uma visão negativa dos testes de invasão. É importante ressaltar que isso não retrata a realidade de um ataque real.
* **Integrável 🡪** É importante definir o quanto o pen-test pode comprometer um sistema ou um processo. E entregar o que foi prometido. Nessa parte devemos deixar claro quais são as responsabilidades. Por exemplo, devemos deixar claro no contrato o seguinte: “Cabe a How2Sec o levantamento, análise, exploração e elaboração do relatório relativos ao teste de intrusão; correções, ajustes, atualizações e re-testes não fazem parte do escopo desta atividade”.
* **Autorização 🡪** Defina um documento de autorização onde o cliente autoriza a execução do pen-test. Inclusive a autorização dos provedores terceiros. **NUNCA INICIE O PEN-TEST SEM ESSE DOCUMENTO**, pois se o cliente disser que você não estava autorizado (na hipótese de algo der errado), você não terá respaldo jurídico.
* **Confidencialidade 🡪** Outro ponto importante, é a total confiabilidade entre as partes envolvidas. É sempre recomendável a assinatura de um **NDA (Non Disclosure Agreement ou Nothing Disclosure Agreement)**, em suma, nada pode ser declarado em relação ao pen-test. Ao assinar o NDA você garante que não vai expor os dados obtidos com o pen-test, assim como o cliente não divulgará seu relatório para empresas terceiras. Neste documento possui clausulas de multas para ambas as partes em caso de descumprimento do acordo.
* **Termo de Pagamento 🡪** Defina claramente qual o valor que deverá ser pago, quando e como. Crie uma clausula caso a empresa não pague na data combinada o valor de multas por atrasos. Podemos trabalhar com dois modelos de pagamentos. O primeiro cobra o valor hora/homem, definindo um valor da sua hora de consultoria e calcule baseado no tempo dos testes. Por exemplo, pen-test de 80 horas com o valor de R$ 300,00 a hora devemos cobrar R$ 24.000,00 (80 \* 300). O segundo é cobrar um valor fixo, onde acordamos com o cliente um valor para a execução dos testes independente do tempo como um valor fechado de R$ 30.000,00 (geralmente usado em pen-test black box).
* **Produto Final 🡪** Qual o tipo de relatório esperado pelo cliente, um relatório executivo ou técnico, ou ainda ambos. A quem se destina o relatório final, ou ainda, quem terá acesso a esse relatório. É importante entregar um relatório de exemplo ou atualizações periódicas para que não haja surpresas no relatório final.
* **Remediações 🡪** As vulnerabilidades exploradas devem ser documentadas com possíveis ações de remediações. Também devemos ter alguém que possa ser notificado se um sistema ficar inutilizado durante um pen-test. Quando detectados dados confidenciais quem deve ser alertado. As remediações não são as correções, deixe isso claro.

# 6 – Escopos Devido a Compliance (Normas, Padrões)

Alguns escopos de pen-test são definidos por Normas e Padrões exigido pelo mercado de atuação do cliente (**compliance**). Nestas normas e padrões são exigidas auditorias de segurança constantes para certificar que a empresa tem competência para atuar no mercado.

Nas auditorias de segurança trabalha-se com padrões de mercado sendo regras obrigatórias (Standards) ou como boas práticas de mercado que são um conjunto de normas com um nível mínimo aceitável de segurança.

Algumas normas conhecidas são:

* **ISO 27.001/27.002** 🡪 Padrões voltado para a gestão da segurança da informação, publicado em 2013.
* **Basileia II** 🡪 Acordo de Capital de Basileia criado pelo Comitê de Supervisão Bancária de Basileia em 2004, fixando 3 pilares e 29 princípios básicos sobre contabilidade e supervisão bancária.
* **PCI-SSC (Payment Card Industry - Security Standards Council)** 🡪 Foi fundada pelas principais bandeiras de cartão de crédito como um fórum global para a disseminação de padrões de segurança na proteção de dados de pagamento e define o PCI-DSS (PCI Data Security Standard).
* **PCI-DSS (Payment Card Industry - Data Security Standard)** 🡪 Especifica recomendações mínima de segurança obrigatória para todas as empresas que participam da rede de captura de pagamento com cartões, o comércio, e prestadores de serviços que processam, armazenam e/ou transmitem eletronicamente dados do portador do cartão de crédito.
* **ITIL (Information Technology Infrastructure Library)** 🡪 É uma biblioteca das melhores práticas de TI, cobrindo todos os aspectos de gerenciamento de serviços de TI.
* **COBIT (Control Objectives For Information and Related Technology)** 🡪 É outra boa prática de mercado referente ao controle da tecnologia da informação e áreas relacionadas, com responsabilidade do grupo de diretores e gerencia executiva.
* **NIST 800 Series** 🡪 É um guia de recomendações de gerenciamento de risco da tecnologia da informação do National Institute of Standards and Organization.
* **HIPAA (Health Insurance Portability and Accountability Act)** 🡪 É uma lei para incluir simplificação administrativa e abuso de saúde e fraudes, que em sua maior parte focada em questões que diz respeito à privacidade das informações de saúde do paciente.

O pen-test é o método de atacar as vulnerabilidades do sistema de forma semelhante a um atacante real, e são utilizados quando esgotou os investimentos de segurança e ainda assim o cliente está buscando verificar se todas as vias de seguranças foram cobertas.

Também não podemos confundir teste de invasão (pen-test) com análise de vulnerabilidade. Um teste de invasão irá confirmar se as vulnerabilidades são exploráveis e qual o grau de risco associado a vulnerabilidade. Já a análise de vulnerabilidade apenas aponta possíveis vulnerabilidades, e não que elas realmente são exploráveis. As análises de vulnerabilidades buscam informações de versões de sistemas e aplicações e comparam com uma base de dados de vulnerabilidade, isso pode causar muitos falsos positivos ou falsos negativos.

Antes de mais nada devemos entender claramente a real necessidade do cliente e o que ele espera do pen-test. Algumas perguntas que podemos fazer ao nosso cliente são:

1. Ele quer o pen-test porque vai lançar um novo produto?
2. Ele quer o pen-test para saber o nível de maturidade da segurança dos produtos/rede?
3. Ele quer saber se os investimentos em segurança (em dispositivos e hardware) estão atendendo e se o investimento dele está em direcionado?
4. Ele quer cumprir algum dos compliance ou normas citadas acima?

# 7 – Fases do Teste de Invasão

Em um pen-test, temos uma serie de fases, onde em cada fase temos determinadas operações a serem realizadas.

O que vai definir a diferença de um teste de invasão e um ataque realizado por um atacante real, são justamente as intenções, o escopo e o espaço de tempo disponível para a realização do teste.

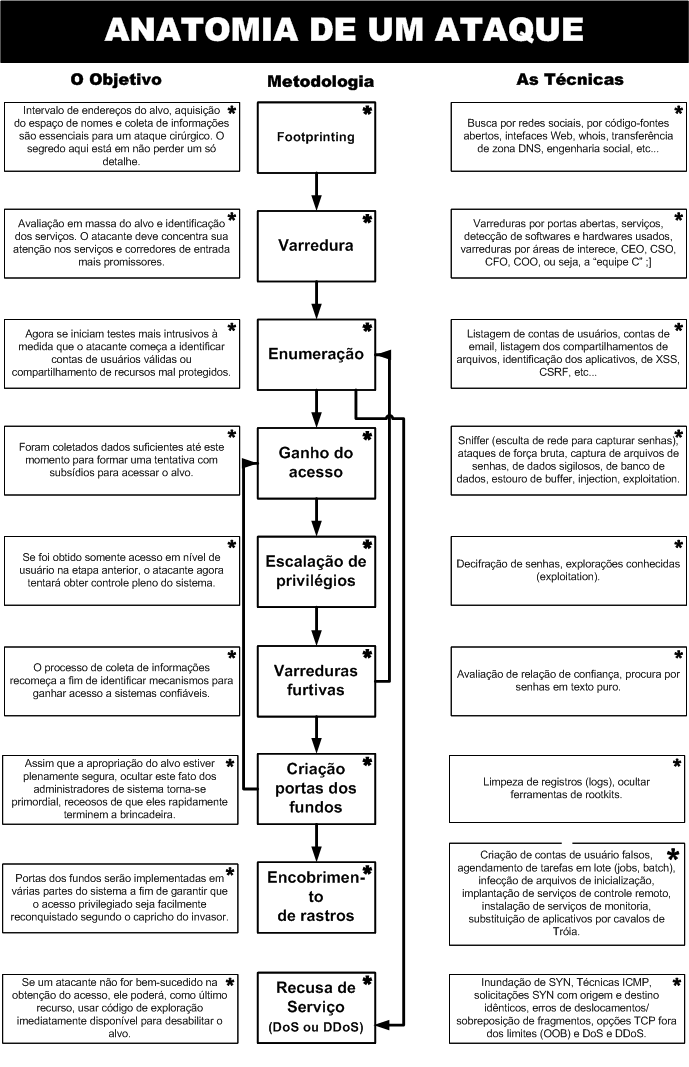
As 5 principais fases de um teste de invasão são**:** Reconnaissance (Reconhecimento), Scanning (Varredura), Gaining Access (Ganhando Acesso), Maintaining Access (Mantendo Acesso) e Covering Tracks (Limpando os Rastros).



Figura 01 – Fases do Teste de Invasão

Porém eu gosto de trabalhar com uma anatomia que serve para qualquer teste de invasão, esta anatomia foi extraída do livro **Hackers Expostos 2º Edição**, e que adaptei para os dias de hoje.

Nesta anatomia de um ataque temos o fluxo do ataque facilitando a visualização, porém, todas as fases apresentadas na anatomia se encontram dentro das 5 fases que iremos trabalhar.



## 7.1 – Reconnaissance (Reconhecimento)

Essa é a fase mais importante de um ataque, e de um teste de invasão.

Você deve aprender o máximo possível sobre o ambiente de um alvo e seus colaboradores antes mesmo de lançar um ataque. Quanto mais informações você conseguir sobre seu alvo, maior será as chances de sucesso, achando os caminhos mais fáceis para obter o sucesso nos testes de invasão.

Os testes de invasão Black Box requerem um tempo considerável, pois os dados não são fornecidos.

A fase do reconhecimento envolve uma pesquisa apurada que inclui pesquisas na Internet que contenha informações sobre o alvo, tais como, os recursos de monitoramento, pessoas e processos, desenhos de infraestrutura, endereços IP atribuído ao alvo externo e interno, tipos de sistemas, engenharia social, serviços públicos, helpdesk, portas abertas para o mundo, onde estão hospedados esses serviços, serviços oferecidos para os clientes e fornecedores do alvo, entre outros.

É um serviço de inteligência, onde o maior número de informação irá gerar melhores resultados.

Qualquer informação que seja vinculado ao alvo é considerado de valor nessa primeira fase:

* Concorrentes
* Nome de funcionários
* Endereços físicos e lógicos
* Telefones (principalmente dos departamentos de RH, TI, Financeiro, etc.)
* Fornecedores
* Comunidades sociais
* Empresas do mesmo grupo
* Definir aplicativos e uso comercial
* Identificar tipos de sistemas
* Identificar portas disponíveis
* Identificar serviços em execução
* Informações capturadas de dados com engenharia social passivamente e ativamente
* Descoberta de documentos

## 7.2 – Scanning (Varreduras)

Nesta fase o pen-tester busca informações mais detalhadas do alvo, que possam revelar os vetores de ataque e enxergar as possibilidades que podem permitir ganhar acesso ao sistema, através da exploração de alguma falha encontrada.

Nesta fase buscamos as vulnerabilidades nas informações que foram colhidas na fase anterior (de reconhecimento). Por exemplo, no reconhecimento você descobre que existe um serviço na porta 80, que executa um serviço web, na fase de varredura você terá que identificar se o servidor web contém uma vulnerabilidade, ainda no exemplo, o alvo utiliza o Apache 1.3, e esta versão tem vulnerabilidades publicadas, porém seu serviço não acaba por aqui, existe outros dispositivos na frente do Servidor Apache vulnerável como IDS/IPS/WAF?

Então nesta fase devemos buscar respostas para algumas perguntas:

* Qual sistema operacional o alvo utiliza?
* Quais os serviços estão sendo executados no alvo?
* Quais serviços estão disponíveis para acesso?
* Quais as versões de cada serviço sendo executado?
* Há IDS/IPS na rede?
* Há honeypots na rede?
* Há firewalls na rede?
* Existe uma rede interna e outra externa, como DMZ?
* Há serviços com acesso público sendo executado em alguma máquina interna?
* Há algum software malicioso sendo executado em alguma máquina?
* Existem fraquezas no que foi encontrado?
* Identificou as vulnerabilidades?
* Descobriu documentos com informações sobre as vulnerabilidades?

A partir dessas informações, o pen-tester pode buscar maiores detalhes na internet ou fóruns especializados em busca de exploit que permitam explorar falhas existentes nas versões dos serviços sendo executados.

## 7.3 – Gaining Access (Ganhando Acesso)

Nesta fase exploramos as vulnerabilidades encontradas nas fases anteriores. É aqui que separamos o pen-test da análise de vulnerabilidades e da Auditória. Pois aqui, iremos explorar as falhas reais provando que a vulnerabilidade deu acesso ao sistema do alvo, tirando todos os falsos positivos e falsos negativos.

Nesta fase devemos ter a autorização expressas do alvo, pois aqui implica nas questões legais, sem autorização dos proprietários dos ativos se torna crime.

Aqui o pen-tester coloca em prática tudo que planejou baseado nas informações obtidas nas fases anteriores.

Dependendo de seus vetores de ataque, ele pode realizar uma série de ataques buscando ganhar acesso ao sistema alvo, por exemplo:

* Ataques de força bruta local
* Ataques de força bruta remoto
* Captura de tráfego de rede
* Ataque de engenharia social
* Ataque as aplicações Web
* Ataque as redes wireless
* Exploração de serviços
* Exploração de sistema operacional
* Atacar outros sistemas ou aplicações (cuidado aqui, tem que ter acordado antes).
* Descobrir contas com poderes em sistemas e rede
* Obter acesso escalado no nível de sistema e rede
* Acessar outros sistemas com as contas com privilégios escalados.

## 7.4 – Maintaining Access (Mantendo Acesso)

Após conseguir o acesso, o atacante busca, de alguma forma, manter o acesso conseguido através de seus ataques. Isso normalmente é utilizado para pivotar (rotear) para outras máquinas que não teríamos acesso direto, porém isto, deve ser feito com extremo cuidado.

O risco de configurar o sistema, implantando uma backdoor ou outro tipo de dispositivo que permita o acesso posterior, é que a ferramenta utilizada pode voltar-se contra você, pois outras pessoas podem descobrir e explorá-la e ganhar acesso facilmente ao sistema comprometido.

Portanto, essa fase, quando realizado durante o pen-test, precisa de extremo cuidado e planejamento para não trazer comprometimento e prejuízos desnecessários ao alvo.

Para evitar isso, podemos criar contas administrativas, túneis criptografados (VPN, SSH), ou outro novo canal de acesso seguro, como conexões ponto a ponto.

## 7.5 – Covering Tracks (Limpando os Rastros)

Outro aspecto importante está na remoção de evidências da invasão. Isso fará com que seja mais difícil de detectar os ataques, reduzindo a reação das barreiras de segurança, feita por dispositivos de detecção de ataque. Remover as evidências inclui apagar usuários falsos, mascarar os canais de acesso existentes, remover os vestígios de adulteração como mensagens de erros causadas pelo pen-test e log do sistema e serviços do alvo.

Como pen-tester tem autorização para realizar os testes, não é necessário apagar os rastros. Isso se torna importante para um pen-tester, apenas se quiser testar, também, a capacidade da equipe de perícia forense e resposta a incidentes de descobrir o que foi feito e recuperar informações alteradas (tem que ser acordado com o cliente).

* Estabelecer vários métodos de acesso à rede alvo.
* Apagar usuários falsos
* Remover evidências de acesso autorizado (registros de log).
* Remover evidências de acesso não autorizados (registros de log)
* Sistemas de reparo impactados pela exploração.
* Injetar dados falsos, se necessário.
* Esconder métodos de comunicação por meios de criptografia.

## 7.6 – Denial of Service (Recusa de Serviço – DoS/DDoS/RDDoS)

Os ataques de Recusa de Serviço (DoS, DDoS, RDDoS) custam às empresas milhões de dólares a cada ano, sendo uma ameaça séria a qualquer sistema ou rede. Esses custos estão relacionados a tempo de sistema fora do ar, perda de receita e o trabalho físico envolvido em identificar e reagir aos ataques.

Essencialmente um ataque de DoS interrompe ou nega completamente serviços a usuários legítimos, redes, sistemas ou outros recursos. O objetivo de tais ataques é normalmente de natureza mal-intencionada e muitas vezes exigem pouca habilidade, pois, as ferramentas que os possibilitam são facilmente encontradas.

Muitas vezes, a segurança da rede ou sistema alvo rechaçará um atacante com menor habilidade. Sentindo-se frustrado e impotente, este atacante lançará um ataque de DoS como seu último recurso. Além da frustação, há indivíduos que têm rixas pessoais ou políticas contra alguém ou alguma organização. Outro motivador tem sido o hacktivism’s e o cyberterrorisms, feito como forma de protesto e demonstração de força, pois os ataques de DoS lhes dão a sensação de poder que o DoS lhes proporcionam. Por exemplo, você com uma arma na cintura teria coragem de ir até uma das fronteiras do Estados Unidos e tentar indisponibilizar seus serviços essenciais? E atrás de um computador lançar um ataque do tipo “apontar e dar um clique” e deixar serviços públicos on-line indisponíveis.

Contudo os hackers habilidosos abominam ataques DoS e as pessoas que as realizam.

Neste contexto, onde entra a parte do pen-tester?

Sim algumas empresas contratam proteção de terceiros (em sua maioria as operadoras) para protegerem seus ativos, ou ainda elas investiram pesados em dispositivos de detecção e prevenção de ataques DoS/DDoS, e desejam que os pen-tester faça os testes para assegurar que estão seguros contra esse ataque. Ou ainda, testar a capacidade de seus links e servidores.

# 8 – Categorias de Teste de Invasão

Podemos dividir em duas categorias de dispositivos e duas categorias de origem dos ataques. As categorias de ataques a dispositivos são: ataques no lado do servidor e ataques no lado cliente. Agora as categorias de origem dos ataques temos: ataques interno e ataques externos. Em um ataque sempre teremos a junção de uma categoria de dispositivo com uma categoria de origem.

Por exemplo, um ataque interno aos servidores, temos a junção das categorias Server Side Attack com a Inside Attack.

## 8.1 – Server Side Attack (Ataque do Lado Servidor)

Ataque ao servidor, foca na tentativa de explorar serviços que estão em um determinado dispositivo. Normalmente não precisam de interação do usuário e provê uma shell remota para o atacante.

São exemplos de ataques a servidores:

* Ataques a serviços (Web, DNS, SMTP, etc.)
* Ataques a aplicativos (Aplicativos Web, aplicativos de acesso remoto, etc.)
* Ataque de força bruta

## 8.2 – Client Side Attack (Ataque do Lado Cliente)

Ataque ao cliente aqui se refere às estações de trabalho (workstation), neste caso nosso foco vai para as aplicações que rodam nos computadores clientes e que normalmente precisam de uma interação da pessoa para que o ataque seja executado.

São exemplos de ataques ao cliente:

* Exploração no Browser (Internet Explorer, Firefox, Safari, Chrome, etc.)
* Exploração de falhas de editores de texto
* Exploração de falhas de clientes de e-mail
* Exploração de falhas em leitores de documentos (PDF, JPG, etc.)
* Exploração de falhas em programas reprodutores de vídeos
* Exploração Humana (Engenharia Social, Phishing)

Nesses casos, o cliente precisa visitar um site, ou abrir um e-mail, abrir um arquivo, uma imagem, um vídeo, que executará um código malicioso ou irá baixar algum malware.

## 8.3 – Inside Attack (Ataque Interno)

Ataque internos originados dentro dos perímetros de segurança da organização. Esses ataques costumam ser feitos para avaliar as questões de segurança interna da organização, que envolve além das questões técnicas, as questões de segurança física (portaria, fiscalização, guardas, monitoria por câmeras, etc.), compliance (politicas, processos, procedimentos, normas, etc.) e dispositivos tecnológicos que colaboram para o ganho de segurança (firewall, IDS/IPS, antivírus, controle de acesso biométrico, portas e fechaduras, acesso aos dispositivos de conexão de rede, etc.).

Essa categoria de ataque permite ao atacante um maior acesso aos recursos de rede.

Temos os seguintes tipos de Insides:

* **Pure Inside** 🡪 Colaborador genuíno da empresa
  + Tem autorização de acesso físico;
  + Tem acesso na rede local (Login);
  + Tem possibilidades de elevar seus privilégios;
  + Podem ser colaboradores ou contratação temporária;
  + Pessoas gananciosas ou desapontadas.
* **Inside Associate** 🡪 Terceiros contratados
  + Tem autorização de acesso físico limitado;
  + Não tem acesso direto a rede local (Login);
  + Muitas vezes faz hora extra;
  + Potencialmente é um espião;
  + Procurar sempre por papeis expostos com informações de acesso aos sistemas;
  + Presta serviços de Manutenção, Portaria, Limpeza ou Guardas.
* **Inside Affiliate** 🡪 Prestadores de serviços, clientes, namorado (a), etc...
  + Estão conectados aos colaboradores;
  + Tem acesso de visitante;
  + Tem cartão de acesso ou números de acesso;
  + Pegam emprestado equipamentos da organização;
  + Atua pesado na engenharia social;
  + Usam de meios ilegais para obter as informações.

## 8.4 – Outside Attack (Ataque Externo)

Ataques externos originados de fora dos perímetros de segurança da organização. Seus ataques estão concentrados na Internet ou conexões de acesso remoto. Essa categoria de ataque costuma ser feitos para avaliar as questões de segurança externa da organização, que envolve além das questões técnicas, as questões de informações sigilosas exposta ao mundo, fragilidades nas senhas dos colaboradores, nível de segurança aplicada eu seus sistemas expostos na Internet, e o quanto comprometeria sua estrutura interna.

Qualquer um com acesso à Internet pode ser um atacante externo.

# 9 – Tipos de Vetores de Ataque

Muitos dos vetores de ataque utilizados pelos atacantes estão em problemas nas seguintes áreas:

* **Sistemas Operacionais** 🡪 Muitos administradores apenas instalam os sistemas operacionais e deixam os sistemas operacionais de forma padrão, além de não aplicaram as atualizações necessárias para sanar as falhas encontradas, resultando em potenciais vulnerabilidades a serem exploradas.
* **Aplicação** 🡪 Normalmente os desenvolvedores não fazem os testes necessários em seus aplicativos. Os motivos normalmente são questões de prazo, e que além de desenvolver testar essa aplicação gera um custo que ninguém costuma pagar. Além disso, os clientes também não fazem os testes necessários e muitas das vezes também não atualizam esses aplicativos, resultando em potenciais vulnerabilidades.
* **Códigos Compactos ou Envelopados** 🡪 Programas com features extras onde os usuários podem customiza-los através de programação como macros ou através de aplicativos que expande as funcionalidades através de plug-ins. Esses aplicativos podem ser usados como exploit do sistema. Muito utilizado como Phishing.
* **Falta de Configuração** 🡪 Sistemas que estão mal configurados, ou simplesmente foram colocados para uso sem ter configurado nenhum item de segurança, principalmente esses dispositivos plug-and-play, de uso extremamente fácil, como, os roteadores wireless.

# 10 – Tipos de Hacking

O pen-tester tem diferentes métodos para testar a segurança dos ativos de uma organização durante a simulação dos testes de invasão. Os métodos mais comuns são:

* **Remote Network (Rede Remota)** 🡪 Os testes de rede remoto simula o ataque vindo pelo Internet. O pen-tester procura vulnerabilidades do lado de fora da rede alvo, transpassando as defesas de acesso à rede, como firewalls, proxy ou vulnerabilidades em roteadores.
* **Remote Dial-Up Network (Redes Discadas)** 🡪 Este tipo de ataque simula uma intrusão ao banco de modem da organização. Antigamente se utilizava a PSTN (Rede Pública de Telefonia) para fazer o acesso a rede interna, hoje em dia essa tecnologia foi substituída por VPN (Redes Virtuais Privadas) que se utilizam de protocolos de padrão aberto, e que tem o mesmo princípio dos acessos discados, porém utiliza a Internet com tuneis criptografados.
* **Local Network (Rede Local)** 🡪 Este tipo de ataque simula um ataque interno (de um colaborador, um fornecedor ou um suposto cliente). Aqui o atacante tem acesso físico aos dispositivos, mesmo sem autorização. Dando algumas vantagens para o atacante em ganhar esses acessos.
* **Stolen Equipment (Roubo de Equipamento)** 🡪 Este tipo de ataque simula um roubo de notebook de um colaborador. Neste ataque a intensão é conseguir o máximo de informações (principalmente as que não deveriam estar no notebook) para que o atacante possa comprometer de alguma forma o alvo. Aqui o atacante procura por nome de usuário, senhas, configurações de segurança e criptografia utilizadas (se utilizada).
* **Social Engineering (Engenharia Social)** 🡪 A engenharia social verifica a integridade dos colaboradores da organização usando telefone ou a comunicação face-a-face para reunir informações para usar em um ataque. Os ataques de engenharia social podem ser usados para adquirir nomes de usuários, senhas, ou outras informações sobre a segurança da organização.
* **Physical Entry (Entrada Física)** 🡪 O ataque de entrada física tenta comprometer as instalações físicas da organização. Um atacante que obtém acesso físico pode plantar vírus, trojans, rootkits, keylogger ou um hardware comprometido (keylogger 🡪 dispositivo físico ou software usado para gravar teclas digitadas), diretamente sobre os sistemas na rede do alvo.

# 11 – Referências

**Referências Bibliográficas**

**[1]** MUNIZ, JOSEPH and LAKHANI, AAMIR – Web Penetration Testing with Kali Linux, 2013, Birmingham – Mumbai, Packet Publishing.

**[2]** GRAVES, KIMBERLY – CEH – Official Ethical Hacker Review Guide, Indianapolis - Indiana, 2007, Wiley Publishing Inc.

**[3]** STUTTARD, DAFYDD and PINTO, MARCUS – The Web Application Hacker’s Handbook, Indianapolis - Indiana, 2º Edition, Wiley Publishing Inc.

**[4]** SCAMBRAY, JOEL, McCLURE, STUART and KURTZ, GEORGE – Hackers Expostos Segredos e Soluções para a Segurança de Redes, São Paulo, 2001, MAKRON Books Ltda.

**[5]** Pen-test Standard – Disponível em: <http://www.pen-test-standard.org/index.php/Main\_Page>, Acessado em: 24/02/2012.

**[6]** MELO, Sandro – Exploração de Vulnerabilidades – Em Redes TCP/IP, Rio de Janeiro, 2006, Alta Books Ltda.

**[7]** MONTORO, Rodrigo – Disponível em: <http://spookerlabs.blogspot.com/2012/01/introducao-ao-snort-serie-snortando.html>, Acessado em: 25/02/2012.

**[8]** DUFFY, Christopher – Aprendendo Pen-test com Python – Utilize scripts Python para executar pen-tests eficazes e eficientes, 1º Ed, São Paulo, 2016, Editora Novatec.