



# TÉCNICAS DE INVASÃO

Copyright © 2018 de Bruno Fraga.

Todos os direitos desta edição reservados à Editora Labrador.

*Coordenação editorial*

Erika Nakahata

*Preparação de texto*

Leonardo do Carmo

*Projeto gráfico, diagramação e capa*

Maurelio Barbosa

*Revisão*

Maurício Katayama

Dados Internacionais de Catalogação na Publicação (CIP)

Angélica Ilacqua CRB-8/7057

Fraga, Bruno

Técnicas de invasão : aprenda as técnicas usadas por hackers em invasões reais / Bruno Fraga ; compilação de Thompson Vangller. – São Paulo : Labrador, 2019.

296 p.

ISBN 978-65-5044-019-0

1. Hackers 2. Computadores – Medidas de segurança 3. Redes de computadores – Medidas de segurança I. Título II. Vangller, Thompson.

19-2005

CDD 005.8

Índice para catálogo sistemático:

1. Computadores : Técnicas de invasão

## **Editora Labrador**

Diretor editorial: Daniel Pinsky

Rua Dr. José Elias, 520 – Alto da Lapa

05083-030 – São Paulo – SP

Telefone: +55 (11) 3641-7446  
[contato@editoralabrador.com.br](mailto:contato@editoralabrador.com.br)  
[www.editoralabrador.com.br](http://www.editoralabrador.com.br)  
[facebook.com/editoralabrador](http://facebook.com/editoralabrador)  
[instagram.com/editoralabrador](http://instagram.com/editoralabrador)

A reprodução de qualquer parte desta obra é ilegal e configura uma apropriação indevida dos direitos intelectuais e patrimoniais do autor.

A editora não é responsável pelo conteúdo deste livro.

O autor conhece os fatos narrados, pelos quais é responsável, assim como se responsabiliza pelos juízos emitidos.



Hello, friend!

# AGRADECIMENTOS



À minha filha, Alice, que me deu todo o impulso para chegar até aqui. Aos meus pais, que me criaram com carinho e amor. À minha esposa, Beatriz, por sempre me apoiar e perder várias noites de sono comigo. E ao Bruno Fraga, por ter aparecido em minha vida como um coelho branco que eu decidi seguir.

*Thompson Vangller*

*Aluno e compilador do livro, com base no Treinamento*

- Morpheus:** Finalmente. Bem-vindo, Neo. Como você deve ter imaginado, eu sou Morpheus.
- Neo:** É uma honra conhecê-lo.
- Morpheus:** Não, a honra é minha. Por favor, venha. Sente-se. Eu imagino que deva estar se sentindo um pouco como Alice. Escorregando pela toca do coelho... Hum?
- Neo:** É, eu acho que sim.
- Morpheus:** Vejo isso em seus olhos. Você é um homem que aceita o que vê, porque pensa estar sonhando. Ironicamente, não está muito longe da verdade. Você acredita em destino, Neo?
- Neo:** Não.
- Morpheus:** Por que não?
- Neo:** Porque eu não gosto da ideia de não poder controlar a minha vida.
- Morpheus:** Eu sei exatamente o que quer dizer. Deixe que eu diga por que está aqui. Está aqui porque sabe de alguma coisa, uma coisa que não sabe explicar, mas você sente. Você sentiu a vida inteira que há alguma coisa errada com o mundo... você não sabe o que é, mas está ali, como uma farpa em sua mente, deixando-o louco. Foi essa sensação que o trouxe a mim. Você sabe do que eu estou falando?
- Neo:** Matrix?
- Morpheus:** Você quer saber o que é Matrix? Matrix está em toda parte. Está à nossa volta. Mesmo agora, nesta sala aqui. Você a vê quando olha pela janela ou quando liga a televisão. Você a sente... quando vai trabalhar, quando vai à igreja, quando paga seus impostos. É o mundo que acredita ser real para que não perceba a verdade.
- Neo:** Que verdade?
- Morpheus:** Que você é um escravo, Neo. Como todo mundo, você nasceu em cativeiro. Nasceu numa prisão que não pode ver, sentir ou tocar. Uma prisão... para a sua mente. Infelizmente, não se pode explicar o que é Matrix. É preciso que veja por si mesmo. Esta é a sua última chance. Depois disto, não haverá retorno.
- [Morpheus abre a mão esquerda, revelando a pílula azul.]
- Morpheus:** Se tomar a pílula azul, fim da história. Vai acordar em sua cama e acreditar no que você quiser.

[*Morpheus abre a mão direita, revelando a pílula vermelha.*]

**Morpheus:** Se tomar a pílula vermelha, fica no País das Maravilhas, e eu vou mostrar até onde vai a toca do coelho.

[*Neo pega a pílula vermelha.*]

**Morpheus:** Lembre-se – eu estou oferecendo a verdade, nada mais.

[*Neo toma a pílula vermelha.*]

**Morpheus:** Venha comigo.

*The Matrix – Adentrando a Toca do Coelho*

# COMENTÁRIOS DO COMPILADOR



Construí esta obra a partir das videoaulas do curso online Técnicas de Invasão e de pesquisas realizadas na internet. As informações coletadas de fontes externas foram modificadas para melhor entendimento do leitor. A citação da fonte pode ser encontrada no rodapé da página.

O propósito desta obra é o de servir como um guia à introdução de Pentest, podendo ser utilizado também como um manual de consulta para realizar ataques clássicos.

O que realmente espero é que o leitor entenda a essência dos acontecimentos e o modo como o atacante pensa, pois as metodologias e ferramentas utilizadas podem mudar com o tempo, já que, todos os dias, novas atualizações de segurança surgem e novas vulnerabilidades são descobertas.

## Sobre o *Técnicas de Invasão*

O Técnicas de Invasão é um projeto idealizado por Bruno Fraga. O objetivo do projeto é conscientizar o leitor sobre os riscos e ameaças existentes no mundo virtual e oferecer cursos altamente desenvolvidos para introdução de testes de invasão.

Apresenta, de modo inteligente e organizado, todo o processo de uma invasão, desde o princípio, e ensina passo a passo as metodologias e técnicas clássicas utilizadas por hackers. Além disso, busca alertar o aluno sobre riscos, apresentando dicas de proteção e pensamentos de hackers maliciosos.

## O que há neste livro?

Este livro cobre as metodologias e técnicas clássicas empregadas por hackers, utilizando ferramentas do Kali Linux e outras ferramentas disponíveis na web, como o Shodan, Censys, Google Hacking etc.

## Quem deve ler este livro?

Este livro é destinado a profissionais de segurança da informação, administradores de sistemas, engenheiros de software, profissionais de TI que buscam o conhecimento em técnicas de invasão, curiosos e pessoas que desejam iniciar uma carreira em TI.

## O que é necessário para realizar os testes?

Para aprender de maneira eficiente todo o conhecimento que o livro apresenta e realizar os testes, é necessário ter:

- uma máquina virtual/física com o sistema operacional Kali Linux;
- uma máquina virtual/física com o sistema operacional Windows;
- uma máquina virtual/física com o sistema operacional Metasploitable;
- acesso à internet.

Recomenda-se, também, que o leitor tenha conhecimento básico de comandos Linux.

## Observação

Cuidado com as aplicações dos conhecimentos ensinados neste livro, pois o uso de muitas ferramentas, técnicas e metodologias ensinadas aqui pode levar à prisão do indivíduo que as executou.

Realize os testes em um ambiente em que você seja o responsável e tenha controle, por exemplo, utilizando máquinas virtuais, rede LAN, seu IP público e domínio.

Na criação deste livro, o uso dessas ferramentas não infringiu nenhuma lei.

# SUMÁRIO

1. SEGURANÇA DA INFORMAÇÃO
2. CONCEITOS BÁSICOS DE REDE
3. CONHECER
4. COLETANDO INFORMAÇÕES
5. ANALISAR
6. ANÁLISE DE VULNERABILIDADES
7. PRIVACIDADE
8. SENHAS
9. CANIVETE SUÍÇO (NETCAT)
10. METASPLOIT
11. ATAQUES NA REDE
12. EXPLORANDO APLICAÇÕES WEB

# APÊNDICES

- A. RUBBER DUCKY - HAK5
- B. COMMANDS LIST - NMAP - NETWORK MAPPER
- C. CÓDIGOS DE STATUS HTTP
- D. CÓDIGOS DE STATUS ICMP



# 1

## CAPÍTULO SEGURANÇA DA INFORMAÇÃO



Segurança da informação<sup>1</sup> está relacionada à proteção de um conjunto de dados, no sentido de preservar o valor que esses dados possuem para um indivíduo ou uma organização.

São características básicas da segurança da informação os atributos de *confidencialidade*, *integridade* e *disponibilidade*, não estando essa segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados.

O conceito de segurança de computadores está intimamente relacionado ao de segurança da informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.

Atualmente, o conceito de segurança da informação está padronizado pela norma ISO/IEC 17799:2005, influenciada pelo padrão inglês (British Standard) BS 7799. A série de normas ISO/IEC 27000 foi reservada para tratar de padrões de segurança da informação, incluindo a complementação ao trabalho original do padrão inglês. A ISO/IEC 27002:2005 continua sendo considerada formalmente como 17799:2005 para fins históricos.

## Conceitos

A segurança da informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa; isto é, aplica-se tanto às informações corporativas como às pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isso, ser estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem a utiliza, pelo ambiente ou infraestrutura que a cerca, ou por pessoas mal-intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

A triade CIA (confidentiality, integrity and availability) – *confidencialidade, integridade e disponibilidade* – representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Outros atributos importantes são a *irretratabilidade* e a *autenticidade*.

Com o evoluir do comércio eletrônico e da sociedade da informação, a privacidade também se tornou uma grande preocupação.

Os atributos básicos (segundo os padrões internacionais) são os seguintes:

**Confidencialidade** – propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

**Integridade** – propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).

**Disponibilidade** – propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

O nível de segurança desejado pode se consubstanciar em uma *política de segurança* que é seguida pela organização ou pessoa, para garantir que, uma vez estabelecidos os princípios, aquele nível desejado seja perseguido e mantido. Para a montagem dessa política, deve-se levar em conta:

- riscos associados à falta de segurança;
- benefícios;
- custos de implementação dos mecanismos.

## Mecanismos de segurança

O suporte para as recomendações de segurança pode ser encontrado em:

**Controles físicos** – são barreiras que limitam o contato ou acesso direto à informação ou à infraestrutura (que garante a existência da informação) que a suporta. Há mecanismos de segurança que apoiam os controles físicos: portas, trancas, paredes, blindagem, guardas etc.

**Controles lógicos** – são barreiras que impedem ou limitam o acesso à informação que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta à alteração não autorizada por elemento mal-intencionado.

Há mecanismos de segurança que apoiam os controles lógicos. São eles:

**Mecanismos de criptografia** – permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para isso algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.

**Assinatura digital** – um conjunto de dados criptografados, associados a um documento com a função de garantir sua integridade.

**Mecanismos de garantia da integridade da informação** – usando funções de “Hashing” ou de checagem, um código único é gerado para garantir que a informação é íntegra.

**Mecanismos de controle de acesso** – palavras-chave, sistemas biométricos, firewalls e cartões inteligentes.

**Mecanismos de certificação** – atestam a validade de um documento.

**Integridade** – medida em que um serviço/informação é genuíno(a), isto é, está protegido(a) contra a personificação por intrusos.

**Honeypot** – é o nome dado a um software cuja função é a de detectar ou de impedir a ação de um cracker, de um spammer, ou de qualquer agente externo estranho ao sistema, enganando-o e fazendo-o pensar que está de fato explorando uma vulnerabilidade daquele sistema.

Há hoje em dia um elevado número de ferramentas e sistemas que pretendem fornecer segurança. Alguns exemplos são os detectores de intrusões, antivírus, firewalls, filtros antispam, fuzzers, analisadores de código etc.

## Ameaças à segurança

As ameaças à segurança da informação são relacionadas diretamente à perda de uma de suas três características principais:

**Perda de confidencialidade** – ocorre quando há uma quebra de sigilo de uma determinada informação (por exemplo, a senha de um usuário ou administrador de sistema), permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários.

**Perda de integridade** – acontece quando uma determinada informação fica exposta a manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação.

**Perda de disponibilidade** – ocorre quando a informação deixa de estar acessível para quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, decorrente da queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção.

## Aspectos legais<sup>2</sup>

A segurança da informação é regida por alguns padrões internacionais que são sugeridos e devem ser seguidos por corporações que desejam aplicá-la em suas atividades diárias.

Algumas delas são as normas da família ISO 27000, que rege a segurança da informação em aspectos gerais, tendo como as normas mais conhecidas a ISO 27001, que realiza a gestão da segurança da informação com relação à empresa, e a ISO 27002, que efetiva a gestão da informação com relação aos profissionais, os quais podem realizar implementações importantes que podem fazer com que uma empresa cresça no aspecto da segurança da informação. Há diversas normas ISO, e você pode conhecê-las no site *The ISO 27000 Directory*: [www.27000.org](http://www.27000.org).

## Segurança da informação no Brasil – direito digital

É o resultado da relação entre a ciência do direito e a ciência da computação, sempre empregando novas tecnologias. Trata-se do conjunto de normas, aplicações, conhecimentos e relações jurídicas, oriundas do universo digital. Como consequência desta interação e da comunicação ocorrida em meio virtual, surge a necessidade de se garantir a validade jurídica das informações prestadas, bem como transações, através do uso de certificados digitais.

*Marcelo de Camilo Tavares Alves<sup>3</sup>*

No Brasil, há algumas leis que se aplicam ao direito digital, como:

A *Lei 12.737/2012*, conhecida como Lei Carolina Dieckmann, que tipifica os crimes cibernéticos.

Art. 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 (três) meses a 1 (um) ano, e multa.<sup>4</sup>

Essa lei é fruto de um casuísmo, em que o inquérito policial relativo à suposta invasão do computador da atriz Carolina Dieckmann sequer foi concluído e nenhuma ação penal foi intentada (porém os acusados foram mais do que pré-julgados). A lei passa, então, a punir determinados delitos, como a “invasão de dispositivos informáticos”, assim dispondo especificamente o Art. 154-A.<sup>5</sup>

Deve-se esclarecer que a invasão, para ser criminosa, deve se dar sem a autorização expressa ou tácita do titular dos dados ou do dispositivo. Logo, o agente que realiza teste de intrusão (pentest, do inglês *penetration test*) não pode ser punido, por não estarem reunidos os elementos do crime. Caberá, no entanto, às empresas de segurança e auditoria adaptarem seus *contratos de serviços* e pesquisa nesse sentido, prevendo expressamente a exclusão de eventual incidência criminosa nas atividades desenvolvidas.

## Acordo de confidencialidade – NDA<sup>6</sup>

Um contrato NDA (*non disclosure agreement*) é um acordo em que as partes que o assinam concordam em manter determinadas informações confidenciais. Para evitar que algum dos envolvidos ou mesmo terceiros tenham acesso a essas informações e as utilizem indevidamente, é possível firmar um NDA.

A principal vantagem desse acordo é a de diminuir as chances de que dados críticos a uma organização ou projeto sejam divulgados, já que um NDA define penalidades para quem descumpre as cláusulas de confidencialidade.

Além disso, um NDA facilita o “caminho jurídico” a ser tomado caso ocorra o vazamento de informações confidenciais, economizando tempo e recursos para a sua organização e aumentando as possibilidades de ganhar causas por quebra de sigilo.

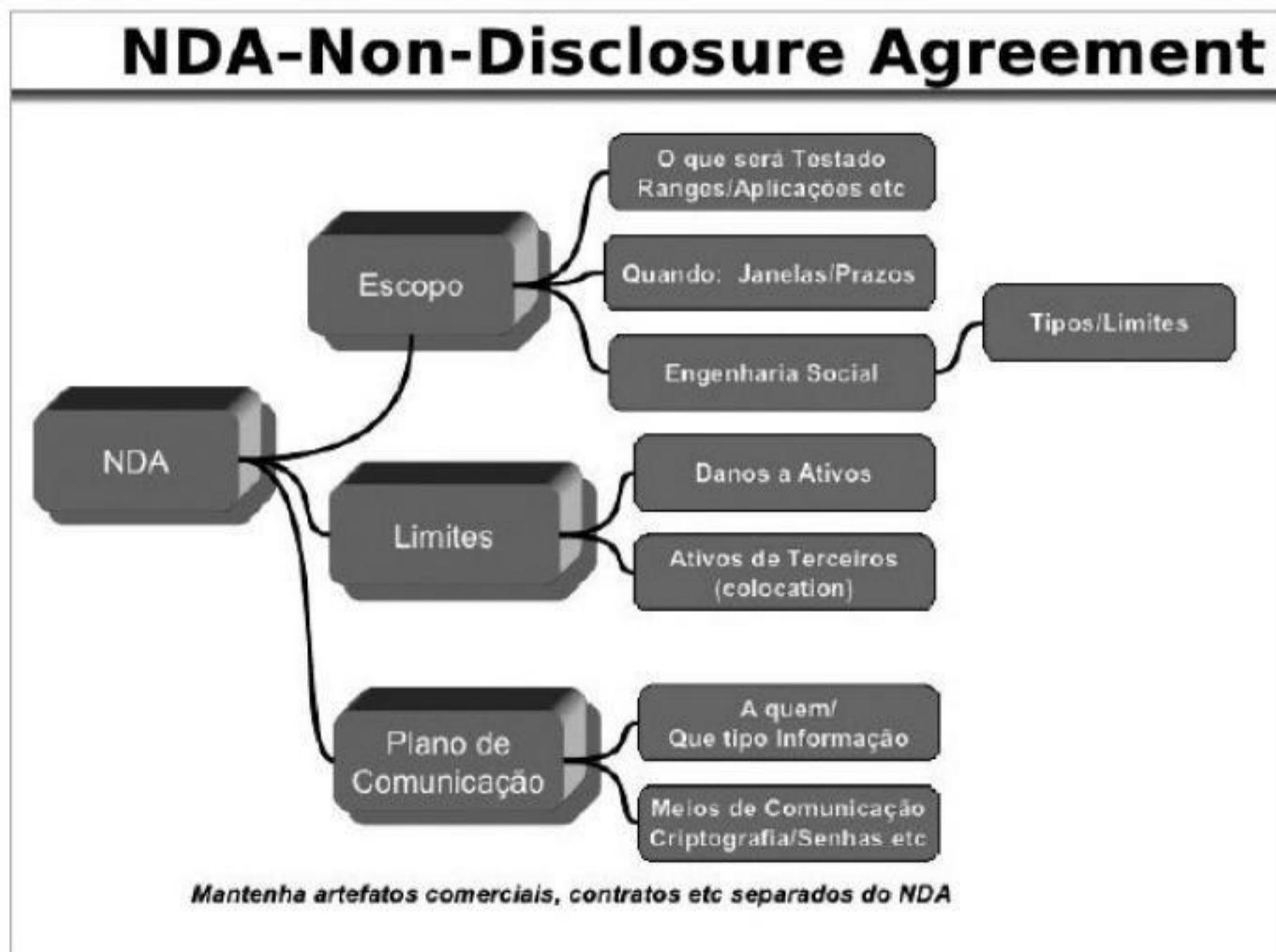
A ISO 27002 define algumas normas para serem seguidas quanto ao código de prática para a gestão da segurança da informação; para implementá-la em uma organização, é necessário que seja estabelecida uma estrutura para gerenciá-la. Para isso, as atividades de

segurança da informação devem ser coordenadas por representantes de diversas partes da organização, com funções e papéis relevantes. Todas as responsabilidades pela segurança da informação também devem estar claramente definidas.

É importante, ainda, que sejam estabelecidos acordos de confidencialidade para proteger as informações de caráter sigiloso, bem como as informações que são acessadas, comunicadas, processadas ou gerenciadas por partes externas, tais como terceiros e clientes.

## Estrutura de um acordo NDA

É de extrema importância para um analista pentest assinar um NDA, com detalhes das condições que a empresa vai disponibilizar e informações das quais esse analista tomará conhecimento.



**Escopo** – ele define o que será testado durante o processo de intrusão, quando e por quanto tempo será realizado. É importante essa definição para que ambas as partes não sejam prejudicadas. Essa importância se dá, por exemplo, porque durante um teste em

períodos de pico de uma empresa a indisponibilidade de um sistema pode causar-lhe danos financeiros.

**Limites** – a definição de limites é uma etapa crucial, pois um ataque pode causar danos em sistemas e equipamentos que podem ser irreversíveis, causando um grande prejuízo financeiro para a empresa.

**Plano de comunicação** – define quem vai receber as informações encontradas e como elas serão disponibilizadas. Essa etapa requer muita atenção devido à possibilidade de as informações que um pentest pode encontrar serem altamente sensíveis.

## Fases do processo de invasão<sup>7</sup>

As fases de um processo de invasão são basicamente divididas em três etapas:

**Conhecer** – resume-se em *coletar informações* do alvo que será invadido, através dos mais diversos meios, como coletar endereços de e-mails, pessoas que se conectam ao alvo, rastrear usuários, explorar o Google Hacking etc.

**Analizar** – a partir dos *dados coletados* na etapa anterior, vamos analisar cada dado para extrair o máximo de informação do alvo. Esta é a principal etapa para uma invasão bem-sucedida, a qual inclui, por exemplo, a realização de varredura de IP, serviços, sistema operacional, versões de serviços etc.

**Explorar** – esta etapa se resume em explorar todas as informações que foram analisadas para ganhar acesso ao alvo, como utilizar exploits, realizar ataques para quebras de senhas, engenharia social etc.

## Ética e código de conduta<sup>8</sup>

A ética é impulsionada pelas expectativas da indústria de segurança da informação sobre o comportamento dos profissionais de segurança durante seu trabalho. A maioria das organizações define essas expectativas através de códigos de conduta, códigos de ética e declarações de conduta. No caso de testes de penetração, trata-se de fazer as escolhas certas, já que usamos poderosas ferramentas que podem fornecer acesso não autorizado, negar serviços e, possivelmente, destruir dados.

Você, sem dúvida, encontrará vários dilemas que vão exigir que considere o código ético e seu raciocínio moral, apesar das suas ações. Além disso, levando em conta as consequências que discutimos previamente, após a discussão, você deve ter as ferramentas certas para tomar a melhor decisão. Todas as nossas ferramentas de pentest podem ser usadas para fortalecer a segurança e a resiliência dos sistemas, mas, de fato, em mão erradas, ou quando usadas com más intenções, podem comprometer sistemas e obter acesso não autorizado a

dados confidenciais.

Embora você queira fazer uso dessas ferramentas, deve se lembrar de que o objetivo do pentest é o de melhorar a segurança do sistema e da organização por meio das atividades. A execução de exploits e de acesso a esses recursos em sistemas que demonstram vulnerabilidades pode ser corrigida quando a extensão do problema é conhecida e compartilhada com aqueles que podem corrigi-la. Porém, se essa informação nunca chega a alguém em uma organização e se a vulnerabilidade nunca for compartilhada com o fornecedor original do software, essas questões não serão corrigidas.

Como profissionais de penetração, temos obrigações éticas e contratuais, de maneira que precisamos nos assegurar de que operamos de uma maneira que não viole esses códigos e não corrompa a confiança dessa profissão.

Para isso, é importante que você tenha o entendimento das suas ações. Para que possa entender o que é necessário para realizar testes de penetração, é importante entender o código de conduta e ética nesta área profissional. Há muito mais para saber a respeito desse tema além do que será descrito neste livro; isso é apenas o começo, a indicação do caminho por onde ir.

Para realizar os testes descritos neste livro, é necessário dispor de um ambiente de teste do qual você tenha o controle de forma legal, para que possa se divertir e aplicar todo o conhecimento disponível sem causar danos reais a uma empresa ou pessoa física.

Precisamos operar profissionalmente, assegurando que temos o conhecimento e o consentimento das partes interessadas para realizar os testes, de modo que nós não devemos realizar testes além do escopo do projeto, a menos que sejam autorizados. Sendo assim, gerencie todos os projetos com eficiência e proteja qualquer propriedade intelectual confiada a você.

Divulgue responsávelmente, compartilhando suas descobertas com as partes interessadas em tempo hábil, nunca tome decisões sozinho, sempre trabalhe em equipe e comunique a informação a quem de fato pertence e às partes interessadas. Não subestime o risco; sempre que você identificar um, não avance, pois pode causar problemas em alguma estrutura.

Conheça a diferença entre não divulgação, divulgação completa, divulgação responsável ou coordenada.

Avance na profissão, compartilhe seu conhecimento com profissionais pentesters e profissionais de segurança. Técnicas de ferramentas em testes de penetração em paralelo com a tecnologia evoluem continuamente, então, trabalhar sempre para avançar nesse campo, compartilhando a informação, é essencial para o crescimento profissional.

Use todas as ferramentas apresentadas neste livro com responsabilidade, pois de fato são ferramentas poderosas.

## EC-Council – Código de ética

Por meio do programa de certificação Ethical Hacker – CEH (Certified Ethical Hacker) –, o membro estará vinculado a esse código de ética, que é destinado a profissionais de pentest. A versão atual pode ser encontrada no site Ec-Council: [www.eccouncil.org/code-of-ethics](http://www.eccouncil.org/code-of-ethics).

Veja alguns dos principais pontos desse código de ética:<sup>9</sup>

**1. Privacidade** – mantenha privadas e confidenciais as informações obtidas em seu trabalho profissional (em particular no que se refere às listas de clientes e informações pessoais do cliente). Não cole, dê, venda ou transfira qualquer informação pessoal (como nome, endereço de e-mail, número da Segurança Social ou outro identificador exclusivo) a um terceiro sem o consentimento prévio do cliente.

**2. Propriedade intelectual** – proteja a propriedade intelectual de outras pessoas confiando em sua própria inovação e esforços, garantindo, assim, que todos os benefícios sejam adquiridos com o seu originador.

**3. Divulgação** – divulgue às pessoas ou autoridades adequadas os perigos potenciais para qualquer cliente de comércio eletrônico. Esses perigos podem incluir comunidades da internet ou o público que você acredita estar razoavelmente associado a um determinado conjunto ou tipo de transações eletrônicas, software ou hardware relacionado.

**4. Área de expertise** – forneça serviços nas suas áreas de competência, e seja honesto e direto sobre quaisquer limitações de sua experiência e educação. Certifique-se de que você é qualificado para qualquer projeto no qual você trabalha ou se propõe a trabalhar por uma combinação adequada de educação, treinamento e experiência.

**5. Uso não autorizado** – nunca use conscientemente softwares ou processos que sejam obtidos ou retidos de forma ilegal ou não ética.

**6. Atividade ilegal** – não se envolva em práticas financeiras enganosas, como suborno, cobrança dupla ou outras práticas financeiras impróprias.

**7. Autorização** – use a propriedade de um cliente ou empregador somente de maneiras adequadamente autorizadas, e com o conhecimento e consentimento do proprietário.

**8. Gerenciamento** – assegure uma boa gestão de qualquer projeto que você liderar, incluindo procedimentos efetivos para promoção de qualidade e divulgação completa de risco.

**9. Compartilhamento de conhecimento** – contribua para o conhecimento de profissionais de comércio eletrônico por meio de estudo constante, compartilhe as lições de

sua experiência com outros membros do conselho da CEH e promova a conscientização pública sobre os benefícios do comércio eletrônico.

## (ISC)<sup>2</sup> – Código de ética

O código de ética da (ISC)<sup>2</sup> aplica-se a membros desta organização e titulares de certificação como o Certified Information Systems Security Professional (CISSP).

Embora este código não seja projetado especificamente para testes de penetração, ele é extremamente simples e tem um conteúdo abrangente para cobrir a maioria das questões éticas que você vai encontrar como profissional de segurança da informação. Verifique o código completo no site [www.isc2.org/ethics](http://www.isc2.org/ethics)

Veja alguns dos principais pontos deste código de ética:

1. Proteger a sociedade, a comunidade e a infraestrutura.
2. Agir com honra, honestidade, justiça, responsabilidade e legalidade.
3. Prover um serviço diligente e competente aos diretores.
4. Avançar e proteger a profissão.

## De que lado?

Há uma discussão na área sobre qual chapéu um profissional da segurança está usando, ou seja, de que lado moral o profissional age com o conhecimento de técnicas de penetração. Normalmente, é definido como *White Hat* (Chapéu Branco), *Black Hat* (Chapéu Preto) e *Grey Hat* (Chapéu Cinza).



**White Hat** – os hackers White Hat optam por usar seus poderes para o bem. Também conhecidos como *hackers éticos*, podem ser empregados de uma empresa, ou contratados para uma demanda específica, que atuam como especialistas em segurança e tentam encontrar buracos de segurança por meio de técnicas de invasão.

Os White Hat empregam os mesmos métodos de hacking que os Black Hat, com uma exceção: eles fazem isso com a permissão do proprietário do sistema, o que torna o processo

completamente legal. Os hackers White Hat realizam testes de penetração, testam os sistemas de segurança no local e realizam avaliações de vulnerabilidade para as empresas.

**Black Hat** – como todos os hackers, os Black Hat geralmente têm um amplo conhecimento sobre a invasão de redes de computadores e a ignorância de protocolos de segurança. Eles também são responsáveis por escreverem malwares, que é um método usado para obter acesso a esses sistemas.

Sua principal motivação é, geralmente, para ganhos pessoais ou financeiros, mas eles também podem estar envolvidos em espionagem cibernética, hacktivismo ou talvez sejam apenas viciados na emoção do cibercrime. Os Black Hat podem variar de amadores, ao espalhar malwares, a hackers experientes que visam roubar dados, especificamente informações financeiras, informações pessoais e credenciais de login. Eles não só procuram roubar dados, mas também procuram modificar ou destruir dados.

**Grey Hat** – como na vida, há áreas cinzentas que não são nem preto nem branco. Os hackers Grey Hat são uma mistura de atividades de Black Hat e White Hat. Muitas vezes os hackers Grey Hat procurarão vulnerabilidades em um sistema sem a permissão ou o conhecimento do proprietário. Se os problemas forem encontrados, eles os denunciarão ao proprietário, às vezes solicitando uma pequena taxa para corrigir o problema. Se o proprietário não responde ou não cumpre com um acordo, às vezes os hackers Grey Hat publicarão online a descoberta recentemente encontrada, para todo o mundo ver.

Hackers desse tipo não são inherentemente maliciosos com suas intenções; eles estão procurando tirar algum proveito de suas descobertas. Geralmente, esses hackers não vão explorar as vulnerabilidades encontradas. No entanto, esse tipo de hacking ainda é considerado ilegal, porque o hacker não recebeu permissão do proprietário antes de tentar atacar o sistema.

Embora a palavra hacker tenda a evocar conotações negativas quando referida, é importante lembrar que os hackers não são criados de forma igual. Se não tivéssemos hackers White Hat procurando diligentemente ameaças e vulnerabilidades antes que os Black Hat possam encontrá-las, provavelmente haveria muito mais atividades envolvendo cibercriminosos que exploram vulnerabilidades e coletam dados confidenciais do que existe agora.<sup>10</sup>

## O processo de penetration test (pentest)<sup>11</sup>

Alguns anos atrás, não havia nenhum padrão para realizar o processo de *pentest*, e, com isso, quando não eram bem organizados, os processos não atingiam os objetivos propostos, devido ao descuido nos resultados, à má documentação e à má organização de relatórios.

Para solucionar esses problemas, profissionais experientes criaram um padrão chamado Penetration Testing Execution Standard (PTES), que possui sete sessões organizadas em um cronograma de engajamento.

Essas sessões cobrem um cronograma aproximado para o pentest do início ao fim. Ele inicia-se com o trabalho que começa antes de utilizar o Metasploit durante todo o caminho, até a entrega do relatório para o cliente, de forma consistente. As sessões são as seguintes:

**1. Interações de pré-engajamento** – envolvem o levantamento de pré-requisitos para o início do pentest, definem o escopo do processo de teste e desenvolvem as regras.

**2. Coleta de informações** – é a atividade associada à descoberta de mais informações sobre o cliente. Essas informações são úteis para fases posteriores do teste.

**3. Modelamento de ameaças** – a modelagem de ameaças utiliza a informação dos ativos e processos de negócio reunidos sobre o cliente para analisar o cenário de ameaças.

É importante que as informações de ativos sejam usadas para determinar os sistemas a serem direcionados para o teste e as informações de processos sejam utilizadas para determinar como atacar esses sistemas.

Com base nas informações de destino, as ameaças e os agentes de ameaças podem ser identificados e mapeados para as informações de ativos. O resultado é o modelo de ameaças que uma organização é suscetível de enfrentar.

**4. Análise de vulnerabilidades** – envolve a descoberta de falhas e fraquezas. Através de uma variedade de métodos e ferramentas de teste, você obterá informações sobre os sistemas em uso e suas vulnerabilidades.

**5. Exploração** – usando as informações de vulnerabilidades e o levantamento de requisitos realizados anteriormente, é nesta etapa que exploramos de fato as vulnerabilidades para obter acesso aos destinos. Alguns sistemas têm controle de segurança que temos que ignorar, desativar ou evitar, e às vezes é preciso tomar uma rota completamente diferente para realizar a meta.

**6. Pós-exploração** – uma vez que conseguimos o acesso a um sistema, precisamos determinar se ele tem algum valor para o nosso propósito e precisamos manter o controle sobre o sistema. A fase pós-exploração explora essas técnicas.

**7. Relatórios** – é necessário documentar o nosso trabalho e apresentar ao cliente em forma de um relatório que apoie o cliente a melhorar sua postura de segurança descoberta durante o teste.

Para mais informações acesse o site oficial do PTES: [www.pentest-standard.org](http://www.pentest-standard.org).

Além dos PTES, devemos ter ciência de outras metodologias de teste. O Instituto Nacional de Padrões e Tecnologias (NIST) produz uma série de publicações relacionadas à

segurança conhecida coletivamente como *NIST 800-115*, um guia técnico para teste de validação de segurança da informação, que foi publicado em 2008 e tem apenas uma pequena seção específica sobre testes de penetração.

O Open Source Security Testing Methodology (OSSTMM) possui um manual que foi publicado em 2010. Atualmente, há uma quarta edição em desenvolvimento, porém, para ter acesso a este manual é necessário ser membro, o que envolve a realização de alguns cursos e um programa de certificação de três níveis para essa metodologia.

O Open Web Application Security Project (OWASP) também possui um guia, o *OWASP Testing Guide v4*, cujo foco principal está em testes de segurança de aplicativos web, mas que tem um valor de grande peso em testes de penetração.

- 
1. SEGURANÇA DA INFORMAÇÃO. In: WIKIPEDIA: a enciclopédia livre. [San Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: [https://pt.wikipedia.org/wiki/Segurança\\_da\\_informação](https://pt.wikipedia.org/wiki/Segurança_da_informação). Acesso em: 14 ago. 2019.
  2. Videoaula TDI – Concepção – Aspectos Legais.
  3. ALVES, Marcelo de Camilo Tavares. Direito Digital. Goiânia, 2009, p. 3. Disponível em: <https://docero.com.br/doc/xc0vec>. Acesso em: 15 ago. 2019.
  4. BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Disponível em: [www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/l12737.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm). Acesso em: 14 ago. 2019.
  5. LEI CAROLINA DIECKMANN. In: WIKIPEDIA: a enciclopédia livre. [San Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: [https://pt.wikipedia.org/wiki/Lei\\_Carolina\\_Dieckmann](https://pt.wikipedia.org/wiki/Lei_Carolina_Dieckmann). Acesso em: 23 ago. 2019.
  6. Videoaula TDI – Concepção – Acordo de confidencialidade.
  7. Videoaula TDI – Concepção – Fases do Processo de Técnicas de Invasão.
  8. Videoaula TDI – Bootcamp – Ética e código de conduta.
  9. EC-COUNCIL. Code of ethics. Disponível em: [www.eccouncil.org/code-of-ethics](http://www.eccouncil.org/code-of-ethics). Acesso em: 14 ago. 2019.
  10. SYMANTEC. What is the difference between Black, White and Grey Hat Hackers? Disponível em: <https://community.norton.com/en/blogs/norton-protection-blog/what-difference-between-black-white-and-grey-hat-hackers>. Acesso em: 14 ago. 2019.
  11. Videoaula TDI – Bootcamp – O Processo de penetration test.



# 2

## CAPÍTULO CONCEITOS BÁSICOS DE REDE



Uma rede consiste em dois ou mais computadores ligados entre si e compartilhando dados, entre outros recursos, como impressoras e comunicação. As redes podem ser classificadas de acordo com sua extensão geográfica, pelo padrão, topologia ou meio de transmissão.

### Extensão geográfica

**Storage Area Network (SAN)** – são redes usadas para armazenamento de arquivos. Por exemplo: backups, servidores de arquivos etc.

**Local Area Network (LAN)** – são redes de alcance local, as quais podem ser redes internas de curto alcance ou redes que alcançam uma área mais elevada. Seu alcance máximo é de aproximadamente 10 km.

**Personal Area Network (PAN)** – são redes pessoais, como bluetooth.

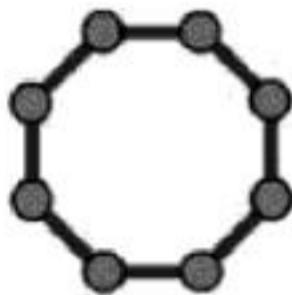
**Metropolitan Area Network (MAN)** – são redes que interligam regiões metropolitanas. Hoje em dia podem até serem confundidas com LANs devido à evolução delas.

**Wide Area Network (WAN)** – são redes de grande extensão que podem interligar redes

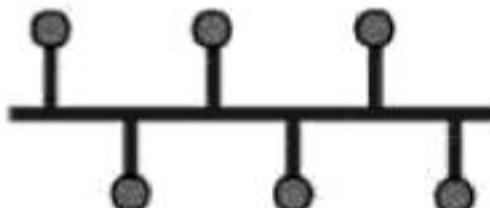
independentes; portanto, é uma rede de alcance mundial. A internet é o melhor exemplo de WAN.

## Topologia

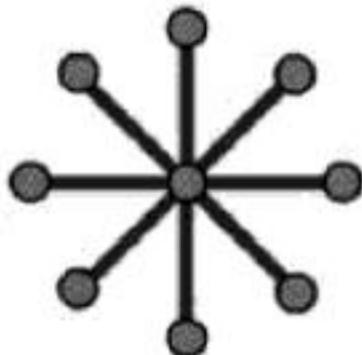
**Rede em anel** – todos os computadores são ligados a um único cabo que passa por todos eles. Um sinal circula por toda a rede e o micro que quer transmitir pega carona no sinal e transmite para o destino. Se um computador para de se comunicar, todos os outros param também.



**Rede em barramento** – todos os computadores são ligados em uma única “barra”, um cabo que recebe todos os outros e faz a transmissão dos dados. Se um dos computadores para, todos os outros param também.



**Rede em estrela** – essa topologia é a mais usada no momento, pois é a mais eficiente. Todos os computadores são ligados a um concentrador, e a facilidade de adicionar e retirar pontos a qualquer momento faz dessa topologia a mais popular. Se um computador perde a conexão, apenas ele não se comunica, não afetando o resto da rede.



**Rede em malha** – é aquela em que se juntam mais de um dos tipos anteriores em uma única rede, atualmente usada para redundância.



## Meios de transmissão

- Rede de cabo coaxial
- Rede de cabo de fibra óptica
- Rede de cabo de par trançado (UTP e STP)
- Rede sem fios
- Rede por infravermelhos
- Rede por micro-ondas
- Rede por rádio

## Compartilhamento de dados

**Cliente/servidor** – arquivos são concentrados em um único servidor, e as estações têm acesso ao servidor para buscar arquivos.

**Peer to peer** – são redes “ponto a ponto” em que os computadores se conectam uns aos outros para fazer o compartilhamento dos arquivos.

## Tipos de servidores

**Servidor de arquivos** – realiza o armazenamento, transferência e o backup dos arquivos.

**Servidor de impressão** – gerencia impressoras, fila de impressão e spool.

**Servidor de mensagens** – gerencia e-mails, mensagens ponto a ponto e conferências de áudio e vídeo.

**Servidor de aplicação** – permite que aplicativos sejam executados remotamente.

**Servidor de comunicação** – Redireciona as requisições de comunicação.

## Componentes de uma rede

**Servidor** – oferta recursos e serviços.

**Cliente** – equipamento ou software que busca por serviços.

**Estação de trabalho** – busca recursos no servidor para produtividade pessoal.

**Nó** – ponto da rede.

**Cabeamento** – estrutura física organizada para oferecer suporte físico à transmissão dos dados.

**Placa de rede** – oferece a conexão do computador com a rede.

### **Hardware de rede (ativos e passivos)**

- Hub
- Switch
- Roteador
- Gateway
- Firewall
- Transceiver

## **Comunicação de dados**

**Transmissão** – para que haja transmissão, é necessário que exista um transmissor, um receptor, um meio e um sinal.

### **Modos de operação**

- **Simplex** – apenas um canal de comunicação, a qual ocorre em apenas um sentido.
- **Half-duplex** – comunicação bidirecional, mas não simultânea.
- **Full-duplex** – comunicação bidirecional e simultânea.

## **Informações analógicas e digitais**

**Analógicas** – variam linearmente com o tempo e podem assumir valores infinitos dentro dos limites impostos.

**Digitais** – são discretas, variam apenas entre 0 e 1.

## **Transmissão em série e paralelo**

**Paralelo** – vários bytes por vez, cabos curtos, muita interferência, rápida.

**Em série** – cabos mais longos, menos interferência, apenas um cabo de comunicação.

## **Transmissão quanto ao sincronismo**

**Síncrona** – um único bloco de informações é transmitido com caracteres de controle e sincronismo.

**Assíncrona** – os bytes são transmitidos com bytes de início e fim. Não há uma cadência na transmissão. É conhecida também como transmissão start stop.

## Protocolos

São como linguagens usadas para fazer a comunicação entre estações de trabalho e os servidores. São regras que garantem a troca de dados entre transmissor e receptor.

**Características** – funcionar em half-duplex, compartilhar um mesmo meio, exigir sincronismo para comunicar, pode sofrer interferência e ocorrência de falhas.

**Tipos de protocolos** – o mais importante é o protocolo TCP/IP, mas também são utilizados o NetBeui e o IPX/SPX.

## O modelo OSI

O modelo Open Systems Interconnection (OSI) foi lançado em 1984 pela International Organization for Standardization.

Trata-se de uma arquitetura-modelo que divide as redes de computadores em sete camadas para obter camadas de abstração. Cada protocolo realiza a inserção de uma funcionalidade assinalada a uma camada específica.

Utilizando o modelo OSI é possível realizar comunicação entre máquinas distintas e definir diretrizes genéricas para a elaboração de redes de computadores independente da tecnologia utilizada, sejam essas redes de curta, média ou longa distância.

Esse modelo exige o cumprimento de etapas para atingir a compatibilidade, portabilidade, interoperabilidade e escalabilidade. São elas: a definição do modelo, a definição dos protocolos de camada e a seleção de perfis funcionais. A primeira delas define o que a camada realmente deve fazer; a segunda faz a definição dos componentes que fazem parte do modelo; e a terceira é realizada pelos órgãos de padronização de cada país.

O modelo OSI é composto por sete camadas, sendo que cada uma delas realiza determinadas funções. As camadas são:

**Aplicação (Application)** – a camada de aplicação serve como a janela onde os processos de aplicativos e usuários podem acessar serviços de rede. Essa camada contém uma variedade de funções normalmente necessárias.

**Apresentação (Presentation)** – a camada de apresentação formata os dados a serem apresentados na camada de aplicação. Ela pode ser considerada o tradutor da rede. Essa camada pode converter dados de um formato usado pela camada de aplicação em um formato comum na estação de envio e, em seguida, converter esse formato comum em um formato conhecido pela camada de aplicação na estação de recepção.

**Sessão (Session)** – a camada de sessão permite o estabelecimento da sessão entre processos em execução em estações diferentes.

**Transporte (Transport)** – a camada de transporte garante que as mensagens sejam entregues sem erros, em sequência e sem perdas ou duplicações. Ela elimina para os protocolos de camadas superiores qualquer preocupação a respeito da transferência de dados entre eles e seus pares.

**Rede (Network)** – a camada de rede controla a operação da sub-rede, decidindo que caminho físico os dados devem seguir com base nas condições da rede, na prioridade do serviço e em outros fatores.

**Dados (Data Link)** – a camada de vínculo de dados proporciona uma transferência de quadros de dados sem erros de um nó para outro por meio da camada física, permitindo que as camadas acima dela assumam a transmissão praticamente sem erros através do vínculo.

**Física (Physical)** – a camada física, a camada inferior do modelo OSI, está encarregada da transmissão e recepção do fluxo de bits brutos não estruturados através de um meio físico. Ela descreve as interfaces elétricas/ópticas, mecânicas e funcionais com o meio físico e transporta os sinais para todas as camadas superiores.

Veja uma tabela de comparação do modelo OSI e o TCP/IP e seus respectivos protocolos e serviços:

Modelo TCP/IP	Protocolos e serviços	Modelo OSI
Aplicação	HTTP, FTP, Telnet, NTP, DHCP, PING	Aplicação
		Apresentação
		Sessão
Transporte	TCP, UDP	Transporte
Rede	IP, ARP, ICMP, IGMP	Rede
Interface de rede	Ethernet	Dados Física

## TCP – Transmission Control Protocol<sup>1</sup>

O Protocolo de Controle de Transmissão (TCP) é um dos protocolos sobre os quais a internet se assenta. Ele é complementado pelo Protocolo da Internet, sendo normalmente chamado de TCP/IP. A versatilidade e robustez do TCP tornou-o adequado a redes globais, já que ele verifica se os dados são enviados pela rede de forma correta, na sequência apropriada e sem

erros.

O TCP é um protocolo de nível da camada de transporte (camada 4) do modelo OSI e é sobre ele que se assentam a maioria das aplicações cibernéticas, como o SSH, FTP, HTTP – portanto, a World Wide Web. O protocolo de controle de transmissão provê confiabilidade, entrega na sequência correta e verificação de erros em pacotes de dados, entre os diferentes nós da rede, para a camada de aplicação.

Aplicações que não requerem um serviço de confiabilidade de entrega de pacotes podem se utilizar de protocolos mais simples, como o User Datagram Protocol (UDP), que provê um serviço que enfatiza a redução de latência da conexão.

### Cabeçalho de uma trama TCP

+	Bits 0 - 3	4 - 9	10 - 15	16 - 31
0	Porta na origem			Porta no destino
32	Número de sequência			
64	Número de confirmação (ACK)			
96	Offset	Reservados	Flags	Janela <i>Window</i>
128	Checksum			Ponteiro de urgência
160	Opções (opcional)			
Padding (até 32)				
224	Dados			
Detalhe do campo Flags				
+	10	11	12	13
96	UrgPtr	ACK	Push	RST
				14
				SYN
				15
				FIN

### Funcionamento do protocolo

O protocolo TCP especifica três fases durante uma conexão: estabelecimento da ligação, transferência e término de ligação. O estabelecimento é feito em três passos, enquanto o término é feito em quatro. Durante a inicialização, são ativados alguns parâmetros, como o Sequence Number (número de sequência), para garantir a entrega ordenada e a robustez durante a transferência.

## Estabelecimento da conexão

Para estabelecer uma conexão, o TCP usa um handshake (aperto de mão) de três vias. Antes que o cliente tente se conectar com o servidor, o servidor deve primeiro ligar e escutar a sua própria porta, para só depois abri-la para conexões: isso é chamado de abertura passiva. Uma vez que a abertura passiva esteja estabelecida, um cliente pode iniciar uma abertura ativa. Para estabelecer uma conexão, o aperto de mão de três vias (ou três etapas) é realizado.

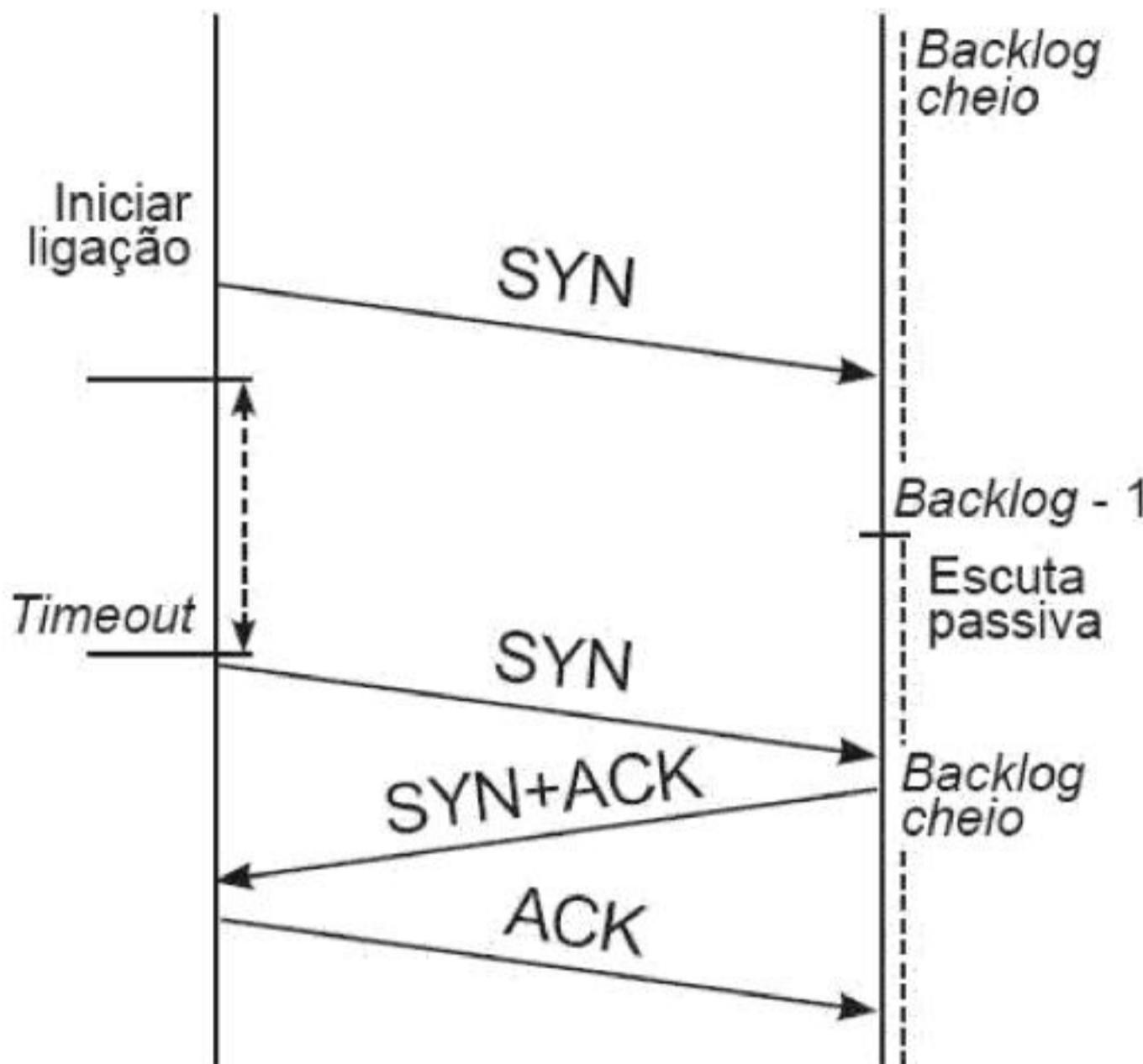
**SYN** – a abertura ativa é realizada por meio do envio de um SYN pelo cliente ao servidor. O cliente define o número de sequência de segmento como um valor aleatório A.

**SYN-ACK** – em resposta, o servidor responde com um SYN-ACK. O número de reconhecimento (acknowledgment) é definido como sendo um a mais que o número de sequência recebido, por exemplo, A+1, e o número de sequência que o servidor escolhe para o pacote é outro número aleatório B.

**ACK** – finalmente, o cliente envia um ACK de volta ao servidor. O número de sequência é definido pelo valor de reconhecimento recebido, por exemplo, A+1, e o número de reconhecimento é definido como um a mais que o número de sequência recebido, por exemplo, B+1.

Neste ponto, o cliente e o servidor receberam um reconhecimento de conexão. As etapas 1 e 2 estabelecem o parâmetro (número de sequência) de conexão para uma direção, e ele é reconhecido. As etapas 2 e 3 estabelecem o parâmetro de conexão (número de sequência) para a outra direção, e ele é reconhecido. Com isso, uma comunicação full-duplex é estabelecida.

# Cliente 1      Servidor



Tipicamente, numa ligação TCP existe aquele designado de servidor (que abre um socket e espera passivamente por ligações) num extremo, e o cliente no outro. O cliente inicia a ligação enviando um pacote TCP com a flag SYN ativa, e espera-se que o servidor aceite a ligação enviando um pacote SYN-ACK.

Se, durante um determinado espaço de tempo, esse pacote não for recebido, ocorre um timeout e o pacote SYN é reenviado. O estabelecimento da ligação é concluído por parte do cliente, que confirma a aceitação do servidor respondendo-lhe com um pacote ACK.

Durante essas trocas, são trocados números de sequência iniciais (ISN) entre os interlocutores que vão servir para identificar os dados ao longo do fluxo, bem como servir de contador de bytes transmitidos durante a fase de transferência de dados (sessão).

No final desta fase, o servidor inscreve o cliente como uma ligação estabelecida numa tabela própria que contém um limite de conexões, o backlog. No caso de o backlog ficar completamente preenchido, a ligação é rejeitada, ignorando (silenciosamente) todos os subsequentes pacotes SYN.

## Transferência de dados (sessão)

Durante a fase de transferência, o TCP está equipado com vários mecanismos que asseguram a confiabilidade e robustez: números de sequência que garantem a entrega ordenada, código detector de erros (checksum) para detecção de falhas em segmentos específicos, confirmação de recepção e temporizadores que permitem o ajuste e contorno de eventuais atrasos e perdas de segmentos.

Como se pode observar pelo cabeçalho TCP, há permanentemente um par de números de sequência, doravante referidos como número de sequência e número de confirmação (acknowledgment). O emissor determina o seu próprio número de sequência e o receptor confirma o segmento usando como número ACK o número de sequência do emissor. Para manter a confiabilidade, o receptor confirma os segmentos indicando que recebeu um determinado número de bytes contíguos. Uma das melhorias introduzidas no TCP foi a possibilidade de o receptor confirmar blocos fora da ordem esperada. Essa característica designa-se por selective ACK, ou apenas SACK.

A remontagem ordenada dos segmentos é feita usando os números de sequência, de 32 bit, que reiniciam a zero quando ultrapassam o valor máximo, 2<sup>31</sup>-1, tomando o valor da diferença. Assim, a escolha do ISN torna-se vital para a robustez deste protocolo.

O campo checksum permite assegurar a integridade do segmento. Ele é expresso em complemento para um, consistindo na soma dos valores (em complemento para um) da trama. A escolha da operação de soma em complemento para um deve-se ao fato de ela poder ser calculada da mesma forma para múltiplos deste comprimento (16 bit, 32 bit, 64 bit etc.) e o resultado, quando encapsulado, será o mesmo. A verificação desse campo por parte do receptor é feita com a recomputação da soma em complemento para um que dará -0 caso o pacote tenha sido recebido intacto.

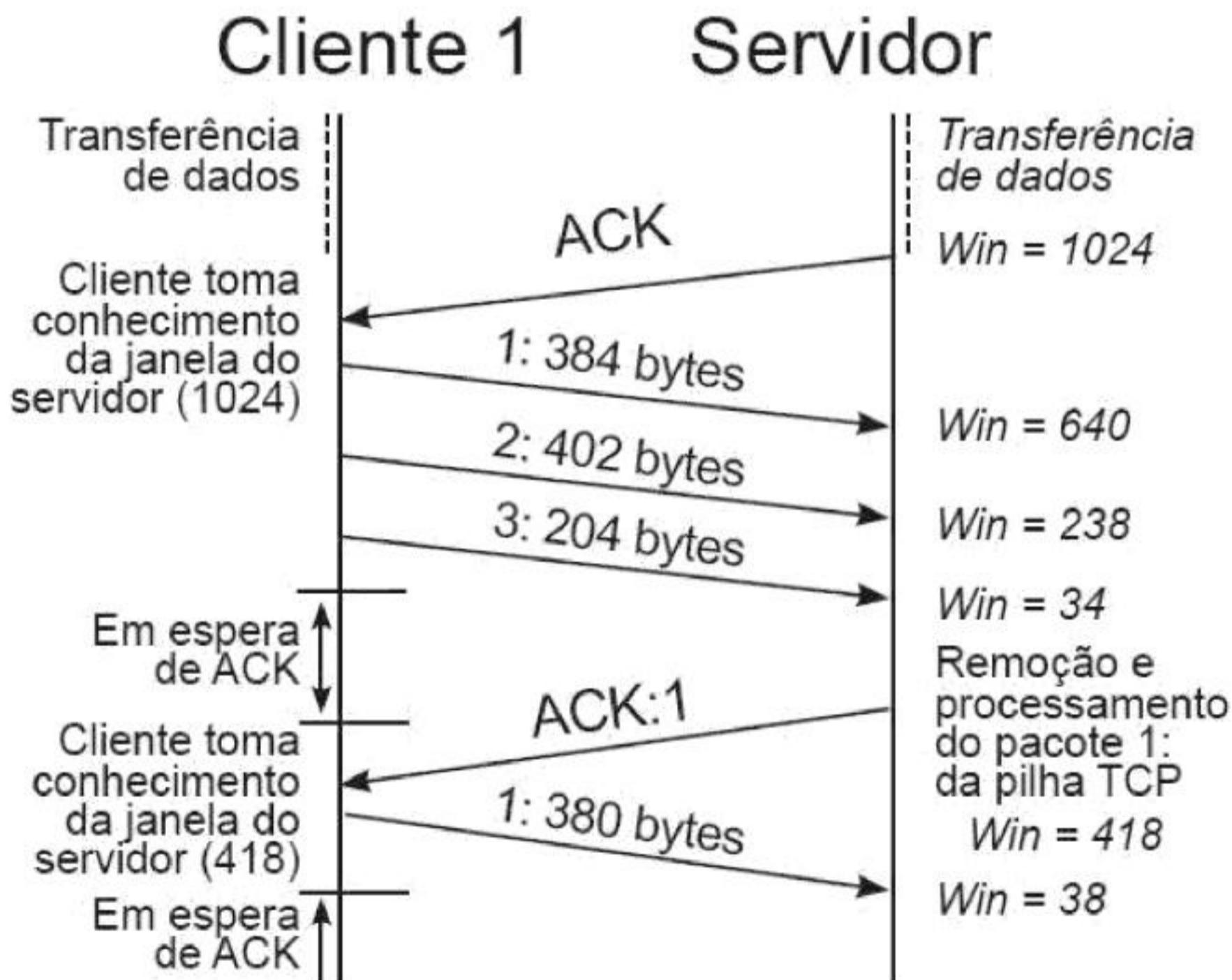
Esta técnica (checksum), embora muito inferior a outros métodos detectores, como o CRC, é parcialmente compensada com a aplicação do CRC ou outros testes de integridade melhores ao nível da camada 2, logo abaixo do TCP, como no caso do PPP e Ethernet. Contudo, isso não torna este campo redundante: com efeito, estudos de tráfego revelam que a introdução de erro é bastante frequente entre hops protegidos por CRC e que esse campo detecta a maioria desses erros.

As confirmações de recepção (ACK) servem também ao emissor para determinar as condições da rede. Dotados de temporizadores, tanto os emissores como receptores podem alterar o fluxo dos dados, contornar eventuais problemas de congestão e, em alguns casos, prevenir o congestionamento da rede. O protocolo está dotado de mecanismos para obter o máximo de performance da rede sem congestioná-la – o envio de tramas por um emissor

mais rápido que qualquer um dos intermediários (hops) ou mesmo do receptor pode inutilizar a rede. São exemplo a janela deslizante e o algoritmo de início-lento.

### Adequação de parâmetros

O cabeçalho TCP possui um parâmetro que permite indicar o espaço livre atual do receptor (emissor quando envia a indicação): a janela (ou window). Assim, o emissor fica a saber que só poderá ter em trânsito aquela quantidade de informação até esperar pela confirmação (ACK) de um dos pacotes – que, por sua vez, trará, com certeza, uma atualização da janela. Curiosamente, a pilha TCP no Windows foi concebida para se autoajustar na maioria dos ambientes e, nas versões atuais, o valor padrão é superior em comparação com versões mais antigas.



Porém, devido ao tamanho do campo, que não pode ser expandido, os limites aparentes da janela variam entre 2 e 65535 bytes, o que é bastante pouco em redes de alto débito e

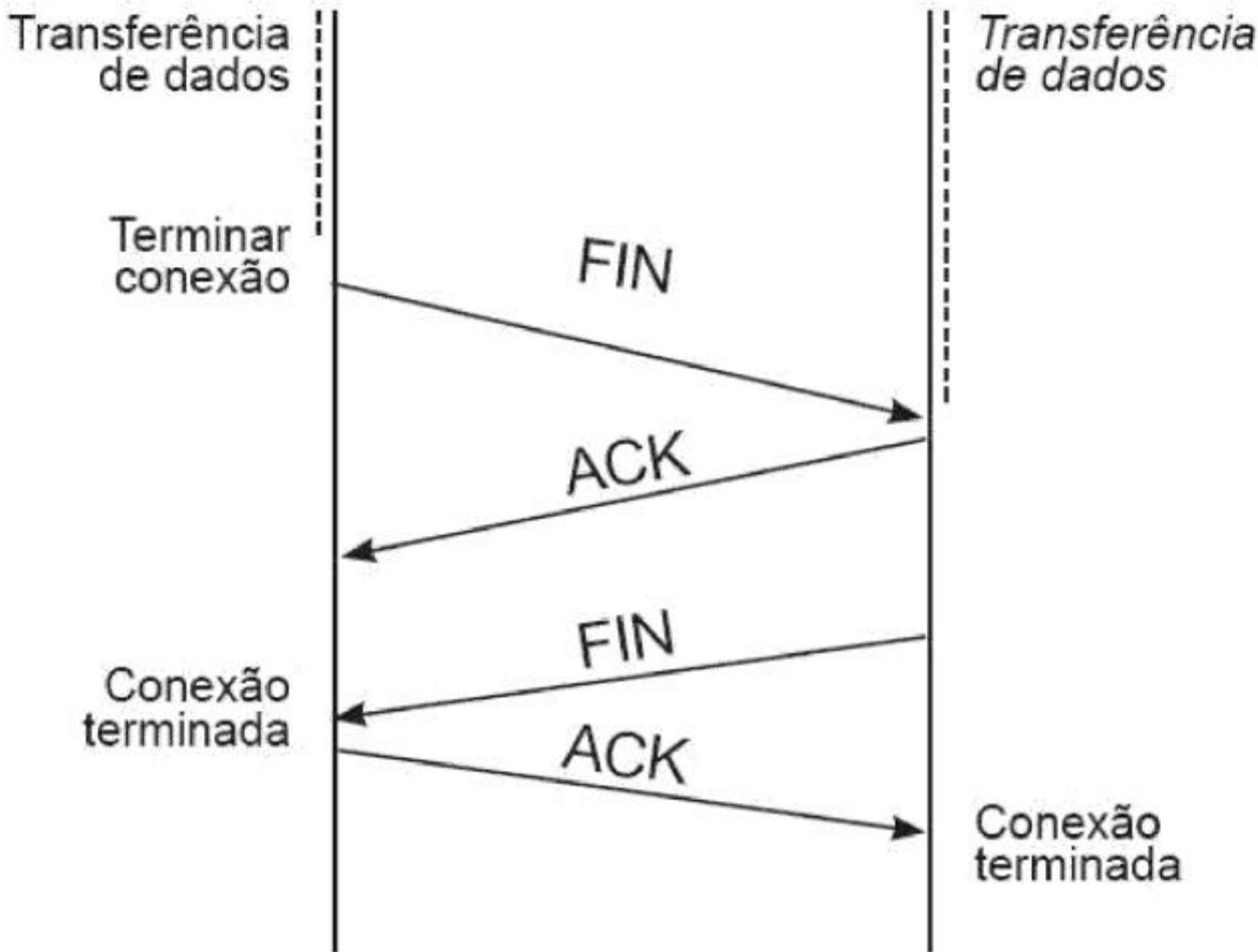
hardware de alta performance. Para contornar essa limitação é usada uma opção especial que permite obter múltiplos do valor da janela, chamado de escala da janela, ou TCP window scale; este valor indica quantas vezes o valor da janela, de 16 bit, deve ser operado por deslocamento de bits (para a esquerda) para obter os múltiplos, podendo variar entre 0 e 14 bytes. Assim, torna-se possível obter janelas de 1 gigabyte. O parâmetro de escala é definido unicamente durante o estabelecimento da ligação.

## Término da ligação

A fase de encerramento da sessão TCP é um processo de quatro etapas, em que cada interlocutor se responsabiliza pelo encerramento do seu lado da ligação. Quando um deles pretende finalizar a sessão, envia um pacote com a flag FIN ativa, ao qual deverá receber uma resposta ACK. Por sua vez, o outro interlocutor vai proceder da mesma forma, enviando um FIN ao qual deverá ser respondido um ACK.

Pode ocorrer, no entanto, que um dos lados não encerre a sessão. Chama-se esse tipo de evento de conexão semiaberta. O lado que não encerrou a sessão poderá continuar a enviar informação pela conexão, mas o outro lado não.

# Cliente 1      Servidor



## Observação

Para saber mais sobre o protocolo TCP/IP verifique a RFC 791: <https://tools.ietf.org/html/rfc791>.

Um Request for Comments (RFC) é um tipo de publicação da Internet Engineering Task Force (IETF) e da Internet Society (ISOC), o principal desenvolvimento técnico de padrões de organismos para a internet.

## ICMP – Internet Control Message Protocol

O ICMP<sup>2</sup> é um protocolo integrante do protocolo IP, definido pelo RFC 792. Ele permite gerenciar as informações relativas aos erros nas máquinas conectadas. Devido aos poucos controles que o protocolo IP realiza, ele não corrige esses erros, mas os mostra para os protocolos das camadas vizinhas. Assim, o ICMP é usado por todos os roteadores para assinalar um erro, chamado de Delivery Problem.

As mensagens ICMP geralmente são enviadas automaticamente em uma das seguintes

situações:

- Um pacote IP não consegue chegar ao seu destino (por exemplo, tempo de vida do pacote expirado).
- O gateway não consegue retransmitir os pacotes na frequência adequada (por exemplo, gateway congestionado).
- O roteador ou encaminhador indica uma rota melhor para a máquina a enviar pacotes.

### Mensagem ICMP encapsulada num datagrama IP

Mensagem ICMP				
Título	Tipo (8 bits)	Código (8 bits)	Checksum (16 bits)	Mensagem (dimensão variável)

### ARP – Address Resolution Protocol

O ARP é um protocolo de telecomunicações usado para resolução de endereços da camada de internet em endereços da camada de enlace, uma função crítica em redes de múltiplos acessos. Foi definido pela RFC 826 em 1982 e o padrão de internet STD 37; também é o nome do programa para manipulação desses endereços na maioria dos sistemas operacionais.

O ARP é usado para mapear um endereço de rede, por exemplo, um endereço IPv4, para um endereço físico como um endereço ethernet, também chamado de endereço MAC. ARP foi implementado com muitas combinações de tecnologias da camada de rede e de enlace de dados.

Em redes Internet Protocol Version 6 (IPv6), a funcionalidade do ARP é fornecida pelo Neighbor Discovery Protocol (NDP).

### Funcionamento do ARP

O ARP é um protocolo de requisição e resposta que é executado e encapsulado pelo protocolo da linha.

Ele é comunicado dentro dos limites de uma única rede, nunca roteado entre nós de

redes. Essa propriedade coloca o ARP na camada de enlace do conjunto de protocolos da internet, enquanto no modelo OSI ele é frequentemente descrito como residindo na camada 3, sendo encapsulado pelos protocolos da camada 2. Entretanto, o ARP não foi desenvolvido no framework OSI.

## HTTP – Hypertext Transfer Protocol

O HTTP<sup>3</sup> é um protocolo de comunicação, na camada de aplicação segundo o modelo OSI, utilizado para sistemas de informação de hipermídia, distribuídos e colaborativos. Ele é a base para a comunicação de dados da World Wide Web.

O HTTP funciona como um protocolo de requisição-resposta no modelo computacional *cliente-servidor*. Um navegador web, por exemplo, pode ser o cliente, e uma aplicação em um computador que hospeda um site da web pode ser o servidor. O cliente submete uma mensagem de requisição HTTP para o servidor. O servidor, que fornece os recursos, como arquivos HTML e outros conteúdos, ou realiza outras funções de interesse do cliente, retorna uma mensagem-resposta para o cliente. A resposta contém informações de estado completas sobre a requisição e pode também conter o conteúdo solicitado no corpo de sua mensagem.

Um navegador web é um exemplo de *agente de usuário* (AU). Outros tipos de agentes de usuário incluem o software de indexação usado por provedores de consulta (web crawler), navegadores vocais, aplicações móveis e outros softwares que acessam, consomem ou exibem conteúdo web.

## DNS – Domain Name System

O DNS<sup>4</sup> é um sistema hierárquico descentralizado de nomes para computadores, serviços ou outros recursos conectados à internet ou a uma rede privada. Associa várias informações com nomes de domínio atribuídos a cada uma das entidades participantes. Mais proeminente, ele traduz nomes de domínio mais prontamente memorizados para os endereços IP numéricos necessários para localizar e identificar serviços de computador e dispositivos com os protocolos de rede subjacentes. Ao fornecer um serviço de diretório distribuído em todo o mundo, o DNS é um componente essencial da funcionalidade da internet, que está em uso desde 1985.

## A consulta DNS<sup>5</sup>

Quando um usuário realiza uma consulta no navegador por alguma página na internet

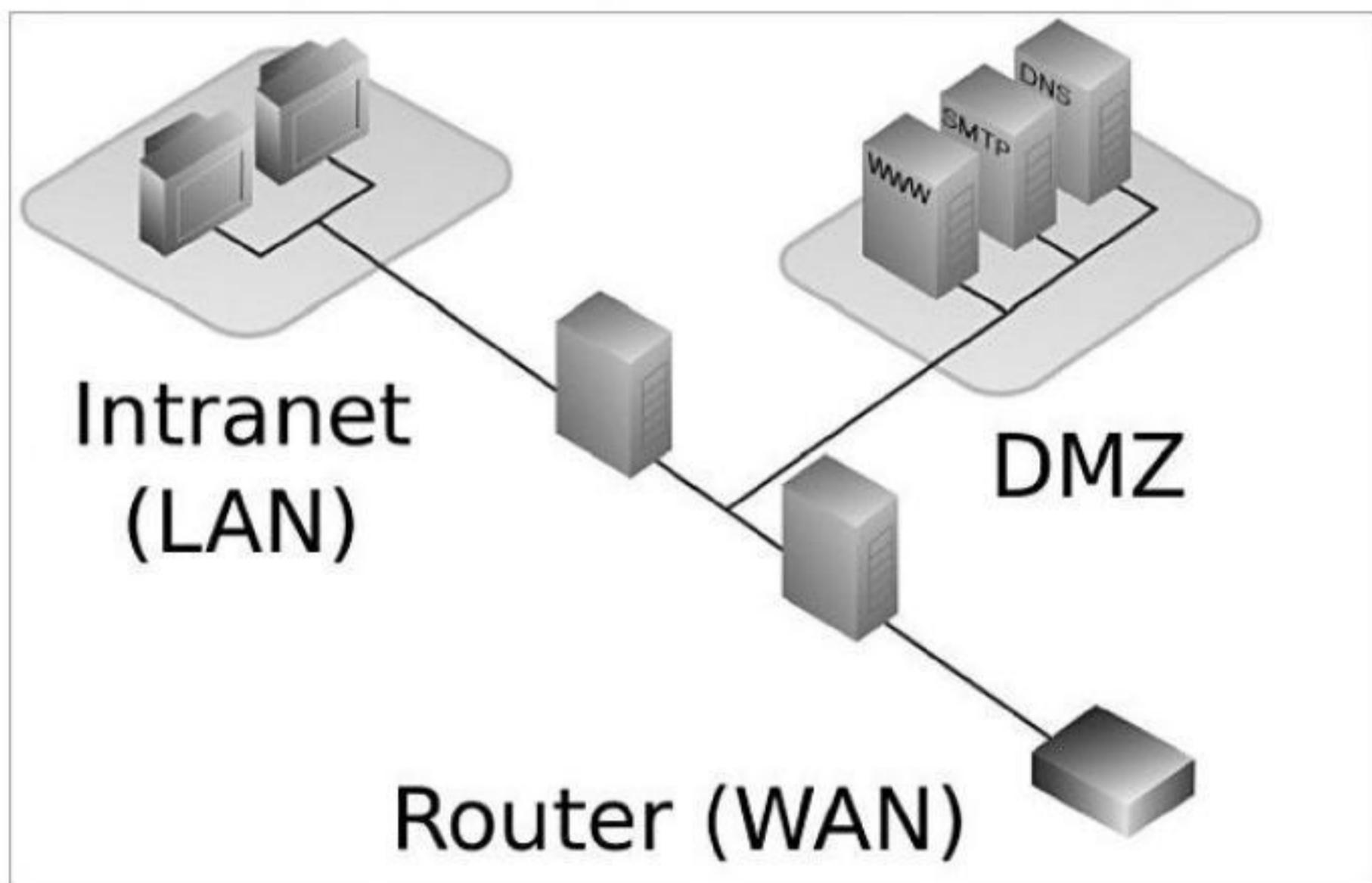
*image  
not  
available*

entre outros.

## DMZ – Demilitarized Zone

Uma DMZ,<sup>8</sup> também conhecida como rede de perímetro, é uma sub-rede física ou lógica que contém e expõe serviços de fronteira externa de uma organização a uma rede maior e não confiável, normalmente a internet. Quaisquer dispositivos situados nesta área – isto é, entre a rede confiável (geralmente a rede privada local) e a rede não confiável (geralmente a internet) – está na zona desmilitarizada.

A função de uma DMZ é manter todos os serviços que possuem acesso externo, tais como servidores HTTP, FTP, de correio eletrônico etc., juntos em uma rede local, limitando assim o potencial dano em caso de comprometimento de algum desses serviços por um invasor. Para atingir esse objetivo os computadores presentes em uma DMZ não devem conter nenhuma forma de acesso à rede local.



A configuração é realizada por meio de *equipamentos de firewall*, que vão realizar o controle de acesso entre a rede local, a internet e a DMZ.

*image  
not  
available*

```
Connected to 172.16.0.12.  
Escape character is '^].  
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntul
```

**172.16.0.12:** indica o IP do host de destino.

**22:** indica a porta a ser testada; neste caso, a porta do SSH.

Observe que ele conecta nessa porta; isso significa que ela está aberta, porém, não é possível obter uma *shell*. Nesse caso, foi apresentado um banner do serviço SSH. Algumas máquinas podem não estar configuradas para apresentar *banner* do serviço.

## TCPdump<sup>13</sup>

O TCPdump é uma ferramenta utilizada para monitorar os pacotes trafegados em uma rede. Ele mostra os cabeçalhos dos pacotes que passam pela interface de rede.

Vamos realizar alguns testes para entender o seu funcionamento. O TCPdump é uma ferramenta que faz parte da suíte de programas do Kali Linux.

Para verificar o tráfego que está ocorrendo na máquina podemos utilizar o comando:

```
root@kali:~# tcpdump -i eth0  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes  
14:55:08.376379  IP kali.ssh > 172.16.0.10.35760: Flags [P.], seq  
2116613311:2116613499, ack 1384995506, win 291, options [nop,nop,TS val 60095  
ecr 6090120], length 188  
14:55:08.376511 IP 172.16.0.10.35760 > kali.ssh: Flags [.], ack 188, win 1444, options  
[nop,nop,TS val 6090132 ecr 60095], length 0  
14:55:08.401493 IP kali.45804 > gateway.domain: 38111+ PTR? 15.0.16.172.in-  
addr.arpa. (42)  
14:55:08.425322 IP gateway.domain > kali.45804: 38111 NXDomain 0/0/0 (42)  
14:55:08.425663 IP kali.36685 > gateway.domain: 25487+ PTR? 1.0.16.172.in-  
addr.arpa. (41)  
...  
^C  
1754 packets captured  
1766 packets received by filter
```

*image  
not  
available*

```
4 packets received by filter  
0 packets dropped by kernel
```

**tcpdump:** executa a aplicação utilitário de rede tcpdump.

**-n:** orienta o TCPdump a não resolver nomes, apresentando somente o endereço IP.

**-c 4:** -c indica a quantidade do pacote a ser apresentado em tela; neste caso, 4 pacotes.

**-i eth0:** indica a interface a ser monitorada; neste caso, a eth0.

**icmp:** indica o protocolo a ser apresentado na saída do comando; neste caso, o protocolo icmp.

**and:** combina a busca do comando com a diretiva a seguir.

**src 172.16.0.15:** especifica a direção do pacote a ser tomada; neste caso, de alguma origem src para o IP da máquina Kali, 172.16.0.15.

Observe que esse comando apresenta em tela apenas os pacotes ICMP de qualquer origem (src) para o destino da própria máquina (172.16.0.15). Esse comando pode ser utilizado para identificar ataques DoS na rede.

## Netstat<sup>14</sup>

O netstat (Network statistic) é uma ferramenta, comum ao Windows, Unix e Linux, utilizada para se obter informações sobre as conexões de rede, tabelas de roteamento, estatísticas de interface e conexões mascaradas.

É um recurso que pode nos ajudar na análise de informações para descobrir conexões maliciosas que estão mascaradas ou estão tentando se conectar em nossa máquina.

O netstat é uma ferramenta que faz parte da suíte de programas do Kali Linux. Para utilizá-la, abra o terminal e digite:

Protocol. Acesso em: 14 ago. 2019.

4. SISTEMA DE NOMES DE DOMÍNIO. *In:* WIKIPEDIA: a enclopédia livre. [São Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: [https://pt.wikipedia.org/wiki/Domain\\_Name\\_System](https://pt.wikipedia.org/wiki/Domain_Name_System). Acesso em: 14 ago. 2019.
5. VERISIGN. Como o sistema de nomes de domínio (DNS) funciona. Disponível em: [https://www.verisign.com/pt\\_BR/website-presence/online/how-dns-works/index.xhtml](https://www.verisign.com/pt_BR/website-presence/online/how-dns-works/index.xhtml). Acesso em: 14 ago. 2019.
6. REDE PRIVADA VIRTUAL. *In:* WIKIPEDIA: a enclopédia livre. [São Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: [https://pt.wikipedia.org/wiki/Virtual\\_private\\_network](https://pt.wikipedia.org/wiki/Virtual_private_network). Acesso em: 14 ago. 2019.
7. PROXY. *In:* WIKIPEDIA: a enclopédia livre. [São Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: <https://pt.wikipedia.org/wiki/Proxy>. Acesso em: 14 ago. 2019.
8. DMZ (COMPUTAÇÃO). *In:* WIKIPEDIA: a enclopédia livre. [São Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: [https://pt.wikipedia.org/wiki/DMZ\\_\(computação\)](https://pt.wikipedia.org/wiki/DMZ_(computação)). Acesso em: 14 ago. 2019.
9. DNS DINÂMICO. *In:* WIKIPEDIA: a enclopédia livre. [São Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: [https://pt.wikipedia.org/wiki/DNS\\_dinâmico](https://pt.wikipedia.org/wiki/DNS_dinâmico). Acesso em: 14 ago. 2019.
10. SECURE SHELL. *In:* WIKIPEDIA: a enclopédia livre. [São Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: [https://pt.wikipedia.org/wiki/Secure\\_Shell](https://pt.wikipedia.org/wiki/Secure_Shell). Acesso em: 14 ago. 2019.
11. Videoaula TDI – Conceitos Básicos de Rede – Telnet.
12. TELNET. *In:* WIKIPEDIA: a enclopédia livre. [São Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: <https://pt.wikipedia.org/wiki/Telnet>. Acesso em: 14 ago. 2019.
13. Videoaula TDI – Conceitos Básicos de Rede – TCPdump.
14. Videoaula TDI – Conceitos Básicos de Rede – Netstat.

## Exemplo 1

The screenshot shows a web browser displaying a job posting. The URL in the address bar is [www.netcarreiras.com.br/vaga-desenvolvedor-lotus-notes-70285.html](http://www.netcarreiras.com.br/vaga-desenvolvedor-lotus-notes-70285.html). The page title is "Desenvolvedor Lotus Notes". Below the title, there is a section titled "/ descrição da vaga". The main content starts with "Sesc Departamento Nacional, localizado em Jacarepaguá, seleciona para:". It describes the position as "Assistente Técnico I (Desenvolvedor Lotus Notes) 01 vaga Contrato por Prazo Determinado (12 meses podendo, a critério da empresa, ser renovado por mais 12 meses)". The "Pré-requisitos" section lists requirements: Ensino superior cursando na área de Tecnologia da Informação, Experiência consistente como Desenvolvedor em plataforma Lotus Notes, Conhecimento em: Web Forms, LotusScript e Lotus Formula, and Desejável conhecimento em: XPages, Desenvolvimento web (HTML, Jquery, CSS) e Metodologia Scrum. The "Atividades" section lists tasks: Desenvolver sistemas e aplicações a partir das solicitações recebidas de analistas de sistemas, Criar interfaces gráficas, manipular bancos de dados e construir relatórios, and Prover apoio técnico em implantações e migrações de sistemas e dados.

Observe que essa vaga nos passa muita informação sobre a estrutura de TI de uma empresa em Jacarepaguá, Rio de Janeiro. É uma vaga para desenvolvedores em *Lotus Notes*. Como pré-requisitos, o site informa métodos de programação e nome das linguagens lá utilizadas.

administrativas, como dono, endereço, CNPJ, telefones e e-mails de contatos.

## IANA WHOIS Service

The IANA WHOIS Service is provided using the WHOIS protocol on port 43. This web gateway will query this query arguments are domain names, IP addresses and AS numbers.

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:      whois.registro.br

domain:     BR

organisation: Comite Gestor da Internet no Brasil
address:    Av. das Nações Unidas, 11541, 7º andar
address:    São Paulo SP 04578-000
address:    Brazil

contact:    administrative
name:       Demi Getschko
organisation: Comite Gestor da Internet no Brasil
address:    Av. das Nações Unidas, 11541, 7º andar
address:    São Paulo SP 04578-000
address:    Brazil
phone:      +55 11 5509 3505
fax-no:     +55 11 5509 3501
e-mail:     demi@registro.br

contact:    technical
name:       Frederico Augusto de Carvalho Neves
organisation: Registro .br
address:    Av. das Nações Unidas, 11541, 7º andar
address:    São Paulo SP 04578-000
address:    Brazil
phone:      +55 11 5509 3505
fax-no:     +55 11 5509 3501
e-mail:     fneves@registro.br
```

## Utilizando o WHOIS no Linux

O WHOIS é uma ferramenta que faz parte da suíte de ferramentas do Kali Linux.

Para utilizá-lo, abra o terminal e digite:

Consultas DNS podem ajudar um atacante a identificar informações de hospedagem de um servidor, sendo ele um site ou serviços, como servidores de e-mail.

Tomando conhecimento dos registros de DNS (A, AAAA, CNAME, MX, NS, PTR e SOA) vamos entender a ferramenta *host*, pois ela faz com que a leitura em servidores de DNS se torne completa. Se nós conseguirmos algumas informações a respeito de serviços de DNS é possível que haja algum tipo de vulnerabilidade no DNS.

Para realizar ataques *man-in-the-middle*, como DNS Spoofing, basicamente temos que entender como os registros do DNS alvo podem estar vulneráveis a esses ataques.

Vamos utilizar a ferramenta *host*, que faz parte da suíte de programas do Kali Linux. Para isso, abra o terminal e digite:

```
root@kali:~# host guardweb.com.br
guardweb.com.br has address 104.31.87.52
guardweb.com.br has address 104.31.86.52
guardweb.com.br has IPv6 address 2400:cb01:2048:1::681f:5734
guardweb.com.br has IPv6 address 2400:cb01:2048:1::681f:5634
guardweb.com.br mail is handled by 10 alt4.aspmx.l.google.com.
guardweb.com.br mail is handled by 10 alt3.aspmx.l.google.com.
guardweb.com.br mail is handled by 5 alt1.aspmx.l.google.com.
guardweb.com.br mail is handled by 5 alt2.aspmx.l.google.com.
guardweb.com.br mail is handled by 1 aspmx.l.google.com.
```

**host:** executa a aplicação host.

**guardweb.com.br:** nome do alvo a ser consultado.

Observe que esse comando retornou o endereço e vários outros registros existentes em sua configuração de DNS.

Podemos utilizar algumas flags para incrementar uma pesquisa em um domínio.

```
root@kali:~# host -t NS guardweb.com.br
guardweb.com.br name server candy.ns.cloudflare.com.
guardweb.com.br name server wesley.ns.cloudflare.com.
```

**-t NS:** exibe os endereços de onde os servidores de nomes estão armazenados.

A partir dessas pesquisas é possível saber as informações dos servidores de DNS que

para um *server root*.

## Realizando uma transferência de zona de DNS

Vamos realizar um teste que vai forçar a transferência de zona de DNS; com isso, é possível que haja algumas vulnerabilidades que vão trazer informações importantes a respeito do *domínio*, como quantas máquinas o host possui e quais delas estão disponíveis na estrutura deste domínio.

Vamos supor um cenário para o teste. Primeiramente, vamos escolher um domínio e verificar quais são os seus servidores de domínio. Abra o terminal e digite:

```
root@kali:~# host -t ns guardweb.com.br
guardweb.com.br name server ns04.guardweb.com.br.
guardweb.com.br name server ns03.guardweb.com.br.
guardweb.com.br name server ns01.guardweb.com.br.
guardweb.com.br name server ns02.guardweb.com.br.
```

**host**: executa a aplicação utilitário de DNS host.

**-t ns**: indica o tipo de consulta sobre o domínio que será buscada; neste caso, ns (name server). **guardweb.com.br**: domínio que será analisado.

Observe que ele vai apresentar todos os servidores de domínios da *guardweb.com.br*.

## Indicando o servidor a ser analisado

Para realizar a transferência de zona de DNS, é necessário informar o NS a ser analisado. É importante testar em todos os servidores de nome.

```
root@kali:~# host -l guardweb.com.br ns01.guardweb.com.br
Using domain server:
Name: ns01.guardweb.com.br
Address: 10.146.0.1#53
Aliases:

Host guardweb.com.br not found: 5(REFUSED)
; Transfer failed.
```

No caso, essa ferramenta não obteve sucesso na tentativa de transferência da zona de DNS devido às configurações no servidor.

## Dnsenum – utilitário DNS

O *dnsenum* é uma ferramenta que faz parte da suíte de programas do Kali Linux. Vamos realizar uma consulta no domínio *guardweb.com.br*. e indicar uma lista de subdomínios para encontrar os hosts. Para utilizá-lo digite no terminal:

```
root@kali:~# fierce -dns guardweb.com.br -w /usr/share/fierce/hosts.txt
```

Option w is ambiguous (wide, wordlist)

DNS Servers for guardweb.com.br:

```
ns01.guardweb.com.br  
ns02.guardweb.com.br  
ns03.guardweb.com.br  
ns04.guardweb.com.br
```

Trying zone transfer first...

```
Testing ns01.guardweb.com.br  
Request timed out or transfer not allowed.  
Testing ns02.guardweb.com.br
```

Whoah, it worked - misconfigured DNS server found:

```
guardweb.com.br. 129600 IN SOA ( ns01.guardweb.com.br. 111.guardweb.com.br.  
2017052301 ;serial  
10800 ;refresh  
3600 ;retry  
604800 ;expire  
86400 ;minimum  
)  
guardweb.com.br. 129600 IN NS ns01.guardweb.com.br.  
guardweb.com.br. 129600 IN NS ns02.guardweb.com.br.  
guardweb.com.br. 129600 IN NS ns03.guardweb.com.br.  
guardweb.com.br. 129600 IN NS ns04.guardweb.com.br.  
guardweb.com.br. 129600 IN MX 5 mx.guardweb.locaweb.com.br.  
guardweb.com.br. 129600 IN MX 10 mx2.guardweb.locaweb.com.br.  
guardweb.com.br. 129600 IN MX 20 mx3.guardweb.locaweb.com.br.  
guardweb.com.br. 129600 IN A 10.146.0.1  
guardweb.com.br. 300 IN TXT ( «v=spf1 ip4:10.146.0.1 ip4:10.146.0.1 ip4:10.146.0.1/29 ip4:10.146.0.1/29  
ip4:10.146.0.1/29 ip4:10.146.0.1/29 ip4:10.146.0.1/29 include:_lw1.guardweb.com.br  
include:_lw2.guardweb.com.br -all»  
)  
444.guardweb.com.br. 129600 IN A 10.146.0.1  
333.guardweb.com.br. 129600 IN CNAME google.com.  
222.guardweb.com.br. 129600 IN A 10.146.0.1  
111.guardweb.com.br. 129600 IN A 10.146.0.1  
1c71fb14edce.guardweb.com.br. 129600 IN CNAME cname.bit.ly.  
555ee.guardweb.com.br. 129600 IN CNAME ( guardweb-1310281670.us-east-1.elb.amazonaws.com. )  
...
```

**fierce**: executa o utilitário de DNS fierce.

## Técnica Google Hacking

Esta técnica consiste na utilização dos operadores, digitados direto no buscador do Google, para realizar as buscas avançadas, criando combinações para filtrar e localizar sequências específicas de texto nos resultados de busca, como versões, mensagens de erro, dados, cartões de bancos, documentos, senhas, telefones, arquivos sensíveis.

### Os operadores

Os operadores mais utilizados são:

- **site** – limita resultados da busca em um site específico, limitados ao domínio buscado;
- **intitle** – busca no título da página e mostra os resultados (ele busca a tag <intitle> no código-fonte da programação HTML do site);
- **inurl** – busca de termos presentes na URL de um site;
- **intext** – busca resultados que estão no texto do texto;
- **filetype** – busca por formatos de arquivos contidos no site (pdf, txt, doc, png...).

### Utilizando os operadores em conjunto

Para obter dados mais precisos, podemos utilizar vários operadores em conjunto, por exemplo:

**site:terra intext:telefone**

Neste operador, estamos filtrando as buscas apenas o site *terra.com* tendo no texto a palavra *telefone*.

**site:com.br filetype:txt intext:senhas**

Neste operador estamos filtrando as buscas apenas nos domínios *.com.br* contendo arquivos do tipo *txt* e no texto a palavra *senhas*.

Provavelmente vamos nos deparar com inúmeros arquivos de texto que contenham senhas de serviços, e-mails, logins. Possivelmente muitos destes documentos não deviam estar expostos para o público.

### Google Hacking Database (GHDB)

É um banco de dados com tags de busca do Google, previamente criadas, para conseguir

- 1) Para identificar um redirecionamento:
  - Abra o Firefox, clique com o botão direito em Inspect Element.
  - Clique na aba Network – com isso você consegue monitorar todo o percurso do seu navegador –, insira o link no buscador da URL e aperte Enter.
  - Verifique no log do campo Network e procure o status 302 (status de redirecionamento HTTP).
- 2) Outro método é utilizar alguma ferramenta que realiza a expansão do link, como *unshorten.it*, que vai mostrar a URL real.
- 3) No caso do MailTracking é possível identificar analisando o e-mail do remetente – geralmente ele vai estar com algumas extensões suspeitas no nome, como *atacante@gmail.com.mailtracking.com*.

## Shodan<sup>3</sup>

Conhecido como o “O Google dos hackers”, o Shodan é uma ferramenta que permite realizar buscas de dispositivos conectados na rede como webcams, roteadores domésticos/empresariais, smartphones, tablets, computadores, servidores, sistemas de videoconferência, sistema de refrigeração, e, além disso, permite obter informações como servidores HTTP, FTP, SSH, Telnet, SNMP e SIP.

### Utilizando o Shodan

Há diversas versões, como aplicativos e a versão do *Shodan online*: [www.shodan.io](http://www.shodan.io).

Para usar todos os recursos é necessário realizar o registro.

Com o Shodan é possível utilizar *operadores* para refinar as buscas. Veja alguns exemplos:

- **country** – limita as buscas por países especificados;
- **city** – limita as buscas por cidades especificadas;
- **port** – limita as buscas somente por serviços que utilizam a porta especificada.

### Exemplos de buscas

```
os:"windows xp" city:"london" port:"80"
```

location.city:London metadata.os:ubuntu 80.http.get.title: "Welcome to Jboss"

The screenshot shows the Censys search interface with the following details:

- Quick Filters:** For all fields, see Data Definitions.
- Autonomous System:**
  - 2.48M AMAZON-02 - Amazon.com, Inc.
  - 1.1M AMAZON-AES - Amazon.com, Inc.
  - 1.02M DIGITALOCEAN-ASN - DigitalOcean, LLC
  - 831.82K OVH
  - 731.48K CLOUDFLAREN - Cloudflare, Inc.
  - [More](#)
- Protocol:**
  - 22.41M 80/http
  - 16.31M 443/https
  - 8.92M 22/ssh
  - 5.95M 21/ftp
  - 4.92M 3306/mysql
  - [More](#)
- Tag:**
  - 28.0M http
- IPv4 Hosts:** Page 1/3,415,692. Results: 35,392,283. Time: 426ms.
- Results:** 35,392,283 hosts found.
- Details:** The results list includes:
  - 18.130.80.20 (ec2-18-130-80-20.eu-west-2.compute.amazonaws.com)
    - AMAZON-02 - Amazon.com, Inc. (16509) → London, England, United Kingdom
    - Ubuntu → 22/ssh, 80/http, 8080/http
    - Welcome to JBoss Application Server 7
    - Q: location.city: London
  - 52.56.105.43 (ec2-52-56-105-43.eu-west-2.compute.amazonaws.com)
    - AMAZON-02 - Amazon.com, Inc. (16509) → London, England, United Kingdom
    - Ubuntu → 22/ssh, 8080/http
    - Q: location.city: London
  - 35.178.16.91 (ec2-35-178-16-91.eu-west-2.compute.amazonaws.com)
    - AMAZON-02 - Amazon.com, Inc. (16509) → London, England, United Kingdom
    - 443/https, 80/http
    - Welcome to JBoss AS → .tyresoft.biz
    - Q: 443.https.get.body. to
  - 52.56.213.249 (ec2-52-56-213-249.eu-west-2.compute.amazonaws.com)
    - AMAZON-02 - Amazon.com, Inc. (16509) → London, England, United Kingdom
    - 8080/http
    - Q: 8080.http.get.body. to
- Map:** Shows the geographical distribution of the hosts.
- Metadata:** Provides detailed information about each host.
- Report:** Generates a detailed report of the findings.

Mostra dispositivos na cidade de *Londres* utilizando o sistema operacional *Ubuntu*.

## Explorando as abas dos resultados apresentados

Na aba *Detalhes* é possível analisar os resultados que são utilizados para encontrar este tipo de pesquisa.

Na aba *WHOIS* é possível obter informações do dono do domínio do IP em que o dispositivo se encontra.

As informações apresentadas pelo Censys podem contribuir bastante para um atacante traçar uma linha estratégica para iniciar um ataque.

## Dicas

- 1) Mais opções sobre o uso do Censys podem ser encontradas no próprio site, na página: <https://censys.io/overview>.
- 2) No site do Censys é possível realizar buscas de operadores que podem ser utilizados

```
[*] Harvesting emails ....  
[*] Searching Google for email addresses from 4linux.com.br  
[*] Extracting emails from Google search results...  
[*] Searching Bing email addresses from 4linux.com.br  
[*] Extracting emails from Bing search results...  
[*] Searching Yahoo for email addresses from 4linux.com.br  
[*] Extracting emails from Yahoo search results...  
[*] Located 4 email addresses for 4linux.com.br  
[*] 5107b343.4070807@4linux.com.br  
[*] contato@4linux.com.br  
[*] marketing@4linux.com.br  
[*] treinamento@4linux.com.br  
[*] Auxiliary module execution completed
```

Observe que ele retornou no console alguns *e-mails* encontrados.

#### Dica

É interessante você saber até que ponto os endereços de e-mail da sua empresa estão expostos, a fim de evitar ser vítima desses ataques.

---

### ~#[Pensando\_fora.da.caixa]

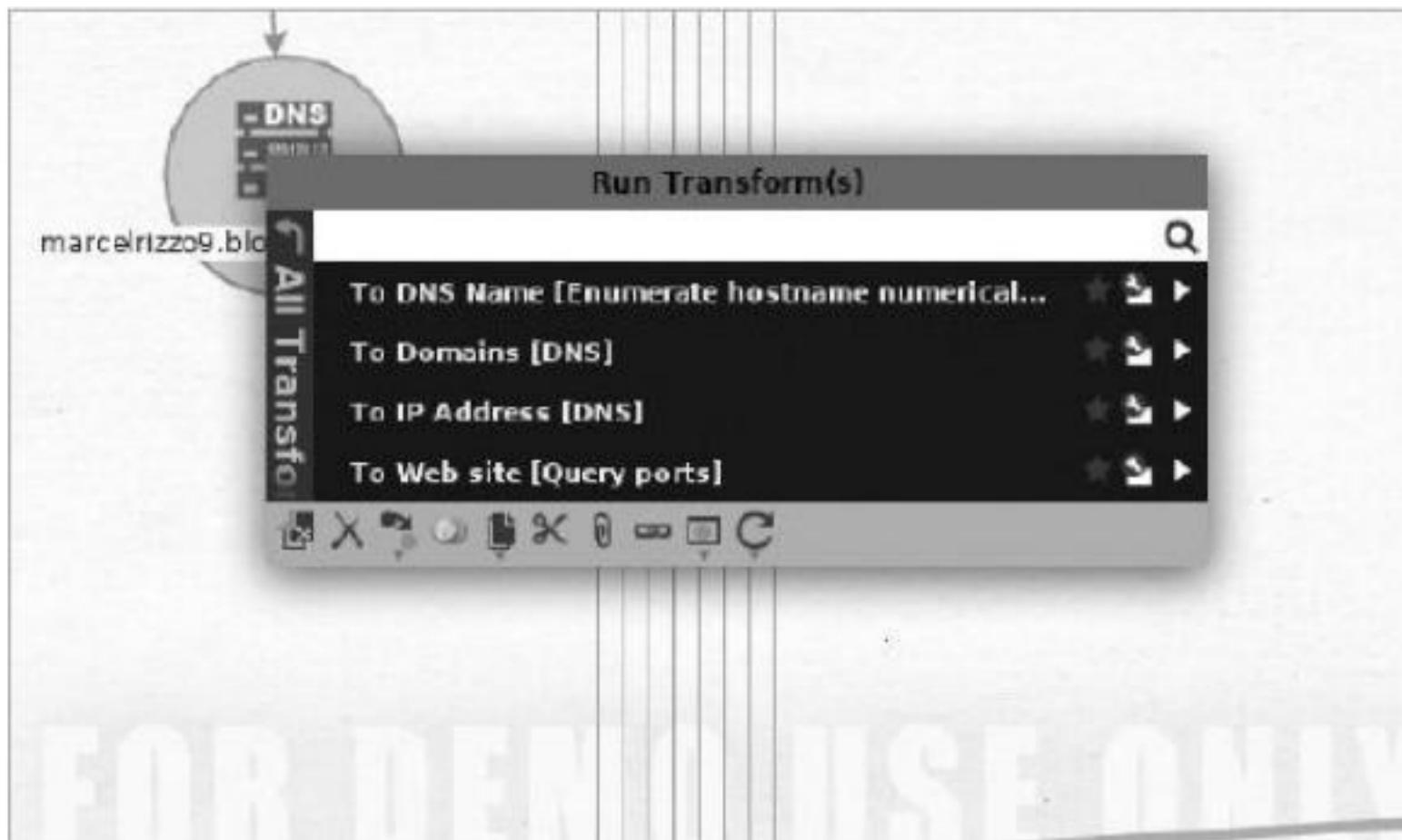
A coleta de e-mails pode ser utilizada para diversos fins, como engenharia social, rastreamento de usuários e engenharia reversa.

## Maltego<sup>6</sup>

O Maltego é uma ferramenta interativa de mineração de dados que processa gráficos direcionados para análise de links. A ferramenta é usada em investigações online para encontrar relações entre peças de informação de várias fontes localizadas na internet.

Ela usa a ideia de transformar para automatizar o processo de consulta de diferentes fontes de dados. Essas informações são exibidas em um gráfico baseado em nó adequado para executar a análise de link.

Atualmente, há três versões do cliente Maltego: *Maltego Community Edition* (CE), *Maltego Classic* e *Maltego XL*. Nossos testes serão focados no Maltego CE.



Converter IP para o nome e vice-versa.

