



Curso Técnico Subsequente de Informática – Módulo 3

Disciplinas: Segurança e Auditoria de Sistemas

Professor: Rodrigo da Costa Barros Macedo

EstudanteS: Diego Pereira, João Vitor Lopes Santos, Marco de Souza

Em informações de negócio devem ser levantadas as seguintes informações:

- Lista de E-mails de funcionários.

chris@reddit.com

steve@reddit.com

jeremy@reddit.com

jason@reddit.com

admin@reddit.com

rram@reddit.com

jeff@reddit.com

david@reddit.com

askanadmin@reddit.com

mike@reddit.com

- Verificar quais e-mails listados sofreram vazamento de dados.

1ª email: chris@reddit.com

pwned?

Oh não - pwned!

Pwned em 18 violações de dados e não encontrou pastas (inscreva-se para pesquisar violações confidenciais)



3 passos para melhorar a segurança

[Comece a usar 1Password.com](#)



2ª: steve@reddit.com

pwned?

Oh não - pwned!

Pwned em 10 violações de dados e não encontrou pastas (inscreva-se para pesquisar violações confidenciais)



3 passos para melhorar a segurança

[Comece a usar 1Password.com](#)



3ª: jeremy@reddit.com

pwned?

Oh não - pwned!

Pwned em 2 violações de dados e não encontrou pastas (inscreva-se para pesquisar violações confidenciais)



3 passos para melhorar a segurança

[Comece a usar 1Password.com](#)




4ª: jason@reddit.com


pwned?

Oh não - pwned!

Pwned em 5 [violações de dados](#) e não encontrou pastas ([inscreva-se](#) para pesquisar violações confidenciais)

**3 passos para melhorar a segurança**

[Comece a usar 1Password.com](#)



5ª: admin@reddit.com

pwned?

Oh não - pwned!

Pwned em 1 [violação de dados](#) e não encontrou pastas ([inscreva-se](#) para pesquisar violações confidenciais)

**3 passos para melhorar a segurança**

[Comece a usar 1Password.com](#)



6ª: rram@reddit.com

pwned?

Oh não - pwned!

Pwned em 3 violações de dados e encontrou 1 pasta (inscreva-se para pesquisar violações confidenciais)



3 passos para melhorar a segurança

Comece a usar 1Password.com






7ª: jeff@reddit.com

pwned?


Boas notícias - nenhum pwnage encontrado!


Sem contas violadas e sem pastas (inscreva-se para pesquisar violações confidenciais)



3 passos para melhorar a segurança

Comece a usar 1Password.com






8ª: david@reddit.com



pwned?

Oh não - pwned!

Pwned em 6 violações de dados e não encontrou pastas (inscreva -se para pesquisar violações confidenciais)

 3 passos para melhorar a segurança

[Comece a usar 1Password.com](#)




9ª: askanadmin@reddit.com




pwned?

Boas notícias - nenhum pwnage encontrado!

Sem contas violadas e sem pastas (inscreva -se para pesquisar violações confidenciais)

 3 passos para melhorar a segurança

[Comece a usar 1Password.com](#)



10ª: mike@reddit.com

pwned?

Oh não - pwned!

Pwned em 5 violações de dados e não encontrou pastas ([inscreva-se](#) para pesquisar violações confidenciais)

 **3 passos para melhorar a segurança** Comece a usar [1Password.com](#)



- Verificar se é retornado algumas informações no domínio via Google Hacking.

[intitle: index of:](#)

intitle:"index of" reddit.com



Todas

Imagens

Notícias

Vídeos

Maps

Mais

Ferramentas

Aproximadamente 5.750 resultados (0,22 segundos)

<https://www.reddit.com> › domain ▾ Traduzir esta página

index-of.es on reddit.com

index-of.es on reddit.com ...

<https://www.reddit.com> › comments ▾ Traduzir esta página

Full index of all Subreddits anywhere? : r/help

4 de mai. de 2021 — Full **index of** all Subreddits anywhere? : r/help ...

<https://www.reddit.com> › comments ▾ Traduzir esta página

Is there an index of all subs on Reddit, organized by content ...

1 de out. de 2017 — Is there an **index of** all subs on Reddit, organized by content category? : r/modhelp ...

<https://www.reddit.com> › comments ▾ Traduzir esta página

What is, "index of" search? : r/Piracy - Reddit

23 de mar. de 2019 — What is, "**index of**" search? : r/Piracy ...

<https://earldouglas.com> › ext › reddit ▾ Traduzir esta página

Index of /ext/reddit.com/ - James Earl Douglas

Index of /ext/reddit.com/ ../ r/ 20-Apr-2022 16:11 -

<https://earldouglas.com> › ext › redd... ▾ Traduzir esta página

Index of /ext/reddit.com/r/ - James Earl Douglas

Index of /ext/reddit.com/r/ ../ haskell/ 20-Apr-2022 17:33 -

Google

intitle:reddit.com



Todas

Vídeos

Imagens

Notícias

Shopping

Mais

Ferramentas

Aproximadamente 508.000 resultados (0,55 segundos)

[https://www.reddit.com > register](https://www.reddit.com/register) Traduzir esta página

reddit.com: Join the worldwide conversation

Create an account on Reddit and become part of our community!

[https://www.reddit.com > wiki > pt-br > faq](https://www.reddit.com/wiki/pt-br/faq)

pt-br/faq - reddit.com

Perguntas mais frequentes (FAQ) **NOTA:** A [versão em inglês]

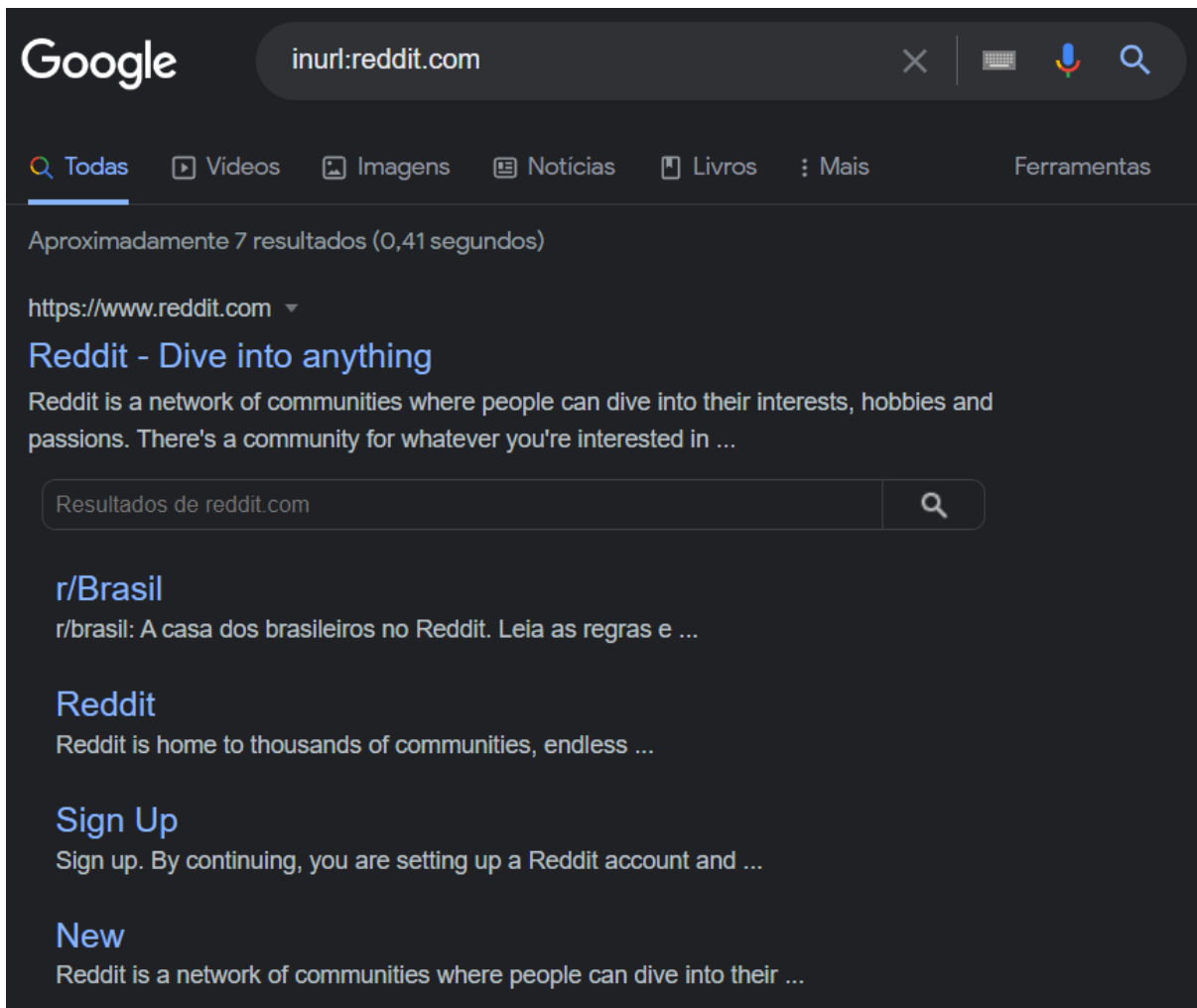
(<https://www.reddit.com/wiki/FAQ>) do FAQ é a versão canônica neste momento. Por favor, use...

[https://www.reddit.com > reddit](https://www.reddit.com/reddit) Traduzir esta página

r/reddit.com icon

The original subreddit, now archived. Meta/Reddit. 935K members • 804 online. Join. Posts · About.

inurl:reddit.com:



- Utilizar a ferramenta TheHarvester via Kali Linux para coleta de informações.

```
root@kali:~# host reddit.com
reddit.com has address 151.101.65.140
reddit.com has address 151.101.1.140
reddit.com has address 151.101.129.140
reddit.com has address 151.101.193.140
reddit.com has IPv6 address 2a04:4e42::396
reddit.com has IPv6 address 2a04:4e42:600::396
reddit.com has IPv6 address 2a04:4e42:200::396
reddit.com has IPv6 address 2a04:4e42:400::396
reddit.com mail is handled by 10 aspmx2.googlemail.com.
reddit.com mail is handled by 1 aspmx.l.google.com.
reddit.com mail is handled by 10 aspmx3.googlemail.com.
reddit.com mail is handled by 5 alt1.aspmx.l.google.com.
reddit.com mail is handled by 5 alt2.aspmx.l.google.com.
```

theharvest: google

```
Harvesting results
No IP addresses found

[+] Emails found:
-----
androidsupport@reddit.com

[+] Hosts found in search engines:
-----

Total hosts: 2

[-] Resolving hostnames IPs...

old.reddit.com:199.232.113.140
www.reddit.com:199.232.113.140
```

thearvest: yahoo

```
Harvesting results
No IP addresses found

[+] Emails found:
-----
u0022@reddit.com

[+] Hosts found in search engines:
-----

Total hosts: 4

[-] Resolving hostnames IPs...

ads.reddit.com:151.101.129.140
mod.reddit.com:199.232.113.140
placedata.reddit.com:199.232.113.140
www.reddit.com:199.232.113.140
```

thearvest: bing

```
Harvesting results
No IP addresses found

[+] Emails found:
-----
api@reddit.com
security@reddit.com

[+] Hosts found in search engines:
-----

Total hosts: 2

[-] Resolving hostnames IPs...

ads.reddit.com:151.101.129.140
www.reddit.com:199.232.113.140
```

- Ano em que o domínio do site começou a ser utilizado; Qual ano, o domínio teve mais acesso; Qual mês costuma ter mais acessos no site, etc.

WayBack Machine: reddit.com

O Reddit.com antes era hospedado em outro domínio, o nome era BuyDomains.com que, como o nome já sugere, era um site de vendas de domínios para uma organização, isso lá em julho de 2002. Em Agosto de 2005 passou a ser o domínio que é hoje Reddit.com um site de notícias. Em Outubro de 2007 foi a primeira vez que foi acessado todos os dias desse mês. Em Janeiro de 2012 foi a primeira vez que o site teve mais de 1000 mil requisições em um único dia. Em Julho de 2021 bateu o recorde de acessos em um único dia: 134,965 requisições, também foi o ano que teve mais acessos.

Em informações de infraestrutura devem ser levantadas as seguintes informações:

- Localização do servidor web.



151.101.128.0/22

FASTLY

Announcing ASNs: 1

Parent Prefix: 151.101.0.0/16

Abuse: abuse@fastly.com

RIR: ARIN

Prefix

Routing

Raw Whois

Announcing ASNs

Country	ASN	Name	Description
	AS54113	FASTLY	Fastly

151.101.128.0/22 Summary

PREFIX: 151.101.128.0/22

NAME: SKYCA-3

DESCRIPTION: Fastly

COUNTRY:

IP ADDRESSES: 1,024

REGIONAL REGISTRY: ARIN

ALLOCATION STATUS: Allocated

ALLOCATION DATE: 1st February 2016

PARENT PREFIX: 151.101.0.0/16

Contacts

EMAIL CONTACTS:

abuse@fastly.com

noc@fastly.com

rir-admin@fastly.com

ABUSE CONTACTS:

abuse@fastly.com

ADDRESS:

PO Box 78266,

San Francisco,

CA,

94107,

US



151.101.0.0/16

FASTLY

Announcing ASNs: 1

Parent Prefix: 151.101.0.0/16

Abuse: abuse@fastly.com

RIR: ARIN

Prefix

Routing

Raw Whois

Announcing ASNs

Country	ASN	Name	Description
	AS54113	FASTLY	Fastly

151.101.0.0/16 Summary

PREFIX: 151.101.0.0/16

NAME: SKYCA-3

DESCRIPTION: Fastly

COUNTRY:

IP ADDRESSES: 65,536

REGIONAL REGISTRY: ARIN

ALLOCATION STATUS: Allocated

ALLOCATION DATE: 1st February 2016

Contacts

EMAIL CONTACTS:

noc@fastly.com

abuse@fastly.com

rir-admin@fastly.com

ABUSE CONTACTS:

abuse@fastly.com

ADDRESS:

PO Box 78266,

San Francisco,

CA,

94107,



US




151.101.193.140

NO RDNS FOUND

Announced Prefixes

Country	Announced Prefix	Prefix Name	Prefix Description	ASN	ASN Description	ASN Name
	151.101.192.0/22	SKYCA-3	Fastly	AS54113	FASTLY	Fastly
	151.101.0.0/16	SKYCA-3	Fastly	AS54113	FASTLY	Fastly

RIR Allocation Summary

PREFIX: 151.101.0.0/16
GEOIP COUNTRY: 
IP ADDRESSES: 65,536



REGIONAL REGISTRY: ARIN
ALLOCATION STATUS: Allocated
ALLOCATION DATE: 1st February 2016



151.101.129.140

NO RDNS FOUND

Announced Prefixes

Country	Announced Prefix	Prefix Name	Prefix Description	ASN	ASN Description	ASN Name
	151.101.128.0/22	SKYCA-3	Fastly	AS54113	FASTLY	Fastly
	151.101.0.0/16	SKYCA-3	Fastly	AS54113	FASTLY	Fastly

RIR Allocation Summary

PREFIX: 151.101.0.0/16
GEOIP COUNTRY: 
IP ADDRESSES: 65,536

REGIONAL REGISTRY: ARIN
ALLOCATION STATUS: Allocated
ALLOCATION DATE: 1st February 2016



151.101.65.140

NO RDNS FOUND

Announced Prefixes

Country	Announced Prefix	Prefix Name	Prefix Description	ASN	ASN Description	ASN Name
	151.101.64.0/22	SKYCA-3	Fastly	AS54113	FASTLY	Fastly
	151.101.0.0/16	SKYCA-3	Fastly	AS54113	FASTLY	Fastly

RIR Allocation Summary

PREFIX: 151.101.0.0/16
GEOIP COUNTRY: 
IP ADDRESSES: 65,536

REGIONAL REGISTRY: ARIN
ALLOCATION STATUS: Allocated
ALLOCATION DATE: 1st February 2016

- Encontrar subdomínios no site (Utilizando o script criado em sala de aula).

```

root@kali:~# ./subtakeover.sh reddit.com
firewall.reddit.com is an alias for reddit.map.fastly.net.
monitoramento.reddit.com is an alias for reddit.map.fastly.net.
intranet.reddit.com is an alias for reddit.map.fastly.net.
ns1.reddit.com is an alias for reddit.map.fastly.net.
ns01.reddit.com is an alias for reddit.map.fastly.net.
mail.reddit.com is an alias for reddit.map.fastly.net.
webmail.reddit.com is an alias for reddit.map.fastly.net.
rh.reddit.com is an alias for dualstack.reddit.map.fastly.net.
sistema.reddit.com is an alias for reddit.map.fastly.net.
homologacao.reddit.com is an alias for reddit.map.fastly.net.
admin.reddit.com is an alias for reddit.map.fastly.net.
api.reddit.com is an alias for reddit.map.fastly.net.
logs.reddit.com is an alias for reddit.map.fastly.net.
devs.reddit.com is an alias for reddit.map.fastly.net.
documentos.reddit.com is an alias for reddit.map.fastly.net.
server.reddit.com is an alias for reddit.map.fastly.net.

```

- Verificar lista de endereço IP ou ASN dos servidores.

ASN: [AS54113](#).



151.101.129.140

NO RDNS FOUND

Announced Prefixes

Country	Announced Prefix	Prefix Name	Prefix Description	ASN	ASN Description	ASN Name
	151.101.128.0/22	SKYCA-3	Fastly	AS54113	FASTLY	Fastly
	151.101.0.0/16	SKYCA-3	Fastly	AS54113	FASTLY	Fastly

RIR Allocation Summary

PREFIX: [151.101.0.0/16](#)

GEOIP COUNTRY:

IP ADDRESSES: 65,536

REGIONAL REGISTRY: ARIN

ALLOCATION STATUS: Allocated

ALLOCATION DATE: 1st February 2016

```
root@kali:~# host reddit.com
reddit.com has address 151.101.1.140
reddit.com has address 151.101.129.140
reddit.com has address 151.101.65.140
reddit.com has address 151.101.193.140
reddit.com has IPv6 address 2a04:4e42::396
reddit.com has IPv6 address 2a04:4e42:600::396
reddit.com has IPv6 address 2a04:4e42:200::396
reddit.com has IPv6 address 2a04:4e42:400::396
reddit.com mail is handled by 10 aspmx2.googlemail.com.
reddit.com mail is handled by 1 aspmx.l.google.com.
reddit.com mail is handled by 10 aspmx3.googlemail.com.
reddit.com mail is handled by 5 alt1.aspmx.l.google.com.
reddit.com mail is handled by 5 alt2.aspmx.l.google.com.
```