



# TÉCNICAS DE INVASÃO

APRENDA AS TÉCNICAS  
USADAS POR HACKERS  
EM INVASÕES REAIS\_

CRIADO POR  
BRUNO FRAGA



EDITORA  
**Labrador**



TÉCNICAS DE  
**INVASÃO**

CRIADO POR  
BRUNO FRAGA



# TÉCNICAS DE INVASÃO

APRENDA AS TÉCNICAS  
USADAS POR HACKERS  
EM INVASÕES REAIS\_

*Compilação*  
Thompson Vangler



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

www.editoralabrador.com.br

facebook.com/editoralabrador

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 Iha, 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 Vangler 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, m 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, ca 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.

¶e 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



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 ns 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 de nição 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 modi car tal informação.

A tríade CIA (con dentiality, integrity and availability) – con dencialidade, 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:

Con dencialidade – 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, caria exposta à alteração não autorizada por elemento malintencionado.

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 é 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 [e ISO 27000 Directory: www.27000.org](http://www.iso27000.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 de ne 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.

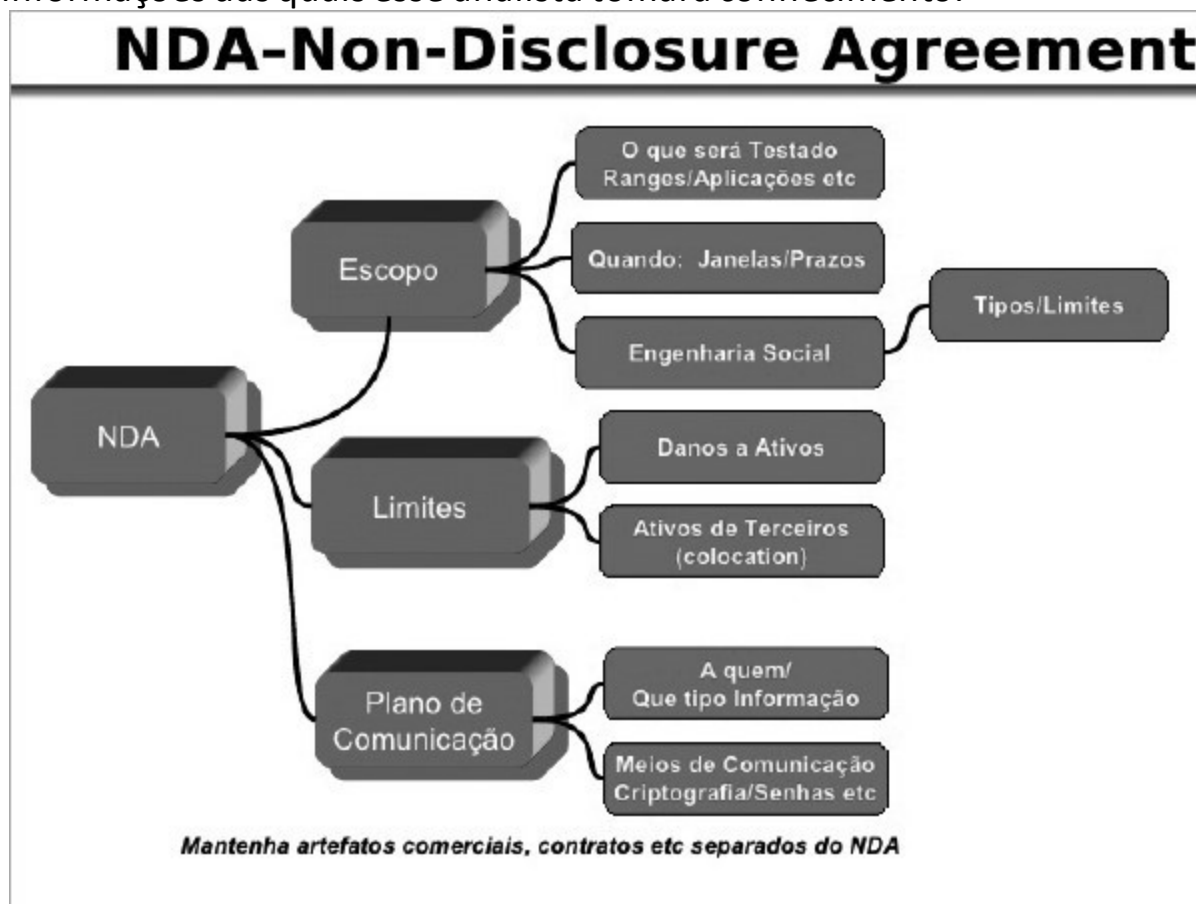
A ISO 27002 define algumas normas para serem seguidas quanto ao código de prática para a gestão da segurança da informação; para implementá-la em uma organização, é necessário que seja estabelecida uma estrutura para gerenciá-la. Para isso, as atividades de segurança da informação devem ser coordenadas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

Analisar – 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 ciência e proteja qualquer propriedade intelectual com a qual você se relaciona.

Divulgue responsabilmente, 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 EcCouncil: [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 colete, 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 consoante 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 nanceiras enganosas, como suborno, cobrança dupla ou outras práticas nanceiras 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 pro

ssional de segurança da informação. Veri que 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 pro ssão.

### De que lado?

Há uma discussão na área sobre qual chapéu um pro ssional da segurança está usando, ou seja, de que lado moral o pro ssional age com o conhecimento de técnicas de penetração. Normalmente, é de nido 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 inerentemente 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 com credenciais 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, de nem 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.penteststandard.org](http://www.penteststandard.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 – Conceção – 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 – Conceção – Acordo de confidencialidade.
7. Videoaula TDI – Conceção – 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-blackwhite-and-grey-hat-hackers>. Acesso em: 14 ago. 2019.
11. Videoaula TDI – Bootcamp – O Processo de penetration test.



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.

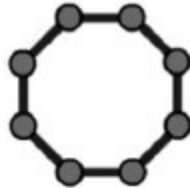
Personal Area Network (PAN) – são redes pessoais, como bluetooth.

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

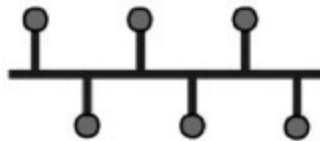
Wide Area Network (WAN) – são redes de grande extensão que podem interligar redes independentes; portanto, é uma rede de alcance mundial. A internet é o melhor exemplo de WAN.

## 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 bra óptica
- Rede de cabo de par trançado (UTP e STP)
- Rede sem os
- 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, la 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 de nível diretivas 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 processos 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:

Aplicação		Aplicação
	HTTP, FTP, Telnet, NTP, DHCP, PING	Apresentação
		Sessão
Transporte	TCP, UDP	Transporte
Rede	IP, ARP, ICMP, IGMP	Rede
		Dados
Interface de rede	Ethernet	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 com habilidade, 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 Window		
128	Checksum			Ponteiro de urgência		
160	Opções (opcional)					
Padding (até 32)						
224	Dados					
Detalhe do campo <i>Flags</i>						
+	10	11	12	13	14	15
96	<i>UrgPtr</i>	ACK	<i>Push</i>	RST	SYN	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

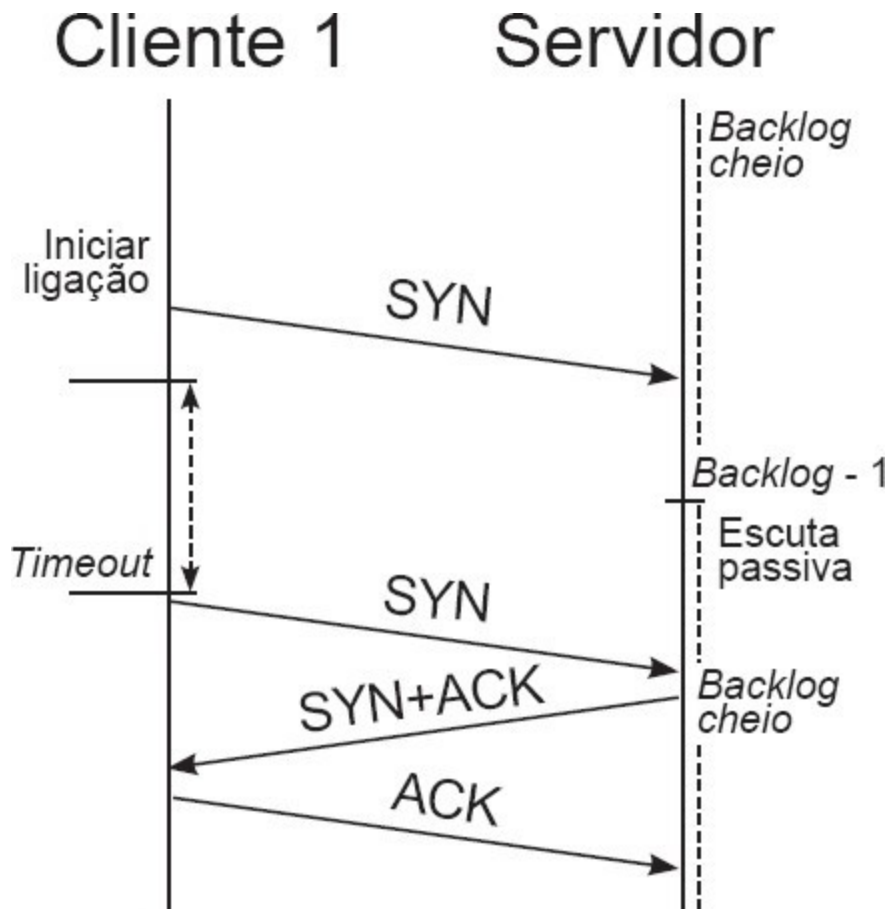
abertura passiva esteja estabelecida, um cliente pode iniciar uma abertura ativa. Para estabelecer uma conexão, o aperto de mão de três vias (ou três etapas) é realizado.

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.



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 ag SYN ativa, e espera-se que o servidor aceite a ligação enviando um pacote SYNACK.

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).

Nesta 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 car completamente preenchido, a ligação é rejeitada, ignorando (silenciosamente) todos os subseqüentes pacotes SYN.

## Transferência de dados (sessão)

Durante a fase de transferência, o TCP está equipado com vários mecanismos que asseguram a con abilidade e robustez: números de sequência que garantem a entrega ordenada, código detector de erros (checksum) para detecção de falhas em segmentos especí cos, con rmação 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 con rmação (acknowledgment). O emissor determina o seu próprio número de sequência e o receptor con rma o segmento usando como número ACK o número de sequência do emissor. Para manter a con abilidade, o receptor con rma os segmentos indicando que recebeu um determinado número de bytes contíguos. Uma das melhorias introduzidas no TCP foi a possibilidade de o receptor con rmar 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,  $2^{31}-1$ , tomando o valor da diferença. Assim, a escolha do ISN torna-se vital para a robustez deste protocolo.

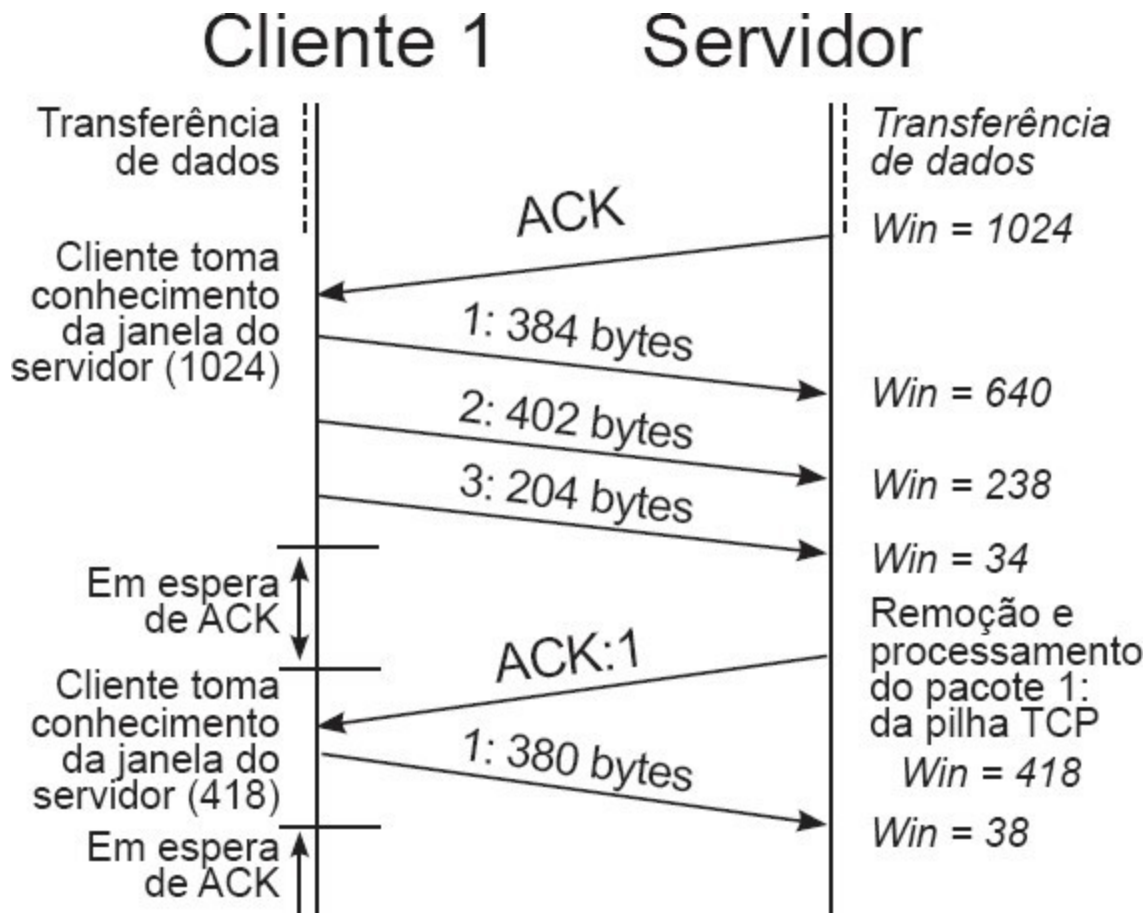
O campo checksum permite assegurar a integridade do segmento. Ele é expresso em complemento para um, consistindo na soma dos valores (em complemento para um) da trama. A escolha da operação de soma em complemento para um deve-se ao fato de ela poder ser calculada da mesma forma para múltiplos deste comprimento (16 bit, 32 bit, 64 bit etc.) e o resultado, quando encapsulado, será o mesmo. A veri cação 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 sabe 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 de nido unicamente durante o estabelecimento da ligação.

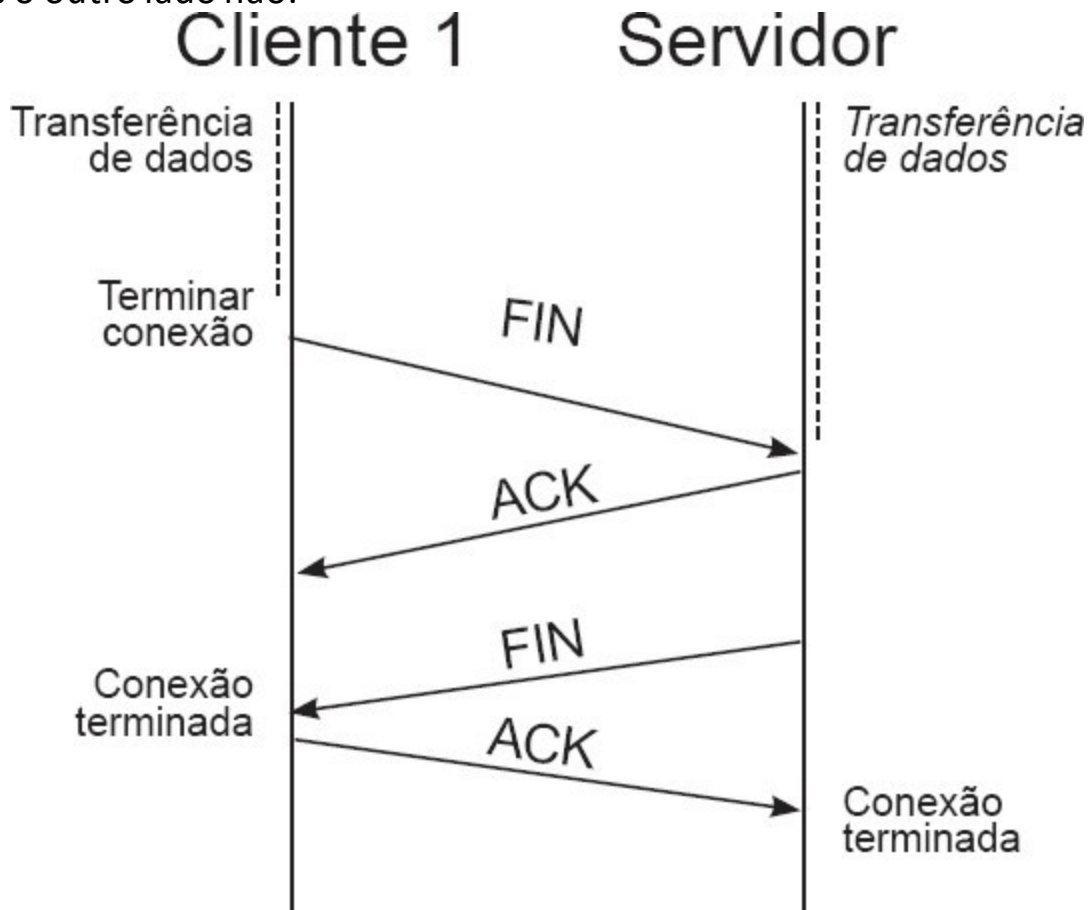
### Término da ligação

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 nalizar a sessão, envia um pacote



com a ag 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. Chamase 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.



#### 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, de nido 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



## 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 de nido 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<sub>3</sub> 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 através do nome, por exemplo, guardweb.com.br, ele envia uma consulta pela internet para encontrar o website solicitado.

Uma consulta é uma pergunta em busca do nome de domínio correspondente ao IP.

Vamos verificar como essas requisições funcionam.

O primeiro servidor a ser consultado interage com o seu solucionador recursivo, que normalmente é operado por um provedor de serviços de internet (ISP).

O solucionador recursivo sabe qual outro servidor de DNS deve consultar para responder à sua pergunta original: “Qual é o endereço IP do website guardweb.com.br?”

Servidores Raiz (Root) – o primeiro tipo de servidor DNS com o qual o solucionador recursivo se comunica é um servidor root. Os servidores root estão em todo o globo e cada um deles possui informações do DNS sobre domínios de primeiro nível como o .br. Para começar a responder à

consulta realizada, o solucionador recursivo pede a um root server informações de DNS sobre o .br.

Servidor de nomes TLD (Top Level Domain) – cada servidor de nomes DNS de domínio de primeiro nível (TLD) armazena informação de endereço para domínios de segundo nível (guardweb.com) dentro do domínio de primeiro nível (.br). Quando sua consulta chega ao servidor TLD, ele responde com o endereço IP do servidor de nomes de domínio, que proporcionará a próxima parte do domínio.

Servidor de nomes de domínio – em seguida, o solucionador recursivo envia a consulta ao servidor nome de domínio. O servidor de DNS conhece o endereço IP do domínio completo, o guardweb.com.br, e essa resposta é enviada ao solucionador recursivo.

NOME DE DOMÍNIO		IPv4		IPv6
guardweb.com.br	104.31.87.52	2400:cb00:2048:1::681f:5734		

À medida que a internet suporta cada vez mais usuários, conteúdos e aplicativos, o padrão original de IP, IPv4, que permite até 4,3 bilhões de endereços IP exclusivos, será substituído pelo IPv6, que suportará 340 undecilhões de endereços IP exclusivos.

## VPN – Virtual Private Network

Uma VPN,<sup>6</sup> rede virtual privada, é uma conexão estabelecida sobre uma infraestrutura pública ou compartilhada, usando tecnologias de tunelamento e criptografia para manter seguros os dados trafegados. VPNs seguras usam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Alguns desses protocolos que são normalmente aplicados em uma VPN são: L2TP, L2F, PPTP e o IPSec. Quando adequadamente implementados, esses protocolos podem assegurar comunicações seguras por meio de redes inseguras.

Deve ser notado que a escolha, a implementação e uso desses protocolos não é algo trivial, e várias soluções de VPN inseguras são distribuídas no mercado. Advertem-se os usuários para que investiguem com cuidado os produtos que fornecem VPNs.

Para se configurar uma VPN, é preciso utilizar serviços de acesso remoto, tal como o RAS, encontrado no Windows 2000 e em versões posteriores, ou o SSH, encontrado nos sistemas GNU/Linux e outras variantes do Unix.

## Funcionamento da VPN

Quando uma rede quer enviar dados para a outra rede através da VPN, um protocolo, como o IPSec, faz o encapsulamento do quadro normal com o cabeçalho IP da rede local e adiciona o cabeçalho IP da internet atribuída ao roteador, um cabeçalho AH, que é o cabeçalho de autenticação, e o cabeçalho ESP, que é o cabeçalho que provê integridade, autenticidade e criptografia à área de dados do pacote. Quando esses dados encapsulados chegarem à outra extremidade, é feito o desencapsulamento do IPSec, e os dados são encaminhados ao referido destino da rede local.

## Proxy

O proxy é um servidor que age como um intermediário para requisições de clientes solicitando recursos de outros servidores. Um cliente conecta-se ao servidor proxy, solicitando algum serviço, como um arquivo, conexão, página web ou outros recursos disponíveis de um servidor diferente, e o proxy avalia a solicitação como um meio de simplificar e controlar sua complexidade.

Os proxies foram inventados para adicionar estrutura e encapsulamento a sistemas distribuídos. Atualmente, a maioria dos proxies é proxy web, facilitando o acesso ao conteúdo na World Wide Web e fornecendo anonimato.

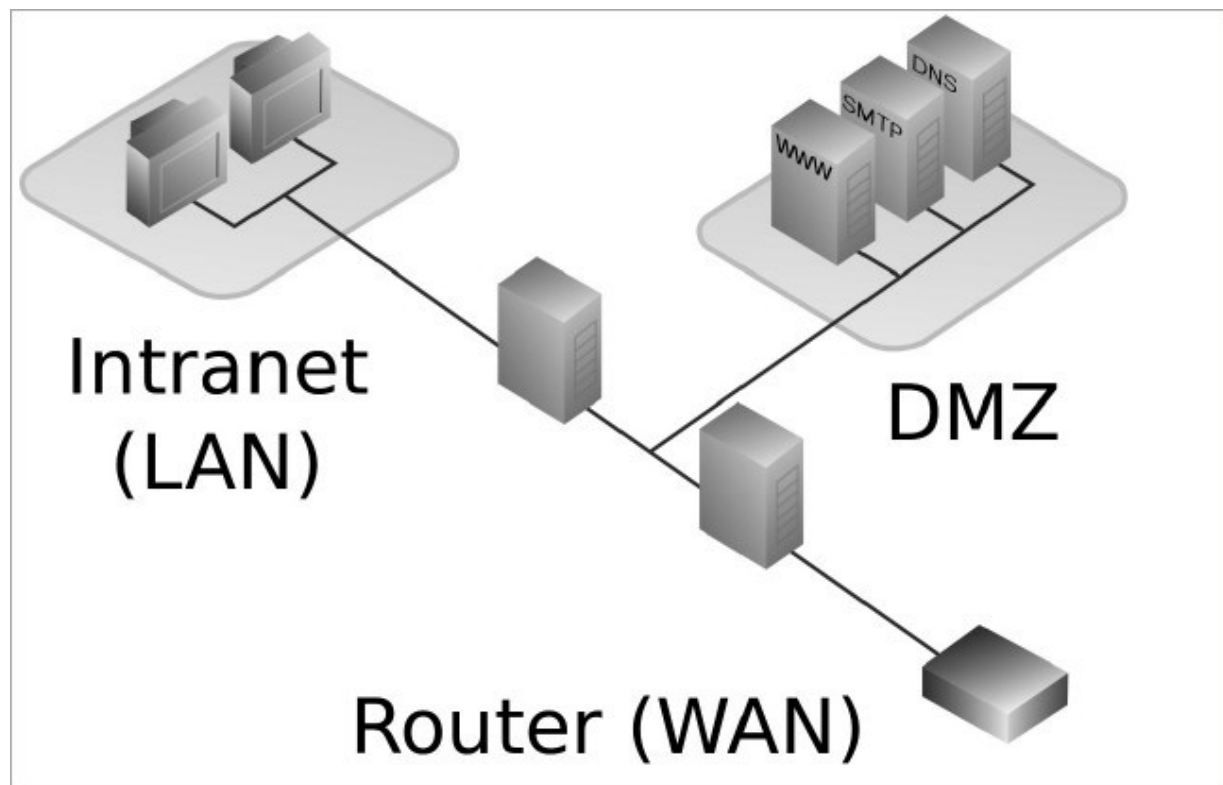
Um servidor proxy pode, opcionalmente, alterar a requisição do cliente ou a resposta do servidor e, algumas vezes, pode disponibilizar esse recurso mesmo sem se conectar ao servidor especificado. Pode também atuar como um servidor que armazena dados em forma de cache em redes de computadores. São instalados em máquinas com ligações tipicamente superiores às dos clientes e com poder de armazenamento elevado.

Esses servidores têm uma série de usos, como filtrar conteúdo, providenciar anonimato, 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 conável, normalmente a internet. Quaisquer dispositivos situados nesta área – isto é, entre a rede conável (geralmente a rede privada local) e a rede não conável (geralmente a internet) – estão 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.

## DynDNS – Dynamic Domain Name System

O DynDNS,<sup>9</sup> ou DNS dinâmico, é um método de atualizar automaticamente um servidor de nomes no Domain Name System (DNS), com a configuração de DynDNS ativando seus nomes de hosts configurados, endereços ou outras informações. Ele é padronizado pelo RFC 2136.

## SSH – Secure Shell

O SSH<sup>10</sup> é um protocolo de rede criptográfico para operação de serviços de rede de forma segura sobre uma rede insegura. A melhor aplicação de exemplo conhecida é para login remoto a sistemas de computadores pelos usuários.

O SSH fornece um canal seguro sobre uma rede insegura em uma arquitetura cliente-servidor, conectando uma aplicação cliente SSH com um servidor SSH. Aplicações comuns incluem login em linha de comando remoto e execução remota de comandos, mas qualquer serviço de rede pode ser protegido com SSH. A especificação do protocolo distingue entre duas versões maiores, referidas como SSH-1 e SSH-2.

A aplicação mais visível do protocolo é para acesso a contas shell em sistemas operacionais do tipo Unix, mas também se verifica algum uso limitado no Windows.

O SSH foi projetado como um substituto para o Telnet e para protocolos de shell remotos inseguros como os protocolos Berkeley rlogin, rsh e rexec. Esses protocolos enviam informações, notavelmente senhas, em texto puro, tornando-os suscetíveis à interceptação e divulgação, usando análise de pacotes. A criptografia usada pelo SSH objetiva fornecer confidencialidade e integridade de dados sobre uma rede insegura, como a internet. Por padrão esse protocolo é atribuído à porta 22.

## Conectando a um host com o SSH – Linux

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

```
root@kali:~# ssh msfadmin@172.16.0.12
```



```

The authenticity of host '172.16.0.12 (172.16.0.12)' can't be
established.
RSA key fingerprint is
SHA256:BQHm5EoHX9GCiF3uVscegPXLQOsuPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.0.12' (RSA) to the list of known
hosts. msfadmin@172.16.0.12's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC
2008 i686

...
msfadmin@metasploitable:~$

```

SSH: executa a aplicação SSH para conectar a um host.

msfadmin@172.16.0.12: msfadmin indica o usuário com credenciais na máquina com o IP 172.16.0.12.

Observe que esse comando iniciou a conexão na máquina 172.16.0.12 com o usuário msfadmin. Como é a primeira vez que essa conexão é realizada, ele vai solicitar a permissão para realizar a troca de chaves de segurança. Após ser realizada a troca de chaves, entramos com a senha do usuário msfadmin e obtivemos acesso à shell deste usuário na máquina remota.

## Transferir arquivos com o scp – Linux

O comando scp utiliza o protocolo SSH para enviar e receber arquivos de outras máquinas Linux. Para utilizá-lo abra o terminal e digite:

```

root@kali:~# scp -P 22 /root/test.txt
msfadmin@172.16.0.12:/home/msfadmin: msfadmin@172.16.0.12'
n password: test.txt 100% 3675KB
30.9MB/s 00:00

```

scp: executa a aplicação para transferir os arquivos scp.

-P 22: indica a porta SSH do host de destino, neste caso a porta padrão 22.

/root/test.txt: indica o arquivo que será transferido.  
msfadmin@172.16.0.12: indica o usuário e IP do host que vai receber os arquivos.

:/home/msfadmin: indica o local onde os arquivos serão gravados no destino.

Acesse a máquina de destino e verifique se o arquivo foi copiado no diretório /home/msfadmin.

## Telnet<sup>11</sup>

O protocolo Telnet é um protocolo padrão da internet que permite obter uma interface de terminais e aplicações pela internet. Este protocolo fornece as regras básicas para ligar um cliente a um servidor.

Ele se baseia em uma conexão TCP para enviar dados em formato ASCII codificados em 8 bits entre os quais se intercalam sequências de controle Telnet. Fornece, assim, um sistema orientado para a comunicação, bidirecional (half-duplex), codificado em 8 bits, fácil de aplicar.

Este é um protocolo básico, no qual outros protocolos da sequência TCP/IP (FTP, SMTP, POP3 etc.) se apoiam. As especificações do Telnet não mencionam a autenticação porque ele está totalmente separado dos aplicativos que o utilizam (o protocolo FTP depende de uma sequência de autenticação acima do Telnet).

Além disso, o Telnet é um protocolo de transferência de dados sem proteção, o que quer dizer que os dados circulam abertamente na rede, ou seja, eles não são criptografados. Quando o protocolo Telnet é utilizado para ligar um hóspede distante a uma máquina que serve como servidor, por padrão esse protocolo é atribuído à porta 23.

## Utilizando o Telnet – Linux<sup>12</sup>

Através do telnet é possível realizar conexões em máquinas remotas e utilizá-lo para testar conexões em portas específicas.

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

```
root@kali:~# telnet 172.16.0.12
```

```
Trying 172.16.0.12...
```

```
Connected to 172.16.0.12.
```

```
Escape character is '^]'.
```

...

Login with msfadmin/msfadmin to get started

metasploitable login:

telnet: executa a aplicação telnet para iniciar uma conexão em um host.  
172.16.0.12: indica o IP do host de destino.

Este comando vai iniciar uma conexão remota no host. Agora vamos utilizar o telnet para testar conexões em portas específicas; abra o terminal e digite:

```
root@kali:~# telnet 172.16.0.12 22
```

```
Trying 172.16.0.12...
```

```
Connected to 172.16.0.12.
```

```
Escape character is '^]'.
```

```
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

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,TSval 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,TSval 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 lter 11 packets dropped by kernel
```

tcpdump: executa a aplicação utilitário de rede tcpdump.

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

Para o processo, pressione Ctrl + C. Observe que esse comando mostra em tela todo o tráfego de pacotes da rede; dessa forma, é muito difícil analisar todos esses pacotes.

Vamos passar algumas opções do TCPdump para obter resultados mais específicos, como capturar o tráfego de protocolos icmp:

```
root@kali:~# tcpdump -n -i eth0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol
decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144
bytes
16:13:28.555029 IP 172.16.0.10 > 172.16.0.15: ICMP echo request, id
20129, seq 18, length 64
16:13:28.555056 IP 172.16.0.15 > 172.16.0.10: ICMP echo reply, id
20129, seq 18, length 64
16:13:28.576266 IP 172.16.0.12 > 172.16.0.15: ICMP echo request, id
9746, seq 36, length 64
16:13:28.576311 IP 172.16.0.15 > 172.16.0.12: ICMP echo reply, id
9746, seq 36, length 64
16:13:29.576604 IP 172.16.0.12 > 172.16.0.15: ICMP echo request, id
9746, seq 37, length 64
```

-n: orienta o TCPdump a não resolver nomes, apresentando somente o endereço IP. icmp: indica o protocolo a ser apresentado na saída do comando, neste caso o protocolo icmp.

Observe que foram apresentados em tela somente os pacotes sem a resolução de nomes na interface eth0 com protocolo icmp. Podemos utilizar esse comando para capturar vários tipos de protocolo, como tcp, ip, ip6 arp, rarp e decnet.

## Salvar capturas – TCPdump

Podemos também salvar a captura dos pacotes em um arquivo com um formato específico, para ser utilizado para leitura posterior pelo TCPdump e outras aplicações como o Wireshark. Abra o terminal e digite:

```
root@kali:~# tcpdump -i eth0 -w tcpdump01.cap
```

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size
262144 bytes
^C40 packets captured
43 packets received by lter
0 packets dropped by kernel
```

-w tcpdump01.cap: orienta o TCPdump a escrever os pacotes capturados em um arquivo; neste caso, o arquivo tcpdump01.cap.

Dessa forma vamos capturar todo o tráfego até a interrupção do programa. Para interromper, pressione as teclas Ctrl + C, mas lembre-se de que é possível realizar a leitura posteriormente.

## Analisar capturas TCPdump

Após capturar o tráfego é possível realizar a leitura deste arquivo e concatenar com outros comandos para filtrar a busca e apresentar em tela apenas as informações específicas. Veja a seguir dois exemplos.

### Capturar pacotes HTTP e HTTPS

```
root@kali:~# tcpdump -r tcpdump01.cap | grep http
reading from file tcpdump01.cap, link-type EN10MB (Ethernet)
16:48:39.842206 IP kali.45934 > ec2-50-19-103-
176.compute1.amazonaws.com.http: Flags
[S], seq 3703792603, win 29200, options [mss 1460,sackOK,TS val
530467 ecr 0,nop,wscale 7], length 0
16:48:40.383868 IP 151.101.61.177.https > kali.36780: Flags [.], seq
54186:55570, ack 1553, win 71, options [nop,nop,TS val 1514293303
ecr 530597], length 1384
...
```

-r tcpdump01.cap: -r orienta o TCPdump a ler um arquivo; neste caso, o arquivo tcpdump01.cap. |: concatena o comando anterior com o comando seguinte.

grep http: ltra o arquivo tcpdump01.cap trazendo informações que contenham a palavra http.

Observe que foi apresentado em tela apenas o tráfego de conexões HTTP e HTTPS realizadas.

### Capturar pacotes UDP

```
root@kali:~# tcpdump -r tcpdump01.cap | grep UDP reading from le
tcpdump01.cap, link-type EN10MB (Ethernet) 17:13:18.166615 IP
172.16.0.10.46899 > kali.44444: UDP, length 1472
17:13:18.202772 IP 172.16.0.10.46899 > kali.44445: UDP, length 1472
17:13:20.870064 IP 172.16.0.10.60509 >
```

|: concatena o comando anterior com o comando seguinte.

grep UDP: ltra o arquivo tcpdump01.cap trazendo informações que contenham a palavra UDP.

Observe que foram apresentados em tela apenas os tráfegos de conexões UDP. Utilizando o grep podemos ltrar qualquer tipo de informações em um arquivo; basta indicar a palavra que você necessita.

### Filtros avançados no TCPdump

Podemos utilizar o comando TCPdump para usar alguns ltros, a m de realizar buscas especí cas de pacotes. Abra o terminal e digite:

```
root@kali:~# tcpdump -n -c 4 -i eth0 icmp and src 172.16.0.15
tcpdump: verbose output suppressed, use -v or -vv for full protocol
decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144
bytes
22:51:33.050794 IP 172.16.0.15 > 172.16.0.10: ICMP echo reply, id
25746, seq 625, length 64
```

```
22:51:34.074810 IP 172.16.0.15 > 172.16.0.10: ICMP echo reply, id
25746, seq 626, length 64
22:51:35.098865 IP 172.16.0.15 > 172.16.0.10: ICMP echo reply, id
25746, seq 627, length 64
22:51:36.122800 IP 172.16.0.15 > 172.16.0.10: ICMP echo reply, id
25746, seq 628, length 64
4 packets captured
4 packets received by lter
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:



```

root@kali:~# netstat -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address      Foreign Address    State
tcp      0  188 172.16.0.15:22     172.16.0.10:37930  ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State      I-Node Path
unix  2    []    DGRAM           17008 /run/user/0/systemd/notify
unix  3    []    DGRAM           9367 /run/systemd/notify
unix  2    []    DGRAM          21661 /run/user/1000/systemd/notify
unix 21    []    DGRAM           9382 /run/systemd/journal/dev-log
unix  3    []    STREAM  CONNECTED  19946 /run/user/0/bus

```

**netstat:** executa o utilitário de rede netstat.

**-n:** indica ao netstat para não resolver nomes.

Este comando apresenta as conexões existentes da máquina:

```

root@kali:~# netstat -na
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address      Foreign Address    State
tcp      0  0 0.0.0.0:22         0.0.0.0:*          LISTEN
tcp      0  0 172.16.0.15:22     172.16.0.10:37930  ESTABLISHED
tcp6     0  0 :::22              :::*                LISTEN
udp      0  0 0.0.0.0:68         0.0.0.0:*
raw6     0  0 :::58              :::*                7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags   Type       State      I-Node Path
unix  2  [ACC]  STREAM  LISTENING  15452 @/tmp/dbus-C0OLmKjL
unix  2  [ACC]  STREAM  LISTENING  17611 @/tmp/dbus-qxiCx6ag
unix  2  [ACC]  STREAM  LISTENING  17831 @/tmp/.ICE-unix/1062
unix  2  [ACC]  STREAM  LISTENING  15674 @/tmp/.X11-unix/X0
unix  2  [ACC]  STREAM  LISTENING  17110 @/tmp/.X11-unix/X1

```

**-a:** exibe todas as conexões existentes no computador.

**-n:** exibe todas as conexões existentes sem resolver nomes.

Observe que dessa forma o TCPdump apresenta todas as conexões existentes do computador, incluindo todos os protocolos e sockets (tcp, udp, raw).

As ags do comando netstat usadas podem ser somadas facilmente. Veja a seguir uma lista de alguns comandos e seus signi cados do netstat:

Exibe o temporizador da conexão, ou seja, há quanto tempo essa conexão está estabelecida. Pode-se combinar à vontade: netstat -autno, netstat -axuo.

Exibe as informações de todas as interfaces ativas. Podemos ter estatísticas de erros de entrada/saída, assim como estatística de tráfego.

Repete o comando ao nal, muito útil para veri car o momento exato que uma conexão é estabelecida ou para ter noção do aumento de tráfego nas interfaces, por exemplo: netstat -ic, netstat -atnc.

Exibe uma lista mais completa. Deve ser combinado com as outras opções, como o netstat -atne.

Com esse comando temos mais duas colunas, USER e INODE, ou seja, o usuário que subiu o processo que originou a abertura da porta e o INODE pertencente.

Exibe o daemon e o PID que estão ligados a essa porta, muito importante para detectarmos o daemon responsável.

---

Exibe as estatísticas dos protocolos, ou seja, quanto foi trafegado em cada protocolo. Podemos fazer combinações para, assim, pegarmos a estatística de um determinado protocolo, por exemplo: netstat -st, netstat -su.

## Filtrando a busca – netstat

Podemos ltrar a busca para encontrar apenas pacotes TCP. Digite no terminal:

```
root@kali:~# netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp    0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp    0      0 172.16.0.15:48430      23.111.11.111:443       ESTABLISHED
tcp    0      0 172.16.0.15:43666      157.240.1.23:443       ESTABLISHED
tcp    0      0 172.16.0.15:37096      0.0.0.0:0               200.221.2.45:80
TIME_WAIT
tcp    0      0 172.16.0.15:56990      173.194.139.252:443    ESTABLISHED
tcp    0      0 172.16.0.15:58080      52.33.209.128:443      TIME_WAIT
tcp    0      0 172.16.0.15:51764
...
```

-t: indica ao netstat para apresentar conexões TCP.

Podemos verificar o estado das conexões realizadas pela máquina.  
Digite no terminal:

```
root@kali:~# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address      Foreign Address    State
tcp      0      0 0.0.0.0:22         0.0.0.0:*         LISTEN
tcp      0      0 172.16.0.15:51746  54.148.10.141:443  TIME_WAIT
        0      0 172.16.0.15:35830  216.58.206.110:443 ESTABLISHED
tcp6     0      0 :::22              :::*              LISTEN
udp      0      0 0.0.0.0:68         0.0.0.0:*
```

Dessa forma, se alguém estiver tentando realizar conexão ou já estiver com ela estabelecida, conseguimos identificar.

Podemos filtrar a busca para descobrir todas as conexões UDP e TCP.  
Digite no terminal:

```
root@kali:~# netstat -tupn
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address      Foreign Address    State  PID/Program name
tcp      0      0 0.0.0.0:22         0.0.0.0:*         LISTEN 1735/sshd
tcp      0      0 172.16.0.15:22     172.16.0.10:37930 ESTABLISHED 1737/sshd: madvan [
tcp      0      0 172.16.0.15:39142  216.58.206.46:443 ESTABLISHED 2752/firefox-esr
tcp      0      0 172.16.0.15:60640  81.20.48.165:80   ESTABLISHED 2752/firefox-esr
tcp6     0      0 :::22              :::*              LISTEN 1735/sshd
udp      0      0 0.0.0.0:68         0.0.0.0:*         670/dhclient
```

Dessa forma, temos as informações de todas as conexões UDP e TCP, mostrando o estado da conexão e a exibição do programa que está utilizando essa conexão.

- 
1. TRANSMISSION CONTROL PROTOCOL. In: WIKIPEDIA: a enciclopédia livre. [São Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: [https://pt.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](https://pt.wikipedia.org/wiki/Transmission_Control_Protocol). Acesso em: 14 ago. 2019.
  2. INTERNET CONTROL MESSAGE PROTOCOL. In: WIKIPEDIA: a enciclopédia livre. [São Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: [https://pt.wikipedia.org/wiki/Internet\\_Control\\_Message\\_Protocol](https://pt.wikipedia.org/wiki/Internet_Control_Message_Protocol). Acesso em: 14 ago. 2019.
  3. HYPERTEXT TRANSFER PROTOCOL. In: WIKIPEDIA: a enciclopédia livre. [São Francisco, CA:

Wikimedia Foundation, 2019]. Disponível em: [https://pt.wikipedia.org/wiki/Hypertext\\_Transfer\\_Protocol](https://pt.wikipedia.org/wiki/Hypertext_Transfer_Protocol). Acesso em: 14 ago. 2019.

4. SISTEMA DE NOMES DE DOMÍNIO. In: WIKIPEDIA: a enciclopédia 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 enciclopédia 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 enciclopédia 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 enciclopédia 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 enciclopédia 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 enciclopédia 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 enciclopédia 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.



Há diversas maneiras de conhecer detalhes sobre um alvo. Para isso, podemos utilizar técnicas simples, que serão abordadas neste capítulo.

### Navegando no site do alvo<sup>1</sup>

Podemos conhecer mais sobre a infraestrutura de TI, nosso alvo, navegando no site, em busca de informações com páginas de erros. Uma possibilidade é inserir na URL alguma página que não existe e verificar a apresentação do erro. Veja o exemplo a seguir:



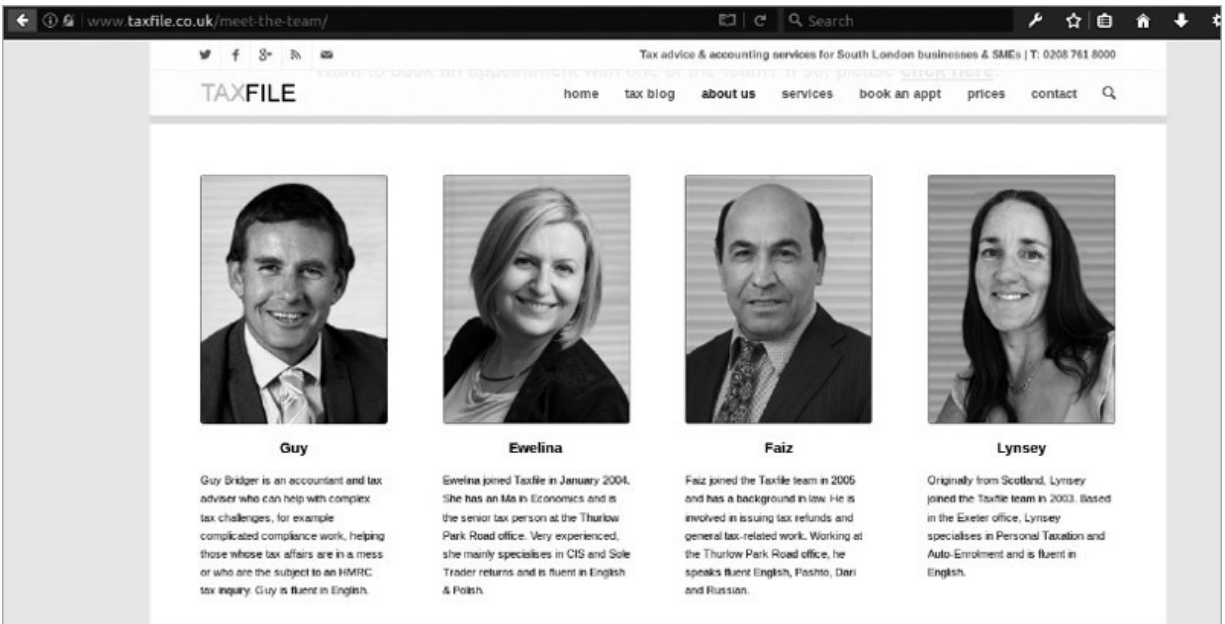
Observe que na URL foi inserida uma página com o nome errado no site e ele retornou uma mensagem de erro HTTP 404 informando que a página procurada não foi encontrada; observe também que ele informou o nome do serviço web, o Apache.

Na própria URL é informado o tipo de linguagem em que o site foi desenvolvido; neste caso, PHP.

<http://temporealcontabilidade.com.br/empresaTT.php>

O conhecimento do alvo não se limita apenas à estrutura de TI. Podemos encontrar em alguns sites de empresas informações sobre os funcionários.

Veja o exemplo a seguir:



É possível analisar informações sobre cada funcionários e aplicar ataques de engenharia social se necessário.

## Sites de emprego<sup>2</sup>

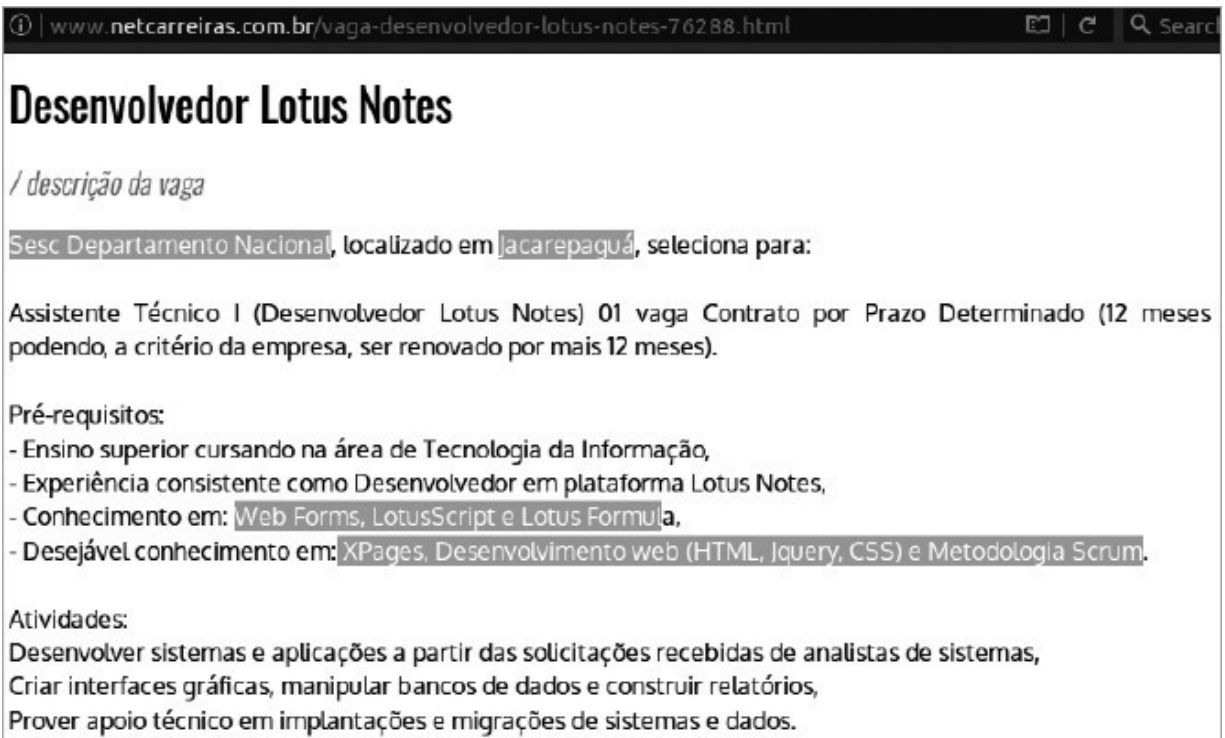
É possível obter informações sobre um alvo procurando em vagas de emprego na área de TI para vericar quais são os sistemas, aplicativos, banco de dados e programas utilizados.

Essas informações podem ser obtidas no próprio site da empresa, na seção “Trabalhe conosco”, ou em sites de busca de vagas, como o LinkedIn.

Alguns sites de busca de emprego podem manter a confidencialidade, ocultando o nome da empresa, mas vamos vericar alguns exemplos em que as empresas estão expostas.



## Exemplo 1



**Desenvolvedor Lotus Notes**

/ descrição da vaga

Sesc Departamento Nacional, localizado em Jacarepaguá, seleciona para:

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).

**Pré-requisitos:**

- 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,
- Desejável conhecimento em: XPages, Desenvolvimento web (HTML, JQuery, CSS) e Metodologia Scrum.


**Atividades:**





Desenvolver sistemas e aplicações a partir das solicitações recebidas de analistas de sistemas,  
Criar interfaces gráficas, manipular bancos de dados e construir relatórios,  
Prover apoio técnico em implantações e migrações de sistemas e dados.

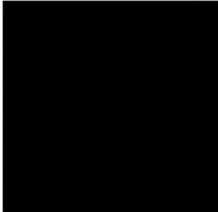
Observe que essa vaga nos passa muita informação sobre a estrutura de TI de uma empresa em Jacarepaguá, Rio de Janeiro. É uma vaga para desenvolvedores em Lotus Notes. Como pré-requisitos, o site informa métodos de programação e nome das linguagens lá utilizadas.


## Exemplo 2





 Home
  My Network
  Jobs
  Messaging



**ANALISTA DE REDES SR**  
 SKY Brasil · São Paulo e Região, Brasil  
 Posted 2 weeks ago · 3,812 views  
 2 alumni work here

### Job description

**Analista de Redes Sr**, na área de Engenharia sistemas de redes e infraestrutura, parte da **VP Engenharia de Transmissão**. O local de trabalho é na região do **Tamboré**, em São Paulo.

**SOBRE A ÁREA DE ENGENHARIA DE TRANSMISSÃO:**

A SKY foi pioneira no lançamento de uma série de novidades que trouxeram inovações tecnológicas para a televisão no Brasil. Isso só foi possível com uma equipe comprometida a entregar um serviço de alta qualidade para clientes em todo o território nacional, utilizando soluções que somente a SKY possui. Quer fazer parte deste time? Venha para a SKY você também!

**Atividades:**

- Administrar e configurar servidores (hardware - Blade e físico) e **VMware**. Atuar com a instalação, administração e suporte de sistemas operacionais dos servidores da engenharia SKY (**Linux e Windows**);
- Monitorar a utilização de recursos de infraestrutura;
- Realizar diagnósticos e atuar na correção de problemas na infraestrutura de server e storage;
- Administrar, configurar e manter os serviços de infraestrutura, como **DNS**, compartilhamento de arquivos, balanceamento de aplicação e AD Fornecer suporte a serviços de HTTP Server (Apache, IIS) e banco de dados (MySQL, SQL Server e Oracle);
- Instalar e administrar a solução de backup Instalar e administrar soluções de NAS (Netapp e Isilon) e de Bloco (hitachi e 3PAR).

**Conhecimentos:**

- **Linux**;
- Conhecimento de **backup via dataprotector**;
- **Storage EMC-ISILON**;
- **Storage 3PAR**;
- **Windows**;
- **DNS, AD e Load Balancer F5**;
- Formação completa;

**Seniority Level**  
Not Applicable

**Industry**  
Telecommunications

**Employment Type**  
Full-time

**Job Functions**  
Engineering

Observe que essa vaga para Analista de Redes Sênior informa: os sistemas operacionais utilizados (Linux, Windows e VMware), os servidores web (Apache e IIS), o banco de dados (MySQL, Oracle e SQL Server) e os equipamentos de armazenamento (storage 3PAR, Hitachi).

---

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

Estas informações que podem ser encontradas em vagas de empregos podem agilizar muito a busca de informações de infraestrutura de TI do alvo a ser analisado.

### Consultas WHOIS

O WHOIS é um mecanismo que registra domínios, IPs e sistemas autônomos na internet e que serve para identificar o proprietário de um site. Alimentado por companhias de hospedagem, ele reúne todas as informações pertencentes a uma página. No Brasil, o WHOIS é atrelado a um CNPJ ou a um CPF.

Tecnicamente falando, o WHOIS é um protocolo TCP que tem como objetivo consultar contato e DNS. Ele apresenta, geralmente, três principais linhas de contato do dono de um website: o contato administrativo; o contato técnico; e o contato de cobrança. Além disso, são exibidos telefones e endereços físicos.

Sabemos que o serviço DNS faz com que todos os nomes na internet sejam resolvidos para o IP. Há uma organização que controla esses registros na internet, o IANA (Internet Assigned Numbers Authority), a autoridade máxima que controla números para protocolos, os domínios de nível superior de código de país e mantém as alocações de endereço IP de todos os roots servers do globo.

No site da IANA podemos encontrar uma lista de todos esses servidores no globo que fazem a administração total de DNS e IPs.

Caso você queira saber mais sobre os roots servers, acesse o link a seguir: [www.iana.org/domains/root/servers](http://www.iana.org/domains/root/servers).

## Utilizando o WHOIS na web

Há muitos serviços na internet que realizam consultas WHOIS. Um deles é uma página no site do IANA: [www.iana.org/whois](http://www.iana.org/whois).

Vamos realizar uma consulta do site da GuardWeb. Entre com o site no campo de pesquisa, como mostra a imagem na página seguinte.

Observe que ele vai retornar informações do IP público do site e informações 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.

<input type="text" value="guardweb.com.br"/>	<input type="button" value="Submit"/>
--	---------------------------------------

```
% 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: Comitê 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: Comitê 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:

```
root@kali:~# whois www.guardweb.com.br
```

```
% Copyright (c) Nic.br  
% The use of the data below is only permitted as described in  
% full by the terms of use at https://registro.br/termo/en.html ,  
% being prohibited its distribution, commercialization or  
% reproduction, in particular, to use it for advertising or  
% any similar purpose.  
% 2017-05-21 20:57:41 (BRT -03:00)
```

```
domain:  guardweb.com.br  
owner:   Bruno Fraga  
owner-c: BRFRA48  
admin-c: BRFRA48  
tech-c:  BRFRA48  
billing-c: BRFRA48  
nserver: candy.ns.cloudflare.com  
nsstat:  20170518 AA  
nslastaa: 20170518  
nserver: wesley.ns.cloudflare.com  
nsstat:  20170518 AA  
nslastaa: 20170518  
saci:    yes  
created: 20160917 #16104777  
changed: 20170506  
expires: 20170917  
status:  published
```

```
nic-hdl-br: BRFRA48  
person:    Bruno Fraga  
created:   20120814  
changed:   20160209
```

```
% Security and mail abuse issues should also be addressed to  
% cert.br, http://www.cert.br/ , respectively to cert@cert.br  
% and mail-abuse@cert.br  
%  
% whois.registro.br accepts only direct match queries. Types  
% of queries are: domain (.br), registrant (tax ID), ticket,  
% provider, contact handle (ID), CIDR block, IP and ASN.
```

whois: executa a aplicação WHOIS. [www.guardweb.com.br](http://www.guardweb.com.br): é o alvo que será consultado.

Observe que ele retornou informações sobre o domínio. Podemos incrementar esta pesquisa com alguns parâmetros, como em qual servidor DNS vamos realizar a pesquisa sobre um domínio. Vamos pesquisar sobre o domínio [www.guardweb.com.br](http://www.guardweb.com.br) em um servidor root em Portugal.

```
root@kali:~# whois www.guardweb.com.br -h whois.dns.pt  
www.guardweb.com.br no match
```

-h: conecta a um servidor para realizar a pesquisa.  
whois.dns.pt: servidor que realizará a consulta.

Observe que ele retornou uma mensagem dizendo que não há nenhum registro sobre o domínio solicitado neste servidor, pois ele não é uma autoridade subordinada ao domínio .com.br. No caso anterior, ele realiza a pesquisa apenas em root servers que são autoridades do domínio especificado, realizando a leitura dos últimos nomes de domínio .br e depois .com até chegar ao nome especificado.

As informações obtidas através do WHOIS são cruciais para traçar uma estratégia de como você pode chegar ao alvo aplicando diversas técnicas, como engenharia social.

## archive.org – o passado<sup>4</sup>

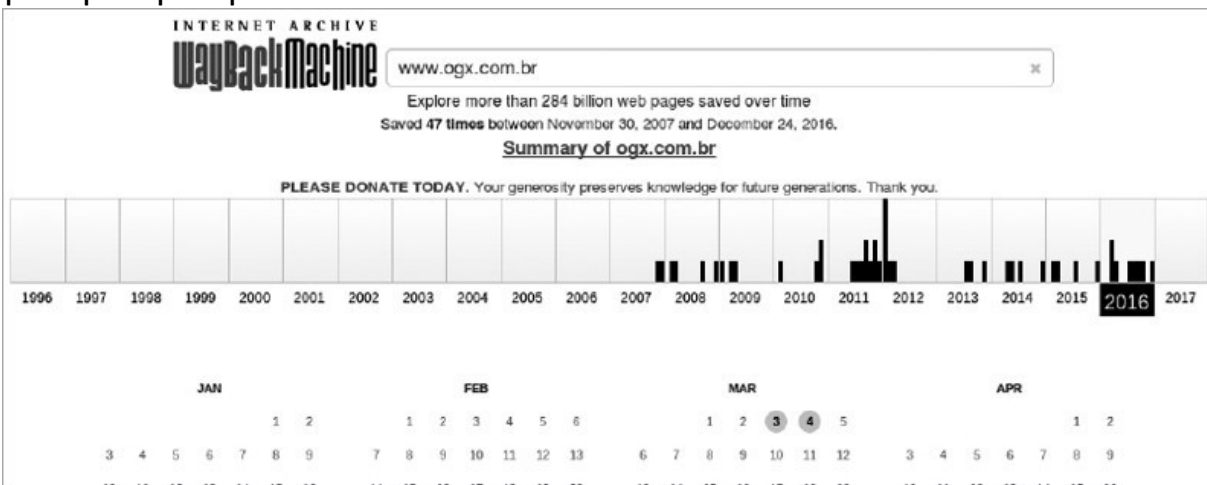
O seu passado te condena.

Anonymous

O Internet Archive ([archive.org](http://archive.org)) é uma organização dedicada a manter um arquivo de recursos multimídia. Ela foi fundada por Brewster Kahle, em 1996. O [archive.org](http://archive.org) inclui diversos dados da web: cópias arquivadas de páginas da internet, com múltiplas cópias de cada página, mostrando assim a evolução da web. O arquivo inclui também softwares, lmes, livros e gravações de áudio. O acervo pretende manter uma cópia digital desses materiais para consulta histórica.

Para utilizá-lo, abra um navegador, acesse o site (<https://archive.org>) e digite no campo de pesquisa o nome do site que deseja buscar.

O processo utilizado é bem simples: ele vai acessar um banco de dados de cache de páginas e mostrar através de uma página organizada e cronológica todos os caches encontrados, sendo possível ser acessados por qualquer pessoa na web.



Como sabemos que nem tudo se inicia perfeitamente – pois, em geral, as coisas vão se ajustando no percurso de sua existência –, e as chances são enormes de que o seu alvo tenha exposto algum dado, informação, com guração ou arquivos multimídias sensíveis na página web, essa ferramenta pode se tornar poderosa nas mãos de um atacante, posto que é possível veri car caches antigos de um site-alvo e coletar informações para diversos ns.

Um atacante passará horas acessando página por página, veri cando e procurando informações sensíveis para traçar uma meta de ataque.

### Observações

- 1) Caso você seja responsável por informações de algum site, veri que - o para saber se há informações sensíveis que foram expostas no passado do site.
- 2) Há con gurações que podem barrar este tipo de consulta, como a utilização de “robots exclusion standard”. Ele bloqueia a navegação de “robôs rastreadores da web” a certos ou a todos os conteúdos

no site, com um simples arquivo na página raiz do site. Veja um exemplo de um arquivo “robot.txt”:

```
User-agent: *  
Disallow: /
```

User-agent: \*: significa que esta seção se aplica a todos os robôs.  
Disallow: /: informa ao robô que não deve visitar nenhuma página do site.

## Consulta DNS

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 ags 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: exhibe os endereços de onde os servidores de nomes estão armazenados.

A partir dessas pesquisas é possível saber as informações dos servidores de DNS que hospedam os servidores e serviços de um alvo específico que um atacante esteja analisando.

Realizando consultas através do DNS, além de obter informações sobre o alvo, é possível também realizar a enumeração de servidores que hospedam esses domínios, sendo possível procurar vulnerabilidades que possam servir para realizar algum tipo de ataque que afete o alvo.

## Brute-force de pesquisa direta DNS

Para agilizar o processo de pesquisa direta de DNS é importante termos scripts que automatizem esse processo; por exemplo, o processo de busca de subdomínios é algo que pode tomar muito tempo de um atacante, mas com scripts é possível obter resultados rapidamente.

Vamos criar um script que realize essa tarefa. Primeiramente, crie ou baixe um arquivo com nomes de subdomínios. Como demonstrado a seguir, utilize o editor de sua preferência:

```
www
mail docs ftp tribo painel
...
```

Agora que temos uma lista com subdomínios, vamos criar o script que vai consultar o nosso arquivo sub-domains.lst.

Para criar o script, utilize um editor de texto e digite os códigos a seguir:

```
#!/bin/bash
for url in $(cat sub-domains.lst);
do host $url.$1 |grep "has address" done
```

#!/bin/bash: indica a shell que o script vai utilizar para processar os comandos.

for url in \$(cat sub-domains.lst): cria uma variável que vai verificar os nomes dentro do arquivo sub-domains.lst.

do host \$url.\$1 |grep "has address": aplica o comando host na variável criada anteriormente e mostra apenas os resultados que serão encontrados, fazendo com que os nomes que ele não encontrar não sejam apresentados na tela.

done: finaliza o script.

Para utilizar esse script, conceda permissão de execução para esse arquivo (chmod +x dns-script.sh) e digite:

```
root@kali:~# ./dns-script.sh guardweb.com.br
tribo.guardweb.com.br has address 104.31.87.52
tribo.guardweb.com.br has address 104.31.86.52
elb077374-1669637565.us-east-1.elb.amazonaws.com has address
23.23.157.46
elb077374-1669637565.us-east-1.elb.amazonaws.com has address
50.19.103.176 elb077374-1669637565.us-east- has address
1.elb.amazonaws.com 23.23.215.151
```

./dns-script.sh: ./executa o arquivo script.sh.

guardweb.com.br: indica a URL em que serão pesquisados os subdomínios.

Observe que esse script retornou apenas as informações claras sobre os subdomínios da guardweb.com.br; dessa forma, foi realizada uma consulta brute-force direta de DNS.

#### Observação

Podemos encontrar arquivos com os inúmeros subdomínios mais utilizados na web. Assim, obteremos mais resultados sobre o alvo em questão.

## Brute-force DNS reverso

Vamos criar um script que realizará a consulta de DNS reverso, o qual vai resolver o endereço IP buscando o nome de domínio associado ao host.

Uma consulta DNS reverso é utilizada quando temos disponível o endereço IP de um host e não sabemos o endereço do domínio, então tentamos resolver o endereço IP por meio do DNS reverso, que procura qual nome de domínio está associado àquele endereço.

Para criar o script, utilize um editor de texto e digite os códigos a seguir:

```
#!/bin/bash for ip
in $(seq 0 255);
```

```
do host $1.$ip done
```

for ip in \$(seq 0 255);: cria uma variável que vai realizar uma sequência de números a ser passada para o próximo comando.

do host \$1.\$ip: recebe uma entrada e combina com a variável ip e, depois, vai repassar para o comando host realizar a pesquisa do IP.

Para utilizar esse script conceda permissão de execução para esse arquivo e digite:

```
root@kali:~# ./dns-reverse.sh 200.221.2
Host 0.2.221.200.in-addr.arpa. not found: 3(NXDOMAIN)
Host 1.2.221.200.in-addr.arpa. not found: 3(NXDOMAIN)
Host 2.2.221.200.in-addr.arpa. not found: 3(NXDOMAIN)
Host 3.2.221.200.in-addr.arpa. not found: 3(NXDOMAIN)
4.2.221.200.in-addr.arpa domain name pointer domredir.bol.com.br.
...
```

Esse script vai pesquisar nomes em todos os IPs dentro da faixa de IP que inicia em 200.221.2 e retornará todo o resultado na tela. Veja que ele encontrou um IP e retornou o nome do servidor encontrado.

## Transferência de zonas DNS

Transferência de zona DNS é um tipo de transação DNS, um dos vários mecanismos disponíveis para os administradores replicarem a base de dados de DNS através de um conjunto de servidores de transferência DNS. Uma transferência de zona pode ocorrer durante qualquer um dos seguintes cenários:

- Quando o serviço de DNS é iniciado no servidor de DNS secundário.
- Quando o tempo de atualização do servidor DNS expira.
- Quando as alterações no arquivo de zona de trabalho são guardadas e há uma lista de notificação.

Se houver um problema de configuração ou atualização do software de qualquer um desses servidores, pode-se explorar uma série de vulnerabilidades, tais como o envenenamento do banco de dados e o comprometimento da integridade e da confidencialidade do banco de dados do DNS primário.

Por exemplo, quando um servidor DNS primário está com a relação de domínios desatualizada e não consegue responder a uma solicitação, ele vai passar a consulta para o servidor secundário. Caso o servidor secundário não encontre uma resposta, ele vai passar 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.

host: executa a aplicação utilitário de DNS host.

-l: faz com que o host execute uma transferência de zona para o nome da zona. Ele transfere a zona imprimindo os registros NS, PTR e endereço A/AAAA na tela.

Observe que a transferência de zona não foi bem-sucedida, então, vamos tentar no segundo NS ns02.guardweb.com.br.

```
root@kali:~# host -l guardweb.com.br ns02.guardweb.com.br
```

Using domain server:

Name: ns02.guardweb.com.br

Address: 10.146.0.1#53

Aliases:

guardweb.com.br name server ns01.guardweb.com.br.

guardweb.com.br name server ns02.guardweb.com.br.

guardweb.com.br name server ns03.guardweb.com.br.

guardweb.com.br. name server ns04.guardweb.com.br..

guardweb.com.br. has address 10.146.0.1

www.01.guardweb.com.br. has address 10.146.0.1

www.0um.guardweb.com.br. has address

10.146.0.13irmas.guardweb.com.br. has address 10.146.0.1

guardweb.com.br. has address 10.146.0.1

www.guardweb.com.br. has address 10.146.0.1

guardweb.com.br. has address 10.146.0.1

guardweb.com.br. has IPv6 address 2804:294:2000:8000::5

guardweb.com.br. has address 10.146.0.1 webmail-191-252-36-

120.guardweb.com.br. has address 10.146.0.1 webmail-191-252-36-

121.guardweb.com.br. has address 10.146.0.1 webmail-191-252-36-

122.guardweb.com.br. has address 10.146.0.1

...

Observe que nesse servidor o comando foi bem-sucedido, e ele trouxe informações de todos os registros de nomes e endereços IPs do domínio guardweb.com.br..

## Brute-force – transferência de zona

Para automatizar este processo é recomendado utilizar scripts. Veja um exemplo de um script que realiza o trabalho apresentado anteriormente:

```
#!/bin/bash
```

```
for server in $(host -t ns $1 | cut -d '"' -f4); do  
host -l $1 $server; done
```

Este script vai consultar os NS do domínio especificado; após isso, ele vai forçar a transferência em cada NS encontrado.

## Ferramentas de enumeração DNS

As ferramentas de enumeração de DNS nos auxiliam a pesquisar um determinado domínio de forma clara e organizada. As ferramentas mais conhecidas são dig e o dnsenum. Vamos testar essas ferramentas.

### Dig – utilitário DNS

O dig é uma ferramenta que faz parte da suíte de programas do Kali Linux.

Para utilizá-lo digite no terminal:



```

root@kali:~# dig -t ns guardweb.com.br

; <<>> DiG 9.10.3-P4-Debian <<>> -t ns guardweb.com.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 11706
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;guardweb.com.br.                IN      NS

;; ANSWER SECTION:
guardweb.com.br.                123117  IN      NS      ns03.guardweb.com.br.
guardweb.com.br.                123117  IN      NS      ns01.guardweb.com.br.
guardweb.com.br.                123117  IN      NS      ns02.guardweb.com.br.
guardweb.com.br.                123117  IN      NS      ns04.guardweb.com.br.

;; ADDITIONAL SECTION:
ns01.guardweb.com.br.          37676   IN      A       10.146.0.1
ns01.guardweb.com.br.          37676   IN      AAAA    10.146.0.1
ns02.guardweb.com.br.          124109  IN      A       10.146.0.1

;; Query time: 13 msec
;; SERVER: 10.146.0.1#53(10.146.0.1)
;; WHEN: Wed May 24 15:59:03 BST 2017
;; MSG SIZE rcvd: 174

```

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

**-t ns:** indica o tipo de registro de DNS a ser consultado; neste caso, NS (name server).

**guardweb.com.br.:** indica o domínio a ser consultado; neste caso, guardweb.com.br..

Observe que ele apresentou em tela os NS registrados para guardweb.com.br. de forma bem organizada e com informações claras sobre o domínio.

É possível também realizar a transferência de domínio com essa ferramenta. Digite no terminal:

```
root@kali:~# dig -t axfr guardweb.com.br.  
;; Connection to 10.146.0.1#53(10.146.0.1) for ns04.guardweb.com.br.  
failed: connection refused
```

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:~# dnsenum --enum guardweb.com.br -f /usr/share/dnsenum/dns.txt
dnsenum.pl VERSION:1.2.3
```

```
Warning: can't load Net::Whois::IP module, whois queries disabled.
```

```
----- guardweb.com.br -----
```

```
Host's addresses:
```

```
guardweb.com.br. 116160 IN A 10.146.0.1
```

```
Name Servers:
```

```
ns01.guardweb.com.br. 34009 IN A 10.146.0.1
ns02.guardweb.com.br. 120442 IN A 10.146.0.1
ns04.guardweb.com.br. 127421 IN A 10.146.0.1
ns03.guardweb.com.br. 127421 IN A 10.146.0.1
```

```
Mail (MX) Servers:
```

```
mx3.guardweb.locaweb.com.br. 1637 IN A 10.146.0.1
mx.guardweb.locaweb.com.br. 1637 IN A 10.146.0.1
mx2.guardweb.locaweb.com.br. 1637 IN A 10.146.0.1
```

```
Trying Zone Transfers and getting Bind Versions:
```

```
Trying Zone Transfer for guardweb.com.br on ns04.guardweb.com.br ...
```

```
AXFR record query failed: REFUSED
```

```
Trying Zone Transfer for guardweb.com.br on ns02.guardweb.com.br ...
```

```
guardweb.com.br. 129600 IN SOA (
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
guardweb.com.br. 129600 IN MX 10
guardweb.com.br. 129600 IN MX 20
guardweb.com.br. 129600 IN A 10.146.0.1
guardweb.com.br. 300 IN TXT (
111.guardweb.com.br. 129600 IN A 10.146.0.1
222.guardweb.com.br. 129600 IN CNAME google.com.
333.guardweb.com.br. 129600 IN A 10.146.0.1
444.guardweb.com.br. 129600 IN A 10.146.0.1
```

```
...
```

dnsenum: executa o utilitário de DNS dnsenum. --enum guardweb.com.br.: indica para realizar a enumeração do domínio guardweb.com.br..

-f /usr/share/dnsenum/dns.txt: realiza a leitura de subdomínios no arquivo dns.txt para executar brute-force.

Observe que o dnsenum trouxe informações importantes, como: Name Servers, Mail (MX) Servers, Zone Transfers, Subdomains, netrange. Essas informações abrem um leque para pesquisas muito grandes sobre os hosts do alvo.

## dnsrecon – utilitário DNS

O dnsrecon é uma ferramenta que faz parte da suíte de programas do Kali Linux. Para utilizá-lo digite no terminal:

```
root@kali:~# dnsrecon -d guardweb.com.br -D /usr/share/dnsrecon/namelist.txt
[*] Performing General Enumeration of Domain: guardweb.com.br
[-] DNSSEC is not configured for guardweb.com.br
[*] SOA ns01.guardweb.com.br 10.146.0.1
[*] NS ns04.guardweb.com.br 10.146.0.1
[*] Bind Version for 10.146.0.1 2.0-guardweb.com.br-s
[*] NS ns04.guardweb.com.br 2804:294:8000:211::5
[*] NS ns03.guardweb.com.br 10.146.0.1
[*] Bind Version for 10.146.0.1 2.0-guardweb.com.br-r
[*] NS ns03.guardweb.com.br 2804:294:8000:211::5::5
[*] NS ns01.guardweb.com.br 10.146.0.1
[*] Bind Version for 10.146.0.1 2.0-guardweb.com.br-rp
[*] NS ns01.guardweb.com.br 10.146.0.1
[*] NS ns02.guardweb.com.br 10.146.0.1
[*] Bind Version for 10.146.0.1 2.0-guardweb.com.br-s
[*] MX mx3.guardweb.locaweb.com.br 10.146.0.1
[*] MX mx.guardweb.locaweb.com.br 10.146.0.1
[*] MX mx2.guardweb.locaweb.com.br 10.146.0.1
[*] A guardweb.com.br 10.146.0.1
[*] TXT guardweb.com.br 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
[*] Enumerating SRV Records
[-] No SRV Records Found for guardweb.com.br
[*] 0 Records Found
```

dnsrecon: executa o utilitário de DNS dnsrecon.

-d guardweb.com.br.: indica o domínio a ser consultado; neste caso, guardweb.com.br..

-D /usr/share/dnsrecon/namelist.txt: realiza a leitura de subdomínios no arquivo namelist.txt para executar brute-force.

Observe que dessa forma o dnsrecon realiza uma enumeração de informações gerais sobre o domínio.

## Fierce – utilitário DNS

O Fierce é uma ferramenta que faz parte da suíte de programas do Kali Linux.

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. )
...
```



erce: executa o utilitário de DNS erce. -d guardweb.com.br.: indica o domínio a ser consultado; neste caso, guardweb.com.br..  
-w /usr/share/erce/hosts.txt: realiza a leitura de subdomínios no arquivo hosts.txt para executar brute-force.

Observe que esse comando apresenta muitas informações sobre o domínio, assim como os comandos anteriores, portanto a utilização dessas ferramentas pode se dar de acordo com a profundidade da necessidade de informações desse tipo.

---

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

As informações que essas ferramentas apresentam podem ser o principal meio para um atacante extrair informações e dar os primeiros passos de um ataque.

- 
1. Videoaula TDI – Conhecer – Navegando no site do alvo.
  2. Videoaula TDI – Conhecer – Sites de emprego.
  3. Videoaula TDI – Conhecer – Consultas WHOIS.
  4. Videoaula TDI – Conhecer – archive.org (o passado).
  5. Videoaula TDI – Conhecer – Consulta DNS.
  6. Videoaula TDI – Conhecer – Script de pesquisa direta DNS.
  7. Videoaula TDI – Conhecer – Brute-force DNS reverso.
  8. Videoaula TDI – Conhecer – Transferência de zona DNS.
  9. Videoaula TDI – Conhecer – Ferramentas de enumeração DNS.



Neste capítulo, vamos apresentar algumas técnicas que podem ajudar a coletar informações. Vamos aprender a rastrear usuários, coletar e-mails, informações de locais de dispositivo e fazer uma introdução ao Google Hacking, uma ótima ferramenta para conhecer muito sobre o alvo.

## Google Hacking<sup>1</sup>

Muitas pessoas usam o buscador do Google para coletar informações variadas, a fim de comprometer milhões de empresas pelo mundo. Muitos criminosos estão manipulando alguns operadores de buscas avançadas do Google para de alguma forma encontrar dados expostos, versões de tecnologias vulneráveis, configurações expostas, cartões de créditos, banco de dados indexados... enfim, de fato são inúmeras as possibilidades.

Você vai aprender a manipulação avançada dos operadores de busca do Google, a técnica chamada Google Hacking. Antes de iniciar, vou apresentar alguns conceitos.



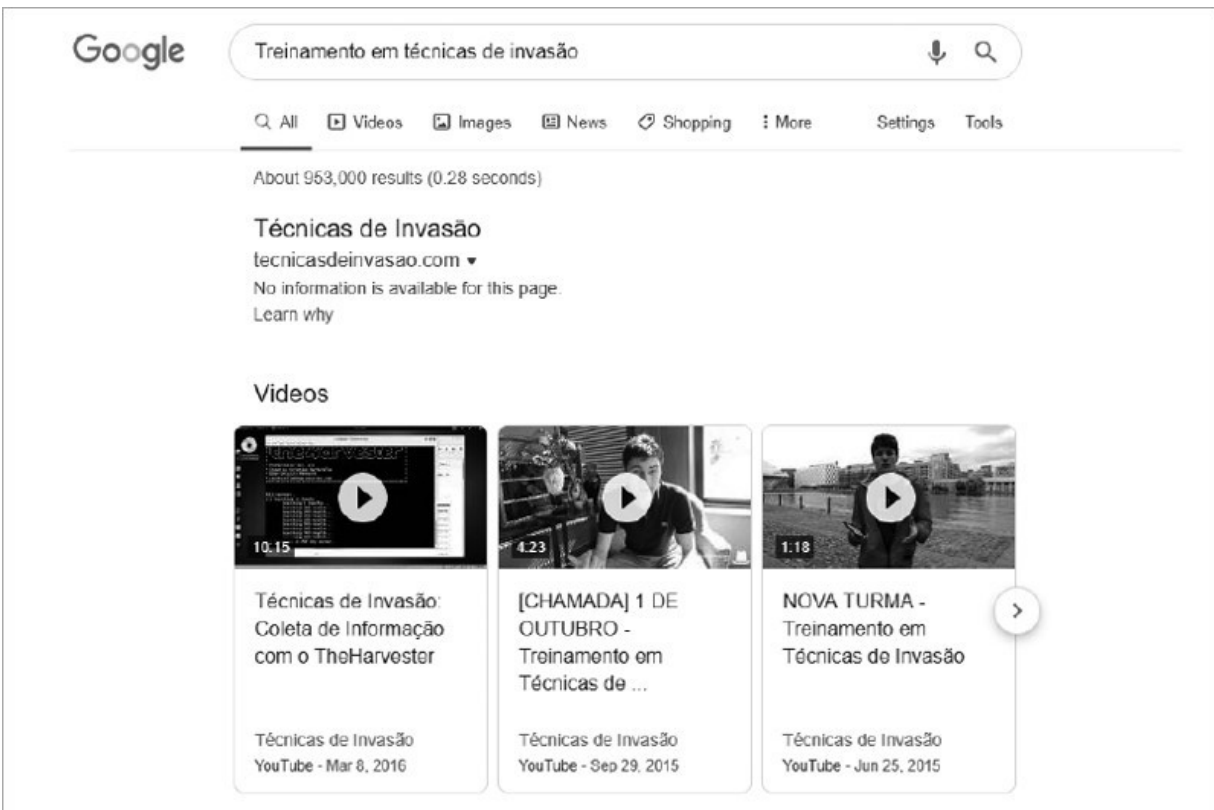
## O Google

Quando realiza uma pesquisa no Google, você não está de fato pesquisando na web, mas sim no índice do Google da web – digamos que em um banco de dados que contém o que o Google indexou da web.

O Google utiliza um software que é uma tecnologia denominada spiders, ou web crawlers, que são robôs que vasculham a web buscando por páginas: sucessivamente eles vão seguindo o link de uma página, o redirecionamento para outra página, e assim eles vão navegando pela web e indexando; dessa maneira, bilhões de páginas e informações cam indexadas e armazenadas em centenas de servidores do Google espalhados pelo mundo.

O Google agrega o resultado de uma busca a partir de palavras-chave no título, descrição e corpo do site. O sistema PageRank é usado pelo motor de busca Google para ajudar a determinar a relevância ou importância de uma página. O PageRank foi desenvolvido pelos fundadores do Google, Larry Page e Sergey Brin, enquanto cursavam a Universidade de Stanford, em 1998. Essa fórmula avalia alguns critérios, classifica a pontuação e apresenta na tela o resultado para o usuário na.

Veja um exemplo de busca no google.com, pelo termo Treinamento em Técnicas de Invasão:



Se analisarmos, podemos verificar que cada resultado tem um título, uma URL e um resumo do texto contido na página.

## 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 fazendo as buscas apenas o site terra.com tendo no texto a palavra telefone.

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

Neste operador estamos fazendo 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 informações específicas.

A partir das tags existentes, podemos encontrar diversas informações importantes sem precisarmos nos preocupar em como desenvolver buscas específicas, utilizando os operadores do Google, e testá-las até conseguirmos que os outros corretos funcionem. O mais importante é a possibilidade de adaptar mais tags de busca para nossas necessidades. No link a seguir está o site para acesso ao GHDB:

Disponível em: [www.exploit-db.com/google-hacking-database](http://www.exploit-db.com/google-hacking-database). Acesso em: 14 ago. 2019.

---

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

### Buscando versões de aplicativos

Algumas páginas utilizam plugins. Os plugins que um determinado site utiliza podem ser coletados. Analisando o código-fonte da página, por exemplo, com uma aplicação WordPress, é possível utilizar diversos plugins de compartilhamento.

Vamos supor que a vulnerabilidade de algum plugin de compartilhamento se tornou pública e possibilitou uma exploração e um ganho de acesso ao alvo; a partir disso, vários crackers podem buscar no Google sites em larga escala que utilizam este plugin, podendo, assim, realizar ataques em massa.

A seguir veremos alguns exemplos.

```
inurl:wp-content/plugins/wp-retina-2x site:com.br
```

Esta busca ltra resultados de sites do domínio .com.br que utilizam o plugin wp-retina-2x.

```
site:gov.br letype:sql intext:senha
```

Esta busca ltra resultados nos sites de domínio do governo brasileiro (.gov.br), buscando por arquivos de banco de dados sql que contenham a palavra senha. É possível obter inúmeros resultados com informações com usuários e senhas que deveriam ser confidenciais.

### Dica

Caso você seja um administrador web, veri que os sites que você administra, buscando arquivos indexados (arquivos.txt, pdf, arquivos de banco etc.).

Para saber mais, acesse as páginas a seguir:

<https://www.oakton.edu/user/2/rjtaylor/cis101/Google%20Hacking%20>

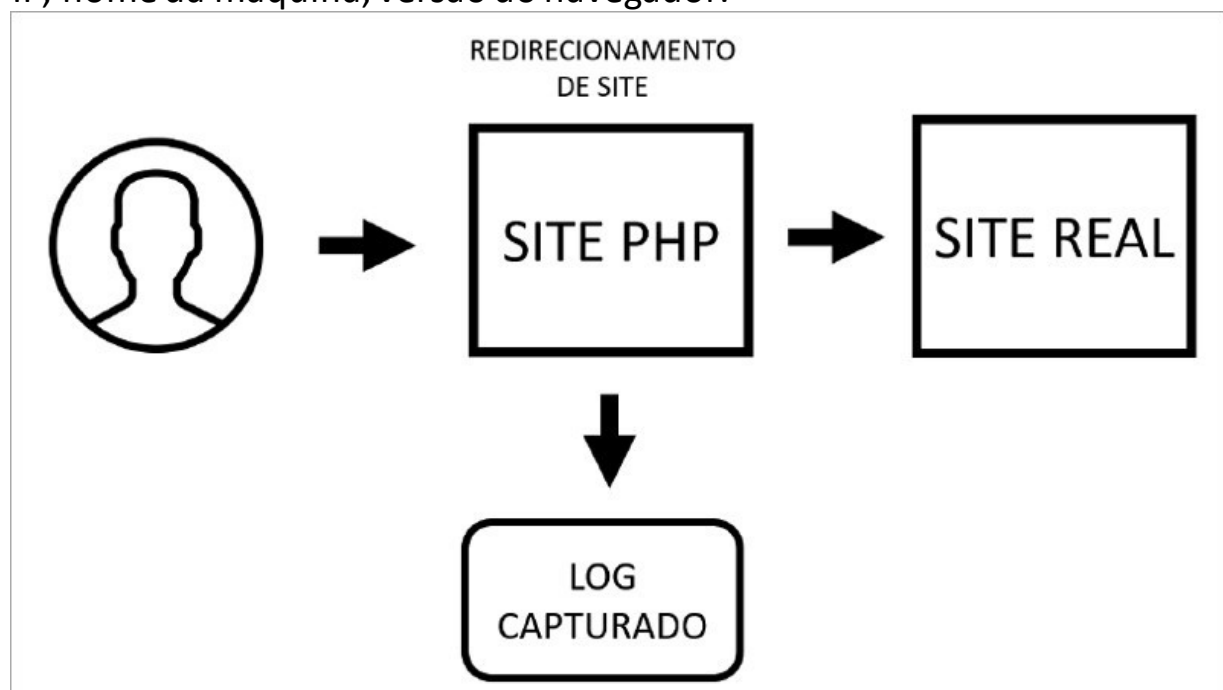
0101.pdf

<http://www.mrjoeyjohnson.com/Google.Hacking.Filters.pdf>

## Rastreamento de usuários<sup>2</sup>

É possível obter resultados de localização, IP, versão do navegador, além de algumas aplicações que o usuário esteja utilizando para realizar a leitura de arquivos enviados por e-mail.

Funcionamento da técnica – o usuário-alvo acessa uma página PHP, que vai coletar e armazenar as informações do log do usuário, que o atacante criou. Geralmente, antes de ser entregue ao alvo utiliza-se um encurtador de URL para mascarar o link real; esta página faz um redirecionamento para a página de destino real, e com isso o atacante tem acesso aos logs do usuário e pode obter data de acesso, como endereço IP, nome da máquina, versão do navegador.



Há ferramentas que realizam a captura de logs do usuário, utilizando esta metodologia; o serviço Blasze IP Logger é um deles: [blasze.com](http://blasze.com).

## Blasze

Veja passo a passo um exemplo de utilização deste método empregado por criminosos usando o Blasze:

1) Cria-se uma mensagem em cujo link o usuário-alvo se sinta atraído a clicar.

O criminoso cria um redirecionamento através da ferramenta

2) blasze.com para o site de destino – por exemplo, um site com matéria real, como um vídeo no YouTube.

3) Antes de inserir o link no e-mail, utiliza-se um encurtador de URL – por exemplo, o goo.gl, com o endereço da URL que o blasze criou.

4) O criminoso envia o link para o usuário-alvo através do e-mail.

5) Após o usuário-alvo clicar no link, o criminoso consegue ver os logs de acesso através do monitor no site do Blasze.

## MailTracking

Pode-se utilizar o mail tracking para obter log de acesso de um determinado alvo, mas também é possível inserir arquivos .pdf, .png ou .doc para descobrir a versão dos aplicativos que o usuário utiliza para abrir tais arquivos.

Sendo assim, o atacante pode procurar vulnerabilidades para os aplicativos específicos, e é possível também rastrear o documento enviado. Confira no site a ferramenta MailTracking: [mailtracking.com](http://mailtracking.com).

Esta ferramenta funciona com metodologia similar ao Blasze, porém com opções avançadas de rastreamento.

É necessário realizar um registro e associar a conta de e-mail do atacante para utilizar a ferramenta. Está disponível tanto em versão grátis como paga, mas é a paga que possui uma entrega efetiva.

---

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

Coletando o endereço IP de uma empresa, é possível descobrir sua localização. Caso o usuário acesse de dentro da rede da empresa, é possível também rastrear documentos através do MailTracking.

Até esse ponto, o criminoso possui dados para explorar vulnerabilidades no browser, nos softwares e realizar um scan no IP externo do alvo.

## Dicas

- 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

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"

The screenshot shows the Shodan search engine interface. The search bar contains the query "os:\"windows xp\" city:\"london\" port:80". The results are categorized into several sections:

- TOTAL RESULTS:** 29
- TOP COUNTRIES:** A world map showing the distribution of results, with the United Kingdom and Canada being the most prominent.
- TOP ORGANIZATIONS:**
  - TalkTalk: 2
  - Rogers Cable: 2
  - HighSpeed Office Limited: 2
  - Verizon Business: 1
  - Venus Business Communications Limited: 1
- TOP OPERATING SYSTEMS:**
  - Windows XP: 29
- TOP PRODUCTS:**
  - Microsoft IIS httpd: 7
  - SonicWALL firewall http config: 1
  - Apache httpd: 1

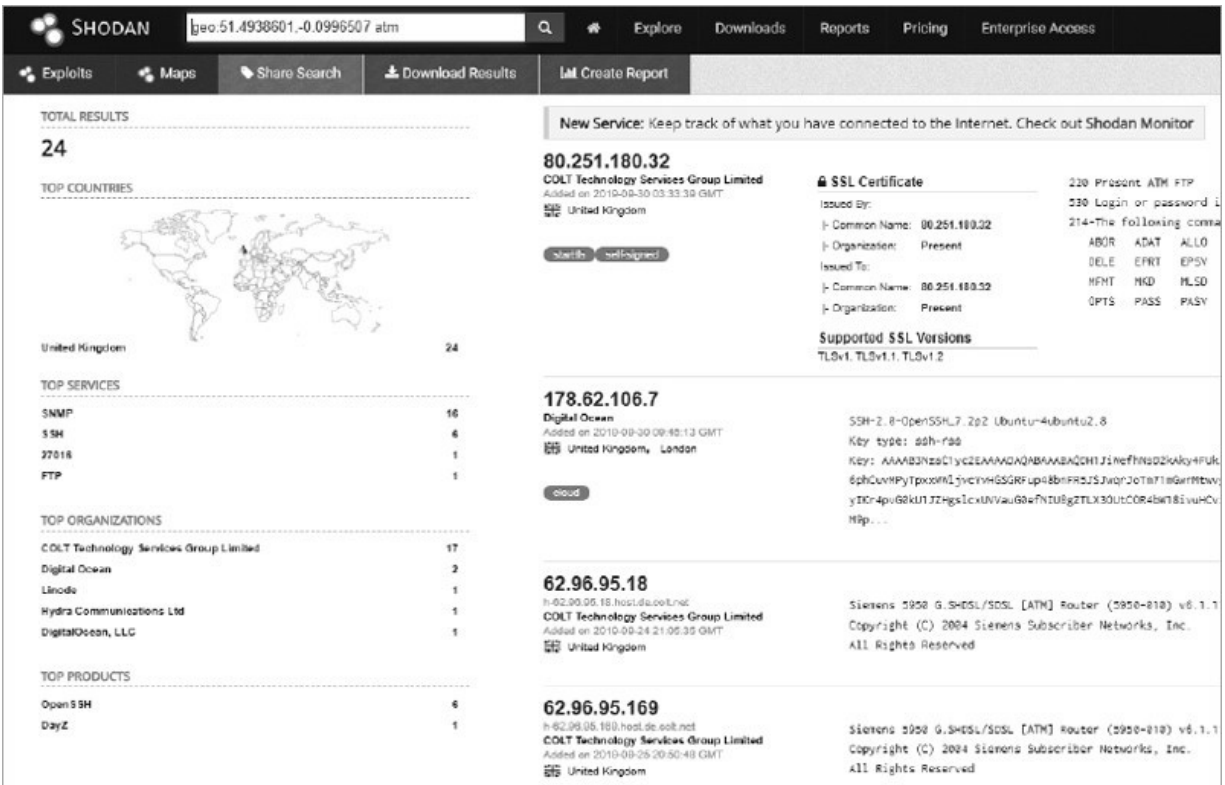
On the right side, there are three detailed results for specific IP addresses:

- 216.75.160.164:** Windows XP, Execulink Telecom, Added on 2019-09-29 07:18:43 GMT, Location: Canada, London. HTTP/1.0 301 Moved Permanently. Location: https://216.75.160.164/
- 89.150.17.113:** Windows XP, Britanik Technologies Ltd, Added on 2019-09-28 00:27:56 GMT, Location: United Kingdom, London. HTTP/1.1 201 Moved Permanently. Location: https://89.150.17.113/view/login.html. Server: Apache. Date: sun, 29 sep 2019 16:50:23 GMT. Pragma: no-cache. Cache-Control: no-store. Content-Type: text/html. Content-Length: 0. Last-Modified: sat, 10 oct 2019 09:05:02 GMT. Connection: Close.
- 89.242.11.98:** Windows XP, TalkTalk, Added on 2019-09-26 23:32:52 GMT, Location: United Kingdom, London. HTTP/1.1 400 Bad Request. Content-Type: text/html. Date: Sun, 29 Sep 2019 23:32:51 GMT. Connection: close. Content-Length: 29.

Ele vai retornar resultados de máquinas utilizando Windows XP com a porta 80 aberta na cidade de Londres.

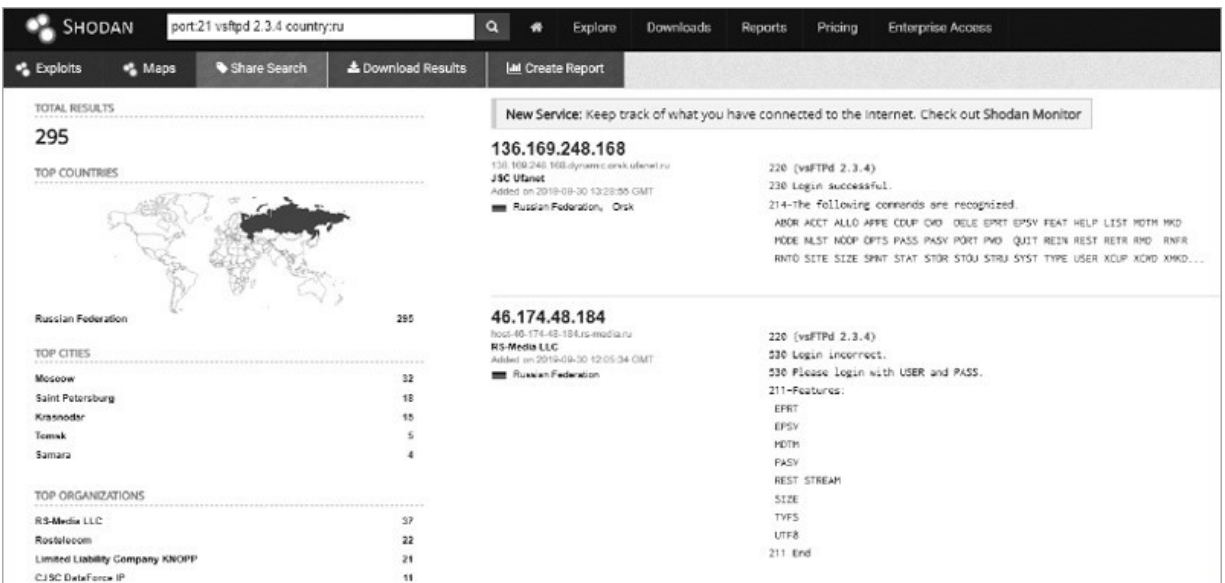
geo:51.4938601,-0.0996507 atm





Ele vai apresentar informações de dispositivos ATM, próximos à geolocalização que foi informada.

port:21 vsftpd 2.3.4 country:ru



Ele vai retornar resultados de máquinas utilizando o serviço FTP com uma versão vulnerável na porta 21, na Rússia.

---

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

Esta é uma ferramenta incrível e muito perigosa, pois um criminoso pode utilizá-la de diversas maneiras: realizar buscas de versões de serviços vulneráveis, localizar dispositivos próximos a ele – através da localização geográfica – e usar dados de banners para realizar engenharia social com pessoas responsáveis pelo dispositivo.

### Censys<sup>4</sup>

O Censys é um motor de busca que permite que os cientistas da computação façam perguntas sobre os dispositivos e redes que compõem a internet.

Impulsionado pela varredura em toda a internet, o Censys permite que os pesquisadores encontrem hosts específicos e criem relatórios agregados sobre como os dispositivos, sites e certificados são configurados e implantados.

### Utilizando o Censys

Para usar o Censys, acesse o site da ferramenta: [censys.io](https://censys.io).

Para utilizar todos os recursos é necessário realizar o registro.

Veja alguns exemplos de busca que podemos realizar:

- `location.country_code:UK` – mostra resultados dos países do Reino Unido;
- `location.city:London` – mostra resultados da cidade de Londres;
- `metadata.os:ubuntu` – mostra resultados de computadores com o sistema operacional Ubuntu;
- `autonomous_system.country_code:BR` – mostra resultados de sistemas autônomos no Brasil;
- `ip:[IP_INICIO IP_FINAL]` – mostra resultados por range de IP;

- 80.http.get.title:"Welcome to Jboss" – procura por banners de servidor web utilizando jboss.

É possível refinar as buscas utilizando vários operadores em conjunto:

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

**Censys** IPv4 Hosts

Results Map Metadata Report

**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 CLOUDFLARENET - Cloudflare, Inc.
- [More](#)

**Protocol:**

- 22.41M 80/http
- 16.31M 443/https
- 8.92M 22/ssh
- 5.95M 21/ftp
- 4.32M 3306/mysql
- [More](#)

**Tag:**

- 28.0M http

**IPv4 Hosts**  
Page: 1/1,415,692 Results: 35,392,283 Time: 458ms

- 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
  - 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
  - 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
  - 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
  - 8080.http.get.body: to

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 para encontrar resultados específicos na sua pesquisa, através de apenas algumas informações que você possui – por exemplo, para encontrar operadores a m de conseguir informações sobre a porta 443:

- Abra a página [censys.io/overview](https://censys.io/overview).
- Clique na aba Data Definitions.
- Faça a pesquisa por 443 no campo de busca.

Ele vai apresentar diversos operadores relacionados à porta 443.

---

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

Alguns criminosos realizam buscas em um determinado IP que já seja do seu conhecimento, por exemplo, o de alguma empresa. Eles podem realizar uma busca no range desse IP para saber se existem outros IPs relacionados ao mesmo range que estão expostos na internet.

IP da empresa alvo: 72.9.105.30

Operador utilizado:

ip:[72.9.105.0 72.9.105.255]

### Coleta de endereços de e-mail<sup>5</sup>

Uma ferramenta que pode ser empregada para coleta de e-mails é o Google

Hacking, utilizando operadores ou simplesmente digitando