

# Fundamentos de PenTest

*Um rápido overview dos conceitos e técnicas de PenTest*

Joas Antonio



# DEDICATÓRIA



<b>Título de capítulo 1</b>	<b>8</b>
<b>Título de capítulo 2</b>	<b>9</b>
<b>Título de capítulo n</b>	<b>10</b>



# PREFÁCIO

# **Conceitos de PenTest e Red Team**



## **Introdução**

Esse livro tem como objetivo trazer fundamentos e conceitos essenciais sobre o PenTest. Não é um livro que se aprofunda totalmente em ferramentas e nem em metodologias, o seu foco é basicamente trazer um overview, no que envolve o mundo de PenTest, além de ajudar a compreender a importância dos testes de invasão e que tipo de profissionais o mercado de trabalho está buscando.

Na minha jornada como profissional de segurança da informação e pesquisador voltado a segurança ofensiva, a carência por livros voltado à um público que está iniciando e quer ingressar na área de PenTest, é muito grande. E claro, com o best-sellers Teste de Invasão da Georgia Wedman e os livros do Daniel Moreno e juntando esse livro, com certeza vai dar uma boa base para quem está começando na área e também para aqueles que já estão atuando, seja de forma profissional ou independente, pois é essencial os fundamentos para que conseguirmos atingir níveis maiores.

Eu espero que esse livro seja útil para você e que com certeza ajude no seu desenvolvimento e na sua carreira como profissional de PenTest e segurança da informação. E com certeza, para que este livro saísse a comunidade de segurança teve um papel importante, seja no âmbito nacional como internacional, pois o vastos materiais que são compartilhados entre os profissionais de segurança da informação foi de suma importância para o desenvolvimento desse material que apresento a você.

## **Pré-requisitos do Livro**

Se você quiser tirar 100% de aproveitamento desse livro, eu recomendo possuir uma boa base em redes de computadores, conhecer dos sistemas operacionais como Linux e Windows, uma boa base em execução de comando como CMD, Bash e Powershell. Ter o mínimo conhecimento em Linguagem de Programação como Python e C e com certeza vontade de aprender. Mas claro, são apenas pré-requisitos, para que você consiga se desenvolver conforme vai lendo o livro.

## **Laboratório**

Um laboratório é essencial para você colocar em prática todo aprendizado desse livro, para isso eu recomendo que você monte um utilizando Virtual Box ou VMWare. No geral eu recomendo que vocês tenham em seu laboratório as seguintes máquinas.

- Windows 7
- Windows 10
- Windows Server 2012
- Windows Server 2016
- Kali Linux ou Parrot
- Metasploitable
- Juice Shop
- Webgoat

<https://www.microsoft.com/pt-br/evalcenter/evaluate-windows-server-2012>

<https://www.kali.org/>

<https://www.parrotsec.org/>

<https://sourceforge.net/projects/metasploitable/>

<https://github.com/bkimminich/juice-shop>

<https://github.com/WebGoat/WebGoat>

## Introdução ao PenTest

Um PenTest (Penetration Testing) ou Teste de invasão é uma avaliação de vulnerabilidades com objetivo de testar as brechas de segurança de uma empresa ou organização para simular um ataque cibernético. Os profissionais de teste de invasão procuram brechas em sistemas para tentar compromete-los e tentar ir o mais longe possível, explorando vulnerabilidades conhecidas ou até mesmo criando uma brecha de segurança para invadir um determinado sistema.

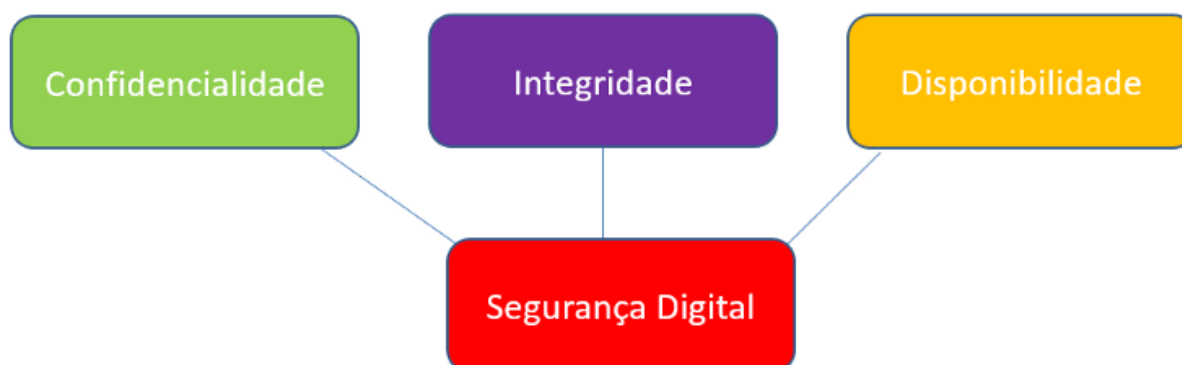
A necessidade de realizar um PenTest hoje em dia é muito grande, pois com o aumento do Ciberataques no mundo inteiro, resultou em uma corrida em busca dos melhores meios para proteger os ativos\* da informação de uma empresa contra qualquer tipo de ameaça que possa surgir, sendo ela pelo meio digital ou pelo meio físico.

O escopo de um PenTest deve ser bem elaborado, principalmente quando falamos de riscos que podem ocorrer em um teste de invasão, seja por erros de configuração do ambiente ou o uso de ferramentas que ocasionam em muito stress, pois devemos ter como principal objetivo, garantir o C.I.D (Confidencialidade, Integridade e Disponibilidade)

**Confidencialidade:** Garantir que a informação só será lida pelo destinatário

**Integridade:** Garantir que a informação não será mudada

**Disponibilidade:** Garantir que a informação esteja disponível a qualquer momento



## Figura 1.1

Esses são os 3 pilares que devem prevalecer na hora de realizar um serviço de PenTest em uma organização.

\*Ativos da informação é tudo aquilo que faz parte no funcionamento da empresa, é um conjunto de informações gerenciadas que mantém a empresa funcionando, seja um servidor que armazena dados confidenciais, o notebook do presidente ou pessoas. Para entender melhor acesse: <https://bit.ly/2ANWUv7>

### Preparando um PenTest

A fase de preparação de um teste de invasão é a mais essencial que tem, pois vamos definir todo Kick-Off (Começo) do projeto e a forma de trabalho realizada.

Em geral, um PenTest é trabalhado por fases, mas tudo isso dependendo da metodologia que você trabalha na hora de realizar os testes, particularmente o PTES é um bom modelo de referência a ser seguido. Mas existem outros modelos como o NIST-800-115, OSSTMM, OWASP e a ISAFF\*.

Porém, muita das vezes o modelo trabalhado é aquele que você ou sua empresa utiliza ou na minoria dos casos, o seu cliente exige uma metodologia a ser seguida, principalmente por questões de compliance.

Mas particularmente o modelo PTES dá uma boa base estrutural das fases de um PenTest, por isso é um modelo que vale a pena conhecer.

### Modelo PTES

- [Fase de Preparação](#)
- [Coleta de Informação](#)
- [Modelagem de Ameaça](#)
- [Análise de Vulnerabilidade](#)
- [Exploração](#)
- [Pós Exploração](#)
- [Relatório](#)

#### Fase de Preparação:

É realizado o Assessment para verificar a necessidade do cliente, escopo dos testes e o mapeamento dos parâmetros para realizar os testes de vulnerabilidade. Assim, você prepara melhor o formato e a metodologia que você vai utilizar para fazer um PenTest.

#### Coleta de Informação:

É realizar a varredura a procura de informações relevantes do seu alvo, seja realizando a coleta de forma passiva ao qual você busca de fontes pública ou até mesmo de forma mais intrusiva, realizando a enumeração dos hosts utilizando Scanners de Rede.

## **Modelagem de Ameaças:**

Com as informações coletadas o atacante vai determinar o impacto que ele pode ocasionar com o que ele tem em mãos, assim desenvolvendo métodos para tentar comprometer o sistema alvo.

## **Análise de Vulnerabilidade:**

Nessa fase o PenTester procura por brechas de segurança que podem ocasionar na exploração, descobrindo brechas na implementação ou no código da aplicação.

## **Exploração:**

É uma das fases cruciais, pois será realizado a exploração das vulnerabilidades encontradas, seja utilizando um exploit\* público ou privado para tentar invadir ou comprometer um alvo.

## **Pós-exploração:**

Após comprometer o seu alvo a fase de pós exploração, garante que você consiga acesso persistente no alvo, escalar privilégios para ter um usuário a nível administrativo, realizar movimentos laterais e pivoting para tentar comprometer outras máquinas na mesma rede ou em sub-rede interna.

## **Relatório:**

É a fase final, porém ela deve ser o início também, pois cada passo realizado durante os testes deve ser devidamente documentada e detalhada, a minha recomendação é que você tenha 2 relatórios. O primeiro é o relatório de produção, ou seja, dos testes que você vai realizando e documentando, até mesmo trabalha-lo como um relatório de linha de tempo. O Segundo é o relatório final, ao qual você vai apresentar para a Gestão e sua equipe técnica escolhida.

\*Para conhecer melhor essas metodologias eu recomendo:  
<https://bit.ly/2AWqIWE>

\***Exploit:** É um script construído que tem como finalidade explorar uma vulnerabilidade, geralmente quando uma vulnerabilidade é encontrada, alguns pesquisadores ou atacantes, criam um exploit para automatizar o processo de comprometimento do alvo ou execução de uma ação maliciosa.

## **Tipos de PenTest**

Existem alguns tipos de PenTest que são realizados no mercado de trabalho, dependendo principalmente da necessidade do cliente naquele momento. No caso os testes são categorizados em 3.

**Black Box:** O profissional não possui conhecimentos do ambiente, assim será necessário

procurar a melhor forma de comprometer um ambiente

Os testes são classificados em dois tipos:

- **Blind Testing:** Este teste verifica se um criminoso pode lançar um ataque com informações severamente limitadas, geralmente os pentesters só recebem o nome da empresa;
- **Double-Blind Testing:** Nesse método, apenas um ou dois funcionários da organização têm conhecimento da realização do teste. Assim o Double-Blind Testing verifica a eficácia do monitoramento de segurança da organização, identificação de incidentes e o processos de resposta;

**Gray Box:** Já combina as duas análises, você vai ter algumas informações essenciais para atuar, geralmente esses acessos consiste só o acesso a rede e assim realizar os testes.

**White Box:** Você já possui conhecimentos de toda a infraestrutura da organização, o seu objetivo é apenas testar as vulnerabilidades e descobrir potenciais brechas também.

## Processo de um PenTest

- Determinar o escopo dos testes;
- Coletar informações do alvo tanto passivamente como ativamente;
- Planejar os métodos para coletar e analisar as informações obtidas de maneira passiva ou ativa;
- Detectar potenciais brechas de segurança, seja enumerando informações, coletando detalhes de portas, versões e serviço do alvo;
- Realizar os testes efetuando a exploração e a pós exploração;
- Analisar os resultados e gerar um relatório;
- Testar a efetividade das remediações;

## **A necessidade de um PenTest**

- Identificar as ameaças e determinar a probabilidade da sua organização sofrer um ataque;
- O Pentest vai prover o nível de maturidade e aceitação de risco da sua organização;
- Entender os principais vetores de ataque e seu impacto no negócio;
- Auxiliar no passo a passo na prevenção de vulnerabilidades;
- Compliance com regulamentações e padrões (ISO 27001, PCI-DSS, LGPD, etc);
- Avaliar a eficiência de dispositivos de segurança da sua rede (Firewalls, IDS, IPS, etc.);

## **O que é Red Team?**

Uma Red Team consiste em profissionais de segurança que atuam como adversários para superar os controles de segurança cibernética . As equipes de Red Team geralmente consistem em hackers éticos independentes que avaliam a segurança dos sistemas de maneira objetiva.

Eles utilizam todas as técnicas disponíveis para encontrar pontos fracos em pessoas, processos e tecnologia, para obter acesso não autorizado aos ativos. Como resultado desses ataques simulados, o red team fazem recomendações e planejam como fortalecer a postura de segurança de uma organização. Geralmente uma metodologia bastante seguida pelo Red Team é o Cyber Kill Chain, por ser utilizado até mesmo dentro do âmbito militar ou em grandes empresas que possui um processo sólido de Red Team.

## **Cyber Kill Chain**

O Cyber Kill Chain trabalha com 5 processos, parecidos com as outras metodologias, mas com objetivos diferentes, enquanto o PTES é voltado à um processo de PenTest profissional, o Cyber Kill Chain já tem como foco trabalhar um cenário de ataque mais realista, utilizado por grupos de atacantes famosos e por centrais de inteligência do mundo todo.

### **1. Reconnaissance (Reconhecimento):**

Durante o estágio de reconhecimento, o ator da ameaça realiza pesquisas sobre o alvo. Esta pesquisa pode ser feita de várias maneiras, como visualização do alvo em sites

públicos, seguindo funcionários da empresa, coletando informações técnicas como IP públicos e servidores web, por exemplo.

O LinkedIn e outros sites de redes sociais facilitam a reunião de informações sobre o alvo e colaboradores. Na maior parte das vezes, o foco fica naqueles que tem cargos que possuem maiores privilégios dentro do sistema da organização, como os analistas de TI de cargos mais altos.

## **2. Weaponization (Armamentos)**

Quando o alvo é identificado e estudado, os atacantes começam a desenvolver seus ataques e as ferramentas que serão utilizadas. Podem tanto ser ferramentas criadas e desenvolvidas por eles mesmo quanto ferramentas compradas na deep web.

Essas ferramentas podem explorar vulnerabilidades de sistemas que sejam publicamente conhecidas ou não.

## **3. Deliver & Exploit & Install (Entrega & Exploração & Instalação)**

A etapa de entrega é quando o atacante vai enviar o seu programa malicioso para o alvo. A forma mais utilizada costuma ser o spear-phishing, que é um vetor de ataque direcionado, ou seja, com alvos bem determinados. A etapa de Exploit é quando o atacante explora alguma vulnerabilidade, seja ela já conhecida ou não. As vulnerabilidades que não são publicamente conhecidas são conhecidas como zero-day.

## **4. Command & Control (Comando e Controle)**

Para que uma ameaça seja considerada uma AT, ou seja, persistente e avançada, vai precisar existir uma comunicação entre a ameaça e o atacante que a enviou. Chamamos essa comunicação de Command & Control.

Logo, quando a ameaça não tem essa comunicação, ela não é considerada persistente, e portanto não é mais uma APT, mas ainda assim pode ser uma ameaça avançada, como por exemplo o famoso caso do Stuxnet, que foi considerado um APT, mas na verdade é apenas um AT (advanced threat). Entenda o caso a partir do artigo do SANS.

## **5. Actions on Objectives (Ações no Objetivo)**

Somente depois de passar por todas as etapas anteriores, o atacante poderá realizar seu objetivo, que pode ser roubo de informações confidenciais, criptografia de dados (com um ransomware, por exemplo), destruição do sistema ou somente entrar no sistema daquela vítima como mais uma etapa para se mover lateralmente pela rede para infectar outro sistema e concluir um objetivo maior.

## **Adversary Emulation**

O Adversary Emulation é um tipo de teste utilizado pelo Red Team que imita uma ameaça real e conhecida por uma organização ao qual combina inteligência de ameaça para definir quais ações e comportamentos o Red Team usa.

Tornando diferente de um PenTest e indo mais além, criando cenários para testar TTPs (Táticas, Técnicas e Procedimentos) de um adversário.

## **Táticas, técnicas e procedimentos ( TTPs )**

É um conceito essencial nos estudos sobre Cyber Terrorismo. O papel dos TTPs na análise do terrorismo é identificar **padrões** individuais **de comportamento** de uma atividade terrorista específica, ou de uma organização terrorista específica, e examinar e categorizar táticas e armas cibernéticas mais usadas por uma atividade terrorista específica ou por uma organização terrorista específicas.

### **APTs (Ameaças Persistentes Avançadas)**

O Advanced Persistent Threat, em uma tradução livre do inglês significa Ameaça Persistente Avançada. É uma expressão comumente usada para se referir a ameaças cibernéticas, em particular a prática de espionagem via internet por intermédio de uma variedade de técnicas de coleta de informações que são consideradas valiosas o suficiente para que o agente espião despense tempo e recursos para obtê-las.

Mesmo quando tem a intenção de acessar ou atacar um alvo específico, um cracker geralmente não é considerado o possível autor de um ataque APT, pois isoladamente um indivíduo raramente dispõe dos recursos necessários à execução de um ataque desses.

### **Mitre Att&ck**

O MITRE introduziu o ATT&CK (Adversarial Tactics, Techniques & Common Knowledge - que traduzindo significa Táticas, técnicas e conhecimento comum dos inimigos) em 2013 como uma forma de descrever e classificar os comportamentos dos inimigos com base em observações do mundo real. O ATT&CK é uma lista estruturada de comportamentos conhecidos do agressor, que foram compilados em táticas e técnicas e expressos em várias matrizes, bem como via STIX/TAXII. Como essa lista é uma representação abrangente dos comportamentos dos agressores ao comprometer as redes, ela é útil para várias análises ofensivas e defensivas, representações e outros mecanismos.

Além de ser bastante útil para o Red Team na hora de validar uma ameaça ou até mesmo simular um ataque na sua organização. Principalmente se naquele período estiver ocorrendo ataques atrelados a grupos APTs que estão visando de maneira particular algum sistema ou tecnologia específica. Assim o Mitre Att&ck trás detalhes de como os atacantes estão agindo e assim o Red Team valida as técnicas utilizadas para auxiliar na implementação dos controles de segurança junto ao Blue Team.

**\*Blue Team:** É o time responsável por garantir a segurança operacional da empresa e efetuar a implementação dos controles de segurança e outros mecanismos de defesa, trabalhando junto ao Red Team para validar se foi ou não bem implementado e quais ações podem ser tomadas para diminuir os riscos ou até mesmo o impacto de um ataque.



# **COLETA DE INFORMAÇÃO, ESCANEAMENTO E ENUMERAÇÃO**

## Introdução

Para construir uma estratégia de invasão, os atacantes precisam reunir informações sobre a rede da organização alvo. Em seguida, eles usam essas informações para localizar a maneira mais fácil de comprometer e burlar os mecanismos de segurança da organização.

Um aspecto essencial do footprinting é identificar o nível de risco associado às informações publicamente acessíveis da organização. Footprinting, a primeira etapa do hacking ético, refere-se ao processo de coleta de informações sobre uma rede-alvo e seu ambiente. Usando footprinting, você pode encontrar uma série de oportunidades para comprometer e avaliar a rede do seu alvo. Depois de concluir o processo de footprinting de maneira metodológica, você obterá o blueprint do perfil de segurança da organização. O termo "blueprint" se refere ao perfil de sistema exclusivo da organização-alvo adquirido por footprinting.

É uma etapa importante em um Teste de invasão, pois a quantidade de informações coletadas se torna um diferencial imenso nos testes. Quanto mais informações forem obtidas, mais alternativas para comprometer um alvo você vai possuir. Por isso é um processo importante e que geralmente tem mais tempo e recursos investidos durante um PenTest, principalmente se for do tipo Black Box.

## Benefícios da coleta da informação

- **Conhecer a postura de segurança:** Executar a coleta de informação contra uma organização, fornece o perfil completo da postura de segurança da organização. Os

hackers podem então analisar o relatório para identificar brechas na postura de segurança da organização e construir um plano de invasão.

- **Reduzir a área de foco:** Ao usar uma combinação de ferramentas e técnicas, os invasores podem pegar uma entidade desconhecida (por exemplo, Organização XYZ) e reduzi-la a um intervalo específico de nomes de domínio, blocos de rede e endereços IP individuais de sistemas que estão conectados diretamente à Internet, bem como muitos outros detalhes relativos à sua postura de segurança.
- **Identificar vulnerabilidades:** Uma coleta detalhada fornece o máximo de informações sobre a organização de destino. Ele permite que o invasor identifique vulnerabilidades nos sistemas de destino para selecionar exploits apropriados. Os invasores podem construir seu próprio banco de dados de informações sobre os pontos fracos de segurança da organização alvo. Esse banco de dados pode ajudar a identificar o elo mais fraco no perímetro de segurança da organização.
- **Desenhar mapa de rede:** combinar técnicas de footprinting com ferramentas como o Tracert para ver as rotas da rede, permite que o invasor crie representações diagramáticas rede do alvo. Especificamente, ele permite que os invasores desenhem um mapa ou esboço da infraestrutura de rede da organização para saber sobre o ambiente real em que vão invadir. Um mapa de rede representa a compreensão do invasor sobre a pegada de Internet do alvo. Esses diagramas de rede podem orientar o invasor na execução de um ataque.

A coleta de informação é categorizado em dois tipos

### **Coleta Passiva:**

A Coleta passiva envolve a coleta de informações sobre o alvo sem interação direta com ele. É útil quando as atividades de coleta de informações não devem ser detectadas pelo alvo. Mas executar a coleta passiva é tecnicamente difícil, e requer um pensamento analítico para definir quais informações são ou não relevantes.

### **Coleta Ativa:**

A Coleta ativa envolve a coleta de informações sobre o alvo com interação direta. No footprinting ativo, o alvo pode reconhecer o processo contínuo de coleta de informações, conforme interagimos abertamente com a rede alvo. A pegada ativa requer mais preparação do que a pegada passiva, pois pode deixar rastros que alertam a organização-alvo.

*Vamos analisar algumas ferramentas utilizadas na Coleta de Informação Passiva e Ativa*

## **Google Hacking**


O Google Hacking se refere ao uso de operadores de pesquisa avançados do Google para criar consultas de pesquisa complexas para extrair informações confidenciais ou ocultas. As informações acessadas são então usadas por invasores para encontrar alvos vulneráveis. A Coleta usando técnicas avançadas de hacking do Google envolve a localização de

sequências específicas de texto nos resultados de pesquisa usando operadores avançados no mecanismo de pesquisa do Google.

## **Robots.txt**

Esse arquivo informa aos rastreadores do mecanismo de pesquisa quais páginas ou arquivos podem ser solicitados do site. Esse recurso é usado principalmente para evitar a sobrecarga do site com solicitações e não funciona como um mecanismo para manter uma página da Web fora dos resultados da pesquisa do Google. Para fazer isso, use diretivas noindex ou proteja sua página com uma senha.

Exemplo:



```
# Notice: Collection of data on Facebook through automated means is
# prohibited unless you have express written permission from Facebook
# and may only be conducted for the limited purpose contained in said
# permission.
# See: http://www.facebook.com/apps/site_scraping_tos_terms.php

User-agent: Applebot
Disallow: /ajax/
Disallow: /album.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /dialog/
Disallow: /fbml/ajax/dialog/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /hashtag/
Disallow: /l.php
Disallow: /moments_app/
Disallow: /p.php
Disallow: /photo.php
Disallow: /photos.php
Disallow: /share.php
Disallow: /share/
Disallow: /sharer.php
Disallow: /sharer/

User-agent: baiduspider
Disallow: /ajax/
Disallow: /album.php
Disallow: /checkpoint/
Disallow: /contact_importer/
Disallow: /dialog/
Disallow: /fbml/ajax/dialog/
Disallow: /feeds/
Disallow: /file_download.php
Disallow: /hashtag/
Disallow: /l.php
Disallow: /moments_app/
Disallow: /p.php
Disallow: /photo.php
Disallow: /photos.php
Disallow: /share.php
Disallow: /share/
Disallow: /sharer.php
Disallow: /sharer/
```

Figura 2.1

Caso queira entender um pouco mais sobre o arquivo robots.txt, eu recomendo o artigo da própria google

<https://developers.google.com/search/docs/advanced/robots/intro?hl=pt-br>

Vamos conhecer alguns dos operadores avançados do Google

---

**intitle**    [intitle:"pentest vs red team"](#)  
:  
Pesquise apenas no título da página por uma palavra ou frase. Use correspondência exata (aspas) para frases.

---

**allintitle**    [allintitle: pentest vs red team](#)  
:  
Pesquise o título da página para cada termo individual seguindo "allintitle:". O mesmo que vários intitle: 's.

---

**inurl**    [footprinting techniques inurl:.com](#)  
:  
Procure uma palavra ou frase (entre aspas) no URL do documento. Pode combinar com outros termos.

---

**allinurl**    [allinurl: pentest windows](#)  
:  
Pesquise o URL para cada termo individual após "allinurl:". O mesmo que vários inurl: 's.

---

**intext**    [intext:"windows exploitation"](#)  
:  
Pesquise uma palavra ou frase (entre aspas), mas apenas no corpo / texto do documento.

---

**allintext**    [allintext: pentest wifi and web](#)  
:  
Pesquise o corpo do texto para cada termo individual após "allintext:". O mesmo que vários intexts: 's.

---

**filetype:** "Google Hacking" filetype:pdf  
**pe:** Corresponde apenas a um tipo de arquivo específico. Alguns exemplos incluem PDF, DOC, XLS, PPT e TXT.

---

**OR** kali linux or parrot  
O padrão de pesquisa do Google é lógico AND entre os termos. Especifique "OU" para um OU lógico (MAIÚSCULAS).

---

**SITE:** kali linux site:kali.org  
Ele filtra o conteúdo pesquisado em um determinado site ou domínio

---

#### **Outros operadores:**

<https://moz.com/learn/seo/search-operators>

<https://ahrefs.com/blog/google-advanced-search-operators/>

#### **Coletando informações com Google Hacking**

Vamos utilizar algumas dorks de pesquisas para encontrar informações sensíveis, configurações expostas e etc. Muitas das vezes por não conter um arquivo robots.txt, muitas configurações ficam expostas e assim sendo possível até mesmo encontrar painel de Login administrativo.

**Dork:** intitle:"index of" intext:"apikey.txt"

Nos retorna um arquivo de texto armazenado na aplicação das chaves de API

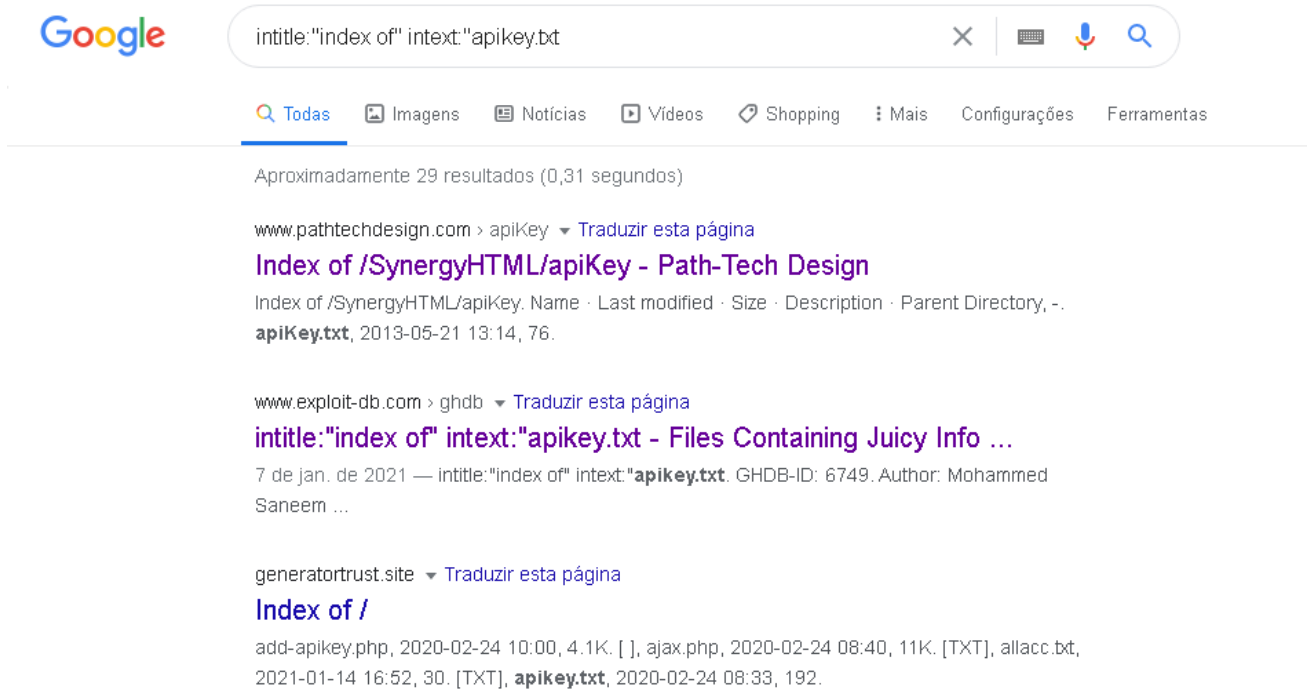


Figura 2.1

**Dork:** `intext:"nome e cpf" filetype:pdf`

Procurando sites que contém informações de nome e cpf no formato PDF



Figura 2.2

**Dork:** `inurl:login.php site:.gov.br`

Procurando por sites que na url contém a página login.php dentro dos domínios .gov.br



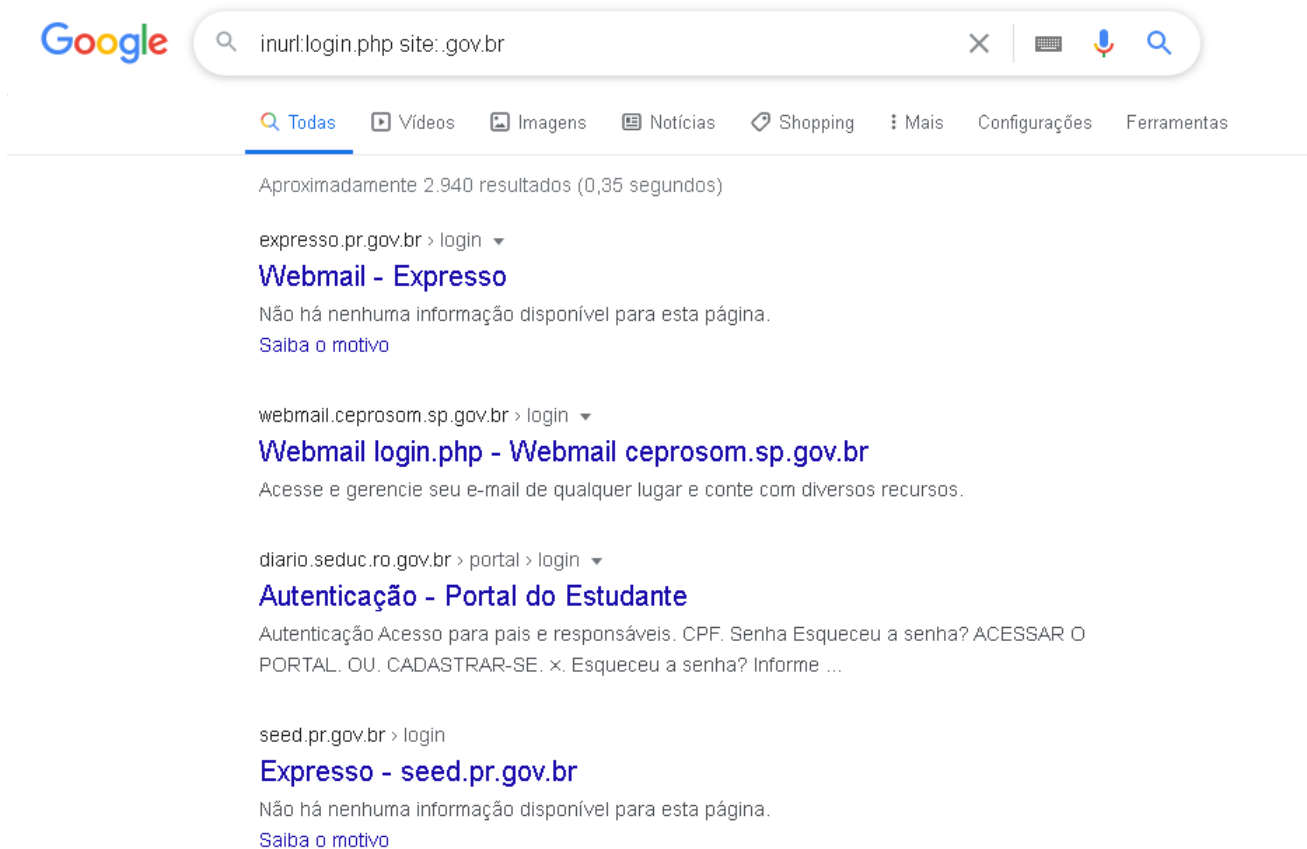


Figura 2.3

**Dork:** Intitle:"index of" windows 7

Ele nos retorna a ISO do Windows 7 em ftps públicos

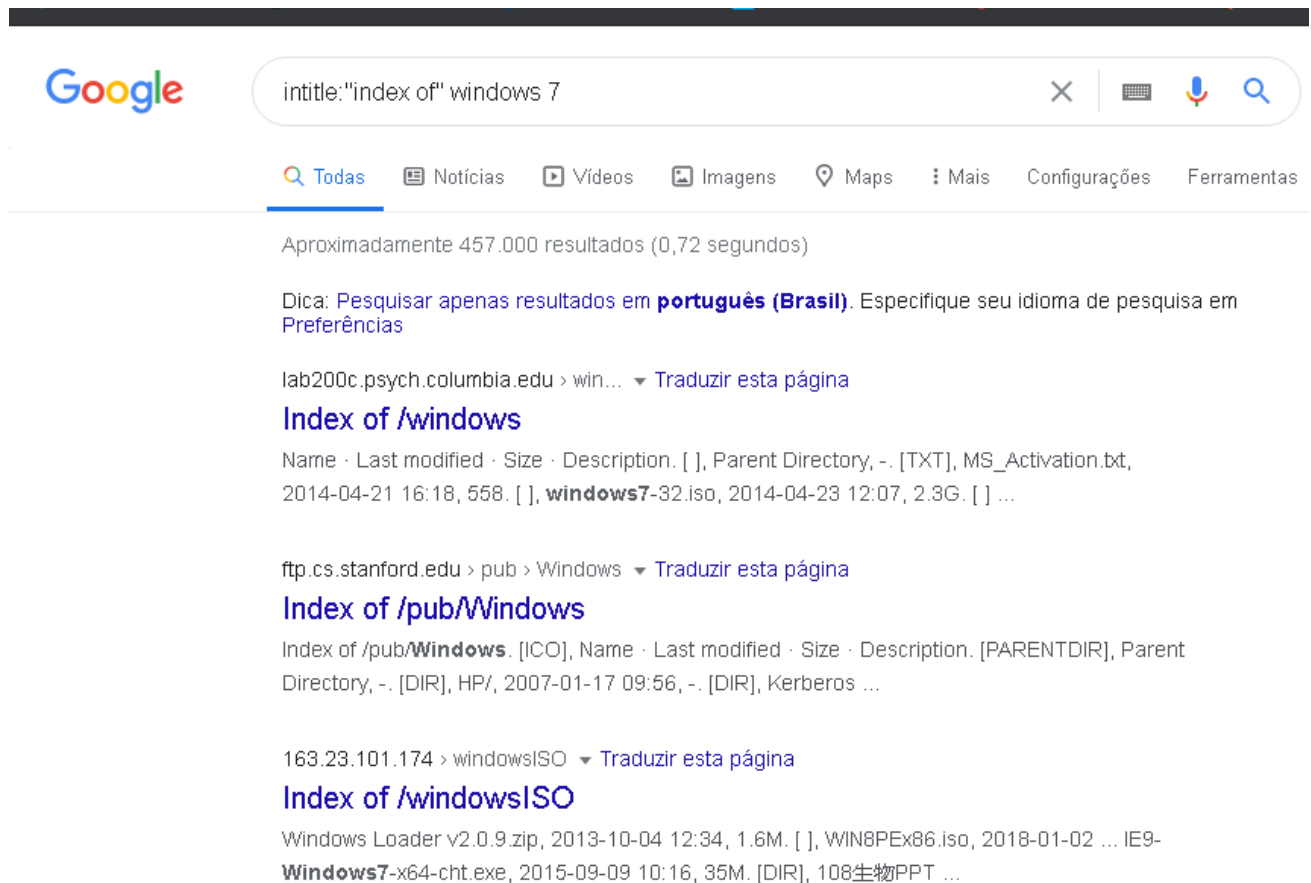


Figura 2.4

**Dork:** inurl:passwords.txt site:.com

Ele retorna os arquivos de senha em txt em sites .com

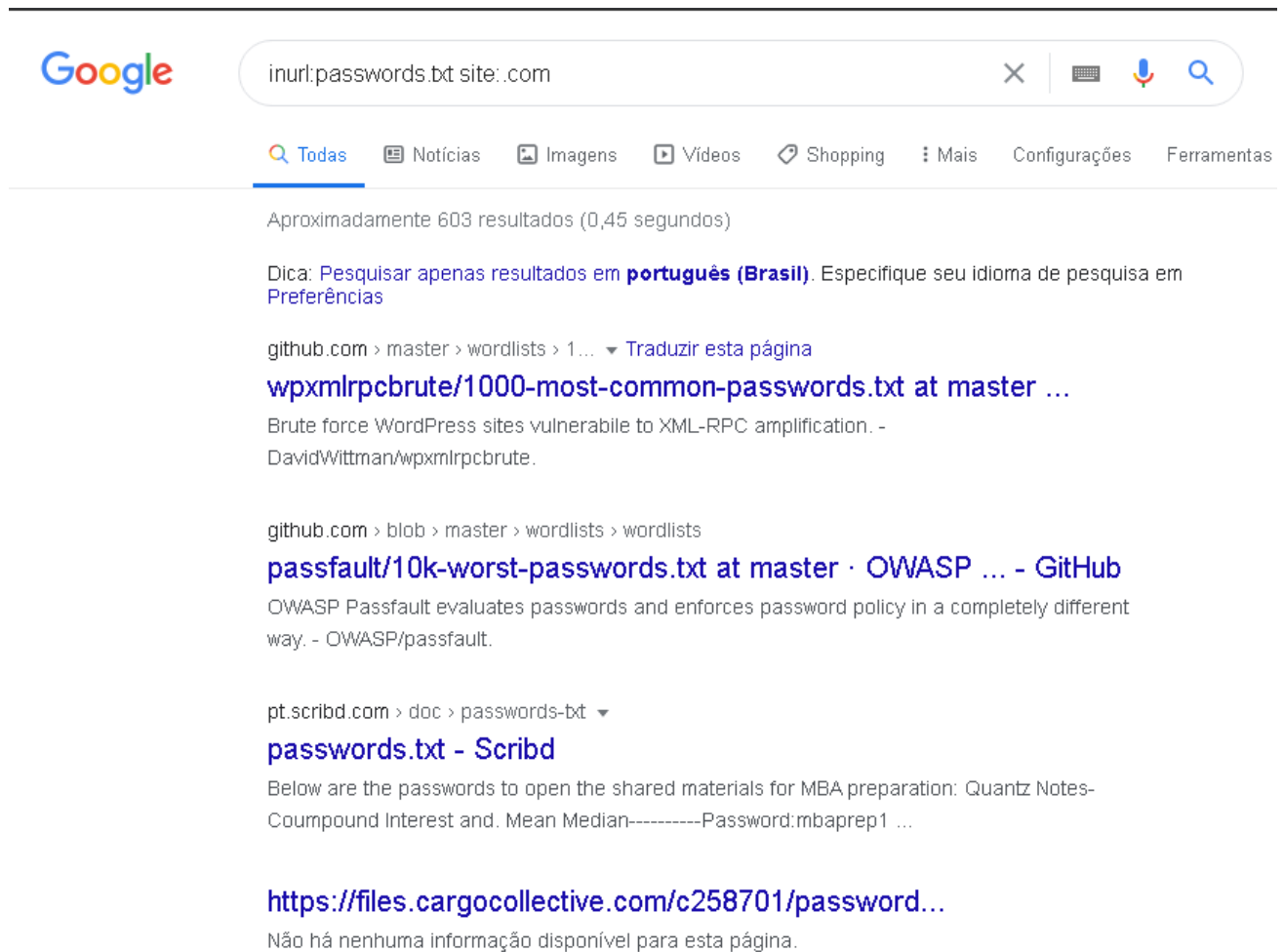


Figura 2.5

**Dork:** intitle:intranet inurl:intranet +intext:"human resources"

Vai nos retornar a intranet de algumas empresas, assim sendo útil para elaborar ataques de engenharia social contra um determinado alvo

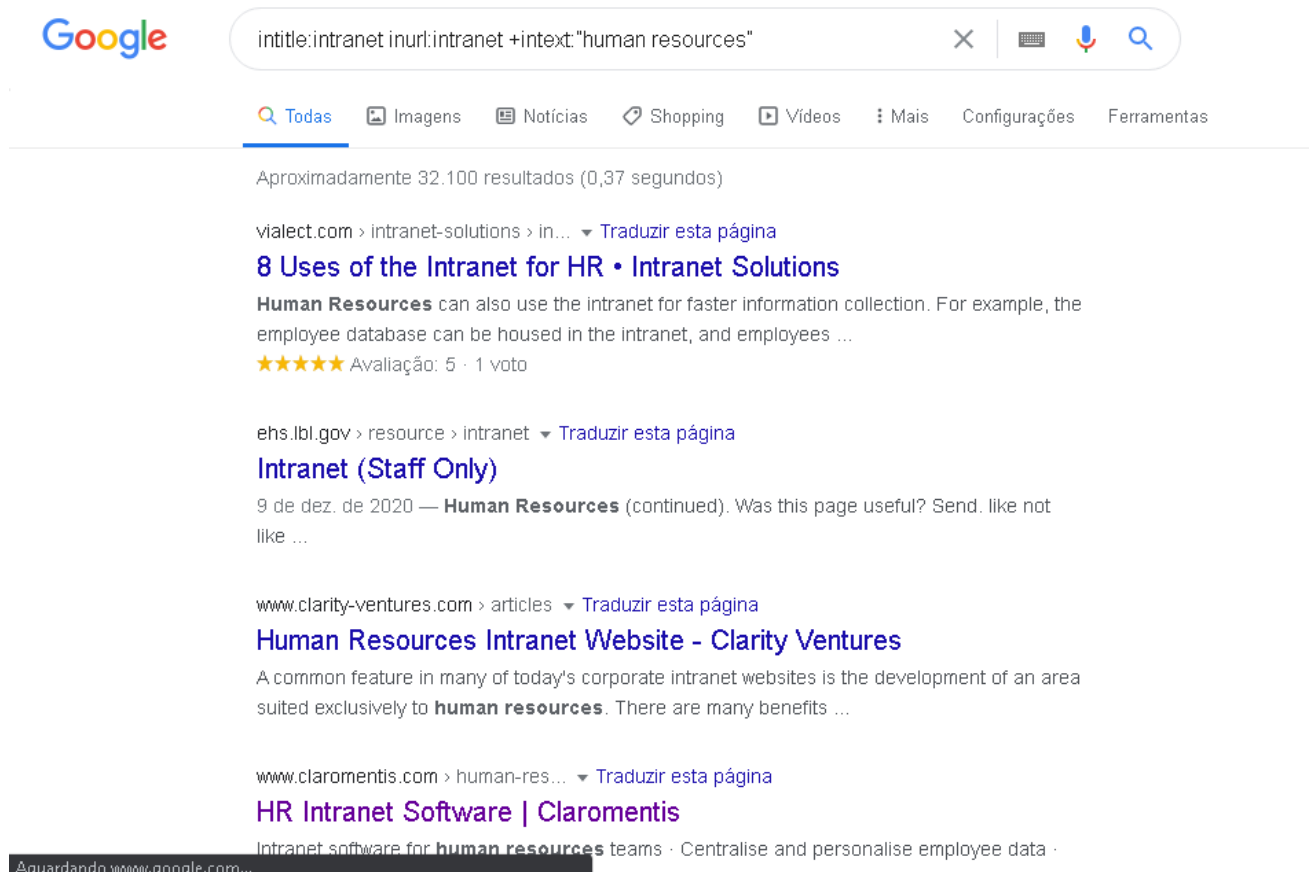


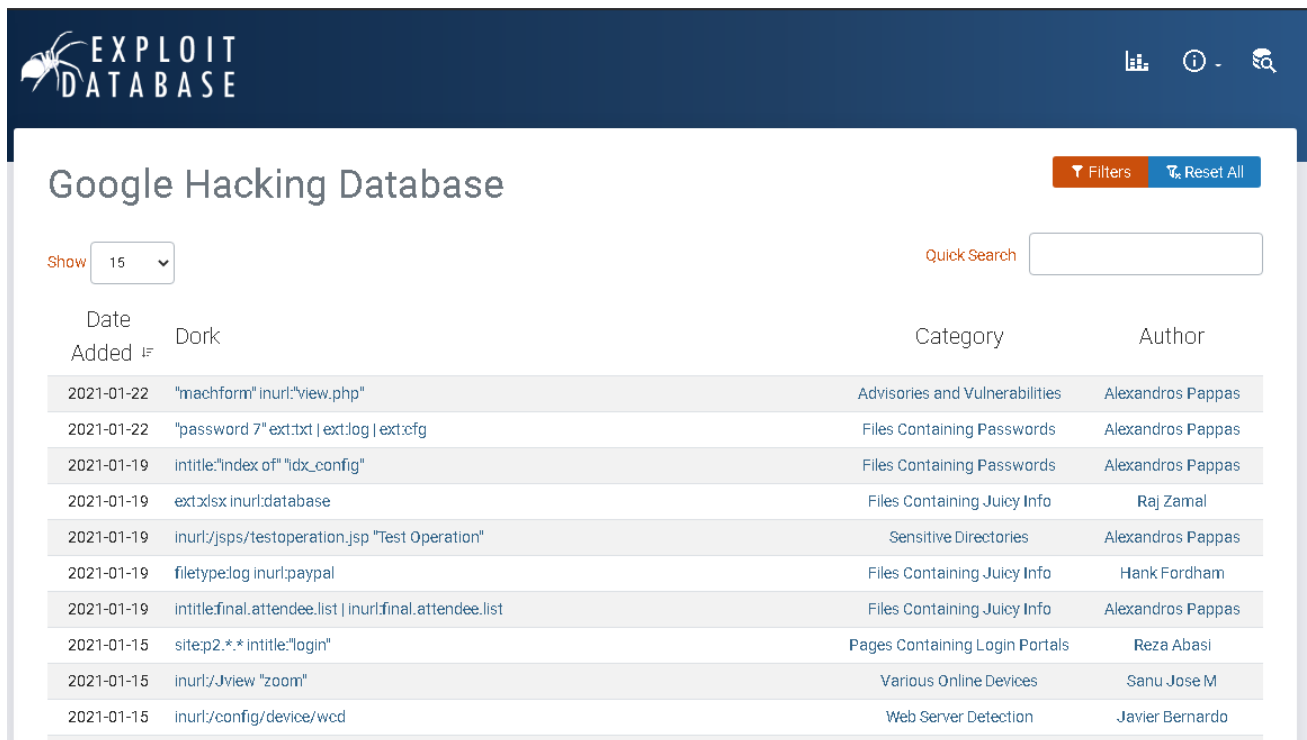
Figura 2.6

## Google Hacking Database

O Google Hacking Database (GHDB) é uma fonte confiável para consultar o escopo cada vez maior do mecanismo de pesquisa do Google. No GHDB, você encontrará termos de pesquisa para arquivos que contêm nomes de usuário, servidores vulneráveis e até mesmo arquivos que contêm senhas.

O Exploit Database é um local compatível com Vulnerabilidades e Exposições Comuns (CVE) de exploits públicos e software vulnerável correspondente, desenvolvido para uso por PenTesters e pesquisadores de vulnerabilidade.

Usando o GHDB dorks, os invasores podem identificar rapidamente todos os exploits e vulnerabilidades publicamente disponíveis da infraestrutura de TI da organização alvo. Os invasores usam operadores de pesquisa avançada do Google para extrair informações confidenciais sobre o alvo, como servidores vulneráveis, mensagens de erro, arquivos confidenciais, páginas de login e sites.



Date Added	Dork	Category	Author
2021-01-22	"machform" inurl:"view.php"	Advisories and Vulnerabilities	Alexandros Pappas
2021-01-22	"password 7" ext:txt   ext:log   ext:cfg	Files Containing Passwords	Alexandros Pappas
2021-01-19	intitle:"index of" "idx_config"	Files Containing Passwords	Alexandros Pappas
2021-01-19	ext:xls inurl:database	Files Containing Juicy Info	Raj Zamal
2021-01-19	inurl:/jsps/testoperation.jsp "Test Operation"	Sensitive Directories	Alexandros Pappas
2021-01-19	filetype:log inurl:paypal	Files Containing Juicy Info	Hank Fordham
2021-01-19	intitle:final.attendee.list   inurl:final.attendee.list	Files Containing Juicy Info	Alexandros Pappas
2021-01-15	site:p2.*.* intitle:"login"	Pages Containing Login Portals	Reza Abasi
2021-01-15	inurl:/Jview "zoom"	Various Online Devices	Sanu Jose M
2021-01-15	inurl:/config/device/wcd	Web Server Detection	Javier Bernardo

Figura 2.8

Além do GHDB, o livro Google Hacking para PenTest é um dos guias mais completos para aprender técnicas de pesquisa avançada utilizando o Google.

## OSINT Framework

**OSINT** é um modelo de inteligência que visa encontrar, selecionar e adquirir informações de fontes públicas e analisá-las para que junto com outras fontes possam produzir um conhecimento. Na comunidade de inteligência, o termo “aberto” refere-se a fontes disponíveis publicamente.

<https://kadimaintelligence.com/sem-categoria/o-que-e-open-source-intelligence-osint/>

O OSINT Framework é uma coleção de técnicas e ferramentas open sources para coleta de informação, estruturado como uma mapa mental <https://osintframework.com/>

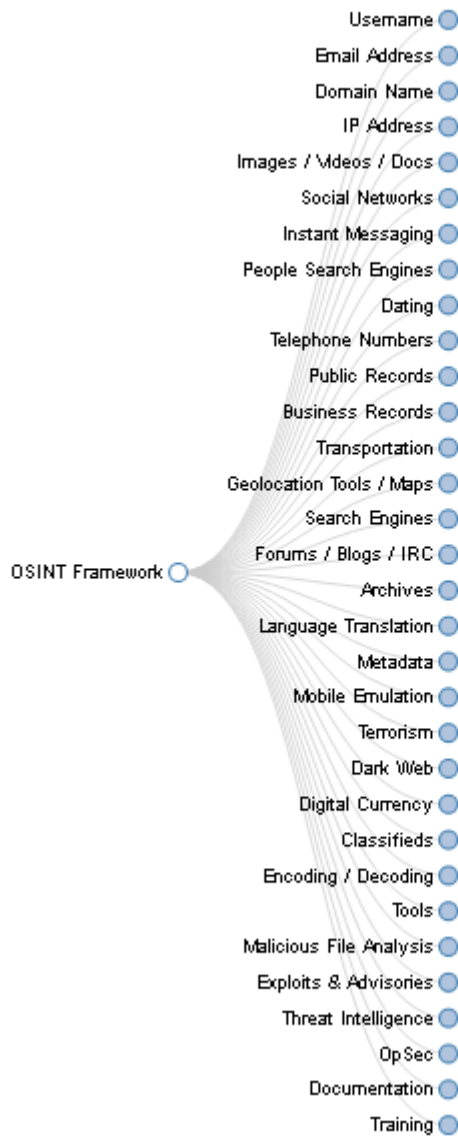


Figura 2.9

(T) - Indica um link para uma ferramenta que deve ser instalada e executada localmente

(D) - Google Dork

(R) - Requer registro

(M) - Indica um URL que contém o termo de pesquisa e o O próprio URL deve ser editado manualmente

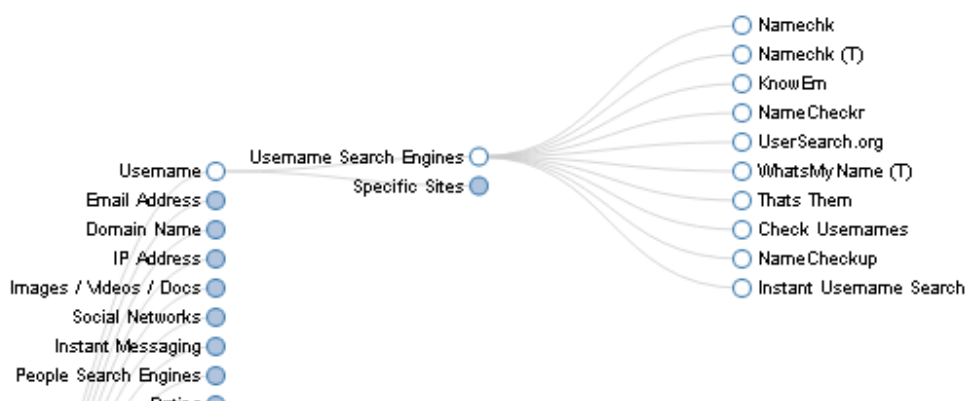


Figura 2.10

O OSINT Framework ele nos trás algumas ferramentas para validar um nome de usuário, obter detalhes de um e-mail, descobrir em quais plataformas o usuário está cadastrado.

Imagine que você tenha o e-mail da vítima e precise elaborar algum Phishing, com certeza utilizando mecanismos de pesquisas de usuário você consegue ter uma noção de quais plataformas o usuário possui conta e assim preparar uma isca para ele.

## Maltegoce

O Maltegoce é uma ferramenta utilizada para OSINT, auxiliando na mineração de dados sobre um alvo e auxiliando no processo perfilação do seu alvo.

Com o Maltego, você pode facilmente extrair dados de fontes diferentes, mesclar automaticamente as informações correspondentes em um gráfico e mapeá-lo visualmente para explorar seu cenário de dados.

Maltego oferece a capacidade de conectar facilmente dados e funcionalidades de diversas fontes usando Transforms. Por meio do Transform Hub, você pode conectar dados de mais de 30 fontes de dados diferentes, em uma variedade de fontes públicas (OSINT), bem como seus próprios dados.

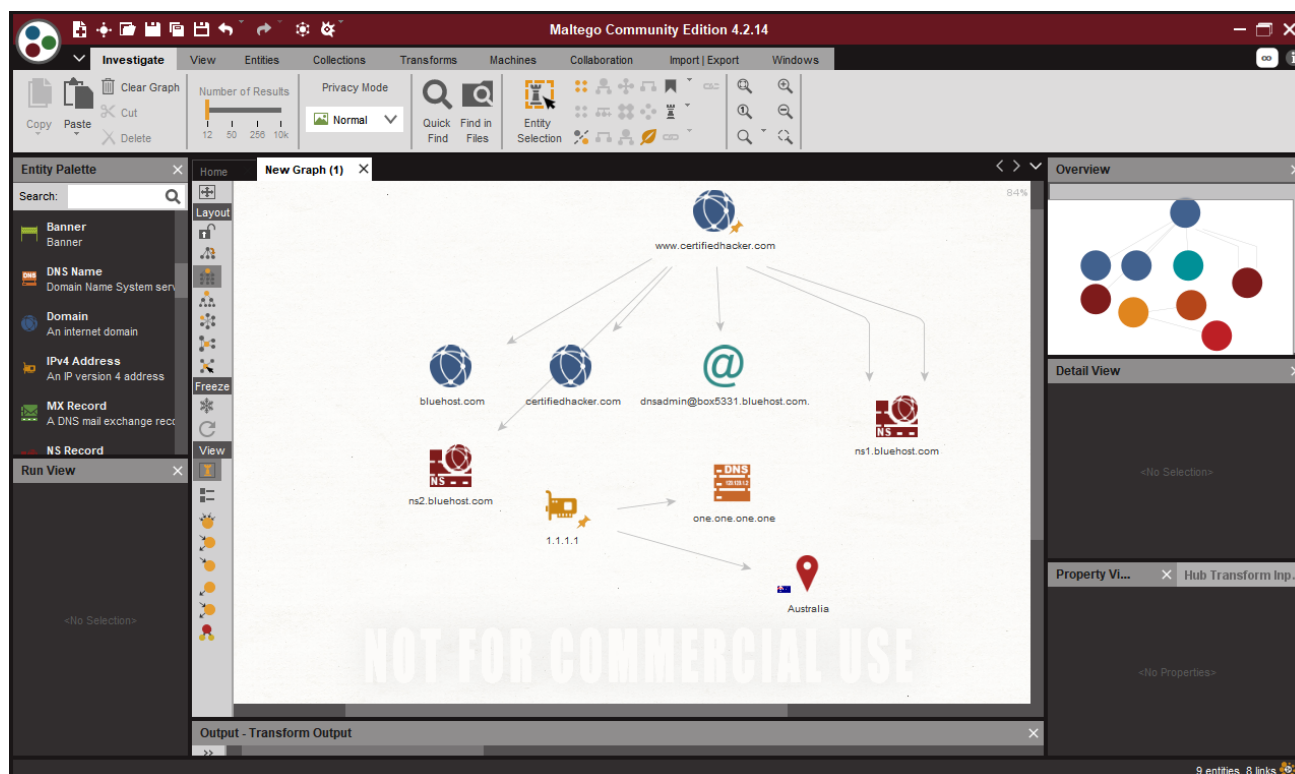


Figura 2.11

A imagem acima mostra um exemplo sistema de utilização, aonde coletamos informações sobre o domínio <http://www.certifiedhacker.com/> e o Endereço IPV4 1.1.1.1

Utilizando os transforms, conseguimos coletar algumas informações e criando um perfil do nosso alvo, podemos buscar por subdomínios, servidores de e-mails, informações do proprietário do domínio, geolocalização e principalmente utilizar plugins para coletar outro tipo de informações mais detalhadas.

Eu recomendo que você estude a ferramenta maltegoce, pois ela é bem útil no trabalho de OSINT e inteligência de ameaças, além de ser uma ferramenta bem completa e que trás um gráfico bem fácil de ser lido.

E para trabalhar com ferramentas de inteligência, com certeza é essencial que você defina uma estratégia antes de tudo, primeiramente buscar informações em outras fontes públicas e ir acrescentando os resultados dentro do maltego para você criar um mapa mental e traçar um perfil do seu alvo.

**Um artigo bem útil para você começar com o maltego:**

<https://docs.maltego.com/support/solutions/articles/15000008704-installing-maltego> (Processo de Instalação)

<https://wondersmithrae.medium.com/a-beginners-guide-to-osint-investigation-with-maltego-6b195f7245cc>

**Exemplo:**

Abra o Maltego, seja no Windows, Kali Linux ou até mesmo no seu Parrot, clique no ícone do Maltego e vá em **New**



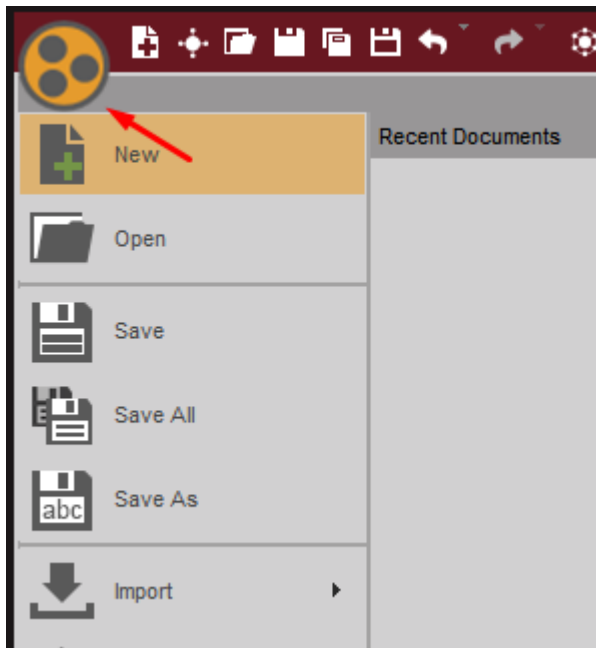


Figura 2.12

Ele vai criar um novo gráfico

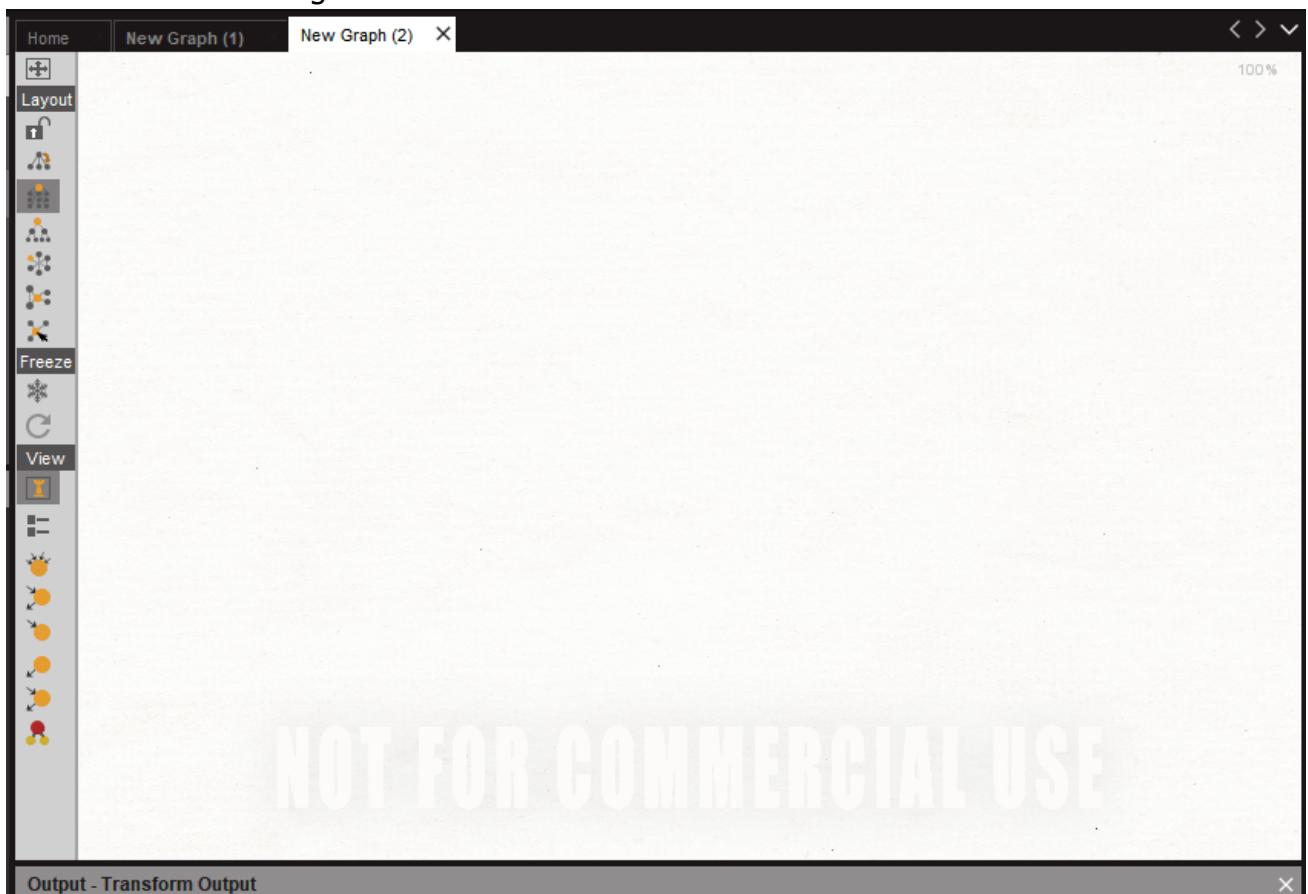


Figura 2.13

Após isso, no menu na lateral esquerda **Entity Palette** vamos selecionar **Domain** e arrastar até o gráfico

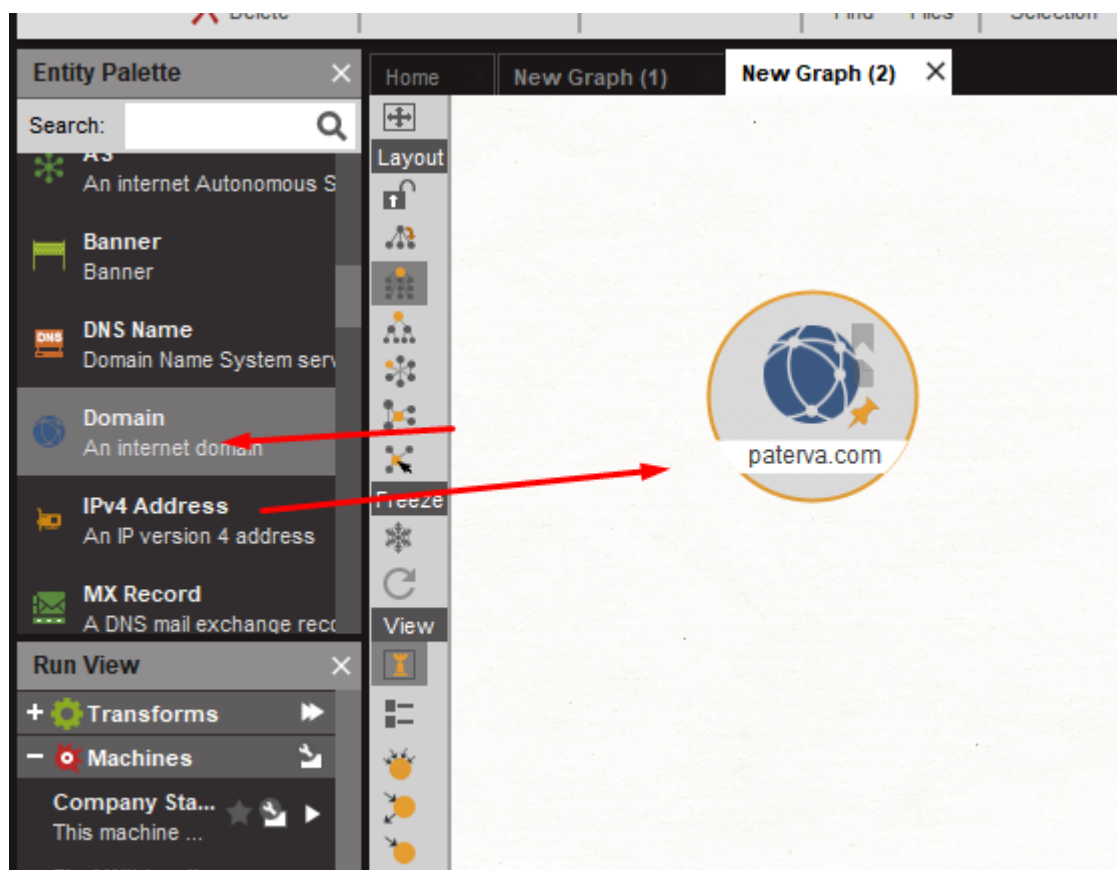


Figura 2.14

Vamos mudar paterva.com para qualquer outro site, eu recomendo utilizar o próprio certifiedhacker.com, pois ele já foi feito para teste.

Agora vamos clicar com botão direito nele e selecionar **NS**, para nos retornar os Servidores de Nome do nosso alvo

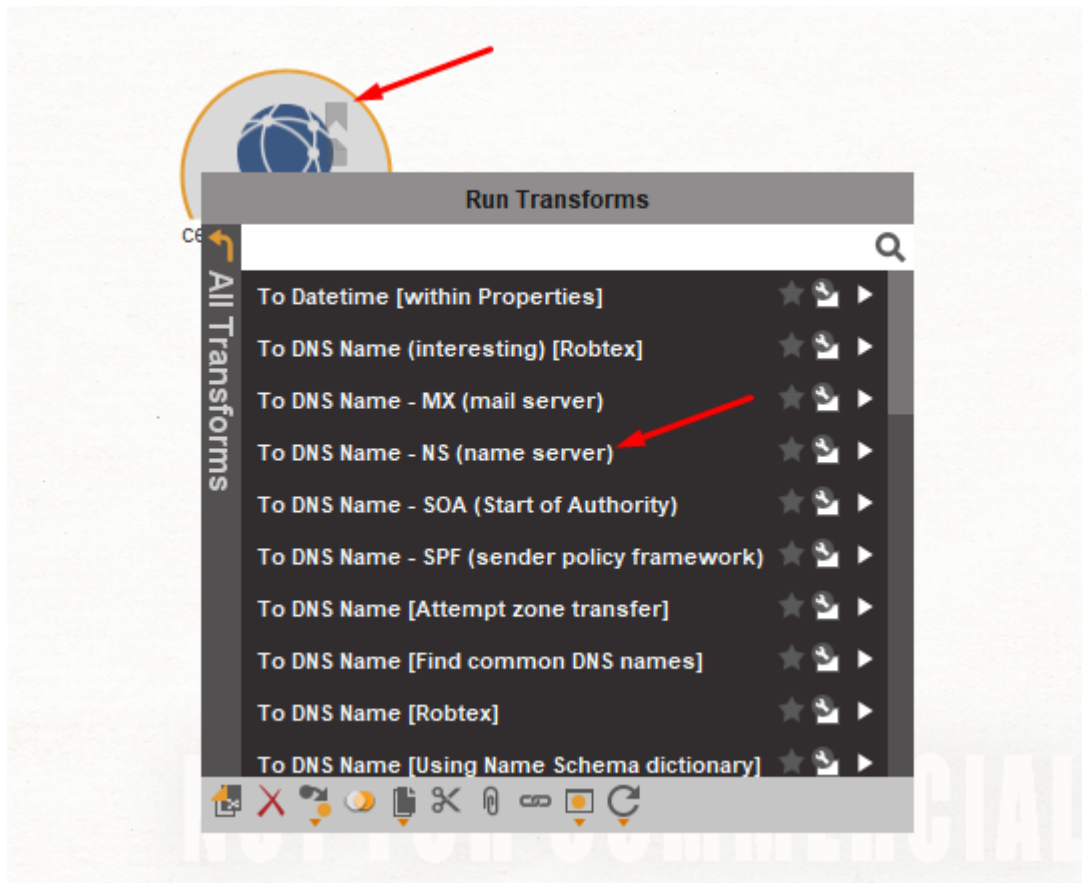


Figura 2.15

Após esse processo, ele vai nos mostrar o Name Server do **certifiedhacker.com**

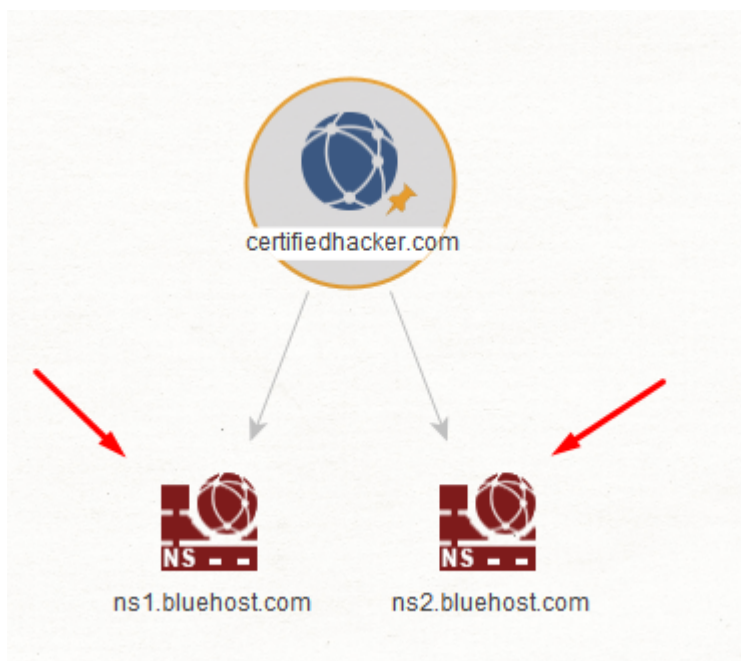


Figura 2.16

Agora você pode utilizar outros transforms para coletar mais informações, além disso, clicando com botão direito nos Name Servers, você pode utilizar transforms específicos para coletar mais informações.

## Wayback Machine

Wayback Machine é um banco de dados digital criado pela organização sem fins lucrativos Internet Archive e que arquiva mais de 475 bilhões de páginas da World Wide Web desde 1996. O Internet Archive proporciona de forma gratuita a possibilidade de visualizar versões arquivadas de páginas de um website.

Site: <https://web.archive.org/>

Podemos utilizar o Wayback para analisar o site do nosso alvo e coletar informações, por exemplo:

- Arquivos de Backup;
- Arquivos de Configuração;
- Informações Sensíveis
- Arquivos de JavaScript com informações sensíveis;
- E páginas que foram removidas ou indexadas posteriormente;

E isso acaba dando uma ótima utilidade ao wayback, principalmente no processo de coleta de informação e levantamento de vulnerabilidades.

Se você acessar o site e digitar o endereço do UOL e ir na opção Calendar, ele vai nos retornar todas as datas que o site foi arquivado



Figura 2.17

Se selecionarmos um ano e clicarmos em uma data, ele vai nos mostrar todos os snapshots que foram feitos em diferentes horário

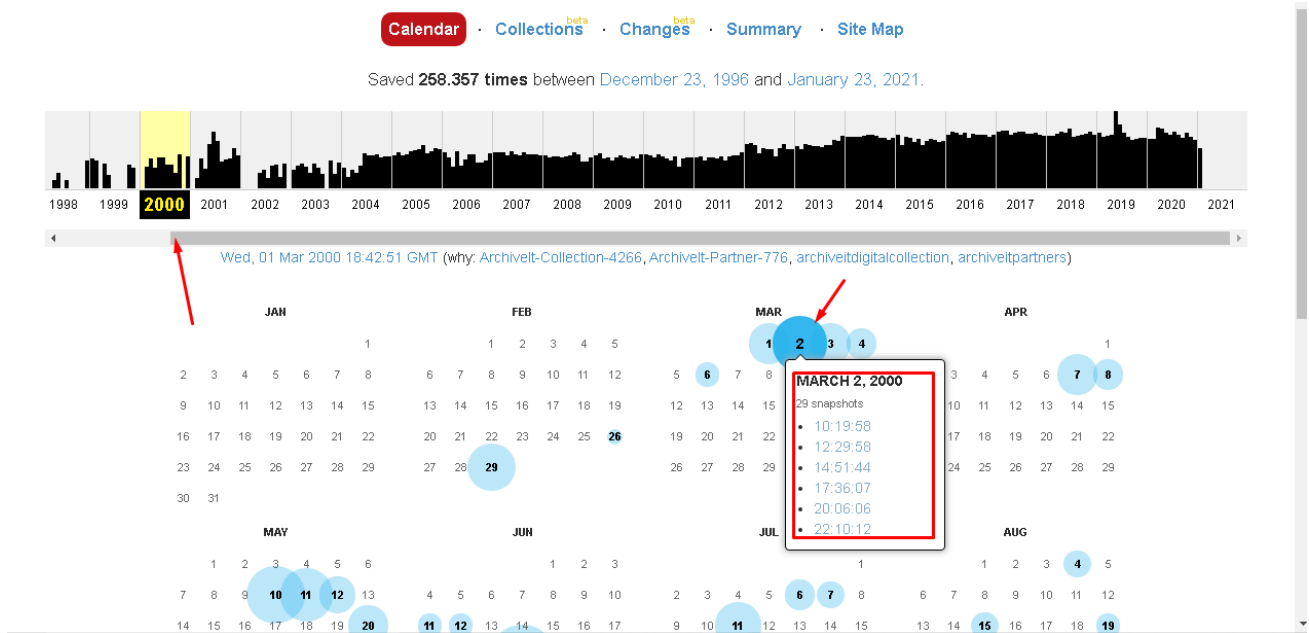


Figura 2.18

Se clicarmos em alguns dos horários, ele vai nos mostrar a interface daquela respectiva data.

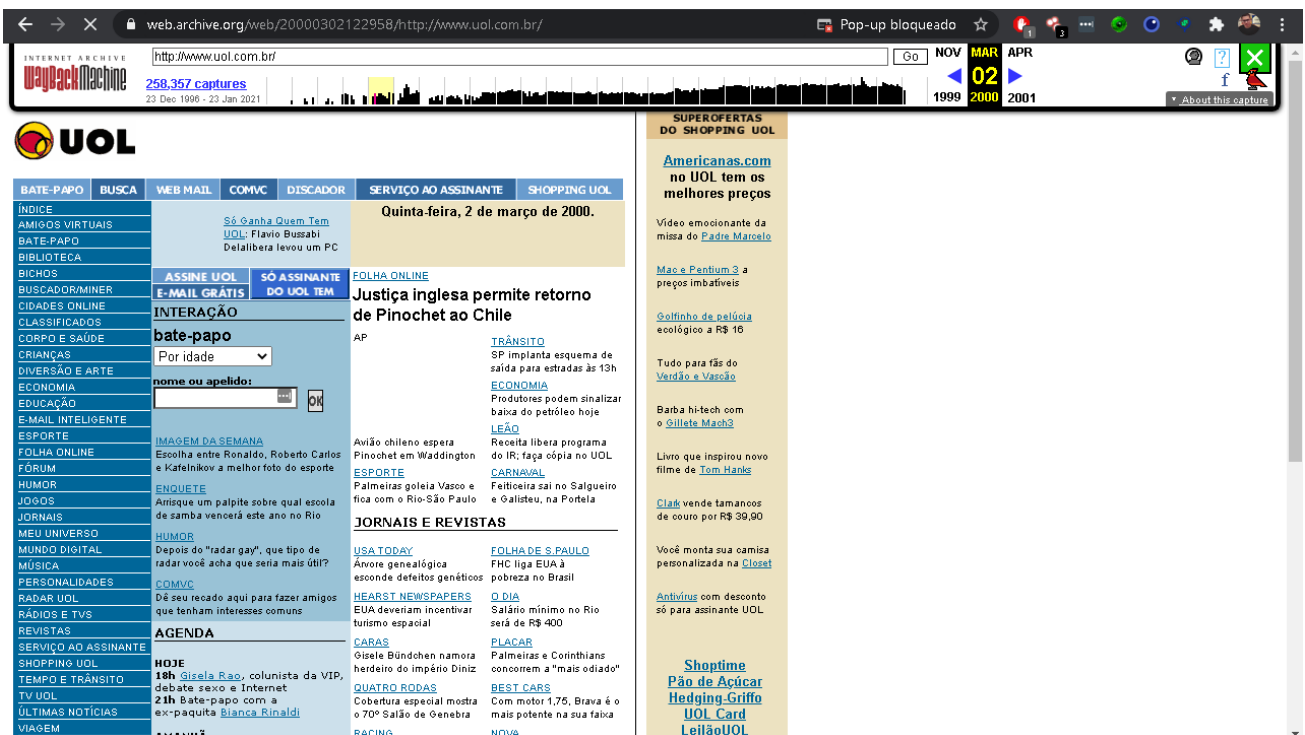


Figura 2.19

Perceba que ele nos mostra como era exatamente o site daquela época, você pode até navegar no site e procurar por informações sensíveis.

Além disso, o wayback pode ser utilizado para recuperar postagens feitas em redes sociais, principalmente o twitter.



Figura 2.20

Nesse exemplo utilizo o Twitter do Bill Gates, quem sabe alguma informação sensível não foi revelada que pode até mesmo beneficiar a concorrência?

É assim que você navega manualmente nas versões mais antigas de um site. É uma ótima ferramenta, mas não é muito prática quando você está testando dezenas de subdomínios e precisa encontrar rapidamente cada arquivo JS ou URL de cada subdomínio presente.

Para auxiliar nesse trabalho, existem algumas ferramentas úteis

<https://github.com/mhmdiaa/waybackunifier>

<https://github.com/daudmalik06/ReconCat>

<https://github.com/EdOverflow/curate>

<https://github.com/tomnomnom/waybackurls>

<https://gist.github.com/mhmdiaa/adf6bff70142e5091792841d4b372050>

## Waybackunifier

A primeira ferramenta é o Waybackunifier. Ele faz a varredura de instantâneos do URL fornecido. Em seguida, ele agrega todas as suas versões anteriores e retorna um arquivo unificado que contém todas as linhas exclusivas já incluídas naquela página.

Então, basicamente, o Waybackunifier cria um único arquivo que contém tudo o que a URL já conteve

## ReconCat

ReconCat retorna todos os URLs de instantâneos disponíveis. Não é o seu conteúdo, apenas os URLs.

A saída está dentro de uma pasta com o nome do domínio que você inseriu. Ele contém um arquivo para cada ano e dentro está a lista de instâncias disponíveis para aquele ano.

Uso: `php recon --url=https://example.com --year=all`

## Waybackurls

Waybackurls retorna uma lista de todos os URLs que o Wayback Machine conhece para um domínio.

Uso: `waybackurls https://example.com`

## Curate

O curate consulta várias ferramentas, incluindo a Wayback Machine. Ele retorna uma lista de URLs encontrados em seu domínio de destino usando essas ferramentas.

Também tem a opção de pesquisar as palavras-chave que você quiser. Isso é útil para detectar informações confidenciais, como senhas e chaves de API, ou novos terminais.

Uso: `curate https://example.com`

## Mais informações:

<https://pentester.land/podcast/2019/03/01/the-bug-hunter-podcast-02.html>

## Netcraft Site Report

O Netcraft Site Report analisa e levanta informações sobre um determinado site, como o endereço IPV4 do site, em qual domínio ele está hospedado, name server, geolocalização e entre outras informações.

**Acesse o site:** <https://sitereport.netcraft.com/>

Vamos pegar a url do site <http://www.certifiedhacker.com/> e colar, após isso vamos dar um **lookup**.

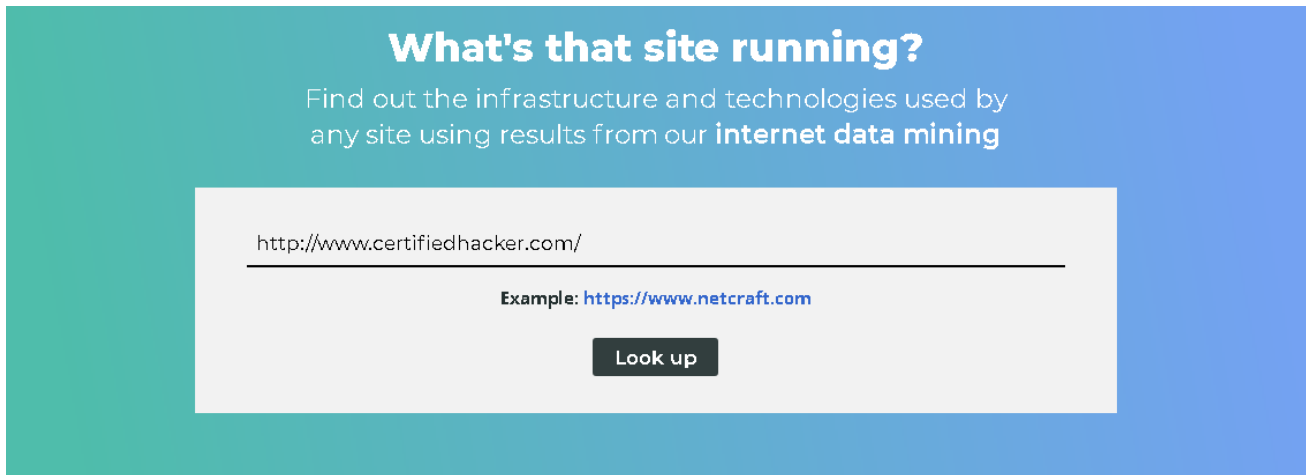


Figura 2.21

Após isso, ele vai analisar o site e nos retornar algumas informações

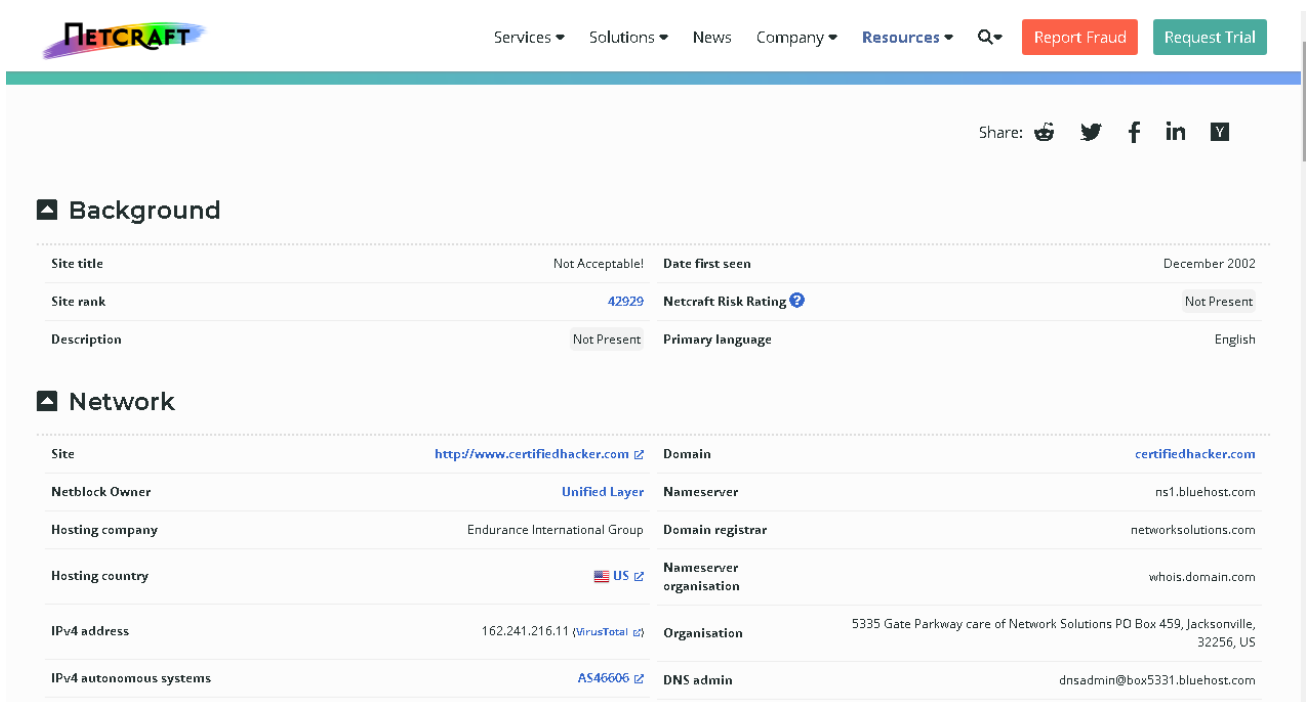


Figura 2.22

Você pode analisar outros sites e obter informações relevantes sobre seu alvo.

## Nslookup

O utilitário NSlookup é usado para pesquisar um endereço IP específico ou vários endereços IP associados a um nome de domínio.

NSlookup é usado quando um usuário pode acessar um recurso especificando seu endereço IP, mas não pode acessá-lo por seu nome DNS

O utilitário Nslookup é usado para corrigir problemas de resolução de nomes. E O comando nslookup pode ser executado no prompt de comando para pesquisar o endereço IP de um



nome DNS. Os subcomandos podem ser usados no final do comando nslookup para realizar consultas.

Para realizar alguma consulta, basta abrir o CMD ou o seu terminal linux e usar o comando nslookup

```
C:\Users\xxx>nslookup uol.com.br
Servidor:  dns.google
Address:  8.8.8.8

Não é resposta autoritativa:
Nome:      uol.com.br
Addresses: 2804:49c:3102:401:ffff:ffff:ffff:36
           2804:49c:3101:401:ffff:ffff:ffff:45
           200.147.3.157
```

Figura 2.23

```
C:\Users\xxx>nslookup www.certifiedhacker.com
Servidor:  dns.google
Address:  8.8.8.8

Não é resposta autoritativa:
Nome:      certifiedhacker.com
Address:   162.241.216.11
Aliases:   www.certifiedhacker.com
```

Figura 2.24

Podemos utilizar queries para aprimorar as nossas consultas DNS, se digitarmos nslookup e depois digitar help, ele vai nos mostrar os comandos do utilitário e os tipos de query que podemos utilizar.

```
C:\Users\xxx>nslookup
Servidor Padrão: dns.google
Address: 8.8.8.8

> help
Comandos: (identificadores aparecem em letras maiúsculas, [] significa opcional)
NOME - exibe informações sobre o host/domínio NOME usando o servidor padrão
NOME1 NOME2 - o mesmo que acima, mas usa NOME2 como servidor
help ou ? - exibe informações sobre comandos comuns
set OPÇÃO - define uma opção
    all - exibe opções, o host e o servidor atual
    [no]debug - exibe informações de depuração
    [no]d2 - exibe informações de depuração completas
    [no]defname - anexa o nome do domínio a cada consulta
    [no]recurse - solicita uma resposta recursiva para a consulta
    [no]search - usa a lista de pesquisa de domínios
    [no]vc - usa sempre um circuito virtual
    domain=NOME - define o nome do domínio padrão como NOME
    srchlist=N1[/N2/.../N6] - define o domínio como N1 e a lista de pesquisa como N1, N2 etc.
    root=NOME - define o servidor raiz como NOME
    retry=X - define o número de tentativas como X
    timeout=X - define o intervalo de tempo limite inicial como X segundos
    type=X - define o tipo de consulta (ex.: A,AAAA,A+AAAA,ANY,CNAME,MX,NS,PTR,SOA,SRV)
    querytype=X - o mesmo que type
    class=X - define a classe da consulta (ex.: IN (Internet), ANY)
    [no]mxsfr - usa a transferência rápida de zona da MS
    ixfrver=X - versão atual a ser usada na solicitação de transferência IXFR
server NOME - define o servidor padrão como NOME, usando o servidor padrão atual
lserver NOME - define o servidor padrão como NOME, usando o servidor inicial
root - define o servidor padrão atual como a raiz
```

Figura 2.25

**Podemos especificar os seguintes tipos de registro de DNS:**

- R: Especifica o endereço IP de um computador.

- CNAME: Especifica um nome canônico para um alias.
- GID Especifica um identificador de grupo de um nome de grupo.
- HINFO: Especifica a CPU e o tipo de sistema operacional de um computador.
- MB: Especifica um nome de domínio de caixa de correio.
- Mg: Especifica um membro do grupo de email.
- MINFO: Especifica informações da caixa de correio ou da lista de mensagens.
- Mr: Especifica o nome de domínio de renomeação de email.
- MX: Especifica o trocador de mensagens.
- Ns: Especifica um servidor de nomes DNS para a zona nomeada.
- PTR: Especifica um nome de computador se a consulta for um endereço IP; caso contrário, especifica o ponteiro para outras informações.
- Soa: Especifica o início de autoridade para uma zona DNS.
- Txt: Especifica as informações de texto.
- UID: Especifica o identificador de usuário.
- UINFO: Especifica as informações do usuário.
- WKS: Descreve um serviço conhecido.

<https://docs.microsoft.com/pt-br/windows-server/administration/windows-commands/nslookup-set-querytype>

Posso utilizar essas queries para levantar informações sobre nosso alvo, por exemplo:

```
> set querytype=MX
> www.certifiedhacker.com
Servidor:  dns.google
Address:  8.8.8.8

Não é resposta autoritativa:
www.certifiedhacker.com canonical name = certifiedhacker.com
certifiedhacker.com      MX preference = 0, mail exchanger = mail.certifiedhacker.com
>
```

Figura 2.26

Na imagem acima, usei o comando **set querytype=mx** para nos retorna o servidor de e-mail utilizado por esse domínio

```
> set querytype=NS
> www.certifiedhacker.com
Servidor:  dns.google
Address:  8.8.8.8

Não é resposta autoritativa:
www.certifiedhacker.com canonical name = certifiedhacker.com
certifiedhacker.com      nameserver = ns2.bluehost.com
certifiedhacker.com      nameserver = ns1.bluehost.com
>
```

Figura 2.27

Nessa imagem acima definimos o tipo da query como NS, para nos retornar os Name Servers do nosso alvo.

Podemos definir outras queries para levantar informações de um domínio específico, como o exemplo abaixo nos mostra

```

> uol.com.br
Servidor:  dns.google
Address:  8.8.8.8

Não é resposta autoritativa:
uol.com.br      nameserver = borges.uol.com.br
uol.com.br      nameserver = charles.uol.com.br
uol.com.br      nameserver = eliot.uol.com.br
>

```

Figura 2.28

O Nslookup é bastante útil para a coleta de informações de DNS de um determinado alvo.

## Dig

Dig é uma ferramenta de redes de computadores, utilizada para consultas sobre registros de DNS de um determinado domínio, host ou IP.

O ISC (*Internet Systems Consortium*), é o grupo responsável pelo seu desenvolvimento, assim como é responsável pelo desenvolvimento do BIND – um dos servidores de **DNS** mais populares e mais usados no mundo. A título de curiosidade, no CentOS, por exemplo, ele é empacotado no dns-utils, que também traz outros utilitários bem conhecidos como o **nslookup**, host, etc.

Vamos ver alguns exemplos de uso:

Se digitarmos apenas **dig** no terminal, ele vai retornar informações do DNS que se encontra no /etc/resolv.conf

```

root@kali:~# dig

; <<>> DiG 9.16.8-Debian <<>>
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 774
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;.                IN      NS

;; ANSWER SECTION:
.                  35683  IN      NS      a.root-servers.net.
.                  35683  IN      NS      b.root-servers.net.
.                  35683  IN      NS      c.root-servers.net.
.                  35683  IN      NS      d.root-servers.net.
.                  35683  IN      NS      e.root-servers.net.
.                  35683  IN      NS      f.root-servers.net.
.                  35683  IN      NS      g.root-servers.net.
.                  35683  IN      NS      h.root-servers.net.
.                  35683  IN      NS      i.root-servers.net.
.                  35683  IN      NS      j.root-servers.net.
.                  35683  IN      NS      k.root-servers.net.
.                  35683  IN      NS      l.root-servers.net.
.                  35683  IN      NS      m.root-servers.net.

;; Query time: 8 msec

```

Figura 2.29

Digitando **dig** [www.certifiedhacker.com](http://www.certifiedhacker.com) ele vai nos retornar informações do respectivo domínio

```
root@kali:~# dig www.certifiedhacker.com

; <<>> DiG 9.16.8-Debian <<>> www.certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 17760
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.certifiedhacker.com.      IN      A

;; ANSWER SECTION:
www.certifiedhacker.com. 14399 IN      CNAME   certifiedhacker.com.
certifiedhacker.com.    14399 IN      A       162.241.216.11

;; Query time: 188 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: dom jan 24 18:16:13 -03 2021
;; MSG SIZE rcvd: 82
```

Figura 2.30

O Comando **dig -h** ele nos retorna as sintaxes do utilitário que podemos utilizar

```
root@kali:~# dig -h
Usage: dig [@global-server] [domain] [q-type] [q-class] {q-opt}
        {global-d-opt} host [@local-server] {local-d-opt}
        [ host [@local-server] {local-d-opt} [ ... ] ]
Where:  domain    is in the Domain Name System
        q-class   is one of (in,hs,ch,...) [default: in]
        q-type    is one of (a,any,mx,ns,soa,hinfo,axfr,txt,...) [default:a]
                (Use ixfr=version for type ixfr)
        q-opt     is one of:
                -4                (use IPv4 query transport only)
                -6                (use IPv6 query transport only)
                -b address[#port] (bind to source address/port)
                -c class          (specify query class)
                -f filename       (batch mode)
                -k keyfile        (specify tsig key file)
                -m                (enable memory usage debugging)
                -p port           (specify port number)
                -q name           (specify query name)
                -r                (do not read ~/.digrc)
                -t type           (specify query type)
                -u                (display times in usec instead of msec)
                -x dot-notation   (shortcut for reverse lookups)
                -y [hmac:]name:key (specify named base64 tsig key)
        d-opt     is of the form +keyword[=value], where keyword is:
                +[no]aaflag      (Set AA flag in query (+[no]aaflag))
```

Figura 2.31

Se digitarmos **dig -t MX** [www.certifiedhacker.com](http://www.certifiedhacker.com) ele vai nos trazer o servidor de e-mail do respectivo domínio, sendo o **-t (tipo de query)**

```

root@kali:~# dig -t MX www.certifiedhacker.com

; <<>> DiG 9.16.8-Debian <<>> -t MX www.certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 14067
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.certifiedhacker.com.      IN      MX

;; ANSWER SECTION:
www.certifiedhacker.com. 14375 IN      CNAME   certifiedhacker.com.
certifiedhacker.com.    14399 IN      MX      0 mail.certifiedhacker.com.

;; Query time: 184 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: dom jan 24 18:18:48 -03 2021
;; MSG SIZE rcvd: 87

```

Figura 2.32

Podemos coletar o Name Server de um domínio, utilizando o comando **dig -t NS** [www.certifiedhacker.com](http://www.certifiedhacker.com)

```

root@kali:~# dig -t NS www.certifiedhacker.com

; <<>> DiG 9.16.8-Debian <<>> -t NS www.certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 4499
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.certifiedhacker.com.      IN      NS

;; ANSWER SECTION:
www.certifiedhacker.com. 14157 IN      CNAME   certifiedhacker.com.
certifiedhacker.com.    21599 IN      NS      ns1.bluehost.com.
certifiedhacker.com.    21599 IN      NS      ns2.bluehost.com.

;; Query time: 188 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: dom jan 24 18:20:15 -03 2021
;; MSG SIZE rcvd: 111

```

Figura 2.33

Além disso, com o Dig você pode validar se um domínio está bem configurado ou não, além de coletar informações essenciais. Você pode testar outros domínios e validar as suas configurações.

## Whois

WHOIS (pronuncia-se "ruís" no Brasil) é um protocolo da pilha TCP/IP (porta 43) específico para consultar informações de contato e DNS sobre entidades na internet.

Uma entidade na internet pode ser um nome de domínio, um endereço IP ou um AS (Sistema Autônomo).

Para cada entidade, o protocolo WHOIS apresenta três tipos de contato: Contato Administrativo (Admin Contact), Contato Técnico (Technical Contact) e Contato de Cobrança (Billing Contact). Estes contatos são informações de responsabilidade do provedor de internet, que as nomeia de acordo com as políticas internas de sua rede.

Para os registros de domínios, os usuários tem a opção de optar por um Whois privado, que esconde os dados do dono do domínio. Esse opção é oferecida de graça por alguns provedores e por um valor anual, por outras

Existem algumas ferramentas de Whois, tanto on-line como em linha de comando.

O Registro Br tem um banco de dados com mais de 3 milhões de registros DNS, e com isso tem uma ferramenta de Whois ao qual podemos consultar alguns domínios.

<https://registro.br/tecnologia/ferramentas/whois>



Whois

uol.com.br

Exibir resultado completo

Copyright © NIC.br  
A utilização dos dados abaixo é permitida somente conforme descrito nos [Termos de Uso](#), sendo proibida a sua distribuição, comercialização ou reprodução, em particular para fins publicitários ou propósitos similares.  
2021-01-24 18:28:58 -03:00 - IP: 170.254.144.154

Domínio <b>uol.com.br</b>	
TITULAR	Universe Online S.A.
DOCUMENTO	01.109.184/0004-38
RESPONSÁVEL	Contato da Entidade UOL
PAÍS	BR
CONTATO DO TITULAR	CAU12
CONTATO TÉCNICO	CTU6
SERVIDOR DNS	eliot.uol.com.br 200.221.11.98 ~
SERVIDOR DNS	borges.uol.com.br 200.147.255.105 ~

Figura 2.34

O Whatsmyip possui algumas ferramentas de pesquisa de DNS e informações de endereços IP, além de uma ferramenta de consulta Whois

<https://www.whatsmyip.org/>

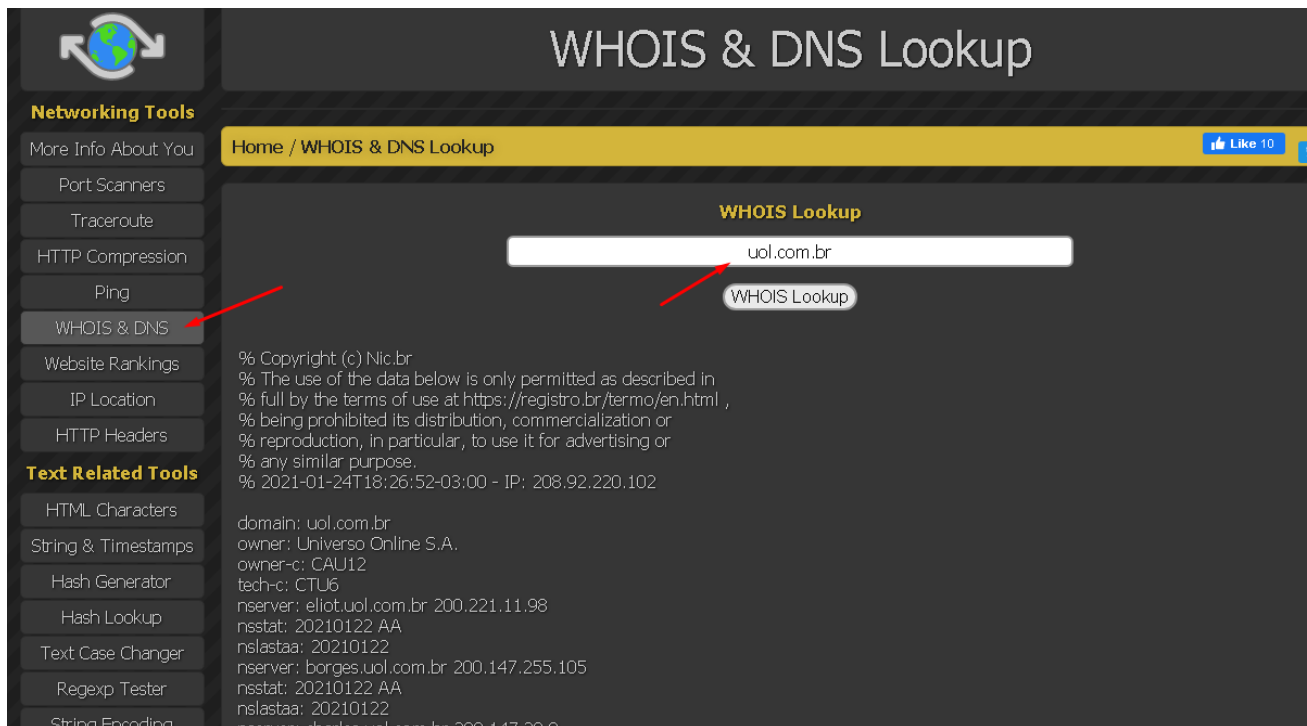


Figura 2.35

No Kali Linux ou Parrot tem o comando Whois que podemos utilizar para fazer as consultas

```
root@kali:~# whois uol.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.
% 2021-01-24T19:48:22-03:00 - IP: 170.254.144.154

domain:      uol.com.br
owner:       Universo Online S.A.
ownerid:     01.109.184/0004-38
responsible: Contato da Entidade UOL
country:     BR
owner-c:     CAU12
tech-c:      CTU6
nservers:    eliot.uol.com.br 200.221.11.98
nsstat:      20210122 AA
nslastaa:    20210122
nservers:    borges.uol.com.br 200.147.255.105
nsstat:      20210122 AA
nslastaa:    20210122
nservers:    charles.uol.com.br 200.147.38.8
nsstat:      20210122 AA
nslastaa:    20210122
created:     19960424 #7137
changed:     20170106
```

Figura 2.36



Um invasor consulta um servidor de banco de dados Whois para obter informações sobre o nome de domínio do seu alvo, além de detalhes de contato de seu proprietário, data de expiração daquele domínio, data de criação e assim por diante. E o servidor Whois responde à consulta com as informações solicitadas. Usando essas informações, um invasor pode criar um mapa da rede da organização-alvo, e enganar os proprietários do domínio utilizando técnicas de engenharia social para obter detalhes internos da rede.

## DNSRecon

O DNSRecon pode executar uma variedade de funções, desde avaliações de segurança até solução de problemas básicos de rede, permitindo que os usuários:

- Verifique os registros de cache do servidor DNS para registros A, AAAA e CNAME, dada uma lista de registros de host em um arquivo de texto
- Enumerar os registros DNS gerais para um determinado domínio (MX, SOA, NS, A, AAAA, SPF e TXT)
- Verificar todos os registros de servidor de nome para transferências de zona
- Verificar a resolução do wildcard
- Realizar enumeração de registro SRV comum e top-level domain (TLD)
- Verifique o subdomínio de força bruta e os registros A e AAAA do host, dados um domínio e uma lista de palavras
- Execute uma pesquisa de registro PTR para um determinado intervalo de IP ou CIDR
- Executar subdomínio e enumeração de host por meio do Google Dorks
- Apresentar descobertas em formato de arquivo de texto para fácil manipulação
- 

Vamos digitar `dnsrecon -h` no terminal para obtermos as informações de sintaxe da ferramenta

```
root@kali:~# dnsrecon -h
usage: dnsrecon.py [-h] -d DOMAIN [-n NS_SERVER] [-r RANGE] [-D DICTIONARY] [-f] [-a] [-s]
                  [-b] [-y] [-k] [-w] [-z] [--threads THREADS] [--lifetime LIFETIME] [--tcp]
                  [--db DB] [-x XML] [-c CSV] [-j JSON] [--iw] [--disable_check_recursion]
                  [--disable_check_bindversion] [-v] [-t TYPE]

optional arguments:
  -h, --help                show this help message and exit
  -d DOMAIN, --domain DOMAIN
                           Target domain.
  -n NS_SERVER, --name_server NS_SERVER
                           Domain server to use. If none is given, the SOA of the target will be
                           used. Multiple servers can be specified using a comma separated list.
  -r RANGE, --range RANGE
                           IP range for reverse lookup brute force in formats (first-last) or in
                           (range/bitmask).
  -D DICTIONARY, --dictionary DICTIONARY
                           Dictionary file of subdomain and hostnames to use for brute force.
                           Filter out of brute force domain lookup, records that resolve to the
                           wildcard defined IP address when saving records.
  -f                         Filter out of brute force domain lookup, records that resolve to the
                           wildcard defined IP address when saving records.
  -a                         Perform AXFR with standard enumeration.
  -s                         Perform a reverse lookup of IPv4 ranges in the SPF record with
                           standard enumeration.
  -b                         Perform Bing enumeration with standard enumeration.
  -y                         Perform Yandex enumeration with standard enumeration.
  -k                         Perform crt.sh enumeration with standard enumeration.
```



Figura 2.37

Se digitarmos `dnsrecon -d www.acme.com` ele vai fazer o reconhecimento do respectivo domínio.

```
root@kali:~# dnsrecon -d www.acme.com
[*] Performing General Enumeration of Domain: www.acme.com
[-] DNSSEC is not configured for www.acme.com
[-] Error while resolving SOA record.
[-] Could not Resolve NS Records for www.acme.com
[-] Could not Resolve MX Records for www.acme.com
[*]      A www.acme.com 157.131.143.13
[*] Enumerating SRV Records
[+] 0 Records Found
root@kali:~#
```

Figura 2.38

Podemos rodar um recon com foco em zonewalk que é o processo de enumeração de todo o conteúdo de zonas DNS assinadas por DNSSEC (uma extensão de segurança do sistema de nomes de domínio que adiciona uma camada de confiança ao DNS fornecendo autenticação.) Essa abordagem de cadeia de confiança, por meio de assinaturas criptográficas, também fornece uma camada adicional de integridade que impede a ocorrência de ataques como Spoofing de DNS.

```
root@kali:~# dnsrecon -d weberdns.de -z
[*] Performing General Enumeration of Domain: weberdns.de
[*] DNSSEC is configured for weberdns.de
[*] DNSKEYs:
[*]      NSEC KSK RSASHA256 03010001b0698ae5f8db77bc1c009402 f011333507facb6a30016ad239ad85f0 3b
15073c779b2a31f65c2b4bdc838405 228b4054887c01f0138201cfeed232ea b56e2aa0a7bc5e0b15a9f838d359edc
d d684b3221c1f3417833ce4d99130c87f b2c6f7d97d744e1fa2377836bcf26dbc ffabc68791553e57c8dc1b0c1f8
05026 60b04970c119a007e50f40f2d4d69660 f5b38a5b4ede8ddb5aca9948b4faa2b8 b439791a7c39679bf7602d4
a900e469f 20e2985cf9cb6fa07f5aefd94b0acc3 5e288981a5b7f222f00f9ad91efaa628 bea64aafea120c5a407
9298629f27d82 7b6331fe91b98e9fb5970a07db8d2ad5 6218825de2be34a1a06d4c099706c755 f7582d53
[*]      NSEC ZSK RSASHA256 03010001bd677a3655d63dd057549cf9 edbab1234eda639d24769749e7fe2979 aa
b838b31bc2be643e8b28e4cccd0638 f34db9b65826ec708841c997867c1ef1 c5582ad3b47a3cf1b6b1f4d62be666b
5 09240362da6c1f3a5a462a3460e2c4ad 4dbbf4afb87b93843836beb52c4faf72 fc9967f0fbe46450002c8bac764
fcf47 20a082fd
[*]      SOA ns0.weberdns.de 194.247.5.13
```

Figura 2.39

```
root@kali:~# dnsrecon -d www.facebook.com -z
[*] Performing General Enumeration of Domain: www.facebook.com
[-] DNSSEC is not configured for www.facebook.com
[*] SOA a.ns.c10r.facebook.com 129.134.30.11
[-] Could not Resolve NS Records for www.facebook.com
[-] Could not Resolve MX Records for www.facebook.com
[*] CNAME www.facebook.com star-mini.c10r.facebook.com
[*] A star-mini.c10r.facebook.com 157.240.226.35
[*] CNAME www.facebook.com star-mini.c10r.facebook.com
[*] AAAA star-mini.c10r.facebook.com 2a03:2880:f148:181:face:b00c:0:25de
[*] Enumerating SRV Records
[+] 0 Records Found
[*] Performing NSEC Zone Walk for www.facebook.com
[*] Getting SOA record for www.facebook.com
[*] Name Server 129.134.30.11 will be used
[-] This zone appears to be misconfigured, no SOA record found.
[*] CNAME www.facebook.com star-mini.c10r.facebook.com
[*] A star-mini.c10r.facebook.com 157.240.226.35
[*] CNAME www.facebook.com star-mini.c10r.facebook.com
[*] AAAA star-mini.c10r.facebook.com 2a03:2880:f148:181:face:b00c:0:25de
[+] 4 records found
```

Figura 2.40

A primeira imagem mostra um Domínio weberdns.de com o DNSSEC configurado e a última mostra um outro domínio o facebook.com sem a configuração do DNSSEC

Além disso, uma transferência de zona bem sucedida pode revelar recursos internos que podem estar publicamente disponíveis e, portanto, facilmente direcionados.

### **Exemplo de transferência de zona bem sucedida:**

```

root@kali:~# dnsrecon -d intelbras.com.br -t axfr
[*] Testing NS Servers for Zone Transfer
[*] Checking for Zone Transfer for intelbras.com.br name servers
[*] Resolving SOA Record
['SOA', 'ns.intelbras.com.br', '192.100.206.137']
[+] SOA ns.intelbras.com.br 192.100.206.137
[*] Resolving NS Records
[*] NS Servers found:
[*] NS ns.intelbras.com.br 192.100.206.137
[*] NS ns.intelbras.com.br 2801:80:be0:d::df23
[*] NS ns2.intelbras.com.br 189.125.77.87
[*] NS ns1.intelbras.com.br 192.100.206.138
[*] NS ns1.intelbras.com.br 2801:80:be0:d::6ed8
[*] Removing any duplicate NS server IP Addresses ...
[*]
[*] Trying NS server 192.100.206.137
[+] [['NS', 'ns.intelbras.com.br', '192.100.206.137'], ['NS', 'ns.intelbras.com.br', '2801:80:be0:d::df23'], ['NS', 'ns2.intelbras.com.br', '189.125.77.87'], ['NS', 'ns1.intelbras.com.br', '192.100.206.138'], ['NS', 'ns1.intelbras.com.br', '2801:80:be0:d::6ed8']] Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] Zone transfer error: REFUSED
Traceback (most recent call last):
  File "/usr/share/dnsrecon/lib/dnshelper.py", line 431, in zone_transfer
    zone = self.from_wire(dns.query.xfr(ns_srv, self._domain))
  File "/usr/share/dnsrecon/lib/dnshelper.py", line 359, in from_wire
    for r in xfr:
  File "/usr/lib/python3/dist-packages/dns/query.py", line 964, in xfr
    raise TransferError(rcode)
dns.query.TransferError: Zone transfer error: REFUSED

```

Figura 2.41

```

[*] Trying NS server 189.125.77.87
[+] [['NS', 'ns.intelbras.com.br', '192.100.206.137'], ['NS', 'ns.intelbras.com.br', '2801:80:be0:d::df23'], ['NS', 'ns2.intelbras.com.br', '189.125.77.87'], ['NS', 'ns1.intelbras.com.br', '192.100.206.138'], ['NS', 'ns1.intelbras.com.br', '2801:80:be0:d::6ed8']] Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*] NS ns.intelbras.com.br 192.100.206.137
[*] NS ns.intelbras.com.br 2801:80:be0:d::df23
[*] NS ns1.intelbras.com.br 192.100.206.138
[*] NS ns1.intelbras.com.br 2801:80:be0:d::6ed8
[*] NS ns2.intelbras.com.br 189.125.77.87
[*] NS ns-884.awsdns-46.net 205.251.195.116
[*] NS ns-884.awsdns-46.net 2600:9000:5303:7400::1
[*] NS ns-1.awsdns-00.com 205.251.192.1
[*] NS ns-1.awsdns-00.com 2600:9000:5300:100::1
[*] NS ns-1586.awsdns-06.co.uk 205.251.198.50
[*] NS ns-1586.awsdns-06.co.uk 2600:9000:5306:3200::1
[*] NS ns-1256.awsdns-29.org 205.251.196.232
[*] NS ns-1256.awsdns-29.org 2600:9000:5304:e800::1
[*] NS ns-625.awsdns-14.net 205.251.194.113
[*] NS ns-625.awsdns-14.net 2600:9000:5302:7100::1
[*] NS ns-1481.awsdns-57.org 205.251.197.201
[*] NS ns-1481.awsdns-57.org 2600:9000:5305:c900::1
[*] NS ns-462.awsdns-57.com 205.251.193.206
[*] NS ns-462.awsdns-57.com 2600:9000:5301:ce00::1
[*] NS ns-2015.awsdns-59.co.uk 205.251.199.223

```

Figura 2.42

Uma falha de implementação no seu servidor de DNS pode revelar informações sensíveis da sua empresa e permitindo que atacantes levanten essas informações para fins maliciosos.

Guia de Hardening para DNS

[https://tools.cisco.com/security/center/resources/dns\\_best\\_practices](https://tools.cisco.com/security/center/resources/dns_best_practices)

The Harvester

Recon-ng

Wigle

Hunter

Pipl

Haveibeenpwned

Insecam

Shodan

Censys

## **Escaneamento e Enumeração de Redes**

O Scanning é o processo de coleta de informações mais detalhado sobre o alvo, usando técnicas de reconhecimento altamente complexas e agressivas. A varredura de rede se refere a um conjunto de procedimentos usados para identificar hosts, portas e serviços em uma rede. O Scanning em rede também é usada para descobrir máquinas ativas em uma rede e identificar o sistema operacional em execução na máquina de destino. É uma das fases mais importantes da coleta de informações para um invasor, que permite que ele crie um perfil da organização alvo. No processo de varredura, o invasor tenta coletar informações, incluindo os endereços IP específicos que podem ser acessados pela rede, o Sistema Operacional do alvo e a arquitetura do sistema, e as portas junto com seus respectivos serviços em execução em cada computador.

Nmap

HPING3

Sublist3r

LDAP Enum

Traceroute and Pathping

SNMP Enumeration

SMBEnum

LDAP Enum

Enum4Linux

Python Scripts (DNS, PortScanner, Web Crawler)

Tricks Recon Bug Bounty

## **Escaneamento de Vulnerabilidades**

Openvas

Nessus

Nikto

Vega

Wpscan

Joomscan

# Técnicas de Engenharia Social

O que é Engenharia Social?

Tipos de Engenharia Social

Técnicas de Engenharia Social

Setoolkit

Spear-Phishing

Email Spoofing

Cloning Websites

Macro Files /Word/Excel

Macro Office Files - DDE

HTA Attacking

GoPhishing

Bad USB

## Exploração de Vulnerabilidades

Conceito de Exploit

Conceito de Payload

Conceito de Shellcode

Conceito de 0day

Exploração de vulnerabilidades em aplicações web

- SQL Injection
- Blind SQL Injection
- XSS Refletido
- XSS Armazenado
- XSS Dom
- Cross Site Request Forgery
- Unrestricted File Upload
- Local File Inclusion
- Remote File Inclusion
- XXE Out-of-Band
- Remote Code Execution
- Explorando Wordpress
- Explorando Tomcat

Exploração de vulnerabilidades em sistema



- Introdução ao Metasploit Framework
- Explorando vulnerabilidades no Windows 7
- Explorando vulnerabilidades no Windows Server 2012
- Criando um payload simples com MSFVenom
- Backdoor no Windows 7, Windows Server 2012, 2016 e Windows 10
- Meterpreter
- Criando um Script simples para Meterpreter
- Powershell Payloads Reverse Shell
- PyFuscation + BypassAV com Powershell
- TheFatRat e Unicorn Payloads
- UnmanagedPowershell
- Veil Evasion
- Reverse Shell no Linux com PHP
- Força Bruta em FTP
- Força Bruta em SSH
- Força Bruta em HTTP
- Explorando serviços vulneráveis no Linux (FTP, IRC, MySQL)

## **Pós Exploração e Escalação de Privilégios**

Conceito de Escalação de Privilégios

Conceitos de Movimento Lateral

Conceitos de Pivoting

Conceitos de Command and Control

Escalação de Privilégios em Windows

- Bypass UAC
- DLL Hijacking
- Powershell Empire
- Força Bruta NTLM
- WinPE
- Golden Ticket Kerberos

Escalação de Privilégios em Linux

- Explorando Kernel Linux
- Explorando serviços vulneráveis
- SUID Privilege Escalation
- LinEnum

Movimento Lateral

- Passthehash
- Psexec
- WMI
- SSH

#### Pivoting

- Metasploit Portfwd
- SSH Tunelling
- Roteamento padrão

#### Command and Control

- Merlin
- TrevorC2
- DNSCat
- Cobalt Strike - Overview
- Covenant - Overview

## Resolvendo CTFs

O que é CTF?

Plataformas de CTF

Máquinas Vulneráveis

Resolvendo máquinas vulnhub

- Mrrobot
- Mrr3b0t
- FowSniff
- LazySysAdmin
- Lampiao
- Photographer

## Conclusão

O início da sua jornada

Indo além nos estudos

Como se tornar um bom PenTester

Desenvolvendo um bom Relatório

Certificações na área de PenTest

Agradecimentos e projetos