



OSINT - Buscando informações públicas

- Informações sobre infraestruturas

Whoami - Quem sou eu ?

- Estudante da Fatec Bauru – Redes
- DevOps – EZ devs
- Estudante de segurança da informação

Historia - Onde se iniciou

- Tudo começou no Foreign Broadcast Information Service (FBIS)
- Jornais
- Revistas
- Televisão
- Pioneiro no uso de Open Source Intelligence (OSINT)
- Deram início ao projeto na década de 1930 na Universidade de Princeton

Historia - Segunda guerra e o FBI

- Sua função era analisar os noticiários por rádio e monitorar publicações oficiais da União das repúblicas Socialistas Soviéticas
- Já em 8 de novembro de 2005 foi anunciado por John Negroponte o Open Source Center (OSC) que é um braço da CIA (depois do 11 de setembro de 2001)
- Coletar , reunir e trabalhar as informações
- Foi ai que deu inicio ao termo OSINT

Leis - O que eu posso e não posso

- Invasão de dispositivos
- Violar mecanismos de segurança para obter vantagem indevida
- Obter informações
- Adulterar
- Destruir
- Graças às técnicas de buscas usando OSINT podemos começar a procura de informações válidas e falhas em possíveis clientes.

Whois - Quem é?

Buscando por informações sobre domínios

- Nome do domínio , quem registrou o domínio
- Quando foi criado e até quando é valido
- Servidores DNS e País
- email de contato ,Nome do responsável ,CPF/CNPJ
- Protocolo TCP que funciona por padrão na porta 43

Whois - Quem é?

Buscando por informações de IPS

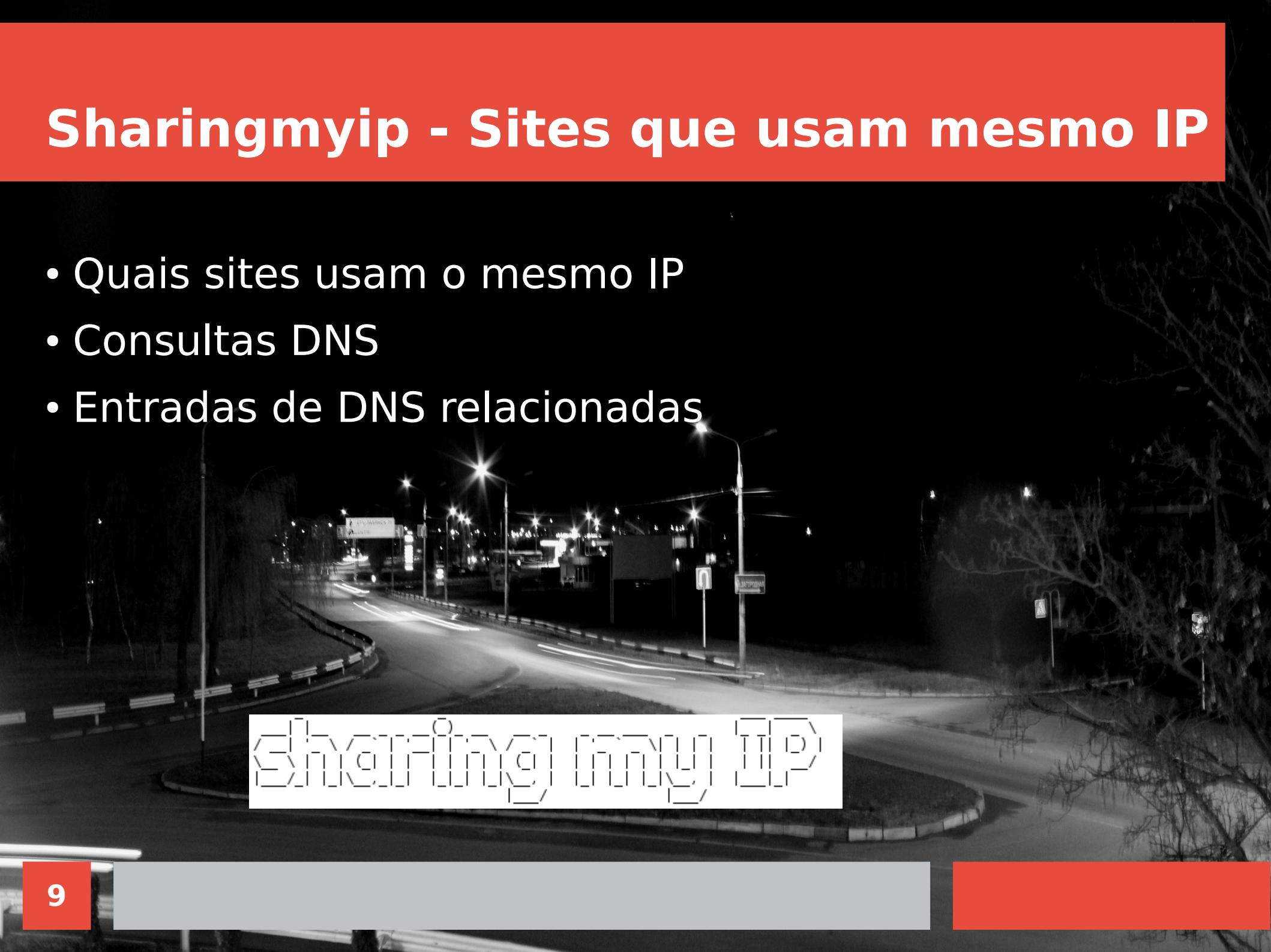
- Range de rede
- CIDR
- Organização responsável
- Endereço
- Cidade
- País

Robots.txt - O que não deve ser achado

- Não querem que sejam indexados pelos Web Crawlers
- Arquivos
- Diretórios
- Clean URLs
- No Clean URLs
- Sempre tenha um arquivo robots.txt na raiz do seu servidor web

Sharingmyip - Sites que usam mesmo IP

- Quais sites usam o mesmo IP
- Consultas DNS
- Entradas de DNS relacionadas



ENCONTRANDO UM IP

DNSDumpster - Informações sobre DNS

- DNS Servers
- Servidores de email
- Registros de DNS
- Possível localização
- Proprietários de blocos de IP

XXXXXX
HACKER TARGET
XXXXXX

Netcraft -

A Netcraft é uma empresa com sede em Bath na Inglaterra , ela é uma empresa que presta serviços

- Anti fraud
- Anti Phishing
- Testes em aplicativos
- Revisão de código
- Pentests

Netcraft -

- Encontrar subdomínios
- Sistema operacional
- Informações sobre o bloco de rede
- Título do site , Rank do site , Descrição , Palavras chaves , Linguagem primária , análise de Risco e etc..
- Site , Domínio, IP , IPv6, Domínio Registrador , Organização responsável , Hospedado em qual país , Empresa que hospeda , DNS reverso ,Email do DNS admin e NameServer



WhatCMS - Reconhecendo CMS

- Conseguem reconhecer mais de 422 CMS's
- Lançado em Dezembro de 2011
- Wordpress, Joomla, Moodle, Drupal, PhpBB
- Meta, Headers, Javascript
- https://whatcms.org/Tech_Reports



WhatCMS

WhatCMS - Reconhecendo CMS + API

- Realizar 1000 (mil) requisições por mês
- 1 requisição a cada 10 segundos
- <https://whatcms.org/Documentation>
- <https://github.com/HA71/pywhatcms>



WhatCMS

Google Hacking -

- Fundada por Larry Page e Serget Brin em 2005.
- Operadores
- Docks
- Exploit DB
- Versões específicas vulneráveis
- Localizar todas as páginas
- Páginas de administração
- Backups de arquivos
- E tudo que pode estar sendo indexado pelo Google.

Bing -

- É um motor de busca desenvolvido pela Microsoft
- Infelizmente pouco usado
- **Operadores**
- Contains
- Filetype
- Url
- Site



Yandex -

- Motor de busca russo
- Lançado em 1997
- Em janeiro de 2015, o Yandex Search gerou 51,2% de todo o tráfego de pesquisa na Rússia
- Podemos usar **Operadores**
- site

Shodan -

- Lançado em 2009 por John Matherly
- Encontrar por dispositivos conectados na internet
- Webcam ,Banco de dados,Servidores,Roteadores etc
- Banners de serviço
- Metadados
- Mensagens de boas vindas
- Versões de serviço
- Common Vulnerabilities and Exposures (CVE)

Shodan -

- Cidade
- País
- Organização
- Hostnames
- ASN
- Serviços
- Portas
- Localização do servidor
- CVE

Shodan - Operadores

- city
- OS
- port
- IP
- NET
- hostname
- Server
- Palavras chaves
- Dorks complexas

Shodan - Via linha de comando CLI

- Usamos Python s2
- <https://account.shodan.io>
- Documentação <https://shodan.readthedocs.io>
- Apenas a versão via linha de comando apresenta CVE



Censys -

- Censys criado em 2015 na universidade de Michigan
- Busca de dispositivos , redes e infraestruturas
- 45 das Fortune 500 usa dados do Censys
- Latitude/Longitude ,País , Rota , Portas abertas e protocolos
- Podemos ver o tipo de servidor usado
- Status do teste
- Titulo do IP usado
- Nome da rede de sites e IPS.



O resultado nos formatos

- Table , JSON , Raw WHOIS

Informações básicas

- Informações básicas do domínio
- Contato para relatar algum abuso
- Informações de Contato , sobre a rede , informações técnicas e administrativas



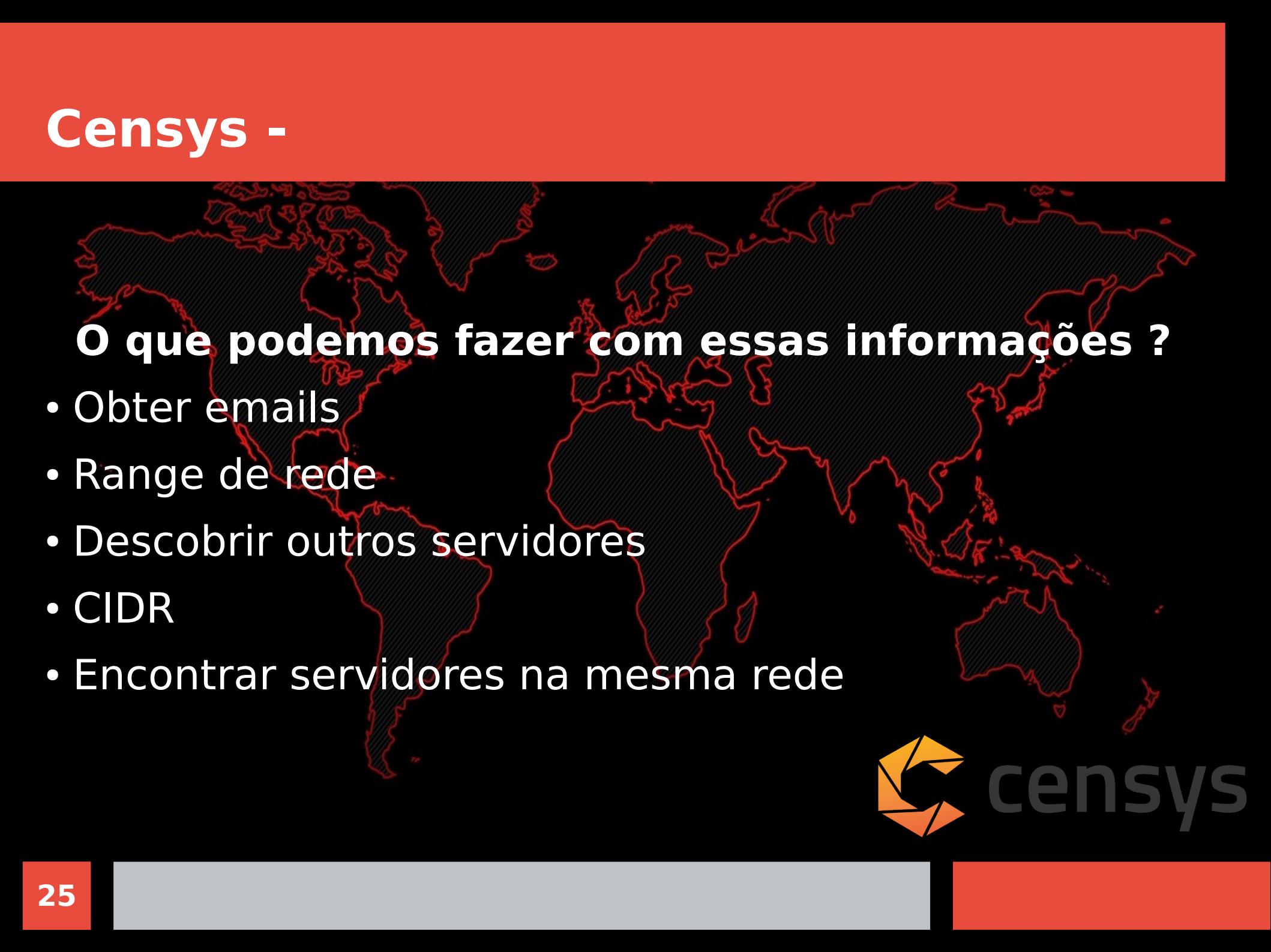
Censys -

Temos informações como por exemplo

- Alexa rank , Protocolos disponível
- Informações sobre as portas que estão abertas
- Qual o servidor usado , Titulo do site
- Informações sobre certificados do HTTPS ,
- Banner do serviço e configurações de DNS



Censys -



O que podemos fazer com essas informações ?

- Obter emails
- Range de rede
- Descobrir outros servidores
- CIDR
- Encontrar servidores na mesma rede





OSINT - Buscando informações públicas

Informações sobre pessoas

- PwnedOrNot , Sherlock , TheHarvester , Photon , Twitter-intelligence e Hunter.io

PwnedOrNot

- O pwnedOrNot usa informações OSINT
- Nos ajuda a encontrar senha
- Encontrar endereços de email comprometidos

Sherlock

- O Sherlock é um projeto que nos auxilia na busca por nomes de usuários nas redes sociais
- Desenvolvido em Python
- Disponível no github
- <https://github.com/sherlock-project/sherlock>

TheHarvester

- O theHarvester é uma ferramenta que nos auxilia na coleta de informações publicas
- Informações de um host
- Obter realizações de emails
- Subdomínios
- nome de funcionários
- Banners
- Chaves GPG
- <https://github.com/laramies/theHarvester>

Photon

- Photon é um projeto que nos auxiliar na busca de informações de um determinado site
- URLs , Parâmetros de URL
- Intel>Email,contas de redes sociais,amazon buckets)
- Arquivos (PDF,PNG,XML)
- Chaves secretas(API keys e hashes)
- Subdomínios
- Relações de DNS
- <https://github.com/s0md3v/Photon/>

Infoga

Com o Infoga podemos coletar informações

- Contas de email , IP , Nome de host e País

Ele usa diversas fontes publicas

- Mecanismos de busca
- Servidores de chave PGP
- Shodan

Twitter-intelligence

- O projeto twitter-intelligence nos ajuda no rastreamento e analise do Twitter
- Desenvolvido em Python e disponivel no github
- <https://github.com/batuhaniskr/twitter-intelligence>

Hunter.io

- Hunter.io é um projeto que nos auxiliar na busca de emails de corporações
- <https://hunter.io/>
- Reconhecimento de possíveis