



## **Curso Técnico Subsequente de Informática – Módulo 3**

**Disciplinas:** Segurança e Auditoria de Sistemas

**Professor:** Rodrigo Macedo

**Discente(s):** Makyson, M<sup>a</sup> Vitória e Valdeane

# **Coleta de Informações**

Grajaú-MA  
2022

# Índice

1. Informações de Negócio.....
  - 1.1 Lista de E-mails de funcionários.
  - 1.2 Verificar quais e-mails listados sofreram vazamento de dados.
  - 1.3 Verificar se é retornado algumas informações no domínio via Google Hacking.
  - 1.4 Utilizar a ferramenta TheHarvester via Kali Linux para coleta de informações.
  - 1.5 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.
2. Informações de Infraestrutura.....
  - 2.1 Localização do servidor web.
  - 2.2 Encontrar subdomínios no site (Utilizando o script criado em sala de aula).
  - 2.3 Verificar lista de endereço IP ou ASN dos servidores.

## 1.1 Lista de E-mails de funcionários.

David Koloski

dkoloski@google.com

Gilberto Contreras

gcontreras@google.com

Brian Hamrick

bhamrick@google.com

Justin Huang

justinhuang@google.com

Nathan Scoglio

scoglio@google.com

Omar Hammad

ohammad@google.com

Duncan Catherine

catduncan@google.com

Agarwal Tushar

agarwaltushar@google.com

Caitlin Cassidy

cassidy@google.com

Michael Brase

mbrase@google.com

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

pwned?

**Oh não - pwned!**

Pwned em 4 [violações de dados](#) e não encontrou pastas ( [inscreva -se](#) para pesquisar violações confidenciais)

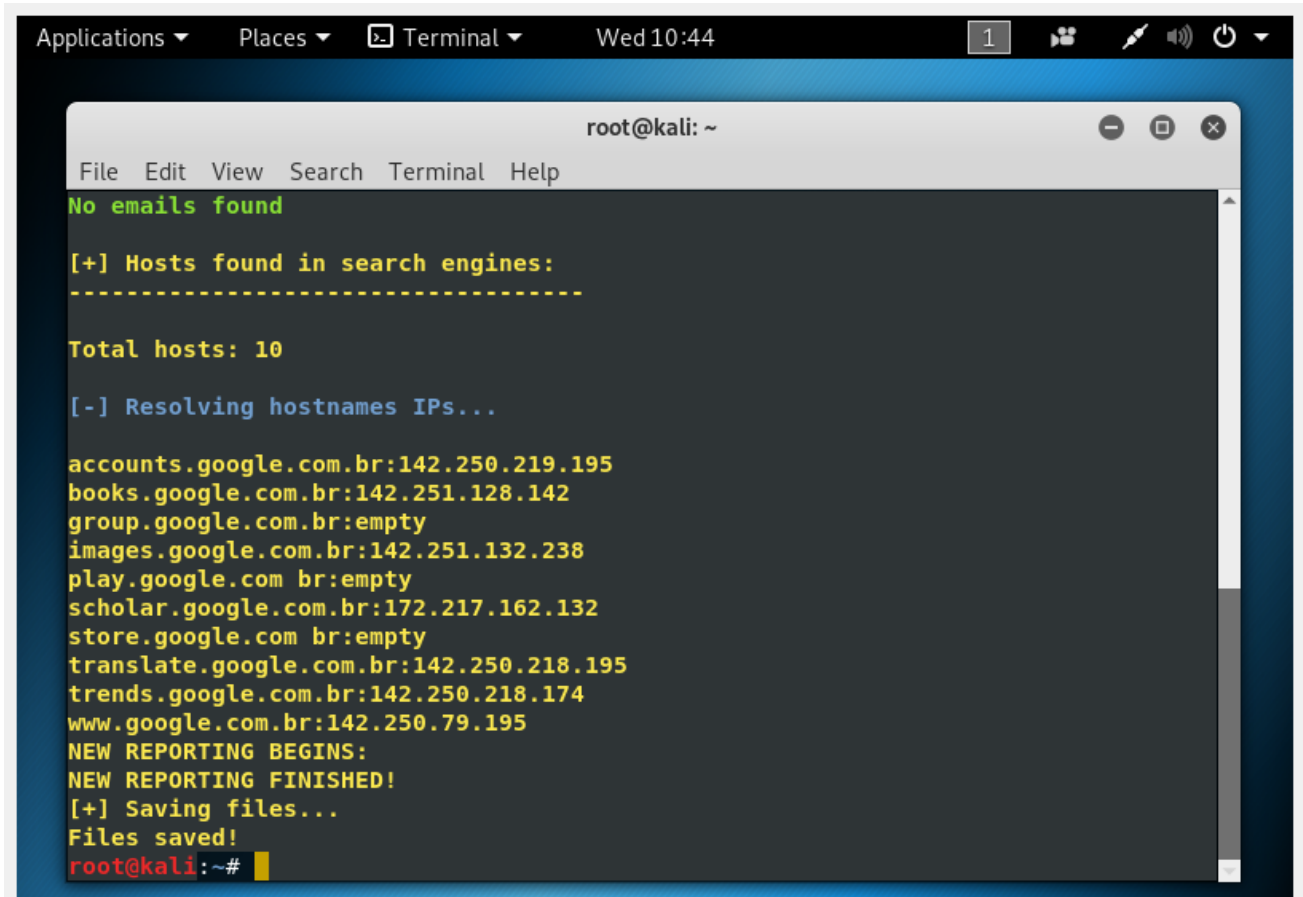
pwned?

**Oh não - pwned!**

Pwned em 6 [violações de dados](#) e encontrou 1 [pasta](#) ( [inscreva -se](#) para pesquisar violações confidenciais)

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

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



```
root@kali: ~  
File Edit View Search Terminal Help  
No emails found  
[+] Hosts found in search engines:  
-----  
Total hosts: 10  
[-] Resolving hostnames IPs...  
accounts.google.com.br:142.250.219.195  
books.google.com.br:142.251.128.142  
group.google.com.br:empty  
images.google.com.br:142.251.132.238  
play.google.com.br:empty  
scholar.google.com.br:172.217.162.132  
store.google.com.br:empty  
translate.google.com.br:142.250.218.195  
trends.google.com.br:142.250.218.174  
www.google.com.br:142.250.79.195  
NEW REPORTING BEGINS:  
NEW REPORTING FINISHED!  
[+] Saving files...  
Files saved!  
root@kali:~#
```

1.5 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.

O domínio que começou a ser utilizado foi Welcome to Google em 1998. No ano de 2019 no dia 11 do mês de Novembro foi quando o site teve mais acessos. Os meses em que o site costuma ser mais acessado são os meses de outubro, novembro e dezembro.

## 2.1 Localização do servidor web.

 Relatório de países

Nome, ASN, IP, Prefixo 

 142.250.218.238  
GRU14 S26-IN-F14.1E100.NET

### Prefixos anunciados

País	Prefixo anunciado	Nome do prefixo	Descrição do prefixo	ASN	Descrição ASN	Nome ASN
	142.250.0.0/15	O GOOGLE	Google LLC	AS15169	O GOOGLE	Google LLC

### Alocação RIR Summery

PREFIXO: 142.250.0.0/15


PAÍS GEOIP: 


ENDEREÇOS IP: 131.072

CADASTRO REGIONAL: ARIN

STATUS DE ALOCAÇÃO: Alocado

DATA DE ALOCAÇÃO: 24 de maio de 2012

 Relatório de países

Nome, ASN, IP, Prefixo 

 142.250.0.0/15  
GOOGLE LLC

Anunciando ASNs: 1      Prefixo pai: 142.250.0.0/15      Abuso: network-abuse@google.com      RIR: ARIN

**Prefixo**  
Roteamento  
Whois brutos

### Anunciando ASNs

País	ASN	Nome	Descrição
	AS15169	O GOOGLE	Google LLC

### 142.250.0.0/15 Resumo

PREFIXO: 142.250.0.0/15

NOME: O GOOGLE

DESCRIÇÃO: Google LLC

PAÍS: 

ENDEREÇOS IP: 131.072

CADASTRO REGIONAL: ARIN

STATUS DE ALOCAÇÃO: Alocado

DATA DE ALOCAÇÃO: 24 de maio de 2012

### Contatos

CONTATOS DE E-MAIL:  
network-abuse@google.com  
arin-contact@google.com

CONTATOS DE ABUSO:  
network-abuse@google.com

ENDEREÇO:  
1600 Amphitheatre Parkway,  
Vista da montanha,  
CA,  
94043,  
NÓS

## 2.2 Encontrar subdomínios no site (Utilizando o script criado em sala de aula)

```
root@kali:~# ./subtakeover.sh google.com
gmail.google.com is an alias for www3.l.google.com.
forms.google.com is an alias for www3.l.google.com.
spreadsheets.google.com is an alias for spreadsheets.l.google.com.
translate.google.com is an alias for www3.l.google.com.
root@kali:~#
```

## 2.3 Verificar lista de endereço IP ou ASN dos servidores.

```
File Edit View Search Terminal Help
root@kali:~# whois google.com
host google.com
connect: Network is unreachable
root@kali:~# host google.com
google.com has address 142.250.79.206
google.com has IPv6 address 2800:3f0:4001:808::200e
google.com mail is handled by 10 smtp.google.com.
root@kali:~#
```