



ATIVIDADE 01 – INFORMATION GATHERING

Autor: ETR00M

Github: <https://github.com/ETR00M/>

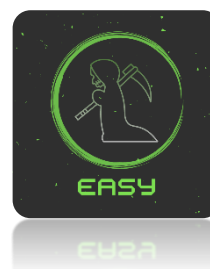
Linkedin: <https://www.linkedin.com/in/ls-anderson/>

Desafio: Pacific Security - Offensive Security 2023

Nível: Fácil;

Categoria: *Recon*;

Tag: reconhecimento/coleta de informações (comandos, ferramentas), pensamento linear.



INTRODUÇÃO

Este documento refere-se a coleta de informações solicitada como parte da Atividade 01 – *Information Gathering* do processo seletivo da Pacific Security - Offensive Security em 2023, conforme descritivo abaixo:

*“Você foi contratado para realizar um mapeamento na empresa OceanSec [...] os detalhes do escopo do projeto (são): a (organização) opera sob o domínio **oceansec.com**. Todos os subdomínios/informações públicas estão dentro do escopo desta atividade (e) sua tarefa é realizar um mapeamento completo [...]. No entanto, **scans de vulnerabilidade e de porta estão fora do escopo** [...]. Utilize todas as informações que encontrar sobre a empresa para compilar o seu relatório.”*

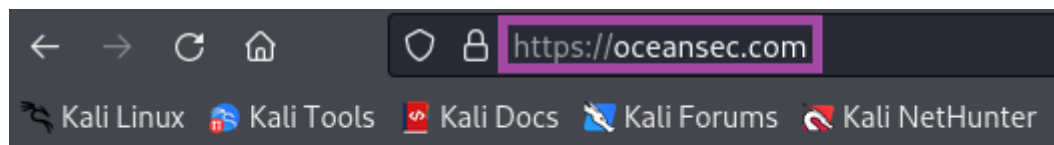
Sendo assim, temos como definição de escopo todos os domínios/subdomínios: **oceansec.com** e como definição de testes: *Information Gathering and Reconnaissance* sem contemplar quaisquer escaneamentos de portas e/ou vulnerabilidades.



DESENVOLVIMENTO

Ao realizar acesso ao site da empresa foi identificado o **erro 522**, indicando que o *Cloudflare* não obteve resposta ao tentar se comunicar com o servidor que hospeda a aplicação, o mesmo código de erro ocorre utilizando ambos os protocolos: **http** e **https**, podendo indicar que o site não está mais ativo.

Comando: **https://oceansec.com**



Connection timed out **Error code 522**

Visit cloudflare.com for more information.

2024-04-03 22:05:10 UTC

A partir de fontes OSINT foi identificado que o site realmente não está mais acessível, como estou realizando a atividade fora do tempo proposto não conseguirei acesso direto a página web para efetuar o mapeamento do site, sendo assim, focarei em informações históricas passíveis de serem encontrados em fontes abertas.

Comando: **https://www.siteconfiavel.com.br/**

oceansec.com
CNPJ: Informação indisponível

Resultado:

Resultados Google	Suspeito	Estranho. Esse site não aparece nas buscas do Google.
Tempo de registro	9 meses	Cuidado. Esse site é relativamente novo.
Categoria do domínio	Popular	Esse tipo de domínio é popular no Brasil
HTTPS	Ativo	Selo SSL válido. Isso é bom.
SSL	Ativo	Esse site possui segurança contra invasores.



O tempo de registro do site é de 9 meses, portanto é um site relativamente novo. Avaliando o perfil da organização no **Linkedin** foi identificado que a empresa foi fundada em 2019, embora ela tenha iniciado suas atividades nesse ano sua presença web iniciou apenas em 2023, o que foi possível comprovar com os serviços: *Internet Archive*, *Linkedin* e *X*.

Site


<https://oceansec.com>

Setor

Segurança de redes e computadores

Tamanho da empresa

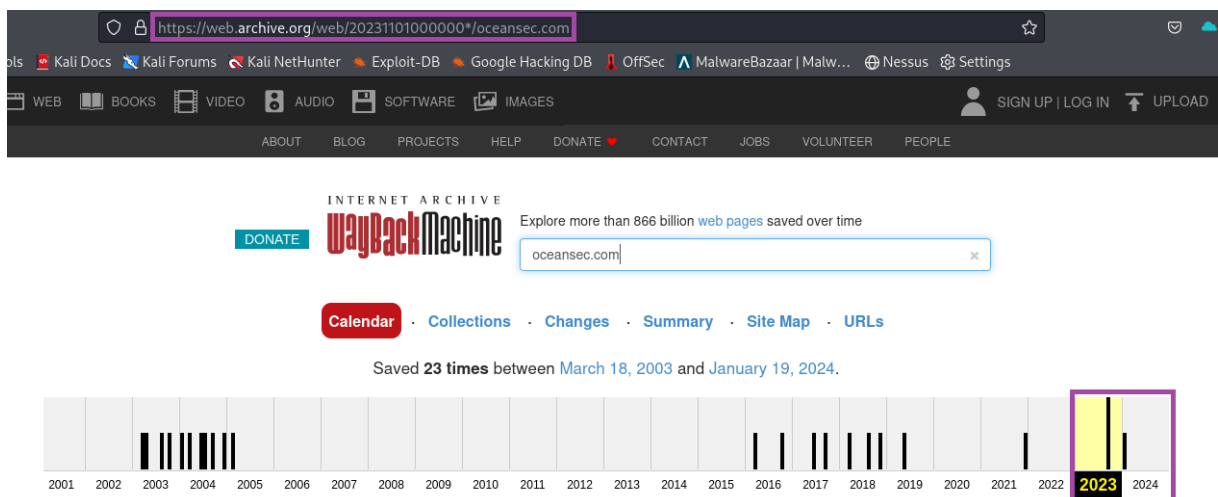
11-50 funcionários

6 usuários associados 

Fundada em

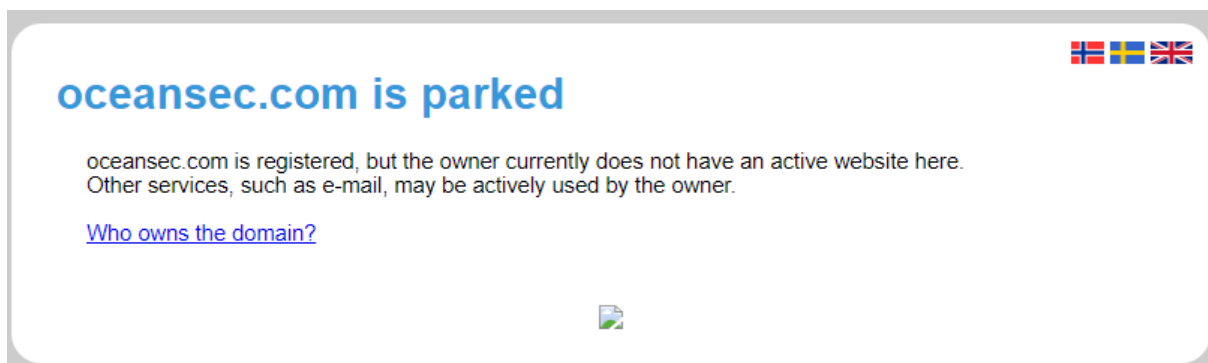
2019

Comando: https://web.archive.org/web/20231101000000*/oceansec.com

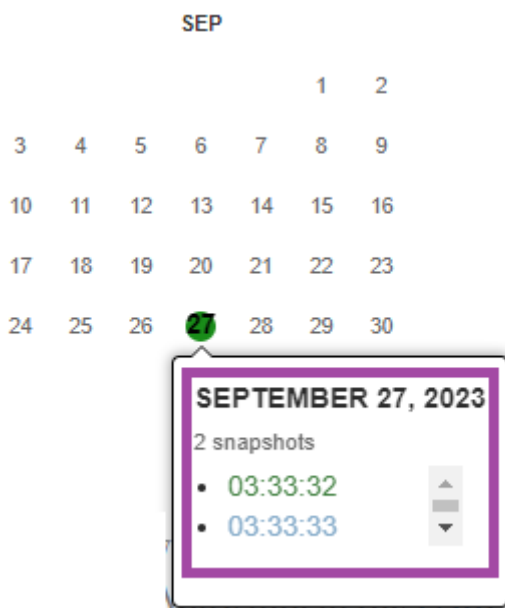




Período anterior a 2023: (<http://oceansec.com/>):



Em 27/09/2023 o site foi publicado em nome da empresa OceanSec, havendo o registro de redirecionamento da página **http** para **https** e primeira coleta da sua *homepage* pelo serviço *Archive.org*.



COLETA DE INFORMAÇÕES DE NEGÓCIO:

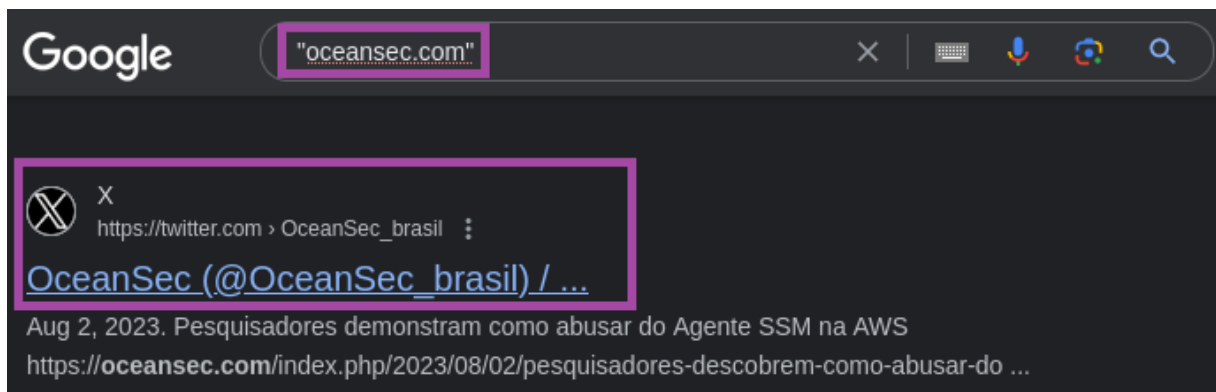
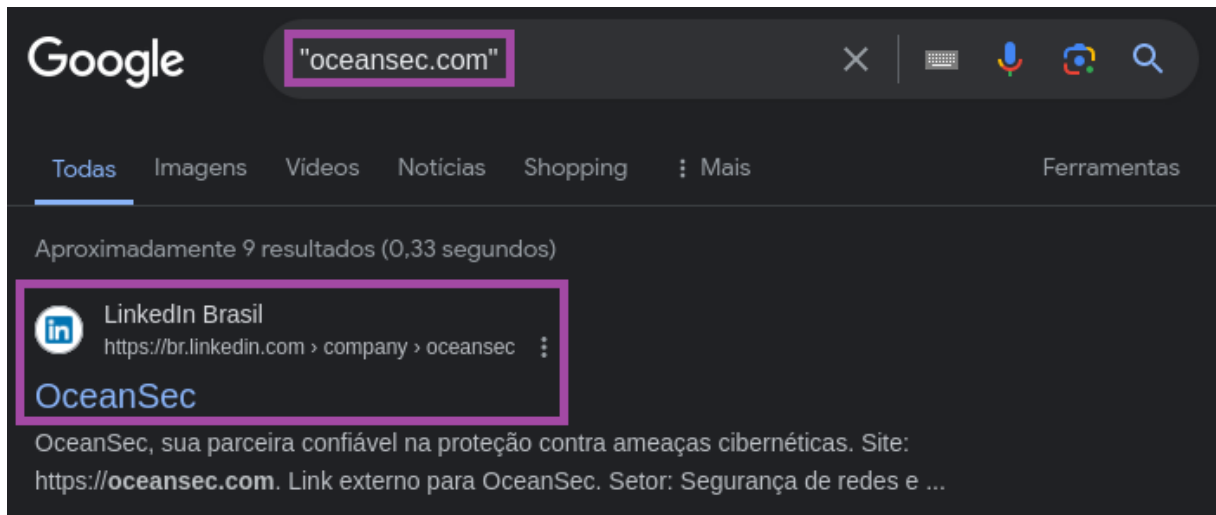
Ramo de atuação – a OceanSec atua na prestação de serviços de cibersegurança, entre eles:

- Análise de Conformidade em Cybersecurity;
- Serviços de Forense Digital e Resposta a Incidentes;
- Gerenciamento e Configuração de Appliances de Segurança.



Presença web – além da avaliação da presença web da organização em sites conhecidos foram utilizados *Google Hacking* e a ferramenta **Sherlock** com o intuito de localizar outros perfis públicos a partir dos nomes de usuários utilizados pela empresa:

Comando: “oceansec.com”





Comando: sherlock OceanSec

```
(kali㉿kali)-[~]
└─$ sherlock OceanSec
[*] Checking username OceanSec on:

[+] Archive.org: https://archive.org/details/@OceanSec
[+] Blogger: https://OceanSec.blogspot.com
[+] CGTrader: https://www.cgtrader.com/OceanSec
[+] CNET: https://www.cnet.com/profiles/OceanSec/
[+] Codecademy: https://www.codecademy.com/profiles/OceanSec
[+] Contently: https://OceanSec.contently.com/
[+] Euw: https://euw.op.gg/summoner/userName=OceanSec
[+] Fiverr: https://www.fiverr.com/OceanSec
[+] G2G: https://www.g2g.com/OceanSec
[+] GeeksforGeeks: https://auth.geeksforgeeks.org/user/OceanSec
[+] GitHub: https://www.github.com/OceanSec
[+] HEXRPG: https://www.hexrpg.com/userinfo/OceanSec
[+] Kongregate: https://www.kongregate.com/accounts/OceanSec
[+] Linktree: https://linktr.ee/OceanSec
[+] NationStates Nation: https://nationstates.net/nation=OceanSec
[+] NationStates Region: https://nationstates.net/region=OceanSec
[+] Oracle Community: https://community.oracle.com/people/OceanSec
[+] Pastebin: https://pastebin.com/u/OceanSec
[+] Polymart: https://polymart.org/user/OceanSec
[+] Roblox: https://www.roblox.com/user.aspx?username=OceanSec
[+] Telegram: https://t.me/OceanSec
[+] metacritic: https://www.metacritic.com/user/OceanSec

[*] Search completed with 22 results
```

Comando: sherlock OceanSec_brasil

```
(kali㉿kali)-[~]
└─$ sherlock OceanSec_brasil
[*] Checking username OceanSec_brasil on:

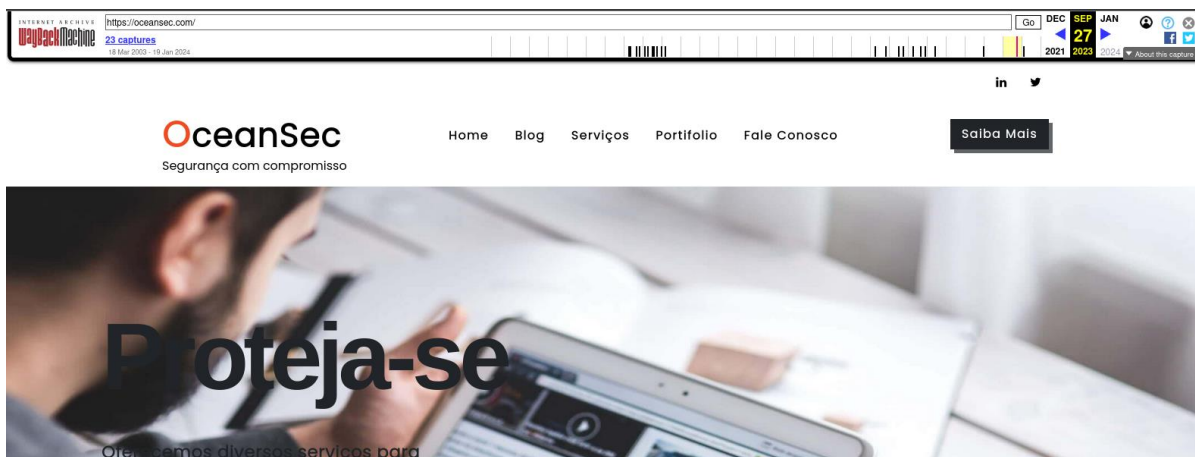
[+] Archive.org: https://archive.org/details/@OceanSec_brasil
[+] CGTrader: https://www.cgtrader.com/OceanSec_brasil
[+] CNET: https://www.cnet.com/profiles/OceanSec_brasil/
[+] Contently: https://OceanSec_brasil.contently.com/
[+] Euw: https://euw.op.gg/summoner/userName=OceanSec_brasil
[+] Fiverr: https://www.fiverr.com/OceanSec_brasil
[+] GeeksforGeeks: https://auth.geeksforgeeks.org/user/OceanSec_brasil
[+] HEXRPG: https://www.hexrpg.com/userinfo/OceanSec_brasil
[+] Kongregate: https://www.kongregate.com/accounts/OceanSec_brasil
[+] Linktree: https://linktr.ee/OceanSec_brasil
[+] NationStates Nation: https://nationstates.net/nation=OceanSec_brasil
[+] NationStates Region: https://nationstates.net/region=OceanSec_brasil
[+] Oracle Community: https://community.oracle.com/people/OceanSec_brasil
[+] Polymart: https://polymart.org/user/OceanSec_brasil
[+] Scribd: https://www.scribd.com/OceanSec_brasil
[+] metacritic: https://www.metacritic.com/user/OceanSec_brasil

[*] Search completed with 16 results
```

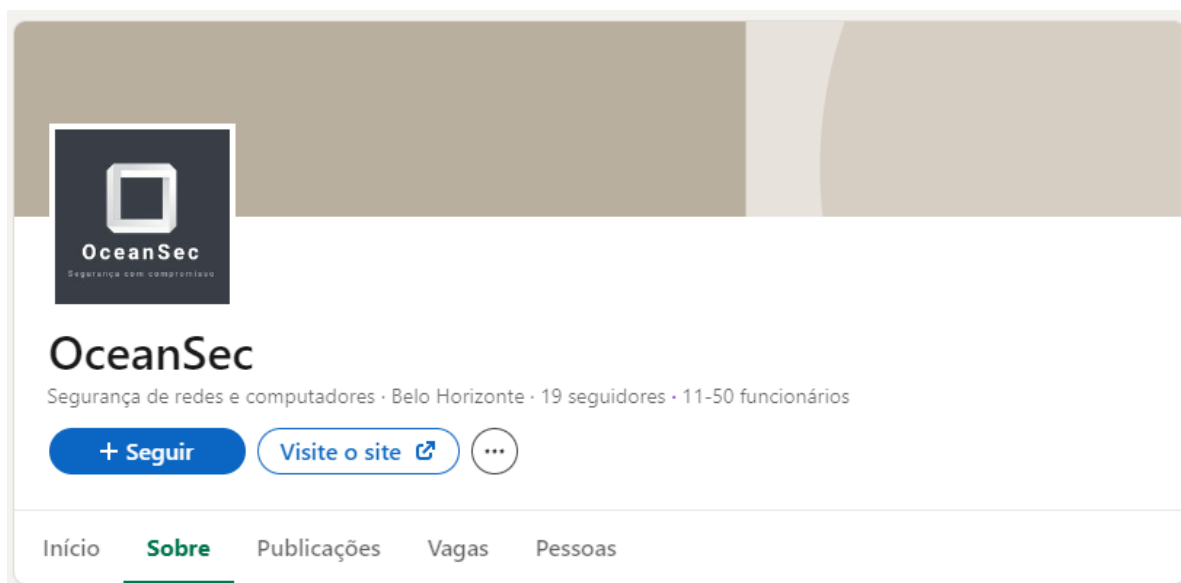


Com essa análise foram localizados os seguintes perfis acessíveis pertencentes a empresa:

- <https://oceansec.com/>




- <https://www.linkedin.com/company/oceansec/>





- https://twitter.com/OceanSec_brasil




...

Follow

OceanSec
@OceanSec_brasil


Twitter Oficial da OceanSec - Segurança com compromisso


oceansec.com  Joined July 2023

33 Following 5 Followers

- https://www.glassdoor.com.br/Vis%C3%A3o-geral/Trabalhar-na-OceanSec-El_IE8977345.13,21.htm

[Entrar](#)**'GLASSDOOR'**

**OceanSec**

 Visão geral
▼

-- Avaliações

-- Vagas

3 Salários

-- Entrevistas

-- Benefícios

-- Fotos

Visão geral da empresa OceanSec

Trabalha aqui? Solicite seu perfil gratuito de empresa.

oceansec.com/
1 a 50 funcionários
Fundada em 2019
[Internet e serviços Web](#)
Concorrentes: Sem informação

Belo Horizonte, Brasil
Tipo: Autônomo
Receita: De US\$ 1 a US\$ 5 milhões



- <https://github.com/OceanSec-Brasil>

The screenshot shows the GitHub profile for 'OceanSec-Brasil'. The header includes the GitHub logo, the repository name 'OceanSec-Brasil', and a search icon. Below the header, there are tabs for 'Overview', 'Repositories' (4), 'Projects', 'Packages', and 'People' (2). The main content area features a profile picture of a square with a white 'O' on a dark background, the name 'OceanSec', and the tagline 'segurança com compromisso'. It also shows '1 follower', a website link 'https://oceansec.com/', and a LinkedIn link 'company/oceansec'.

- <https://pastebin.com/u/oceansec>

The screenshot shows the Pastebin profile for 'Oceansec's Pastebin'. The header includes the Pastebin logo, navigation links for 'API', 'TOOLS', 'FAQ', and a '+ paste' button, along with a search bar. The profile section shows a user icon, the name 'Oceansec's Pastebin', and statistics: 124 views, 265 downloads, 0 stars, and '211 DAYS AGO'. Below this is a table of pastes.

NAME / TITLE	ADDED	EXPIRES	HITS	COMMENTS	SYNTAX
interno	Sep 19th, 2023	Never	272	0	None

Funcionários/Usuários conhecidos – dentre os usuários no **LinkedIn** foi identificado como dono da empresa a Camila Cardoso.

- linkedin.com/in/camilaa-cardosoo

The screenshot shows the LinkedIn profile of Camila Cardoso. The header features a circular profile picture (redacted with a black box) and a background image of a city at night with digital overlays. The name 'Camila Cardoso' is followed by '3°' and 'CEO & Founder na OceanSec'. The location is 'Belo Horizonte, Minas Gerais, Brasil' and there is a link for 'Informações de contato'. It also shows '5 conexões'. On the right, there are two logos: 'OceanSec' and 'Fundação Getulio Vargas'.



- linkedin.com/in/lucas-silva-761346257



Lucas Silva · 2º

Desenvolvedor Pleno na OceanSec

São Paulo, São Paulo, Brasil · [Informações de contato](#)

341 conexões



OceanSec



Estácio

- linkedin.com/in/guilherme-luiz-neves-497b1323b



Guilherme Luiz Neves · 2º

Information Security Specialist at OceanSec

São Paulo, Brasil · [Informações de contato](#)

- linkedin.com/in/julio-a-a8b728288



Julio A. (He/Him) · 3º

Salesman at OceanSec

Brasil · [Informações de contato](#)

2 conexões



OceanSec

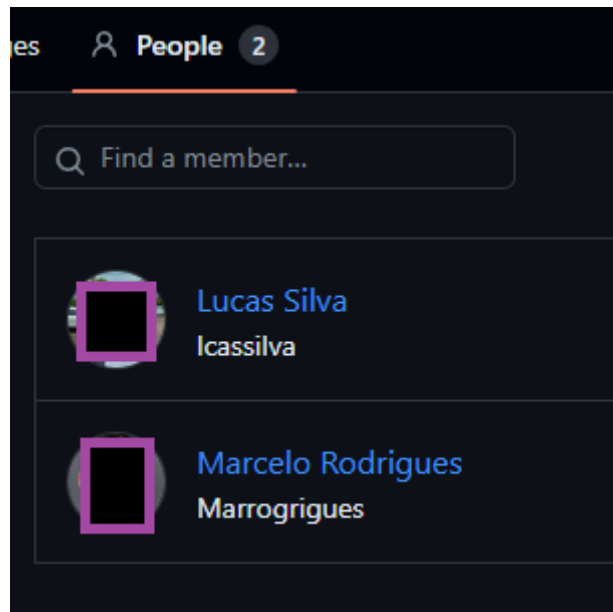
**Usuário do LinkedIn**

CTO na OceanSec
Belo Horizonte, MG

**Usuário do LinkedIn**

Engenheiro de software na OceanSec
São Paulo, Brazil

- <https://github.com/orgs/OceanSec-Brasil/people>

**Tecnologias encontradas:**

- DNS: Cloudflare;
- CMS: WordPress;

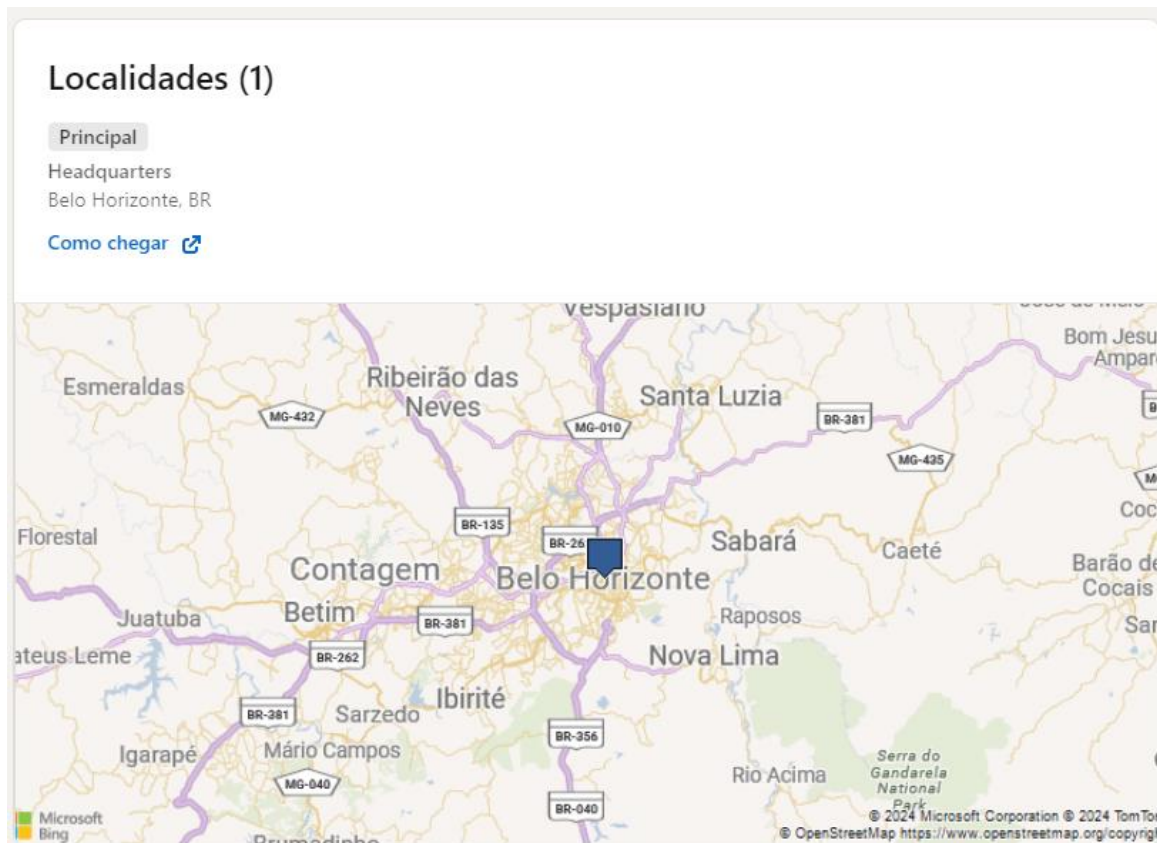
```
<link rel="https://api.w.org/" href="https://oceansc  
json/wp/v2/pages/10"/><link rel="EditURI" type="appl  
<meta name="generator" content="WordPress 6.3.1"/>  
<link rel="shortlink" href="https://web.archive.org/  
<link rel="alternate" type="application/json+oembed"
```

- Programming languages: PHP, Python, Ruby;
- Suite: Microsoft 365.



COLETA DE INFORMAÇÕES DE INFRAESTRUTURA

Localização da empresa – segundo informações no **LinkedIn** o prédio da organização está localizado em Belo Horizonte, Brasil.



Endereços IP's – o domínio **oceansec.com** é traduzido para os endereços IPv4: 104.21.82.112 e 172.67.200.174, além disso, o registro DNS para o servidor de e-mail é o **oceansec-com.mail.protection.outlook.com** nos indicando que a empresa utiliza serviços de Exchange do Office 365 da Microsoft.

Comando: **host oceansec.com**

```
(kali@kali)-[~]  
$ host oceansec.com  
oceansec.com has address 104.21.82.112  
oceansec.com has address 172.67.200.174  
oceansec.com has IPv6 address 2606:4700:3030::6815:5270  
oceansec.com has IPv6 address 2606:4700:3035::ac43:c8ae  
oceansec.com mail is handled by 0 oceansec-com.mail.protection.outlook.com.
```



Geolocalização dos IP's – ambos os endereços IP's são providos pela *CloudFlare Inc.* e estão localizados na região da américa do norte, mais especificamente nos Estados Unidos.


Comando: <https://www.abuseipdb.com/check/104.21.82.112>

104.21.82.112 was found in our database!

This IP was reported **4** times. Confidence of Abuse is **0%**:



0%

ISP	CloudFlare Inc.
Usage Type	Content Delivery Network
Domain Name	cloudflare.com
Country	 United States of America
City	San Francisco, California


Comando: <https://www.abuseipdb.com/check/172.67.200.174>

172.67.200.174 was found in our database!

This IP was reported **2** times. Confidence of Abuse is **0%**:



0%

ISP	CloudFlare Inc.
Usage Type	Content Delivery Network
Domain Name	cloudflare.com
Country	 United States of America
City	San Francisco, California



DNS da organização – os *Name Systems* coletados estão apresentados abaixo:

Comando: `host -t ns oceansec.com`

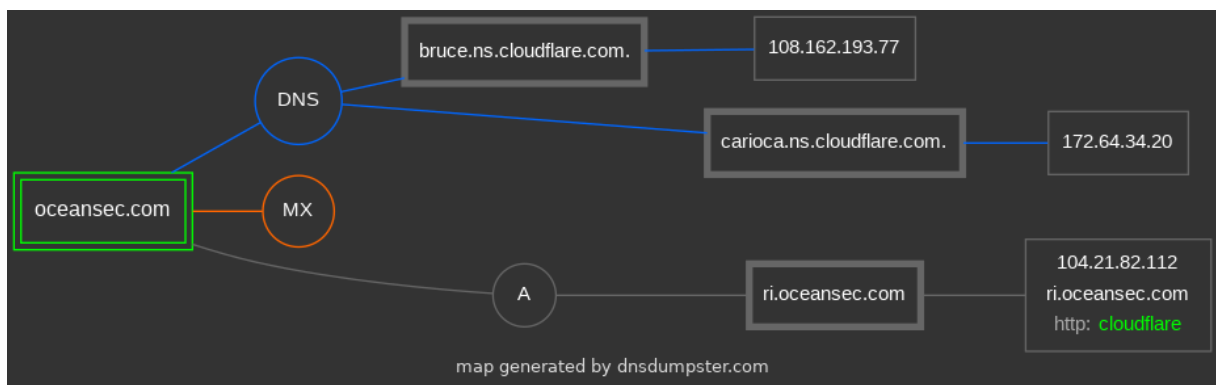
```
(kali㉿kali)-[~]  
$ host -t ns oceansec.com  
oceansec.com name server bruce.ns.cloudflare.com.  
oceansec.com name server carioca.ns.cloudflare.com.
```

Comando: `host -t SOA oceansec.com`

```
(kali㉿kali)-[~]  
$ host -t SOA oceansec.com  
oceansec.com has SOA record bruce.ns.cloudflare.com. dns.cloudflare.com. 2336288  
785 10000 2400 604800 1800
```

Resumo das informações de domínio localizadas até o momento:

Comando: <https://dnsdumpster.com/static/map/oceansec.com.png>



Ao verificar as informações no *TXT Record* foi identificado um desafio para ser resolvido, este desafio apresenta uma sequência de textos codificados:

```
(kali㉿kali)-[~]  
$ host -t txt oceansec.com  
oceansec.com descriptive text "Desafio:VDJ0bFLXNVraV010VTJWdWFHRLRaV2QxY21FPQ=="  
oceansec.com descriptive text "NETORGFI14081318.onmicrosoft.com"  
oceansec.com descriptive text "google-site-verification=hr2lITTsiuR2UfQQFr05bXSz  
6C9f4JTa4Dqp1LRbyIQ"  
oceansec.com descriptive text "v=spf1 include:secureserver.net -all"
```



Pelo padrão do código apresentado na *tag* “Desafio” é possível identificar que seu formato de codificação é **base64**, sendo assim, efetuei a decodificação a partir da CLI do Linux, após decodificação inicial uma nova *string* codificada também em **base64** foi retornada, sendo necessário um novo *decode*:

Comandos:

- `echo "VDJObFlXNVraV010VTJWdWFHRlRaV2QxY21FPQ==" | base64 -d`
- `echo "T2NlYW5TZWMtU2VuaGFTZWd1cmE=" | base64 -d`

```
(kali㉿kali)-[~]  
$ echo "VDJObFlXNVraV010VTJWdWFHRlRaV2QxY21FPQ==" | base64 -d  
T2NlYW5TZWMtU2VuaGFTZWd1cmE=  
  
(kali㉿kali)-[~]  
$ echo "T2NlYW5TZWMtU2VuaGFTZWd1cmE=" | base64 -d  
OceanSec-SenhaSegura
```

Domínios e Subdomínios – a partir das informações coletadas durante o reconhecimento de negócio foi identificado um perfil no **Pastebin** que continha informações relevantes a respeito de sua infraestrutura interna a partir da exposição do arquivo “*interno.txt*” publicado em 19/09/2023:

Comando: <https://pastebin.com/2hBwMazT>

The screenshot shows a Pastebin interface for a post titled "interno" by user "OCEANSEC". The post was created on September 19th, 2023, at 282 views and 0 stars. It is marked as "NEVER" and has an "ADD COMMENT" button. A banner at the top asks if the user is a member of Pastebin yet, with a "Sign Up" link. Below the banner, the post content is displayed as a text file named "texto.txt" (1.97 KB, None). The content of the file is as follows:

```
1. --- OCEANSEC INTERNAL WEB APPLICATIONS LIST ---  
2.  
3. Lista de ativos internos:
```




Segue informações detalhadas na tabela abaixo:

OCEANSEC INTERNAL WEB APPLICATIONS LIST	
Lista de ativos internos (https://pastebin.com/1T0juuGY)	
ACCESSIBLE VIA VPN ONLY	
VPN ACCESS DETAILS	
VPN Endpoint	vpn.oceansec.com
Protocol	OpenVPN
Contact for VPN issues	IT Support Team (itsupport@oceansec.com)
OceanHR	
URL	hr.oceansec.local
Description	Sistema interno de Recursos Humanos para gerenciamento de funcionários, folha de pagamento e benefícios
Maintenance	HR Team & IT Dept.
Contact	Sarah Lee (slee@oceansec.com)
OceanWiki	
URL	wiki.oceansec.local
Description	Wiki interno para documentação de processos, políticas e manuais
Maintenance	IT Dept.
Contact	Mike Taylor (mtaylor@oceansec.com)
OceanCloud	
URL	cloud.oceansec.local
Description	Solução de armazenamento e compartilhamento de arquivos para equipes
Maintenance	IT Dept.
Contact	Emily Clark (eclark@oceansec.com)
OceanTickets	
URL	tickets.oceansec.local

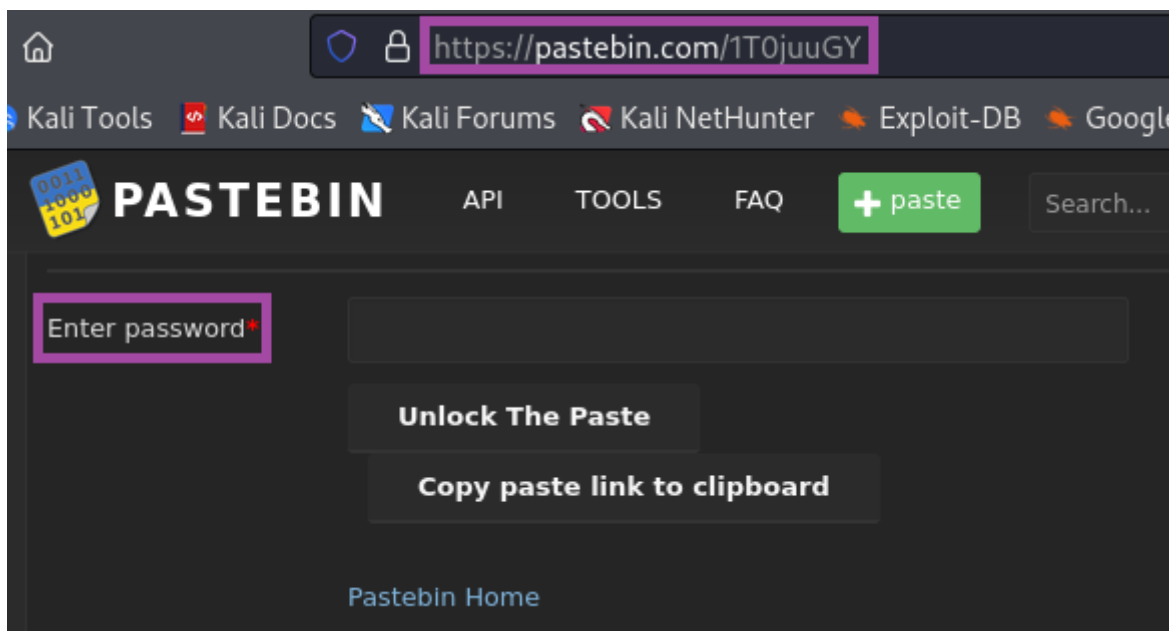


Description	Sistema de suporte técnico e gestão de tickets
Maintenance	IT Support Team
Contact	Bob Jones (bjones@oceansec.com)
OceanAnalytics	
URL	analytics.oceansec.local
Description	Dashboard de análise e visualização de dados de vendas e performance
Maintenance	Finance & Sales Dept.
Contact	Alice Smith (asmith@oceansec.com)
OceanDevOps	
URL	devops.oceansec.local
Description	Plataforma para desenvolvedores gerenciarem e monitorarem o ciclo de vida de aplicações
Maintenance	Development Team
Contact	John Doe (jdoe@oceansec.com)
OceanTraining	
URL	training.oceansec.local
Description	Plataforma E-Learning para treinamentos internos e onboarding de novos funcionários
Maintenance	HR & Training Dept.
Contact	Maria Rodriguez (mrodriguez@oceansec.com)
Note: This information is fictitious and is meant solely for the OceanSec educational challenge	

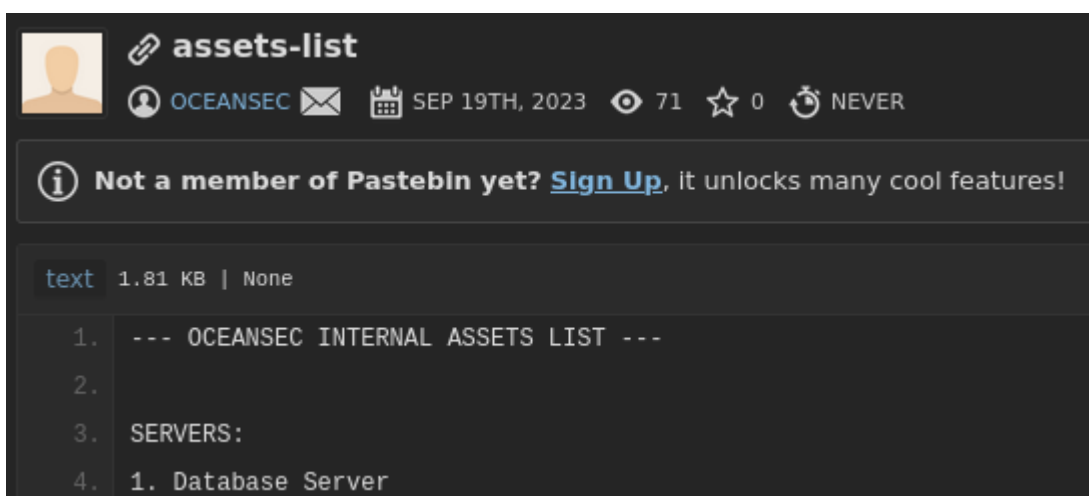


Dentre as informações expostas no **Pastebin** há um link para outro arquivo pertencente a organização publicada na plataforma:

Comando: <https://pastebin.com/1T0juuGY>



O acesso ao conteúdo deste arquivo só é permitido mediante a utilização da senha correta, anteriormente foi localizado a credencial a partir da decodificação da *string* em **base64** do desafio no registro TXT no DNS: a senha “**OceanSec-SenhaSegura**” concede acesso ao arquivo “**assets-list.exe**”:





Segue informações detalhadas abaixo:

OCEANSEC INTERNAL ASSETS LIST	
SERVERS	
Database Server	
IP	192.168.1.10
OS	Linux Ubuntu 20.04
Description	Main database server hosting customer information
Administrator	John Doe (jdoe@oceansec.com)
Web Application Server	
IP	192.168.1.15
OS	Linux CentOS 7
Description	Hosts the main OceanSec web application
Administrator	Alice Smith (asmith@oceansec.com)
Backup Server	
IP	192.168.1.20
OS	Linux Debian 10
Description	Weekly backups of all servers
Administrator	Bob Jones (bjones@oceansec.com)
NETWORK DEVICES	
Main Router	
IP	192.168.1.1
Brand	Cisco
Model	RV340
Administrator	Network Team (network@oceansec.com)
Secondary Switch	
IP	192.168.1.2
Brand	HP
Model	ProCurve 2824
Administrator	Network Team (network@oceansec.com)
WORKSTATIONS	



Finance Team	
IP Range	192.168.1.50-192.168.1.59
OS	Windows 10
Description	Used by the finance department to handle invoices and billing
Point of Contact	Emily Clark (eclark@oceansec.com)
Development Team	
IP Range	192.168.1.100-192.168.1.120
OS	MacOS Big Sur
Description	Used by developers to write and test software
Point of Contact	Mike Taylor (mtaylor@oceansec.com)
HR Team	
IP Range	192.168.1.30-192.168.1.35
OS	Windows 10
Description	Used by HR for recruitment and employee management
Point of Contact	Sarah Lee (slee@oceansec.com)
PASSWORDS	
(Yes, we know this shouldn't be here, but it's a challenge, remember?)	
Database Server	Pa\$\$w0rd123
Web App Server	W3bS3rv3r2023!
Backup Server	B@ck1tUpNow
Note: This information is fictitious and is meant solely for the OceanSec educational challenge.	



CONCLUSÃO

Conforme identificado durante a atividade proposta o reconhecimento e a coleta de informações são etapas cruciais de um *Pentest*, pois a partir delas interagimos pela primeira vez com o alvo, aprofundando nosso conhecimento sobre as suas atividades, relações, comportamentos e infraestrutura. Com isso reunimos informações relevantes e identificamos possíveis pontos de entrada a partir do mapeamento da superfície de ataque, os quais podem ser utilizados posteriormente no processo de escaneamento de portas, enumeração de serviços e avaliação de vulnerabilidades.

No escopo abordado foram identificadas pessoas com papéis importantes na organização que podem se tornar alvos de engenharia social durante uma abordagem ativa de reconhecimento. Além disso, também foram identificadas algumas tecnologias utilizadas pelo alvo passíveis de serem localizadas de forma passiva, porém o ponto mais relevante da análise realizada foi a exposição de dados no **Pastebin** que possibilitou um levantamento completo da infraestrutura de ativos da organização como: departamentos, domínios, endereços de e-mail de colaboradores e caixas de distribuição, nomenclaturas internas, descrição de serviços, contatos de referenciais técnicos, *range* de endereços IP's, Sistemas Operacionais, servidores críticos, workstations, equipamentos de rede e impressoras.

Além das informações descritas acima também foi localizado um item com alto potencial de risco a OceanSec, sendo este a exposição de credenciais corporativas que fornecem acesso a serviços críticos como: servidores de Banco de Dados, Aplicação Web e Backup de Dados. Com os resultados obtidos é possível definir uma estratégia de ataque partindo para análise de vulnerabilidades nos serviços enumerados, além do mapeamento completo dos registros na base de dados e possível comprometimento dos arquivos de backup da organização dependendo do objetivo dos testes definidos no escopo inicial.