iTeam
fazendo diferente

[+]

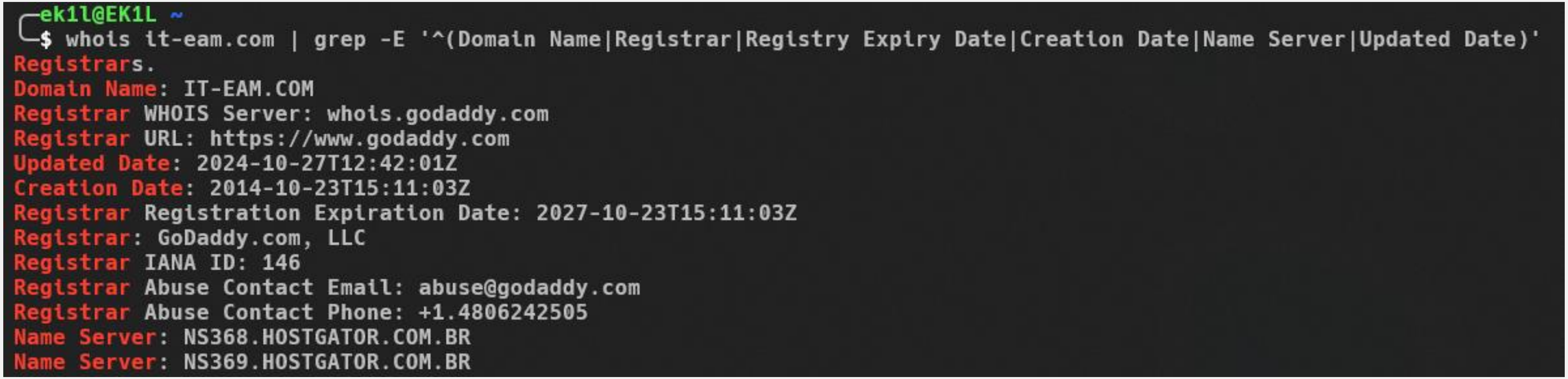
External

Recognition

Red Team

Enumeração Inicial de domínio

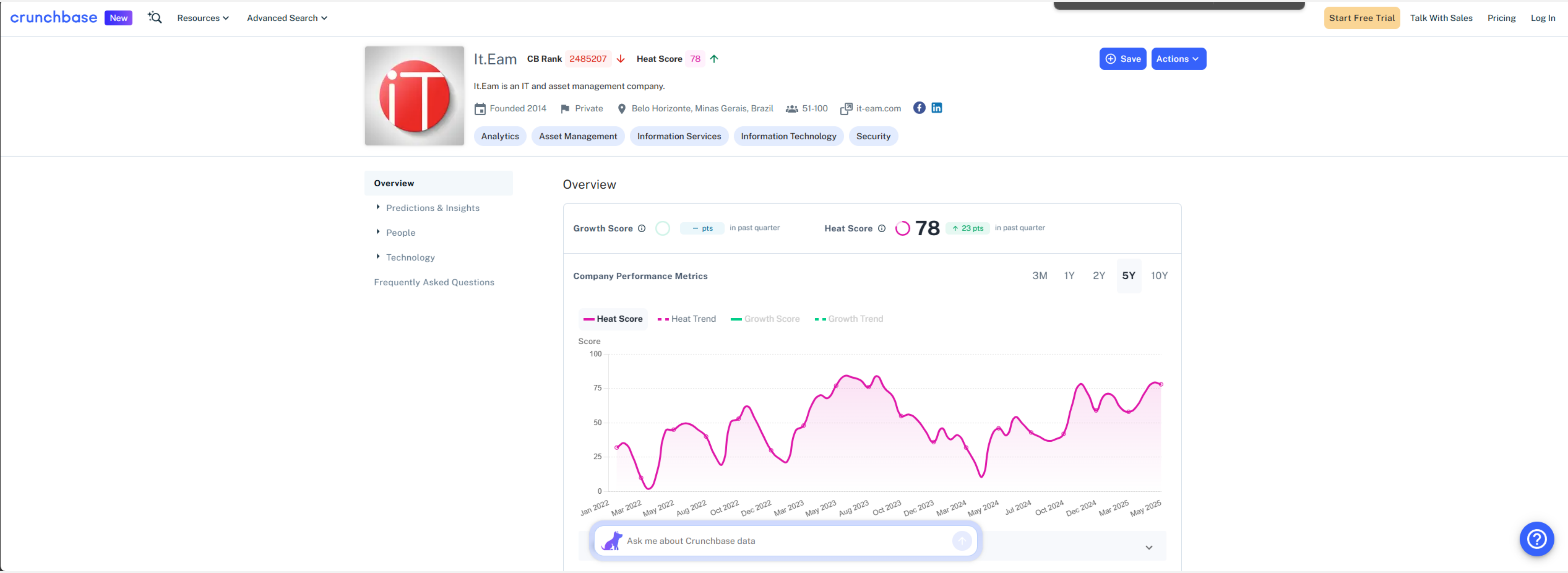
Pesquisa por whois



```
┌─ek1l@EK1L ~
└─$ whois it-eam.com | grep -E '^(Domain Name|Registrar|Registry Expiry Date|Creation Date|Name Server|Updated Date)'
Registrars.
Domain Name: IT-EAM.COM
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2024-10-27T12:42:01Z
Creation Date: 2014-10-23T15:11:03Z
Registrar Registration Expiration Date: 2027-10-23T15:11:03Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Name Server: NS368.HOSTGATOR.COM.BR
Name Server: NS369.HOSTGATOR.COM.BR
```

Red Team

Aquisições da empresa



crunchbase New | Resources | Advanced Search | Start Free Trial | Talk With Sales | Pricing | Log In

It.Eam CB Rank 2485207 ↓ Heat Score 78 ↑

Save | Actions

It.Eam is an IT and asset management company.

Founded 2014 | Private | Belo Horizonte, Minas Gerais, Brazil | 51-100 | it-eam.com

Analytics | Asset Management | Information Services | Information Technology | Security

- Overview
- Predictions & Insights
- People
- Technology
- Frequently Asked Questions

Overview

Growth Score — pts in past quarter

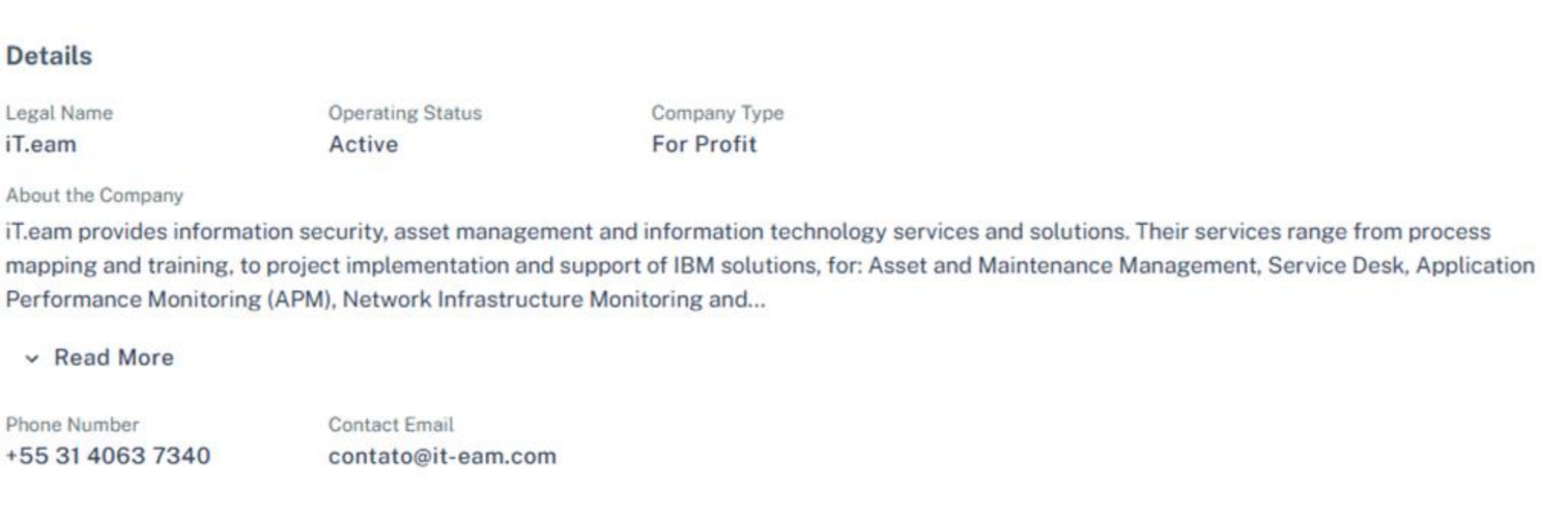
Heat Score 78 ↑ 23 pts in past quarter

Company Performance Metrics 3M 1Y 2Y 5Y 10Y

Ask me about Crunchbase data

Crunchbase

Aquisições da empresa



Details

Legal Name	Operating Status	Company Type
iT.eam	Active	For Profit

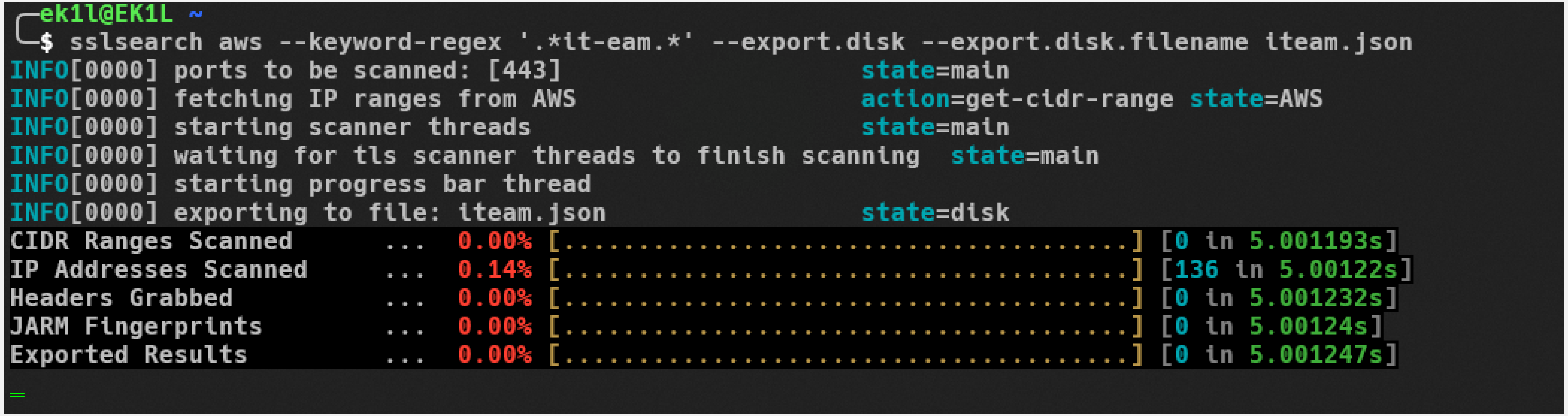
About the Company

iT.eam provides information security, asset management and information technology services and solutions. Their services range from process mapping and training, to project implementation and support of IBM solutions, for: Asset and Maintenance Management, Service Desk, Application Performance Monitoring (APM), Network Infrastructure Monitoring and...

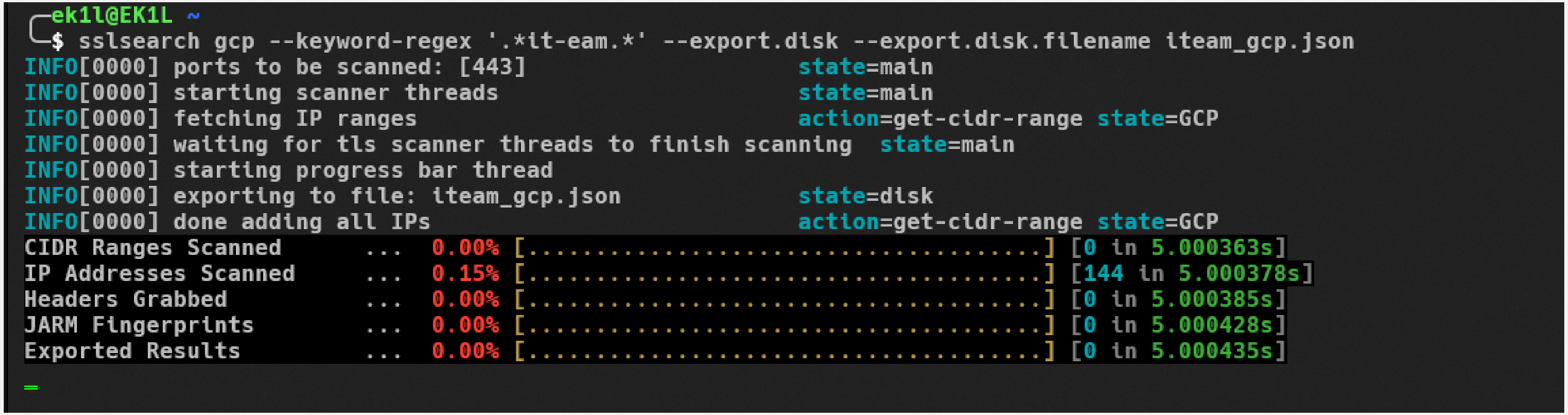
Phone Number	Contact Email
+55 31 4063 7340	contato@it-eam.com

Crunchbase

CLOUD ENUMERATION

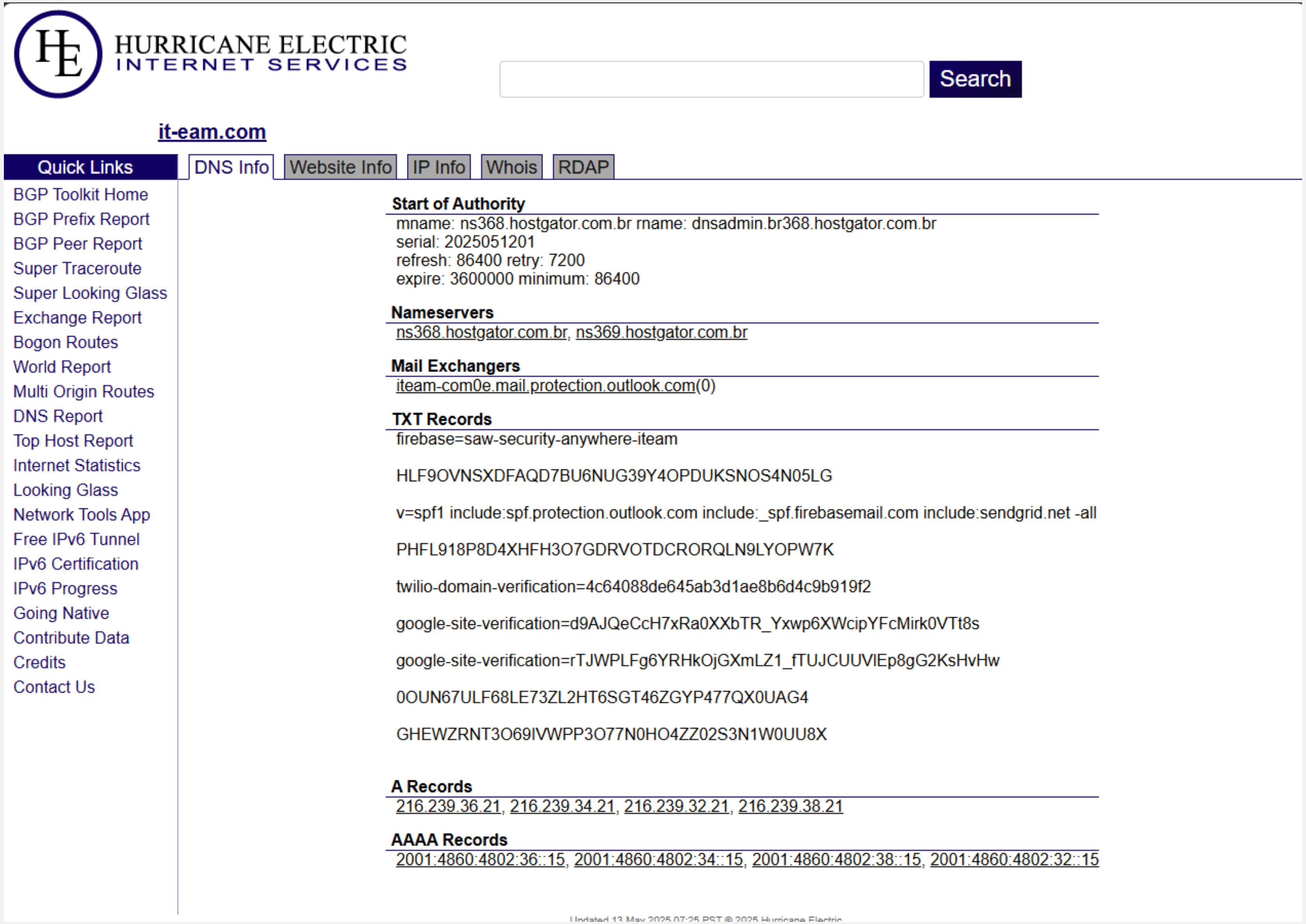


```
┌─ek1l@EK1L ~
└─$ sslsearch aws --keyword-regex '.*it-eam.*' --export.disk --export.disk.filename iteam.json
INFO[0000] ports to be scanned: [443]                      state=main
INFO[0000] fetching IP ranges from AWS                     action=get-cidr-range state=AWS
INFO[0000] starting scanner threads                        state=main
INFO[0000] waiting for tls scanner threads to finish scanning  state=main
INFO[0000] starting progress bar thread
INFO[0000] exporting to file: iteam.json                   state=disk
CIDR Ranges Scanned       ...  0.00% [.......................................] [0 in 5.001193s]
IP Addresses Scanned      ...  0.14% [.......................................] [136 in 5.00122s]
Headers Grabbed           ...  0.00% [.......................................] [0 in 5.001232s]
JARM Fingerprints         ...  0.00% [.......................................] [0 in 5.00124s]
Exported Results          ...  0.00% [.......................................] [0 in 5.001247s]

═
```



```
┌─ek1l@EK1L ~
└─$ sslsearch gcp --keyword-regex '.*it-eam.*' --export.disk --export.disk.filename iteam_gcp.json
INFO[0000] ports to be scanned: [443]                      state=main
INFO[0000] starting scanner threads                        state=main
INFO[0000] fetching IP ranges                              action=get-cidr-range state=GCP
INFO[0000] waiting for tls scanner threads to finish scanning  state=main
INFO[0000] starting progress bar thread
INFO[0000] exporting to file: iteam_gcp.json               state=disk
INFO[0000] done adding all IPs                             action=get-cidr-range state=GCP
CIDR Ranges Scanned       ...  0.00% [.......................................] [0 in 5.000363s]
IP Addresses Scanned      ...  0.15% [.......................................] [144 in 5.000378s]
Headers Grabbed           ...  0.00% [.......................................] [0 in 5.000385s]
JARM Fingerprints         ...  0.00% [.......................................] [0 in 5.000428s]
Exported Results          ...  0.00% [.......................................] [0 in 5.000435s]

═
```

ASN



it-eam.com

Start of Authority

mname: ns368.hostgator.com.br rname: dnsadmin.br368.hostgator.com.br
serial: 2025051201
refresh: 86400 retry: 7200
expire: 3600000 minimum: 86400

Nameservers

ns368.hostgator.com.br, ns369.hostgator.com.br

Mail Exchangers

iteam-com0e.mail.protection.outlook.com(0)

TXT Records

firebase=saw-security-anywhere-iteam

HLF9OVNSXDFAQD7BU6NUG39Y4OPDUKSNOS4N05LG

v=spf1 include:spf.protection.outlook.com include:_spf.firebasemail.com include:sendgrid.net -all

PHFL918P8D4XHFH3O7GDRVOTDCRORQLN9LYOPW7K

twilio-domain-verification=4c64088de645ab3d1ae8b6d4c9b919f2

google-site-verification=d9AJQeCcH7xRa0XXbTR_Yxwp6XWcipYFcMirk0VTt8s

google-site-verification=rTJWPLFg6YRHkOjGXmLZ1_fTUJCUUVlEp8gG2KsHvHw

0OUN67ULF68LE73ZL2HT6SGT46ZGYP477QX0UAG4

GHEWZRNT3O69IVWPP3O77N0HO4ZZ02S3N1W0UU8X

A Records

216.239.36.21, 216.239.34.21, 216.239.32.21, 216.239.38.21

AAAA Records

2001:4860:4802:36::15, 2001:4860:4802:34::15, 2001:4860:4802:38::15, 2001:4860:4802:32::15

Updated 13 May 2025 07:25 PST © 2025 Hurricane Electric

ASN

🌍 **AFRINIC (África)**
🔗 https://www.afrinic.net/
Exemplo: Uma empresa com sede em **Nigéria** ou **África do Sul** pode ter blocos registrados aqui.

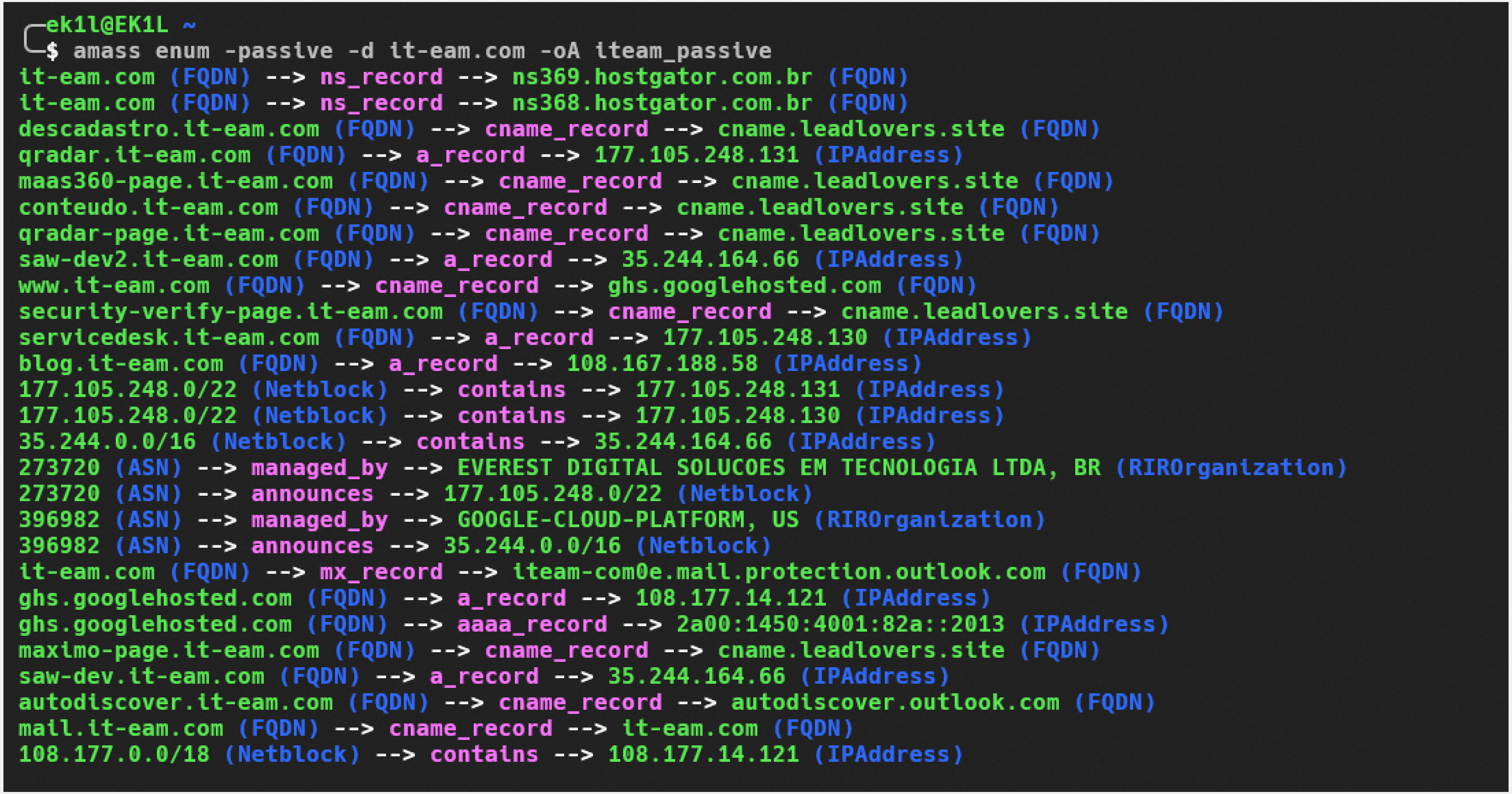
🌎 **ARIN (América do Norte)**
🔗 https://www.arin.net
Exemplo: Uma empresa nos **Estados Unidos** como a **Amazon** provavelmente terá blocos e ASN registrados aqui.

🌏 **APNIC (Ásia-Pacífico)**
🔗 https://www.apnic.net/
Exemplo: Empresas da **Índia, China ou Japão**, como **Alibaba Cloud**, terão dados registrados no APNIC.

🌐 **LACNIC (América Latina)**
🔗 https://www.lacnic.net/
Exemplo: Para empresas no **Brasil**, como **Vivo (Telefônica)** ou **Oi**, o LACNIC traz dados WHOIS relevantes.

🌍 **RIPE NCC (Europa e Oriente Médio)**
🔗 https://www.ripe.net/
Exemplo: Empresas da **Alemanha, França, Inglaterra**, como a **OVH**, terão seus ASNs e IPs registrados aqui.

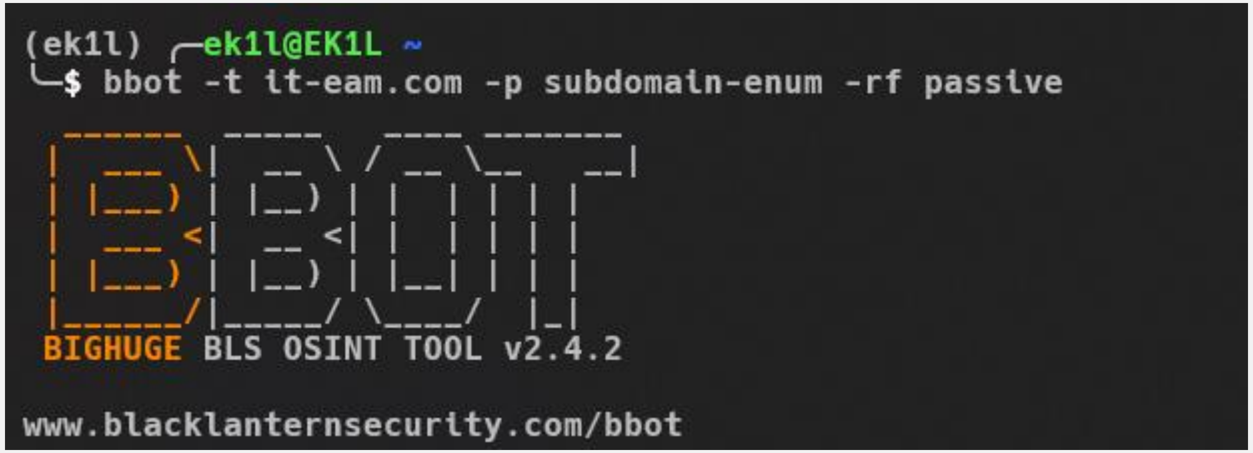
ASN



```
┌─ek1l@EK1L ~
└─$ amass enum -passive -d it-eam.com -oA iteam_passive
it-eam.com (FQDN) --> ns_record --> ns369.hostgator.com.br (FQDN)
it-eam.com (FQDN) --> ns_record --> ns368.hostgator.com.br (FQDN)
descadastro.it-eam.com (FQDN) --> cname_record --> cname.leadlovers.site (FQDN)
qradar.it-eam.com (FQDN) --> a_record --> 177.105.248.131 (IPAddress)
maas360-page.it-eam.com (FQDN) --> cname_record --> cname.leadlovers.site (FQDN)
conteudo.it-eam.com (FQDN) --> cname_record --> cname.leadlovers.site (FQDN)
qradar-page.it-eam.com (FQDN) --> cname_record --> cname.leadlovers.site (FQDN)
saw-dev2.it-eam.com (FQDN) --> a_record --> 35.244.164.66 (IPAddress)
www.it-eam.com (FQDN) --> cname_record --> ghs.googlehosted.com (FQDN)
security-verify-page.it-eam.com (FQDN) --> cname_record --> cname.leadlovers.site (FQDN)
servicedesk.it-eam.com (FQDN) --> a_record --> 177.105.248.130 (IPAddress)
blog.it-eam.com (FQDN) --> a_record --> 108.167.188.58 (IPAddress)
177.105.248.0/22 (Netblock) --> contains --> 177.105.248.131 (IPAddress)
177.105.248.0/22 (Netblock) --> contains --> 177.105.248.130 (IPAddress)
35.244.0.0/16 (Netblock) --> contains --> 35.244.164.66 (IPAddress)
273720 (ASN) --> managed_by --> EVEREST DIGITAL SOLUCOES EM TECNOLOGIA LTDA, BR (RIROrganization)
273720 (ASN) --> announces --> 177.105.248.0/22 (Netblock)
396982 (ASN) --> managed_by --> GOOGLE-CLOUD-PLATFORM, US (RIROrganization)
396982 (ASN) --> announces --> 35.244.0.0/16 (Netblock)
it-eam.com (FQDN) --> mx_record --> iteam-com0e.mail.protection.outlook.com (FQDN)
ghs.googlehosted.com (FQDN) --> a_record --> 108.177.14.121 (IPAddress)
ghs.googlehosted.com (FQDN) --> aaaa_record --> 2a00:1450:4001:82a::2013 (IPAddress)
maximo-page.it-eam.com (FQDN) --> cname_record --> cname.leadlovers.site (FQDN)
saw-dev.it-eam.com (FQDN) --> a_record --> 35.244.164.66 (IPAddress)
autodiscover.it-eam.com (FQDN) --> cname_record --> autodiscover.outlook.com (FQDN)
mail.it-eam.com (FQDN) --> cname_record --> it-eam.com (FQDN)
108.177.0.0/18 (Netblock) --> contains --> 108.177.14.121 (IPAddress)
```

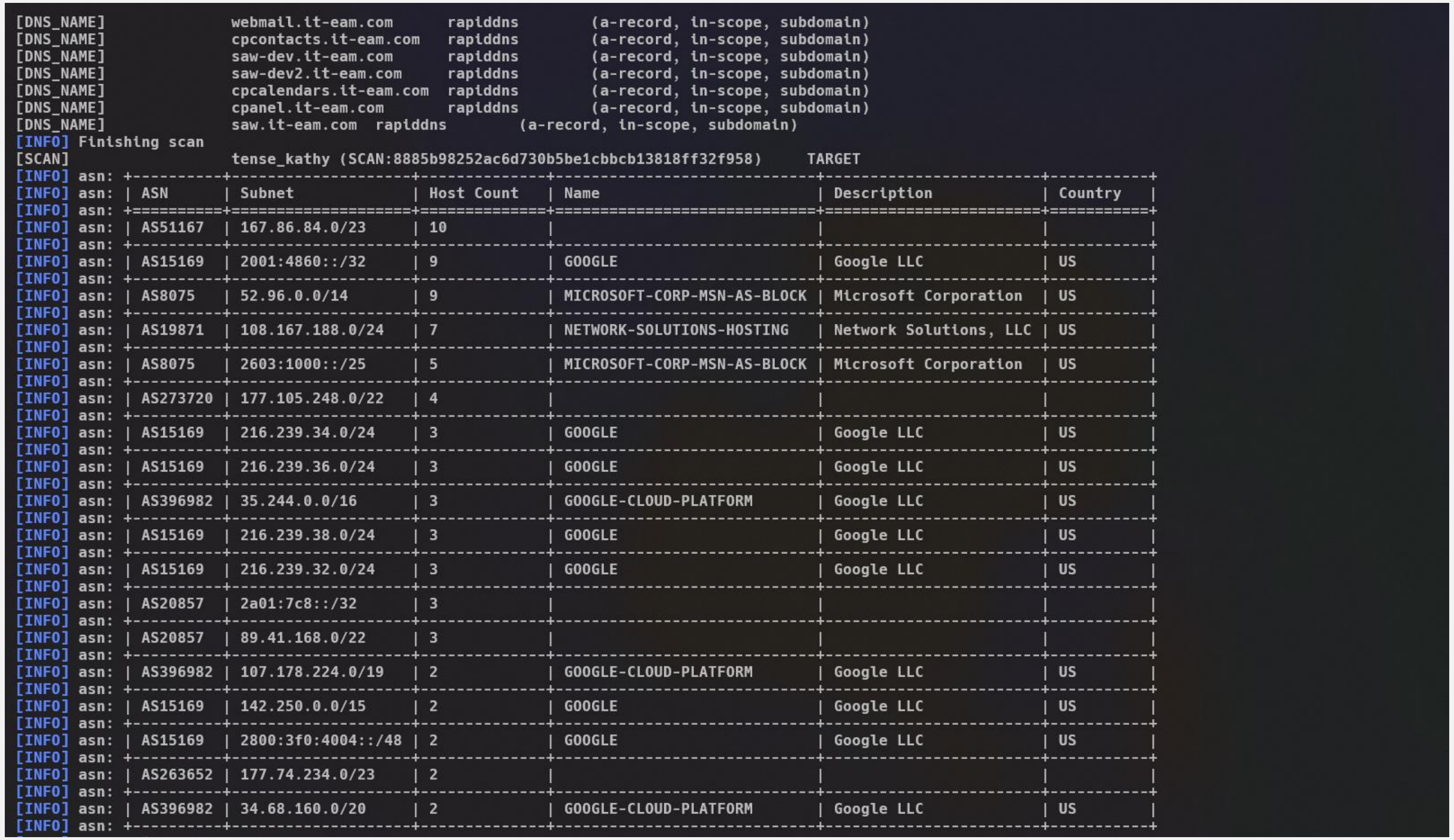
Red Team

ASN



```
(ek1l) ┌─ek1l@EK1L ~
└─$ bbot -t it-eam.com -p subdomain-enum -rf passive

 ______  _____   ____  _______
|  ___ \|  __ \ / __ \__   __|
| |___) | |__) | |  | | | |
|  ___ <|  __ <| |  | | | |
| |___) | |__) | |__| | | |
|______/|_____/ \____/  |_|
BIGHUGE BLS OSINT TOOL v2.4.2

www.blacklanternsecurity.com/bbot
```

[blacklanternsecurity/bbot: The recursive internet scanner for hackers. 🧡]



```
[DNS_NAME]              webmail.it-eam.com      rapiddns        (a-record, in-scope, subdomain)
[DNS_NAME]              cpcontacts.it-eam.com   rapiddns        (a-record, in-scope, subdomain)
[DNS_NAME]              saw-dev.it-eam.com      rapiddns        (a-record, in-scope, subdomain)
[DNS_NAME]              saw-dev2.it-eam.com     rapiddns        (a-record, in-scope, subdomain)
[DNS_NAME]              cpcalendars.it-eam.com  rapiddns        (a-record, in-scope, subdomain)
[DNS_NAME]              cpanel.it-eam.com       rapiddns        (a-record, in-scope, subdomain)
[DNS_NAME]              saw.it-eam.com  rapiddns        (a-record, in-scope, subdomain)
[INFO] Finishing scan
[SCAN]                  tense_kathy (SCAN:8885b98252ac6d730b5be1cbbcb13818ff32f958)     TARGET
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | ASN      | Subnet             | Host Count   | Name                        | Description            | Country    |
[INFO] asn: +==========+====================+==============+=============================+========================+============+
[INFO] asn: | AS51167  | 167.86.84.0/23     | 10           |                             |                        |            |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS15169  | 2001:4860::/32     | 9            | GOOGLE                      | Google LLC             | US         |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS8075   | 52.96.0.0/14       | 9            | MICROSOFT-CORP-MSN-AS-BLOCK | Microsoft Corporation  | US         |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS19871  | 108.167.188.0/24   | 7            | NETWORK-SOLUTIONS-HOSTING   | Network Solutions, LLC | US         |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS8075   | 2603:1000::/25     | 5            | MICROSOFT-CORP-MSN-AS-BLOCK | Microsoft Corporation  | US         |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS273720 | 177.105.248.0/22   | 4            |                             |                        |            |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS15169  | 216.239.34.0/24    | 3            | GOOGLE                      | Google LLC             | US         |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS15169  | 216.239.36.0/24    | 3            | GOOGLE                      | Google LLC             | US         |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS396982 | 35.244.0.0/16      | 3            | GOOGLE-CLOUD-PLATFORM       | Google LLC             | US         |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS15169  | 216.239.38.0/24    | 3            | GOOGLE                      | Google LLC             | US         |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS15169  | 216.239.32.0/24    | 3            | GOOGLE                      | Google LLC             | US         |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS20857  | 2a01:7c8::/32      | 3            |                             |                        |            |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS20857  | 89.41.168.0/22     | 3            |                             |                        |            |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS396982 | 107.178.224.0/19   | 2            | GOOGLE-CLOUD-PLATFORM       | Google LLC             | US         |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS15169  | 142.250.0.0/15     | 2            | GOOGLE                      | Google LLC             | US         |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS15169  | 2800:3f0:4004::/48 | 2            | GOOGLE                      | Google LLC             | US         |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS263652 | 177.74.234.0/23    | 2            |                             |                        |            |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
[INFO] asn: | AS396982 | 34.68.160.0/20     | 2            | GOOGLE-CLOUD-PLATFORM       | Google LLC             | US         |
[INFO] asn: +----------+--------------------+--------------+-----------------------------+------------------------+------------+
```

DNS REVERSO

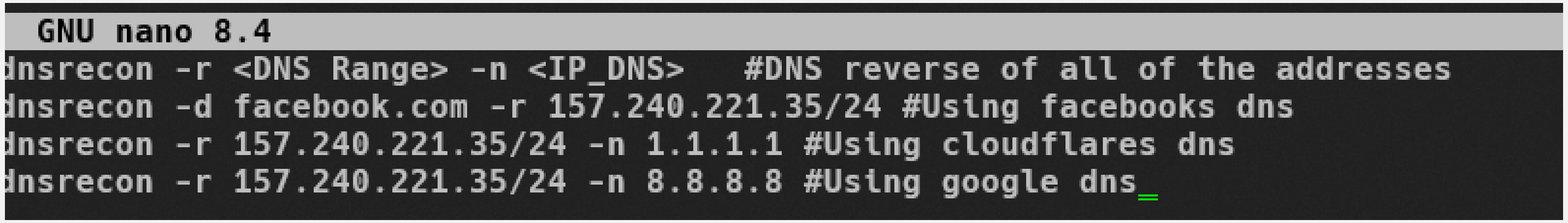
Mapear infraestrutura da organização

- IPs dentro de um ASN geralmente pertencem à mesma entidade ou grupo corporativo.
- O DNS reverso ajuda a:
  - Confirmar a *relevância* de determinados blocos de IP.
  - Entender o *papel de cada IP* (ex: firewall1.corp.com, rdp01.vpn.corp.com).

Encontrar domínios adicionais ou relacionados

- Às vezes, domínios completamente diferentes mas pertencentes à mesma empresa aparecem em reversos de IPs do ASN.
  - Exemplo: server.partnercorp.net resolvendo para um IP do ASN da evilcorp.com.

DNS REVERSO

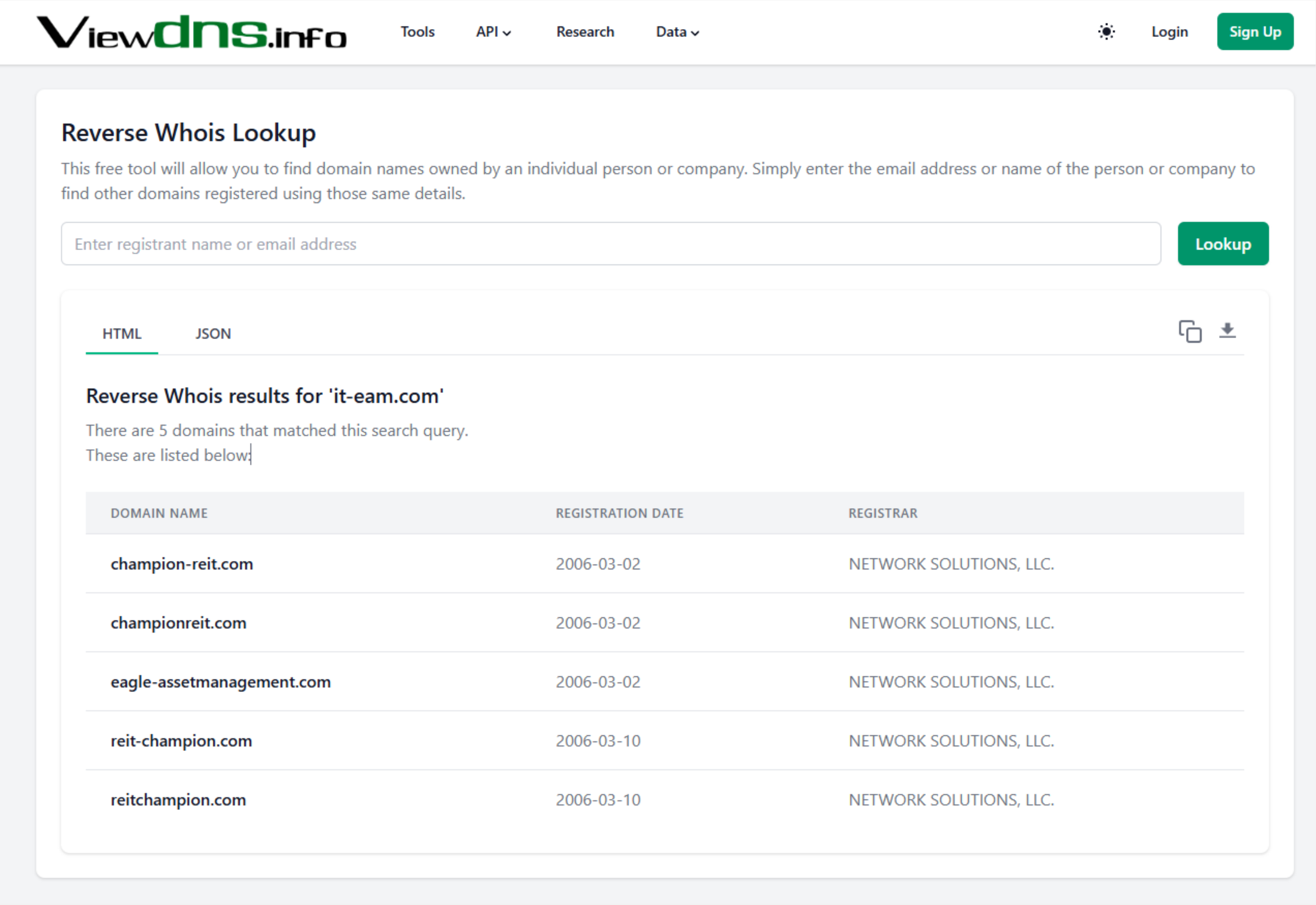


```
 GNU nano 8.4
dnsrecon -r <DNS Range> -n <IP_DNS>   #DNS reverse of all of the addresses
dnsrecon -d facebook.com -r 157.240.221.35/24 #Using facebooks dns
dnsrecon -r 157.240.221.35/24 -n 1.1.1.1 #Using cloudflares dns
dnsrecon -r 157.240.221.35/24 -n 8.8.8.8 #Using google dns
```

Reverse Whois

Ferramentas de Reverse WHOIS

- https://viewdns.info/reversewhois/
- https://domaineye.com/reverse-whois
- https://www.reversewhois.io/
- https://www.whoxy.com/
- http://reversewhois.domaintools.com/
- https://drs.whoisxmlapi.com/reverse-whois-search
- https://www.domainiq.com/



Reverse Whois Lookup

This free tool will allow you to find domain names owned by an individual person or company. Simply enter the email address or name of the person or company to find other domains registered using those same details.

Enter registrant name or email address

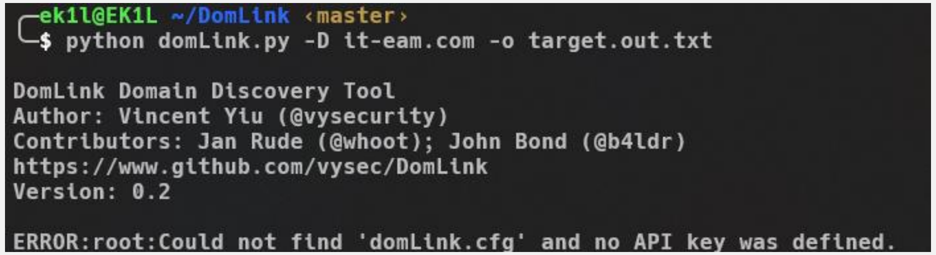
Reverse Whois results for 'it-eam.com'

There are 5 domains that matched this search query.
These are listed below:

DOMAIN NAME	REGISTRATION DATE	REGISTRAR
champion-reit.com	2006-03-02	NETWORK SOLUTIONS, LLC.
championreit.com	2006-03-02	NETWORK SOLUTIONS, LLC.
eagle-assetmanagement.com	2006-03-02	NETWORK SOLUTIONS, LLC.
reit-champion.com	2006-03-10	NETWORK SOLUTIONS, LLC.
reitchampion.com	2006-03-10	NETWORK SOLUTIONS, LLC.

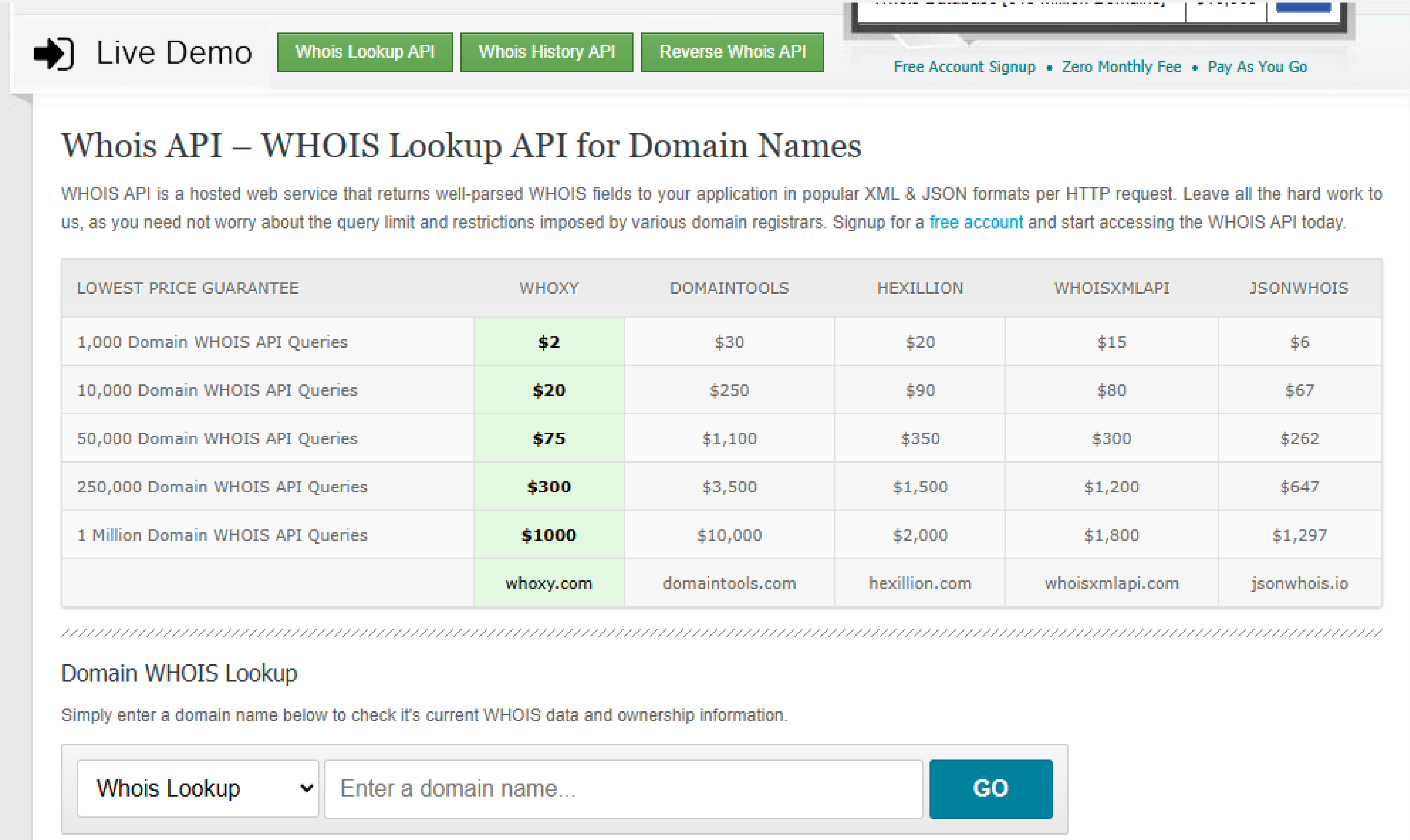
Red Team

Reverse Whois



```
╭─ek1l@EK1L ~/DomLink ‹master›
╰─$ python domLink.py -D it-eam.com -o target.out.txt

DomLink Domain Discovery Tool
Author: Vincent Yiu (@vysecurity)
Contributors: Jan Rude (@whoot); John Bond (@b4ldr)
https://www.github.com/vysec/DomLink
Version: 0.2

ERROR:root:Could not find 'domLink.cfg' and no API key was defined.
```

[vysecurity/DomLink: A tool to link a domain with registered organisation names and emails, to other domains.]



Whois API – WHOIS Lookup API for Domain Names

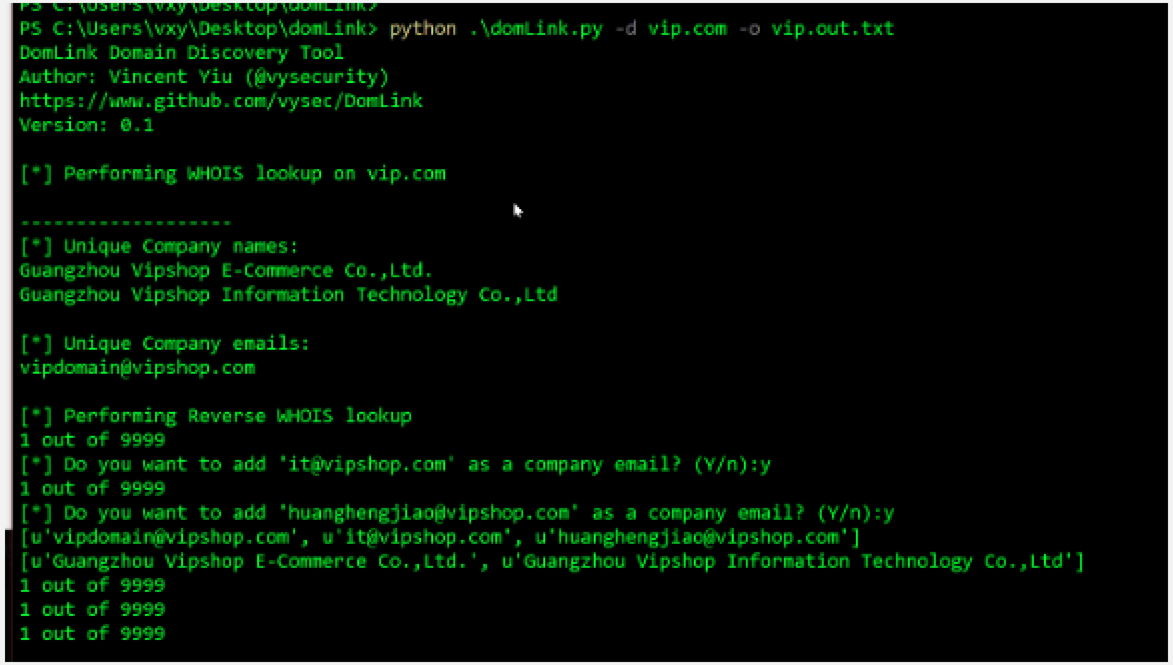
WHOIS API is a hosted web service that returns well-parsed WHOIS fields to your application in popular XML & JSON formats per HTTP request. Leave all the hard work to us, as you need not worry about the query limit and restrictions imposed by various domain registrars. Signup for a free account and start accessing the WHOIS API today.

LOWEST PRICE GUARANTEE	WHOXY	DOMAINTOOLS	HEXILLION	WHOISXMLAPI	JSONWHOIS
1,000 Domain WHOIS API Queries	**$2**	$30	$20	$15	$6
10,000 Domain WHOIS API Queries	**$20**	$250	$90	$80	$67
50,000 Domain WHOIS API Queries	**$75**	$1,100	$350	$300	$262
250,000 Domain WHOIS API Queries	**$300**	$3,500	$1,500	$1,200	$647
1 Million Domain WHOIS API Queries	**$1000**	$10,000	$2,000	$1,800	$1,297
	whoxy.com	domaintools.com	hexillion.com	whoisxmlapi.com	jsonwhois.io

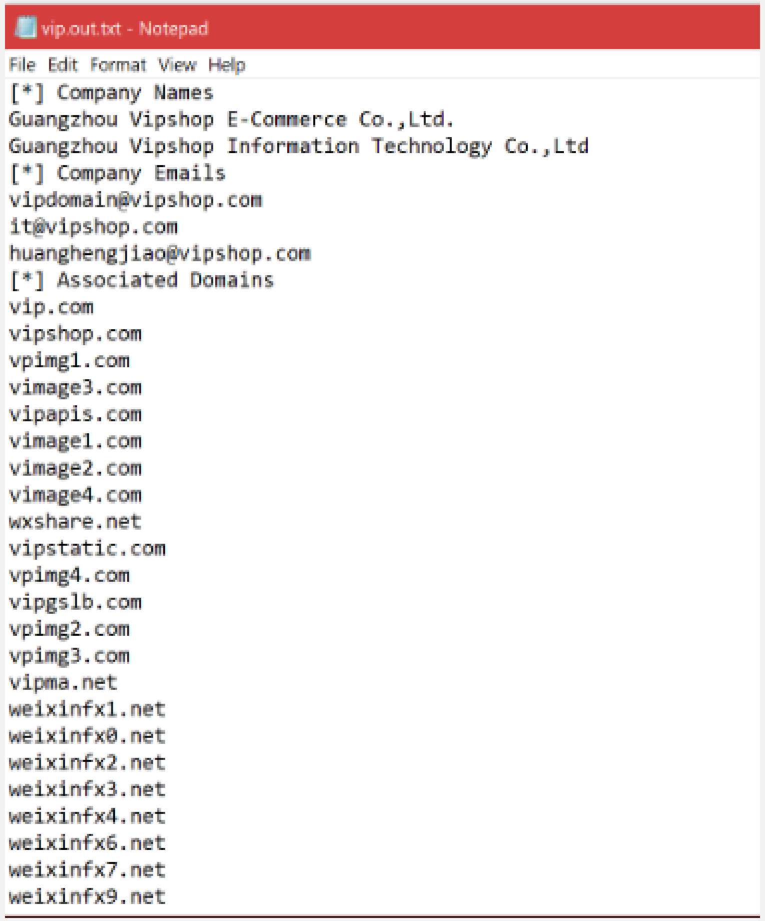
Domain WHOIS Lookup

Simply enter a domain name below to check it's current WHOIS data and ownership information.

Reverse Whois

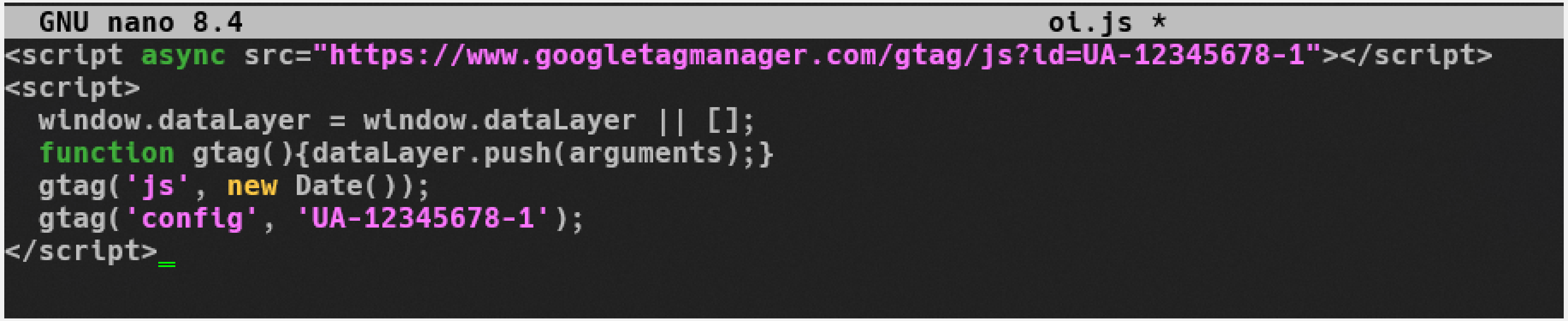


```
PS C:\Users\vxy\Desktop\domLink>
PS C:\Users\vxy\Desktop\domLink> python .\domLink.py -d vip.com -o vip.out.txt
DomLink Domain Discovery Tool
Author: Vincent Yiu (@vysecurity)
https://www.github.com/vysec/DomLink
Version: 0.1

[*] Performing WHOIS lookup on vip.com

-------------------
[*] Unique Company names:
Guangzhou Vipshop E-Commerce Co.,Ltd.
Guangzhou Vipshop Information Technology Co.,Ltd

[*] Unique Company emails:
vipdomain@vipshop.com

[*] Performing Reverse WHOIS lookup
1 out of 9999
[*] Do you want to add 'it@vipshop.com' as a company email? (Y/n):y
1 out of 9999
[*] Do you want to add 'huanghengjiao@vipshop.com' as a company email? (Y/n):y
[u'vipdomain@vipshop.com', u'it@vipshop.com', u'huanghengjiao@vipshop.com']
[u'Guangzhou Vipshop E-Commerce Co.,Ltd.', u'Guangzhou Vipshop Information Technology Co.,Ltd']
1 out of 9999
1 out of 9999
1 out of 9999
```

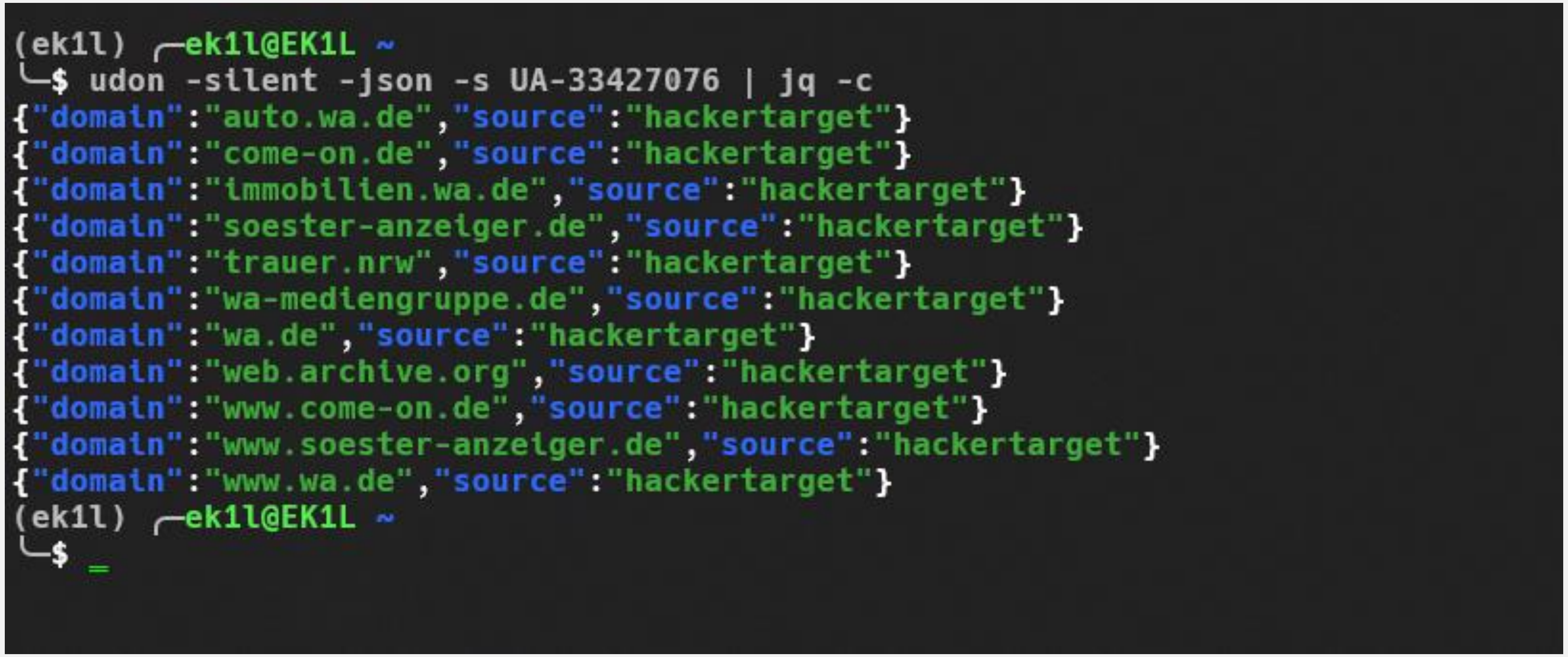


```
[*] Company Names
Guangzhou Vipshop E-Commerce Co.,Ltd.
Guangzhou Vipshop Information Technology Co.,Ltd
[*] Company Emails
vipdomain@vipshop.com
it@vipshop.com
huanghengjiao@vipshop.com
[*] Associated Domains
vip.com
vipshop.com
vpimg1.com
vimage3.com
vipapis.com
vimage1.com
vimage2.com
vimage4.com
wxshare.net
vipstatic.com
vpimg4.com
vipgslb.com
vpimg2.com
vpimg3.com
vipma.net
weixinfx1.net
weixinfx0.net
weixinfx2.net
weixinfx3.net
weixinfx4.net
weixinfx6.net
weixinfx7.net
weixinfx9.net
```

Trackers



```
  GNU nano 8.4                                            oi.js *
<script async src="https://www.googletagmanager.com/gtag/js?id=UA-12345678-1"></script>
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());
  gtag('config', 'UA-12345678-1');
</script>
```



```
(ek1l) ┌─ek1l@EK1L ~
└─$ udon -silent -json -s UA-33427076 | jq -c
{"domain":"auto.wa.de","source":"hackertarget"}
{"domain":"come-on.de","source":"hackertarget"}
{"domain":"immobilien.wa.de","source":"hackertarget"}
{"domain":"soester-anzeiger.de","source":"hackertarget"}
{"domain":"trauer.nrw","source":"hackertarget"}
{"domain":"wa-mediengruppe.de","source":"hackertarget"}
{"domain":"wa.de","source":"hackertarget"}
{"domain":"web.archive.org","source":"hackertarget"}
{"domain":"www.come-on.de","source":"hackertarget"}
{"domain":"www.soester-anzeiger.de","source":"hackertarget"}
{"domain":"www.wa.de","source":"hackertarget"}
(ek1l) ┌─ek1l@EK1L ~
└─$
```

dhn/udon: A simple tool that helps to find assets/domains based on the Google Analytics ID.

Trackers

- Udon

→ Descobre domínios que compartilham o mesmo UA-ID (Google Analytics antigo).
Ideal para OSINT, mapeamento de superfície e reconhecimento em bug bounties.

- BuiltWith

→ Ferramenta de fingerprinting que mostra tecnologias usadas por sites, incluindo Google Analytics IDs.

- SiteSleuth

→ Realiza correlação entre domínios com base em identificadores como Google Analytics, IP, DNS etc.

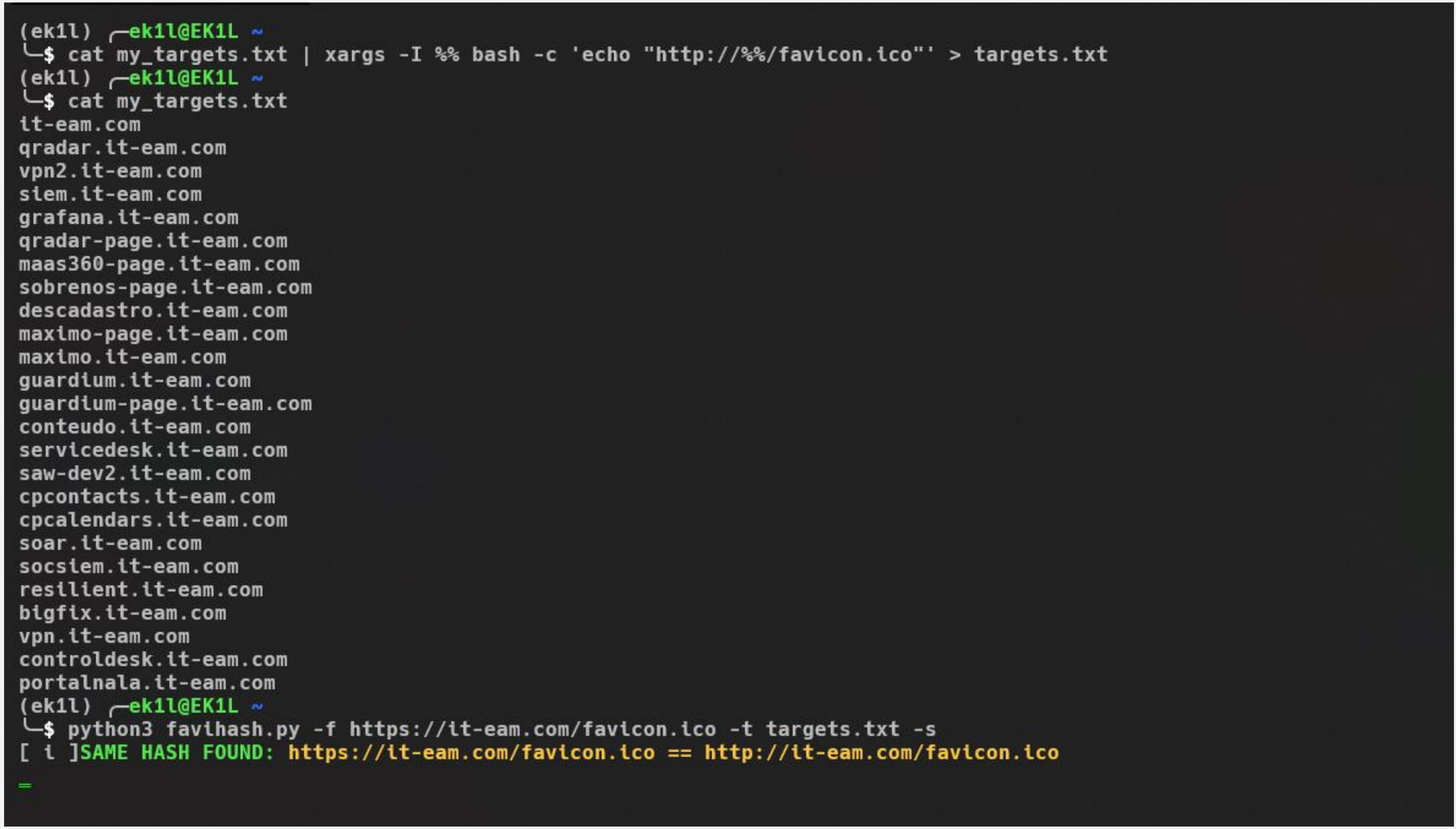
- PublicWWW

→ Motor de busca em código-fonte HTML. Pesquise por trechos como "UA-12345678" para encontrar sites com o mesmo ID.

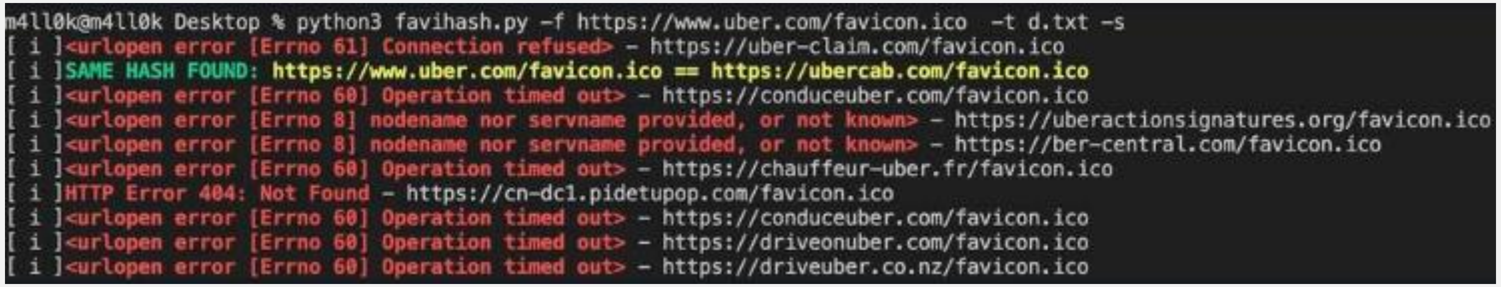
- SpyOnWeb

→ Fornece relacionamentos entre domínios com base em Google Analytics, AdSense e IP compartilhado.

Trackers



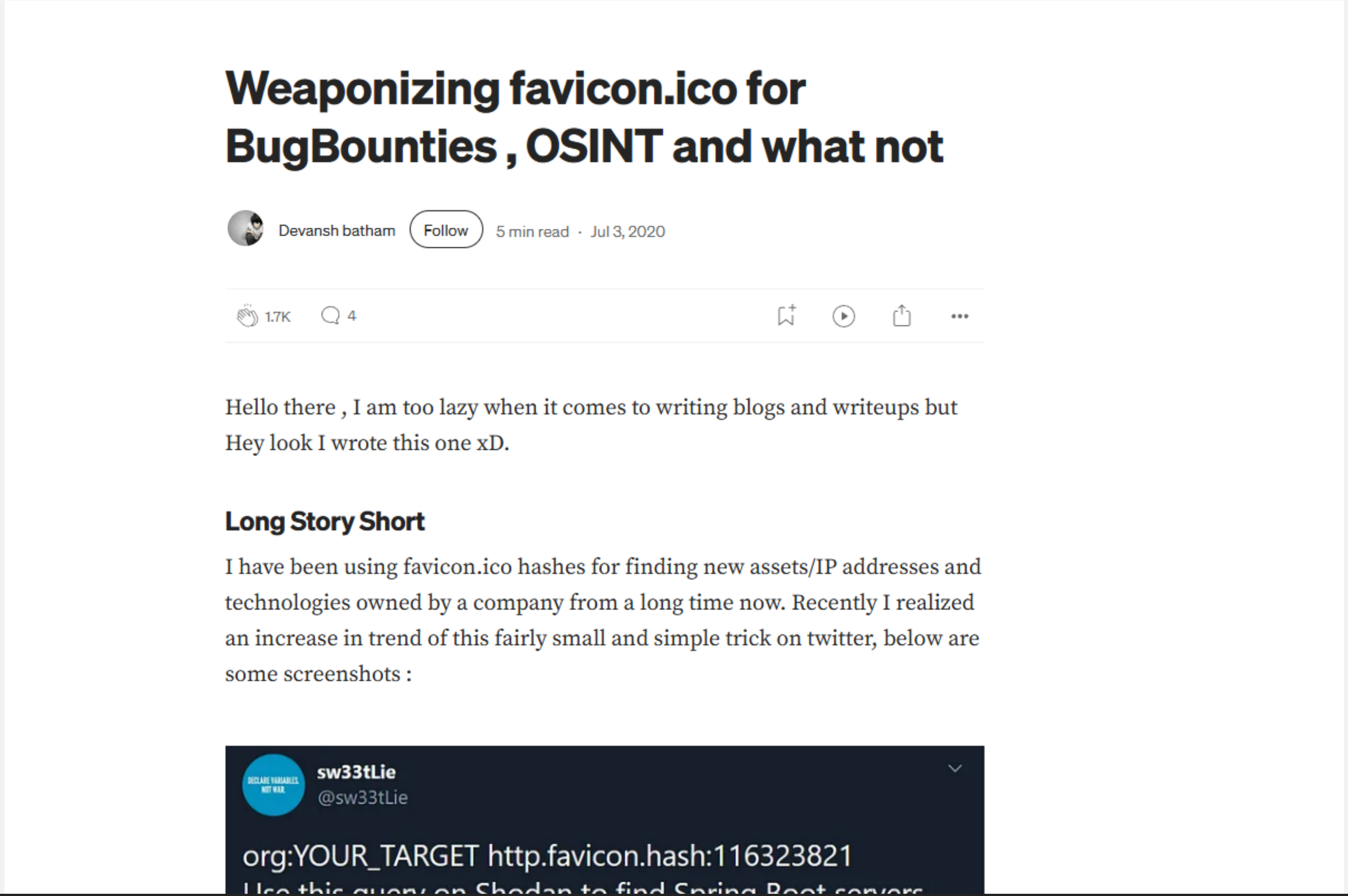
```
(ek1l) ┌─ek1l@EK1L ~
└─$ cat my_targets.txt | xargs -I %% bash -c 'echo "http://%%/favicon.ico"' > targets.txt
(ek1l) ┌─ek1l@EK1L ~
└─$ cat my_targets.txt
it-eam.com
qradar.it-eam.com
vpn2.it-eam.com
siem.it-eam.com
grafana.it-eam.com
qradar-page.it-eam.com
maas360-page.it-eam.com
sobrenos-page.it-eam.com
descadastro.it-eam.com
maximo-page.it-eam.com
maximo.it-eam.com
guardium.it-eam.com
guardium-page.it-eam.com
conteudo.it-eam.com
servicedesk.it-eam.com
saw-dev2.it-eam.com
cpcontacts.it-eam.com
cpcalendars.it-eam.com
soar.it-eam.com
socsiem.it-eam.com
resilient.it-eam.com
bigfix.it-eam.com
vpn.it-eam.com
controldesk.it-eam.com
portalnala.it-eam.com
(ek1l) ┌─ek1l@EK1L ~
└─$ python3 favihash.py -f https://it-eam.com/favicon.ico -t targets.txt -s
[ i ]SAME HASH FOUND: https://it-eam.com/favicon.ico == http://it-eam.com/favicon.ico
```



```
m4ll0k@m4ll0k Desktop % python3 favihash.py -f https://www.uber.com/favicon.ico  -t d.txt -s
[ i ]<urlopen error [Errno 61] Connection refused> - https://uber-claim.com/favicon.ico
[ i ]SAME HASH FOUND: https://www.uber.com/favicon.ico == https://ubercab.com/favicon.ico
[ i ]<urlopen error [Errno 60] Operation timed out> - https://conduceuber.com/favicon.ico
[ i ]<urlopen error [Errno 8] nodename nor servname provided, or not known> - https://uberactionsignatures.org/favicon.ico
[ i ]<urlopen error [Errno 8] nodename nor servname provided, or not known> - https://ber-central.com/favicon.ico
[ i ]<urlopen error [Errno 60] Operation timed out> - https://chauffeur-uber.fr/favicon.ico
[ i ]HTTP Error 404: Not Found - https://cn-dc1.pidetupop.com/favicon.ico
[ i ]<urlopen error [Errno 60] Operation timed out> - https://conduceuber.com/favicon.ico
[ i ]<urlopen error [Errno 60] Operation timed out> - https://driveonuber.com/favicon.ico
[ i ]<urlopen error [Errno 60] Operation timed out> - https://driveuber.co.nz/favicon.ico
```

Red Team

Trackers



Weaponizing favicon.ico for BugBounties , OSINT and what not

Devansh batham Follow 5 min read · Jul 3, 2020

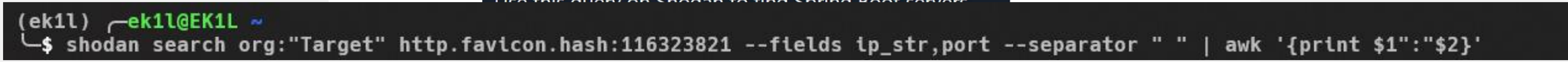
Hello there , I am too lazy when it comes to writing blogs and writeups but Hey look I wrote this one xD.

Long Story Short

I have been using favicon.ico hashes for finding new assets/IP addresses and technologies owned by a company from a long time now. Recently I realized an increase in trend of this fairly small and simple trick on twitter, below are some screenshots :

sw33tLie
@sw33tLie

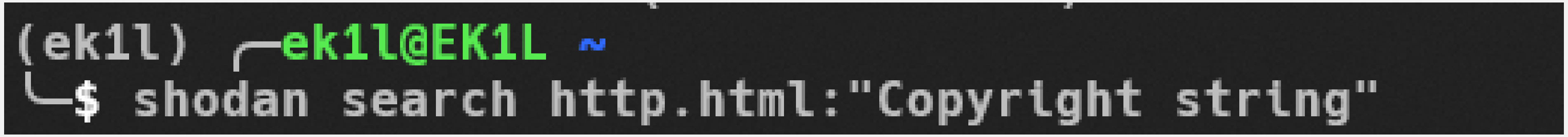
org:YOUR_TARGET http.favicon.hash:116323821
Use this query on Shodan to find Spring Boot servers



```
(ek1l) ┌─ek1l@EK1L ~
└─$ shodan search org:"Target" http.favicon.hash:116323821 --fields ip_str,port --separator " " | awk '{print $1":"$2}'
```

Weaponizing favicon.ico for BugBounties , OSINT and what not | by Devansh batham | Medium

Trackers

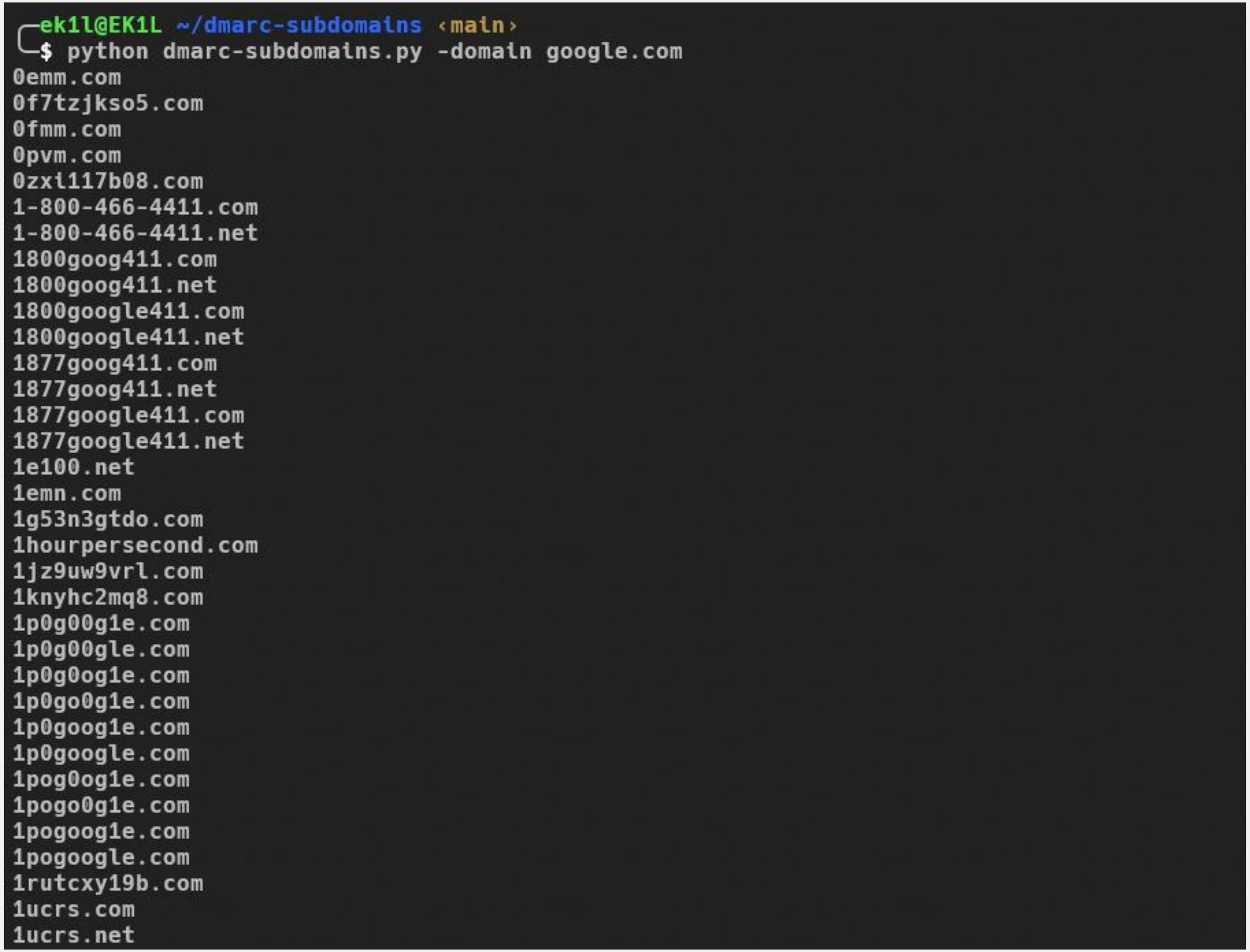


```
(ek1l) ┌─ek1l@EK1L ~
└─$ shodan search http.html:"Copyright string"
```

Information DMARC

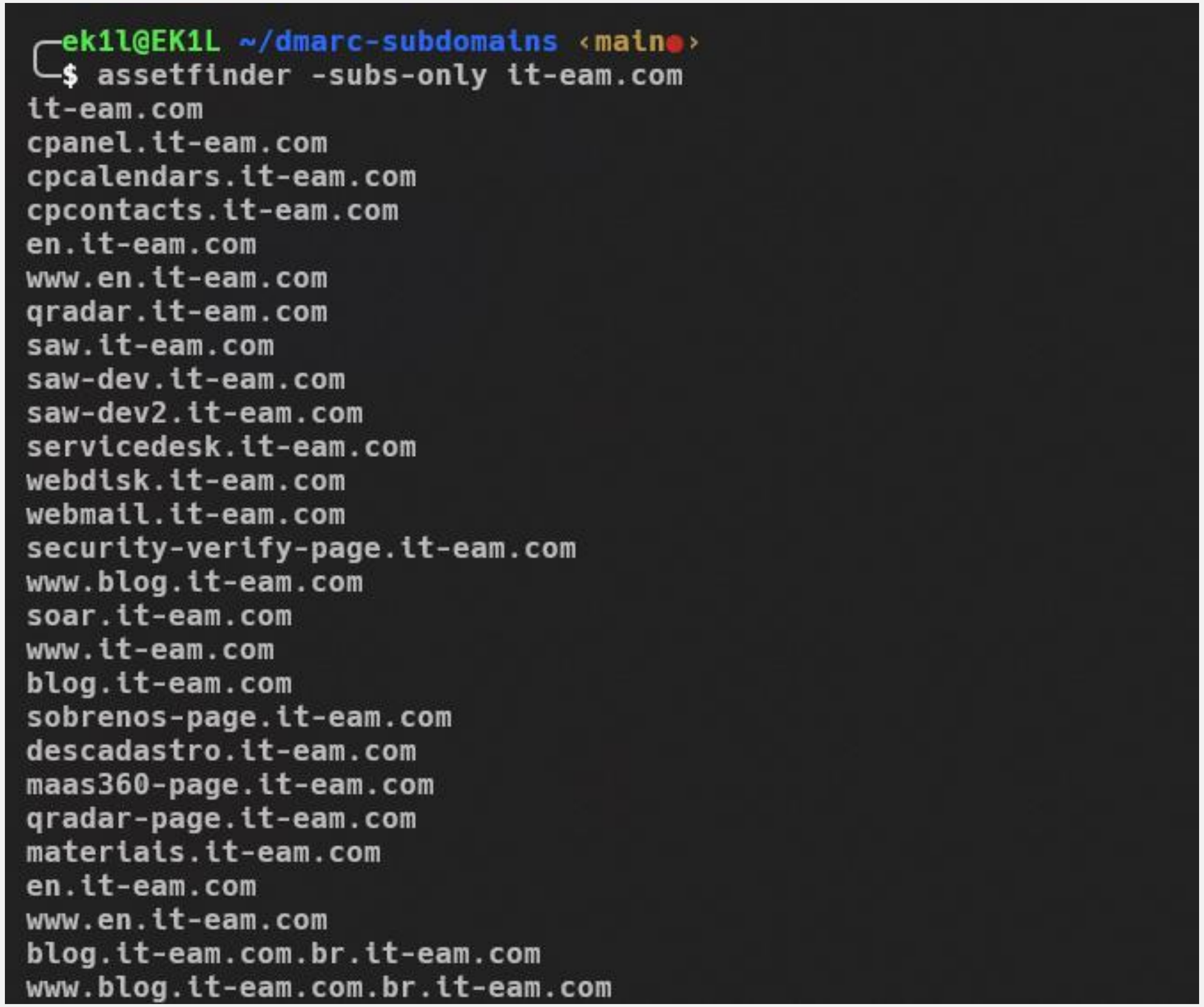
Tedixx/dmarc-subdomains: Tool to parse subdomains from dmarc.live

- Consultará os **registros DNS** para o domínio google.com.
- Procurará o **registro DMARC** para esse domínio.
- Verificará se há subdomínios configurados no registro DMARC.



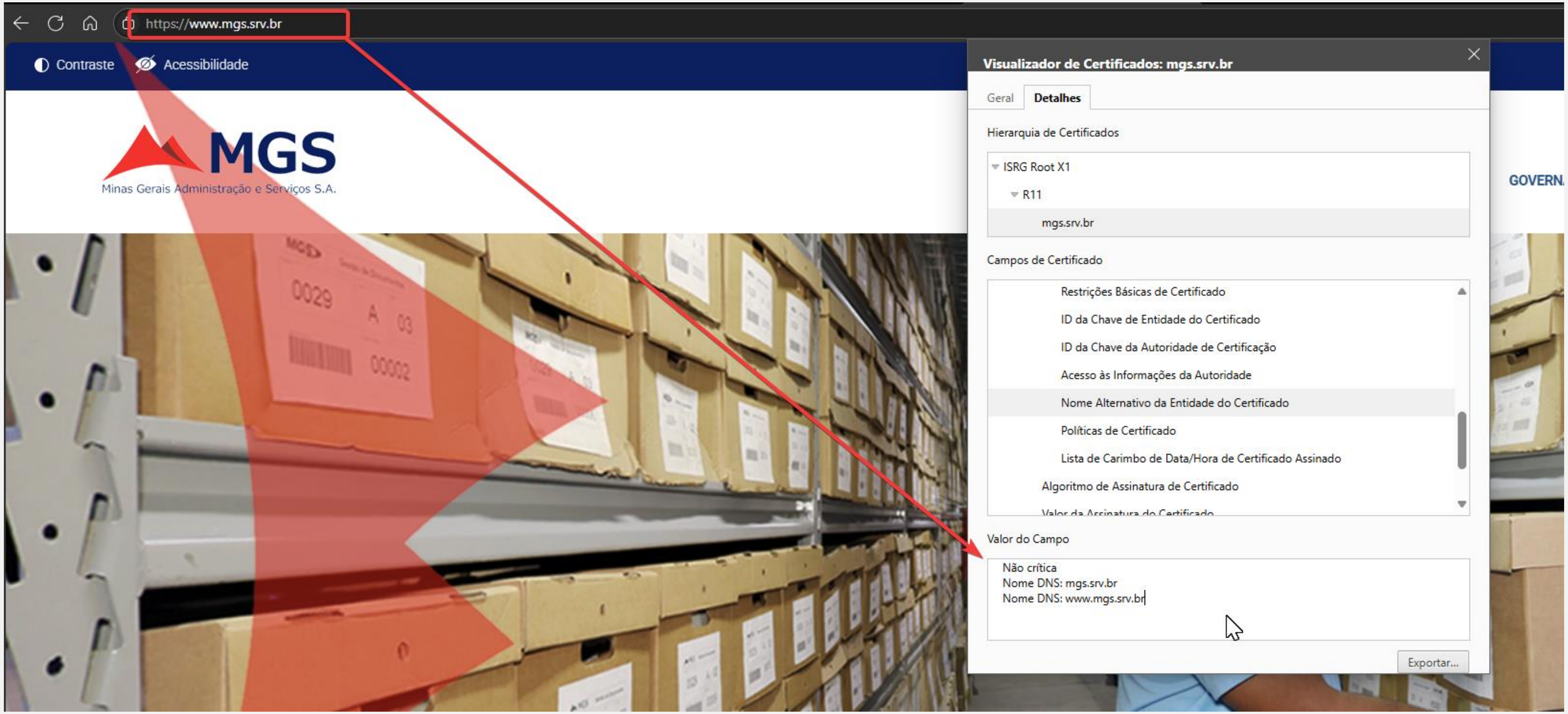
```
┌─ek1l@EK1L ~/dmarc-subdomains ‹main›
└─$ python dmarc-subdomains.py -domain google.com
0emm.com
0f7tzjkso5.com
0fmm.com
0pvm.com
0zxi117b08.com
1-800-466-4411.com
1-800-466-4411.net
1800goog411.com
1800goog411.net
1800google411.com
1800google411.net
1877goog411.com
1877goog411.net
1877google411.com
1877google411.net
1e100.net
1emn.com
1g53n3gtdo.com
1hourpersecond.com
1jz9uw9vrl.com
1knyhc2mq8.com
1p0g00g1e.com
1p0g00gle.com
1p0g0og1e.com
1p0go0g1e.com
1p0goog1e.com
1p0google.com
1pog0og1e.com
1pogo0g1e.com
1pogoog1e.com
1pogoogle.com
1rutcxy19b.com
1ucrs.com
1ucrs.net
```

Certificate SSL



```
╭─ek1l@EK1L ~/dmarc-subdomains ‹main●›
╰─$ assetfinder -subs-only it-eam.com
it-eam.com
cpanel.it-eam.com
cpcalendars.it-eam.com
cpcontacts.it-eam.com
en.it-eam.com
www.en.it-eam.com
qradar.it-eam.com
saw.it-eam.com
saw-dev.it-eam.com
saw-dev2.it-eam.com
servicedesk.it-eam.com
webdisk.it-eam.com
webmail.it-eam.com
security-verify-page.it-eam.com
www.blog.it-eam.com
soar.it-eam.com
www.it-eam.com
blog.it-eam.com
sobrenos-page.it-eam.com
descadastro.it-eam.com
maas360-page.it-eam.com
qradar-page.it-eam.com
materials.it-eam.com
en.it-eam.com
www.en.it-eam.com
blog.it-eam.com.br.it-eam.com
www.blog.it-eam.com.br.it-eam.com
```

Certificate SSL



Visualizador de Certificados: mgs.srv.br

Hierarquia de Certificados

- ISRG Root X1
  - R11
    - mgs.srv.br

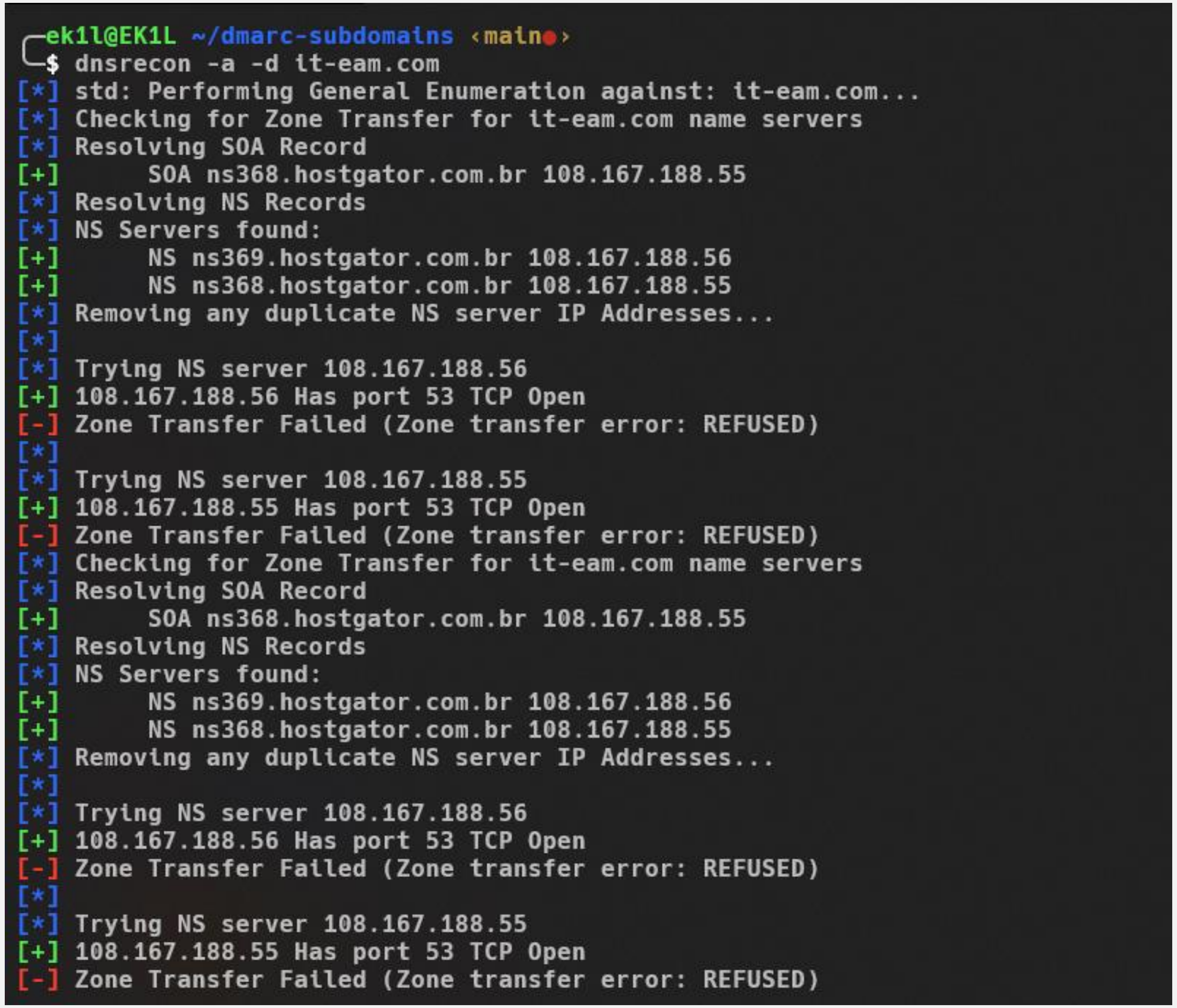
Campos de Certificado

- Restrições Básicas de Certificado
- ID da Chave de Entidade do Certificado
- ID da Chave da Autoridade de Certificação
- Acesso às Informações da Autoridade
- Nome Alternativo da Entidade do Certificado
- Políticas de Certificado
- Lista de Carimbo de Data/Hora de Certificado Assinado
- Algoritmo de Assinatura de Certificado
- Valor da Assinatura do Certificado

Valor do Campo

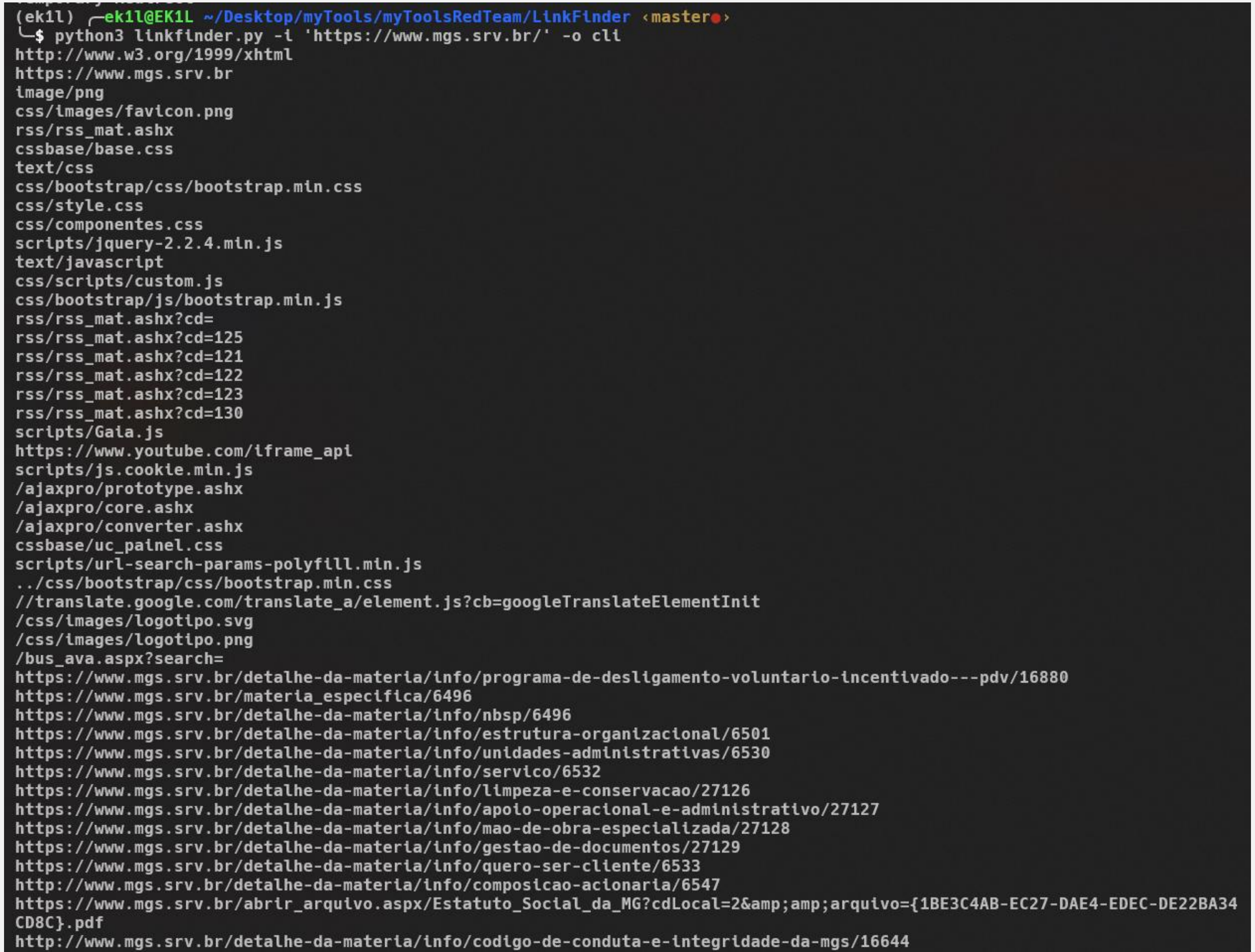
```
Não crítica
Nome DNS: mgs.srv.br
Nome DNS: www.mgs.srv.br
```

Zone Transfer



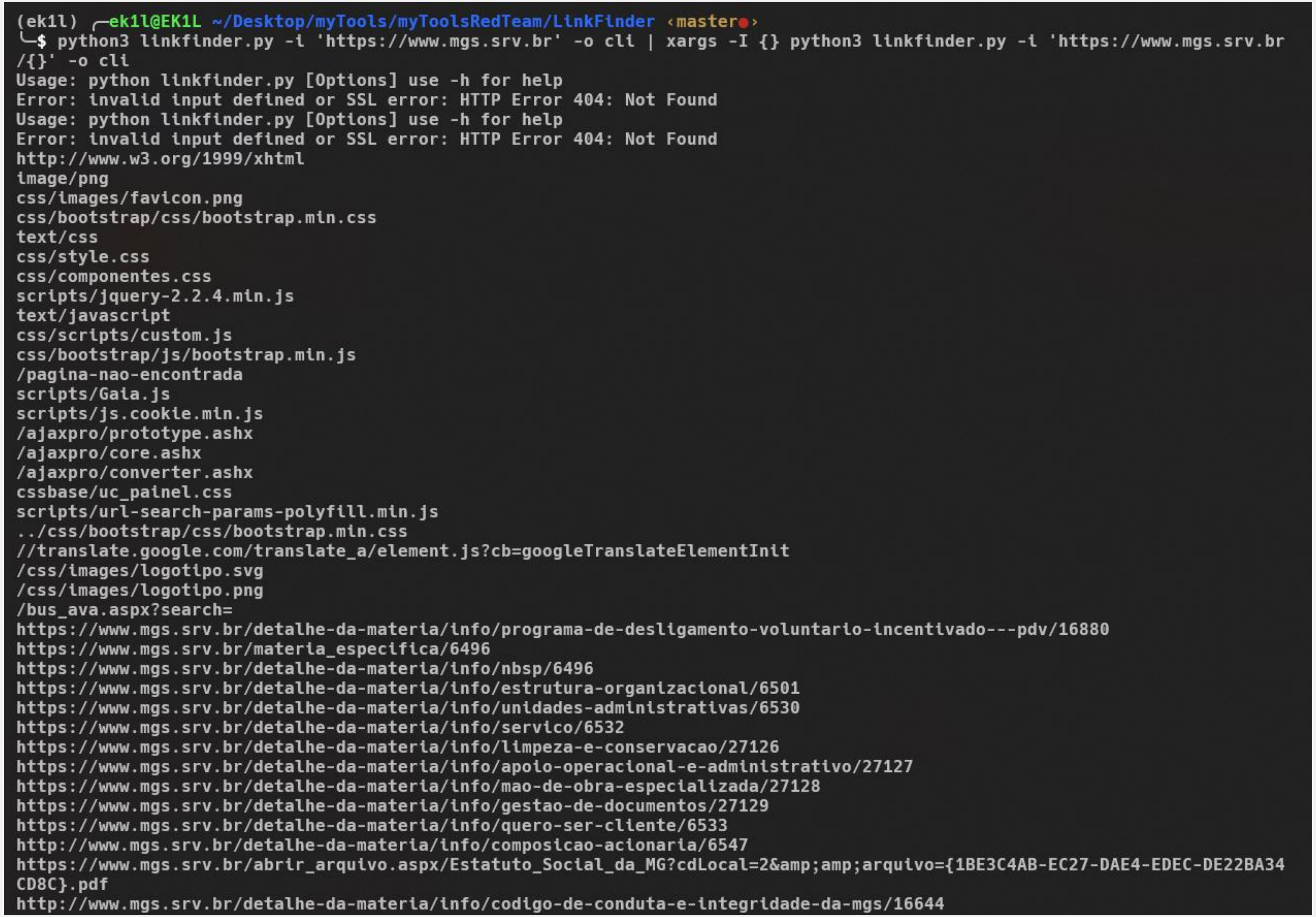
```
┌─ek1l@EK1L ~/dmarc-subdomains ‹main●›
└─$ dnsrecon -a -d it-eam.com
[*] std: Performing General Enumeration against: it-eam.com...
[*] Checking for Zone Transfer for it-eam.com name servers
[*] Resolving SOA Record
[+]      SOA ns368.hostgator.com.br 108.167.188.55
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS ns369.hostgator.com.br 108.167.188.56
[+]      NS ns368.hostgator.com.br 108.167.188.55
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 108.167.188.56
[+] 108.167.188.56 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 108.167.188.55
[+] 108.167.188.55 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*] Checking for Zone Transfer for it-eam.com name servers
[*] Resolving SOA Record
[+]      SOA ns368.hostgator.com.br 108.167.188.55
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS ns369.hostgator.com.br 108.167.188.56
[+]      NS ns368.hostgator.com.br 108.167.188.55
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 108.167.188.56
[+] 108.167.188.56 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 108.167.188.55
[+] 108.167.188.55 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
```

Automating Processes



```
(ek1l) ┌─ek1l@EK1L ~/Desktop/myTools/myToolsRedTeam/LinkFinder ‹master●›
└─$ python3 linkfinder.py -i 'https://www.mgs.srv.br/' -o cli
http://www.w3.org/1999/xhtml
https://www.mgs.srv.br
image/png
css/images/favicon.png
rss/rss_mat.ashx
cssbase/base.css
text/css
css/bootstrap/css/bootstrap.min.css
css/style.css
css/componentes.css
scripts/jquery-2.2.4.min.js
text/javascript
css/scripts/custom.js
css/bootstrap/js/bootstrap.min.js
rss/rss_mat.ashx?cd=
rss/rss_mat.ashx?cd=125
rss/rss_mat.ashx?cd=121
rss/rss_mat.ashx?cd=122
rss/rss_mat.ashx?cd=123
rss/rss_mat.ashx?cd=130
scripts/Gaia.js
https://www.youtube.com/iframe_api
scripts/js.cookie.min.js
/ajaxpro/prototype.ashx
/ajaxpro/core.ashx
/ajaxpro/converter.ashx
cssbase/uc_painel.css
scripts/url-search-params-polyfill.min.js
../css/bootstrap/css/bootstrap.min.css
//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit
/css/images/logotipo.svg
/css/images/logotipo.png
/bus_ava.aspx?search=
https://www.mgs.srv.br/detalhe-da-materia/info/programa-de-desligamento-voluntario-incentivado---pdv/16880
https://www.mgs.srv.br/materia_especifica/6496
https://www.mgs.srv.br/detalhe-da-materia/info/nbsp/6496
https://www.mgs.srv.br/detalhe-da-materia/info/estrutura-organizacional/6501
https://www.mgs.srv.br/detalhe-da-materia/info/unidades-administrativas/6530
https://www.mgs.srv.br/detalhe-da-materia/info/servico/6532
https://www.mgs.srv.br/detalhe-da-materia/info/limpeza-e-conservacao/27126
https://www.mgs.srv.br/detalhe-da-materia/info/apoio-operacional-e-administrativo/27127
https://www.mgs.srv.br/detalhe-da-materia/info/mao-de-obra-especializada/27128
https://www.mgs.srv.br/detalhe-da-materia/info/gestao-de-documentos/27129
https://www.mgs.srv.br/detalhe-da-materia/info/quero-ser-cliente/6533
http://www.mgs.srv.br/detalhe-da-materia/info/composicao-acionaria/6547
https://www.mgs.srv.br/abrir_arquivo.aspx/Estatuto_Social_da_MG?cdLocal=2&amp;amp;arquivo={1BE3C4AB-EC27-DAE4-EDEC-DE22BA34
CD8C}.pdf
http://www.mgs.srv.br/detalhe-da-materia/info/codigo-de-conduta-e-integridade-da-mgs/16644
```

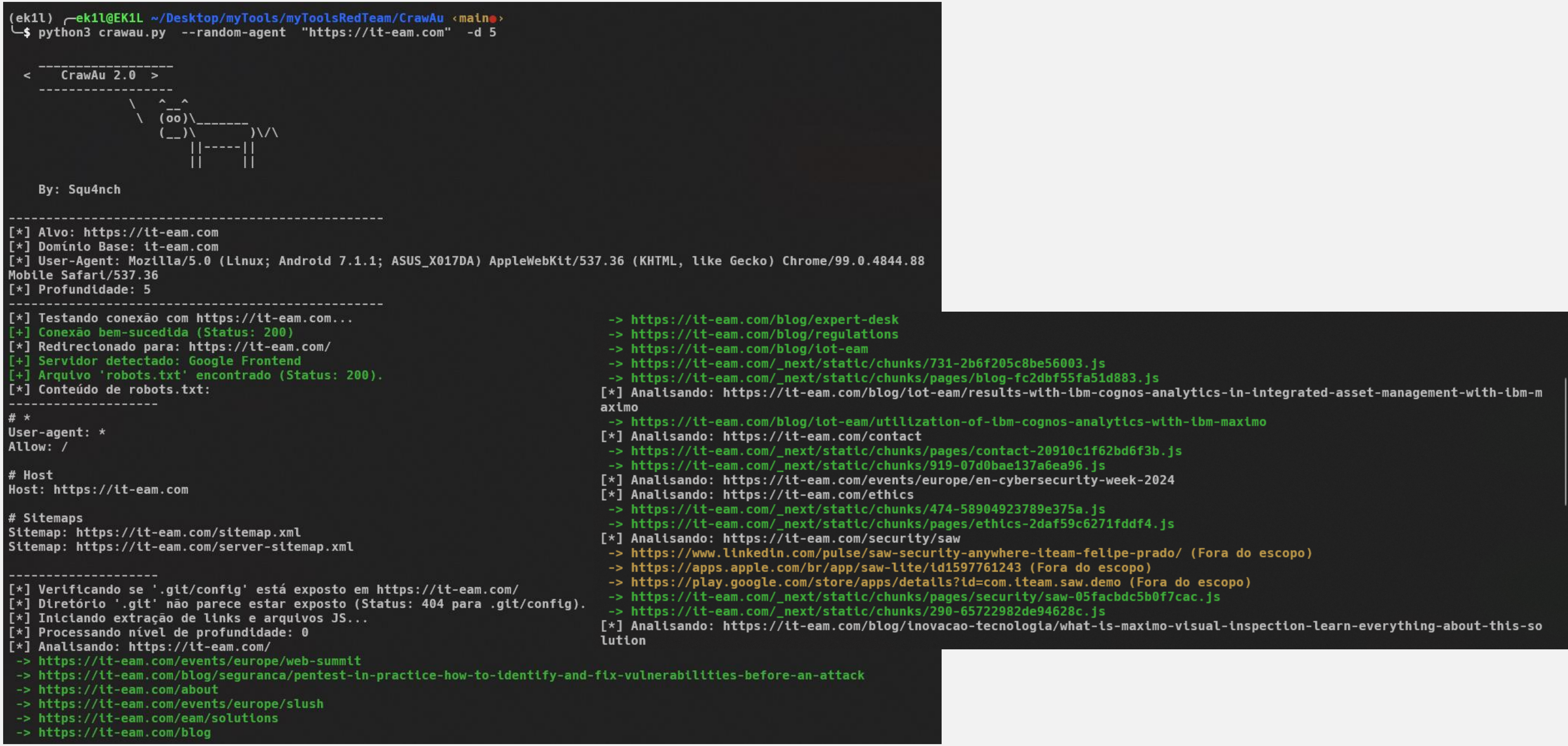
Automating Processes



```
(ek1l) ┌─ek1l@EK1L ~/Desktop/myTools/myToolsRedTeam/LinkFinder ‹master●›
└─$ python3 linkfinder.py -i 'https://www.mgs.srv.br' -o cli | xargs -I {} python3 linkfinder.py -i 'https://www.mgs.srv.br
/{}' -o cli
Usage: python linkfinder.py [Options] use -h for help
Error: invalid input defined or SSL error: HTTP Error 404: Not Found
Usage: python linkfinder.py [Options] use -h for help
Error: invalid input defined or SSL error: HTTP Error 404: Not Found
http://www.w3.org/1999/xhtml
image/png
css/images/favicon.png
css/bootstrap/css/bootstrap.min.css
text/css
css/style.css
css/componentes.css
scripts/jquery-2.2.4.min.js
text/javascript
css/scripts/custom.js
css/bootstrap/js/bootstrap.min.js
/pagina-nao-encontrada
scripts/Gaia.js
scripts/js.cookie.min.js
/ajaxpro/prototype.ashx
/ajaxpro/core.ashx
/ajaxpro/converter.ashx
cssbase/uc_painel.css
scripts/url-search-params-polyfill.min.js
../css/bootstrap/css/bootstrap.min.css
//translate.google.com/translate_a/element.js?cb=googleTranslateElementInit
/css/images/logotipo.svg
/css/images/logotipo.png
/bus_ava.aspx?search=
https://www.mgs.srv.br/detalhe-da-materia/info/programa-de-desligamento-voluntario-incentivado---pdv/16880
https://www.mgs.srv.br/materia_especifica/6496
https://www.mgs.srv.br/detalhe-da-materia/info/nbsp/6496
https://www.mgs.srv.br/detalhe-da-materia/info/estrutura-organizacional/6501
https://www.mgs.srv.br/detalhe-da-materia/info/unidades-administrativas/6530
https://www.mgs.srv.br/detalhe-da-materia/info/servico/6532
https://www.mgs.srv.br/detalhe-da-materia/info/limpeza-e-conservacao/27126
https://www.mgs.srv.br/detalhe-da-materia/info/apoio-operacional-e-administrativo/27127
https://www.mgs.srv.br/detalhe-da-materia/info/mao-de-obra-especializada/27128
https://www.mgs.srv.br/detalhe-da-materia/info/gestao-de-documentos/27129
https://www.mgs.srv.br/detalhe-da-materia/info/quero-ser-cliente/6533
http://www.mgs.srv.br/detalhe-da-materia/info/composicao-acionaria/6547
https://www.mgs.srv.br/abrir_arquivo.aspx/Estatuto_Social_da_MG?cdLocal=2&amp;amp;arquivo={1BE3C4AB-EC27-DAE4-EDEC-DE22BA34
CD8C}.pdf
http://www.mgs.srv.br/detalhe-da-materia/info/codigo-de-conduta-e-integridade-da-mgs/16644
```

Red Team

Automating Processes

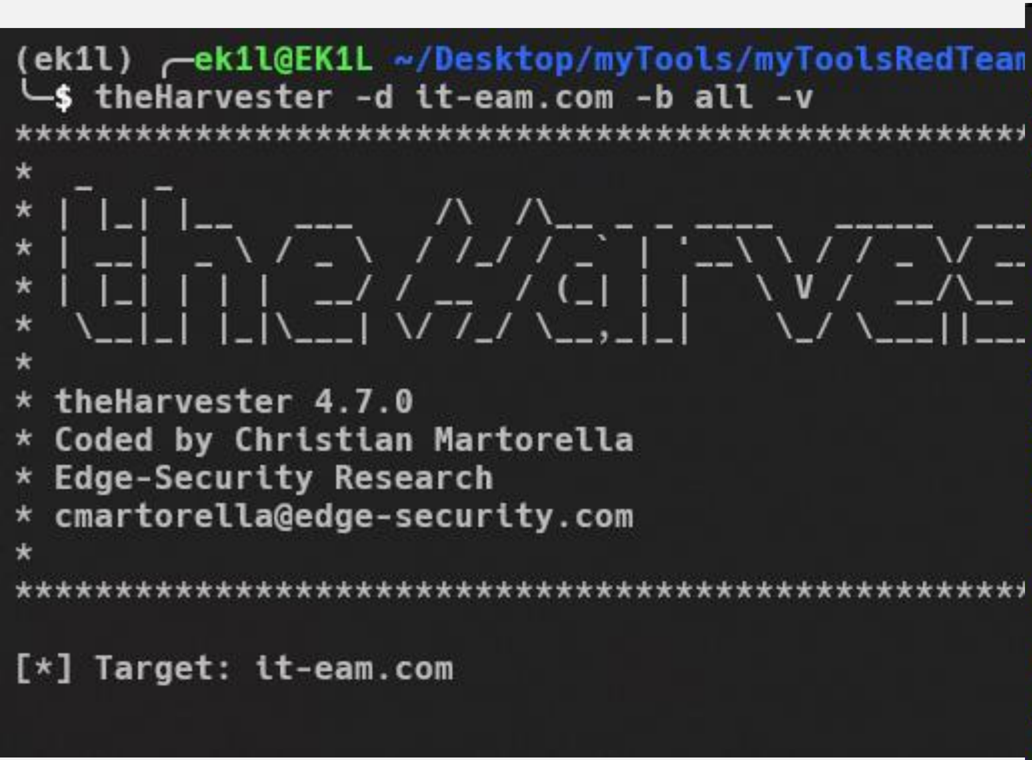


```
(ek1l) ┌─ek1l@EK1L ~/Desktop/myTools/myToolsRedTeam/CrawAu ‹main●›
└─$ python3 crawau.py  --random-agent  "https://it-eam.com"  -d 5


    ------------------
  <    CrawAu 2.0  >
    ------------------
                \   ^__^
                 \  (oo)\_______
                    (__)\       )\/\
                        ||-----||
                        ||     ||


    By: Squ4nch

--------------------------------------------------
[*] Alvo: https://it-eam.com
[*] Domínio Base: it-eam.com
[*] User-Agent: Mozilla/5.0 (Linux; Android 7.1.1; ASUS_X017DA) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.88
Mobile Safari/537.36
[*] Profundidade: 5
--------------------------------------------------
[*] Testando conexão com https://it-eam.com...
[+] Conexão bem-sucedida (Status: 200)
[*] Redirecionado para: https://it-eam.com/
[+] Servidor detectado: Google Frontend
[+] Arquivo 'robots.txt' encontrado (Status: 200).
[*] Conteúdo de robots.txt:
--------------------
# *
User-agent: *
Allow: /

# Host
Host: https://it-eam.com

# Sitemaps
Sitemap: https://it-eam.com/sitemap.xml
Sitemap: https://it-eam.com/server-sitemap.xml

--------------------
[*] Verificando se '.git/config' está exposto em https://it-eam.com/
[*] Diretório '.git' não parece estar exposto (Status: 404 para .git/config).
[*] Iniciando extração de links e arquivos JS...
[*] Processando nível de profundidade: 0
[*] Analisando: https://it-eam.com/
 -> https://it-eam.com/events/europe/web-summit
 -> https://it-eam.com/blog/seguranca/pentest-in-practice-how-to-identify-and-fix-vulnerabilities-before-an-attack
 -> https://it-eam.com/about
 -> https://it-eam.com/events/europe/slush
 -> https://it-eam.com/eam/solutions
 -> https://it-eam.com/blog
```

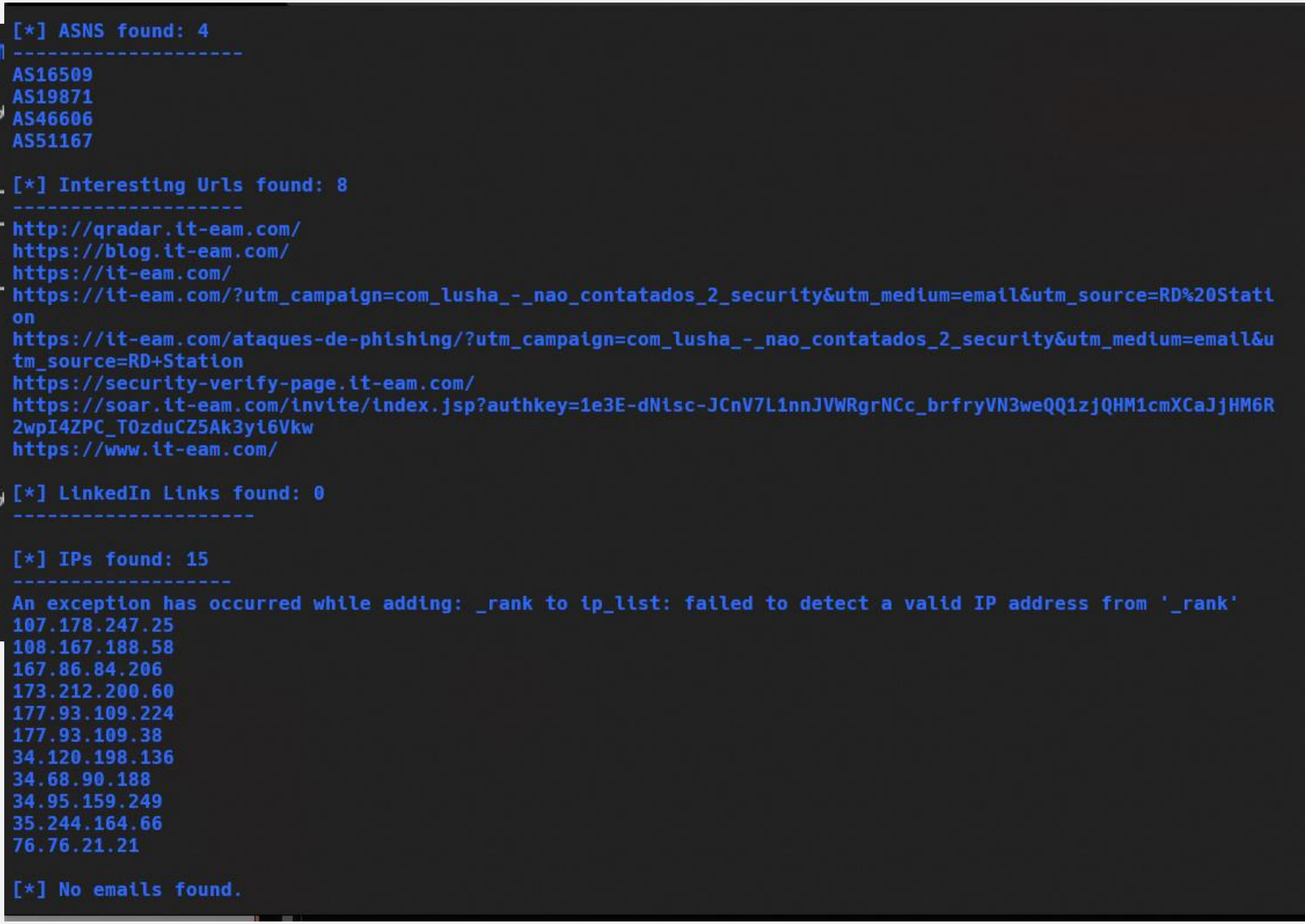
```
 -> https://it-eam.com/blog/expert-desk
 -> https://it-eam.com/blog/regulations
 -> https://it-eam.com/blog/iot-eam
 -> https://it-eam.com/_next/static/chunks/731-2b6f205c8be56003.js
 -> https://it-eam.com/_next/static/chunks/pages/blog-fc2dbf55fa51d883.js
[*] Analisando: https://it-eam.com/blog/iot-eam/results-with-ibm-cognos-analytics-in-integrated-asset-management-with-ibm-m
aximo
 -> https://it-eam.com/blog/iot-eam/utilization-of-ibm-cognos-analytics-with-ibm-maximo
[*] Analisando: https://it-eam.com/contact
 -> https://it-eam.com/_next/static/chunks/pages/contact-20910c1f62bd6f3b.js
 -> https://it-eam.com/_next/static/chunks/919-07d0bae137a6ea96.js
[*] Analisando: https://it-eam.com/events/europe/en-cybersecurity-week-2024
[*] Analisando: https://it-eam.com/ethics
 -> https://it-eam.com/_next/static/chunks/474-58904923789e375a.js
 -> https://it-eam.com/_next/static/chunks/pages/ethics-2daf59c6271fddf4.js
[*] Analisando: https://it-eam.com/security/saw
 -> https://www.linkedin.com/pulse/saw-security-anywhere-iteam-felipe-prado/ (Fora do escopo)
 -> https://apps.apple.com/br/app/saw-lite/id1597761243 (Fora do escopo)
 -> https://play.google.com/store/apps/details?id=com.iteam.saw.demo (Fora do escopo)
 -> https://it-eam.com/_next/static/chunks/pages/security/saw-05facbdc5b0f7cac.js
 -> https://it-eam.com/_next/static/chunks/290-65722982de94628c.js
[*] Analisando: https://it-eam.com/blog/inovacao-tecnologia/what-is-maximo-visual-inspection-learn-everything-about-this-so
lution
```

Red Team

Automating Processes

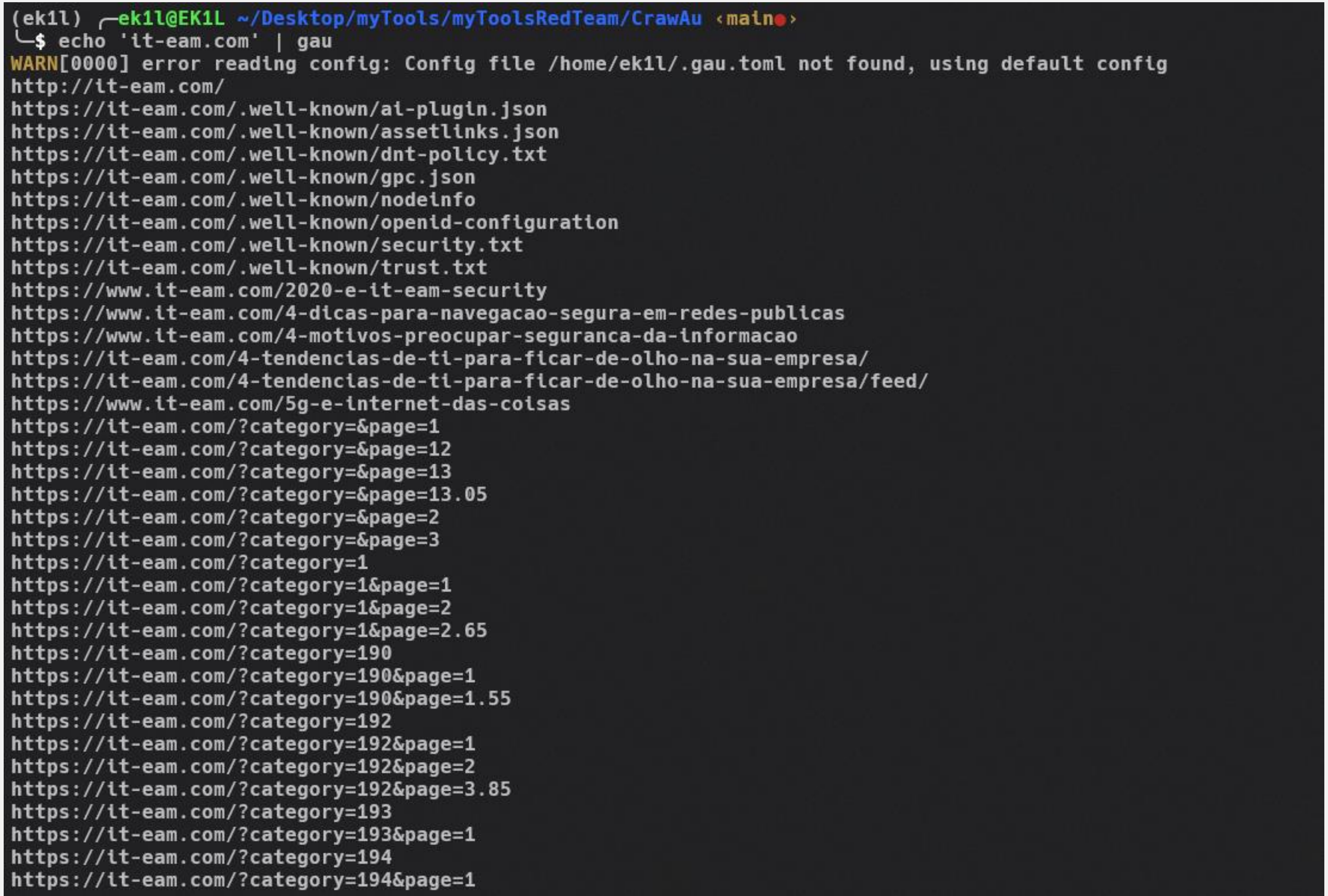


```
(ek1l) ┌─ek1l@EK1L ~/Desktop/myTools/myToolsRedTeam
└─$ theHarvester -d it-eam.com -b all -v
***************************************************
*
*  _   _                                            
* | |_| |__   ___    /\  /\__ _ _ ____   _____ ___
* | __| _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___
*
* theHarvester 4.7.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
***************************************************

[*] Target: it-eam.com
```



```
[*] ASNS found: 4
--------------------
AS16509
AS19871
AS46606
AS51167

[*] Interesting Urls found: 8
--------------------
http://qradar.it-eam.com/
https://blog.it-eam.com/
https://it-eam.com/
https://it-eam.com/?utm_campaign=com_lusha_-_nao_contatados_2_security&utm_medium=email&utm_source=RD%20Stati
on
https://it-eam.com/ataques-de-phishing/?utm_campaign=com_lusha_-_nao_contatados_2_security&utm_medium=email&u
tm_source=RD+Station
https://security-verify-page.it-eam.com/
https://soar.it-eam.com/invite/index.jsp?authkey=1e3E-dNisc-JCnV7L1nnJVWRgrNCc_brfryVN3weQQ1zjQHM1cmXCaJjHM6R
2wpI4ZPC_TOzduCZ5Ak3yi6Vkw
https://www.it-eam.com/

[*] LinkedIn Links found: 0
---------------------

[*] IPs found: 15
-------------------
An exception has occurred while adding: _rank to ip_list: failed to detect a valid IP address from '_rank'
107.178.247.25
108.167.188.58
167.86.84.206
173.212.200.60
177.93.109.224
177.93.109.38
34.120.198.136
34.68.90.188
34.95.159.249
35.244.164.66
76.76.21.21

[*] No emails found.
```

Automating Processes



```
(ek1l) ┌─ek1l@EK1L ~/Desktop/myTools/myToolsRedTeam/CrawAu ‹main●›
└─$ echo 'it-eam.com' | gau
WARN[0000] error reading config: Config file /home/ek1l/.gau.toml not found, using default config
http://it-eam.com/
https://it-eam.com/.well-known/ai-plugin.json
https://it-eam.com/.well-known/assetlinks.json
https://it-eam.com/.well-known/dnt-policy.txt
https://it-eam.com/.well-known/gpc.json
https://it-eam.com/.well-known/nodeinfo
https://it-eam.com/.well-known/openid-configuration
https://it-eam.com/.well-known/security.txt
https://it-eam.com/.well-known/trust.txt
https://www.it-eam.com/2020-e-it-eam-security
https://www.it-eam.com/4-dicas-para-navegacao-segura-em-redes-publicas
https://www.it-eam.com/4-motivos-preocupar-seguranca-da-informacao
https://it-eam.com/4-tendencias-de-ti-para-ficar-de-olho-na-sua-empresa/
https://it-eam.com/4-tendencias-de-ti-para-ficar-de-olho-na-sua-empresa/feed/
https://www.it-eam.com/5g-e-internet-das-coisas
https://it-eam.com/?category=&page=1
https://it-eam.com/?category=&page=12
https://it-eam.com/?category=&page=13
https://it-eam.com/?category=&page=13.05
https://it-eam.com/?category=&page=2
https://it-eam.com/?category=&page=3
https://it-eam.com/?category=1
https://it-eam.com/?category=1&page=1
https://it-eam.com/?category=1&page=2
https://it-eam.com/?category=1&page=2.65
https://it-eam.com/?category=190
https://it-eam.com/?category=190&page=1
https://it-eam.com/?category=190&page=1.55
https://it-eam.com/?category=192
https://it-eam.com/?category=192&page=1
https://it-eam.com/?category=192&page=2
https://it-eam.com/?category=192&page=3.85
https://it-eam.com/?category=193
https://it-eam.com/?category=193&page=1
https://it-eam.com/?category=194
https://it-eam.com/?category=194&page=1
```

Brute Force DNS

Fontes para Listas de Subdomínios e DNS

1. Listas de Subdomínios

- Best DNS Wordlist (Assetnote)
- Subdomain Bruteforce List (localdomain.pw)

Ferramentas e Repositórios Úteis

2. Ferramentas e Repositórios no GitHub

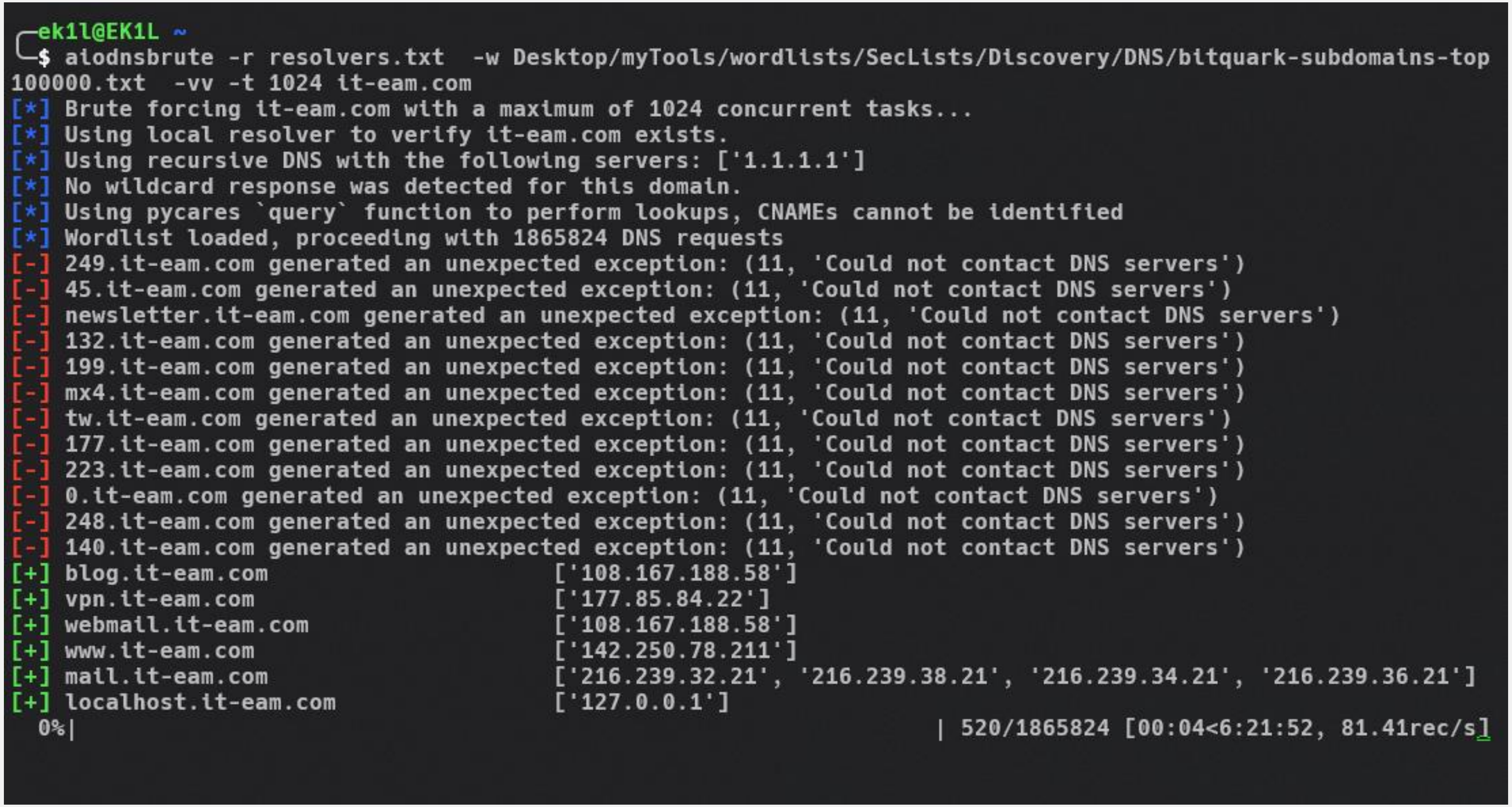
- Commonspeak
- SecLists (DNS Discovery)

Gists e Scripts para Pentest

3. Gist de Pentest

- Gist de JHaddix

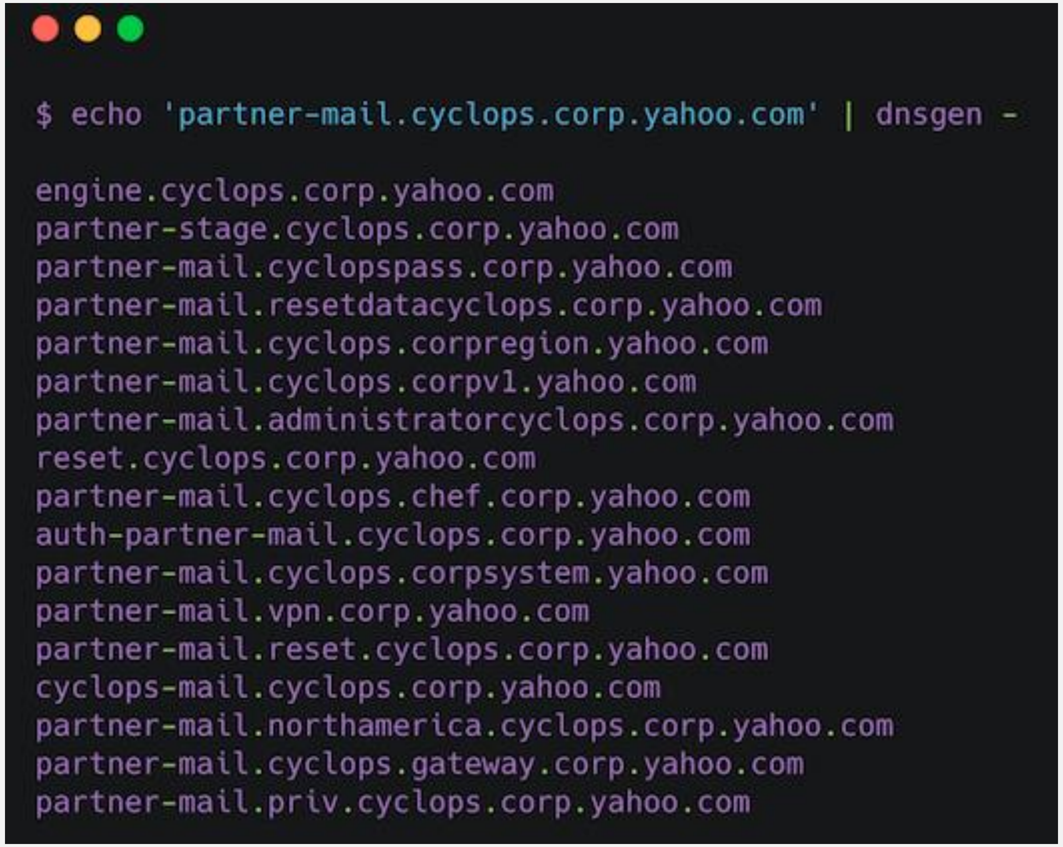
Brute Force DNS



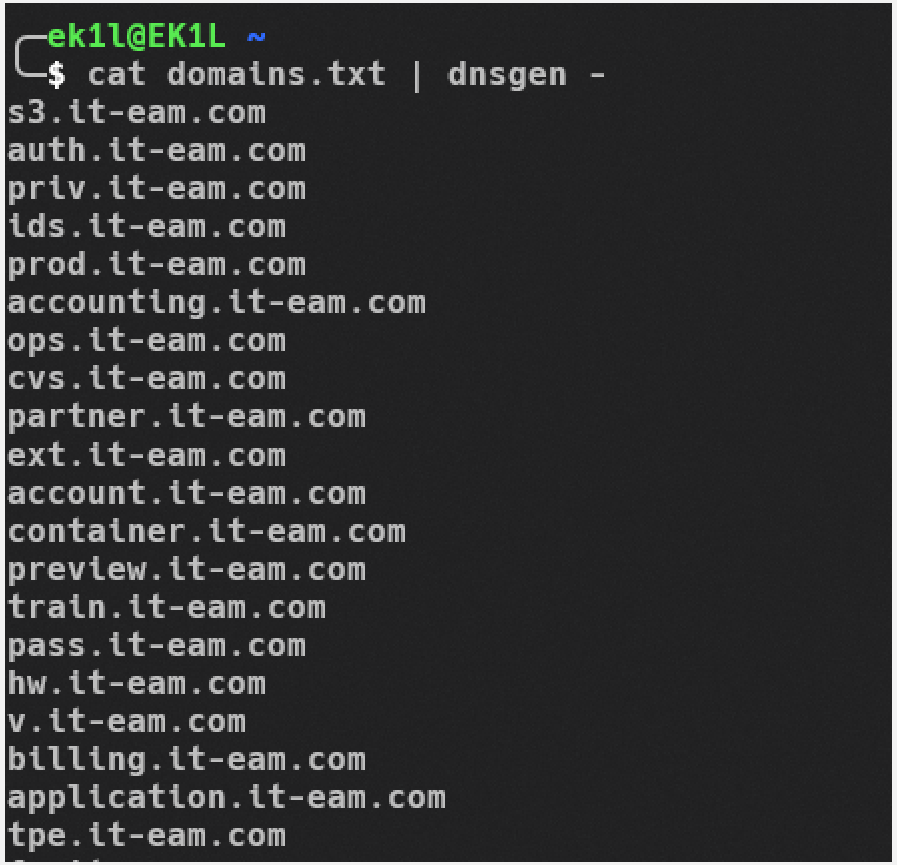
```
┌─ek1l@EK1L ~
└─$ aiodnsbrute -r resolvers.txt  -w Desktop/myTools/wordlists/SecLists/Discovery/DNS/bitquark-subdomains-top
100000.txt  -vv -t 1024 it-eam.com
[*] Brute forcing it-eam.com with a maximum of 1024 concurrent tasks...
[*] Using local resolver to verify it-eam.com exists.
[*] Using recursive DNS with the following servers: ['1.1.1.1']
[*] No wildcard response was detected for this domain.
[*] Using pycares `query` function to perform lookups, CNAMEs cannot be identified
[*] Wordlist loaded, proceeding with 1865824 DNS requests
[-] 249.it-eam.com generated an unexpected exception: (11, 'Could not contact DNS servers')
[-] 45.it-eam.com generated an unexpected exception: (11, 'Could not contact DNS servers')
[-] newsletter.it-eam.com generated an unexpected exception: (11, 'Could not contact DNS servers')
[-] 132.it-eam.com generated an unexpected exception: (11, 'Could not contact DNS servers')
[-] 199.it-eam.com generated an unexpected exception: (11, 'Could not contact DNS servers')
[-] mx4.it-eam.com generated an unexpected exception: (11, 'Could not contact DNS servers')
[-] tw.it-eam.com generated an unexpected exception: (11, 'Could not contact DNS servers')
[-] 177.it-eam.com generated an unexpected exception: (11, 'Could not contact DNS servers')
[-] 223.it-eam.com generated an unexpected exception: (11, 'Could not contact DNS servers')
[-] 0.it-eam.com generated an unexpected exception: (11, 'Could not contact DNS servers')
[-] 248.it-eam.com generated an unexpected exception: (11, 'Could not contact DNS servers')
[-] 140.it-eam.com generated an unexpected exception: (11, 'Could not contact DNS servers')
[+] blog.it-eam.com                     ['108.167.188.58']
[+] vpn.it-eam.com                      ['177.85.84.22']
[+] webmail.it-eam.com                  ['108.167.188.58']
[+] www.it-eam.com                      ['142.250.78.211']
[+] mail.it-eam.com                     ['216.239.32.21', '216.239.38.21', '216.239.34.21', '216.239.36.21']
[+] localhost.it-eam.com                ['127.0.0.1']
  0%|                                                                   | 520/1865824 [00:04<6:21:52, 81.41rec/s]
```

resolvers/resolvers.txt at main · trickest/resolvers

DNS NAME PERMUTATION



```
$ echo 'partner-mail.cyclops.corp.yahoo.com' | dnsgen -

engine.cyclops.corp.yahoo.com
partner-stage.cyclops.corp.yahoo.com
partner-mail.cyclopspass.corp.yahoo.com
partner-mail.resetdatacyclops.corp.yahoo.com
partner-mail.cyclops.corpregion.yahoo.com
partner-mail.cyclops.corpv1.yahoo.com
partner-mail.administratorcyclops.corp.yahoo.com
reset.cyclops.corp.yahoo.com
partner-mail.cyclops.chef.corp.yahoo.com
auth-partner-mail.cyclops.corp.yahoo.com
partner-mail.cyclops.corpsystem.yahoo.com
partner-mail.vpn.corp.yahoo.com
partner-mail.reset.cyclops.corp.yahoo.com
cyclops-mail.cyclops.corp.yahoo.com
partner-mail.northamerica.cyclops.corp.yahoo.com
partner-mail.cyclops.gateway.corp.yahoo.com
partner-mail.priv.cyclops.corp.yahoo.com
```



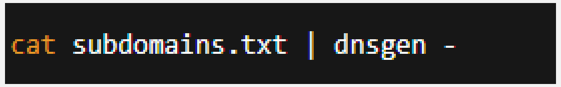
```
┌──ek1l@EK1L ~
└─$ cat domains.txt | dnsgen -
s3.it-eam.com
auth.it-eam.com
priv.it-eam.com
ids.it-eam.com
prod.it-eam.com
accounting.it-eam.com
ops.it-eam.com
cvs.it-eam.com
partner.it-eam.com
ext.it-eam.com
account.it-eam.com
container.it-eam.com
preview.it-eam.com
train.it-eam.com
pass.it-eam.com
hw.it-eam.com
v.it-eam.com
billing.it-eam.com
application.it-eam.com
tpe.it-eam.com
```

DNS NAME PERMUTATION

🧪 dnsgen

•Gera permutações a partir de domínios e subdomínios.

- 📦 GitHub
- 💡 **Exemplo:**

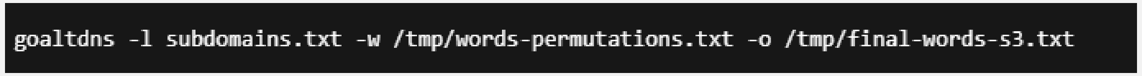


```
cat subdomains.txt | dnsgen -
```

🧩 goaltdns

•Gera permutações com base em dicionários.

- 📦 GitHub
- 📄 Lista de palavras
- 💡 **Exemplo:**

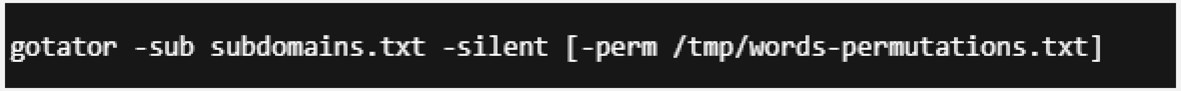


```
goaltdns -l subdomains.txt -w /tmp/words-permutations.txt -o /tmp/final-words-s3.txt
```

🌀 gotator

•Permuta subdomínios, com ou sem wordlist personalizada.

- 📦 GitHub
- 💡 **Exemplo:**

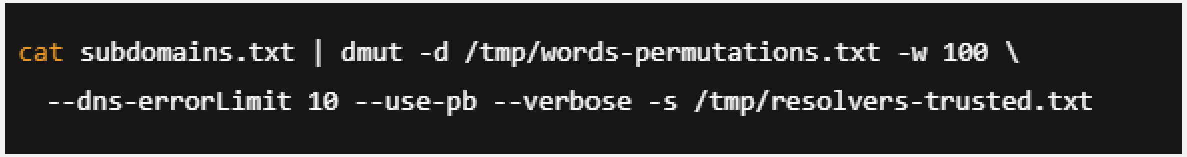


```
gotator -sub subdomains.txt -silent [-perm /tmp/words-permutations.txt]
```

🔄 dmut

•Realiza mutações, permutações e alterações.

- 📦 GitHub
- 📄 Lista de palavras
- 💡 **Exemplo:**



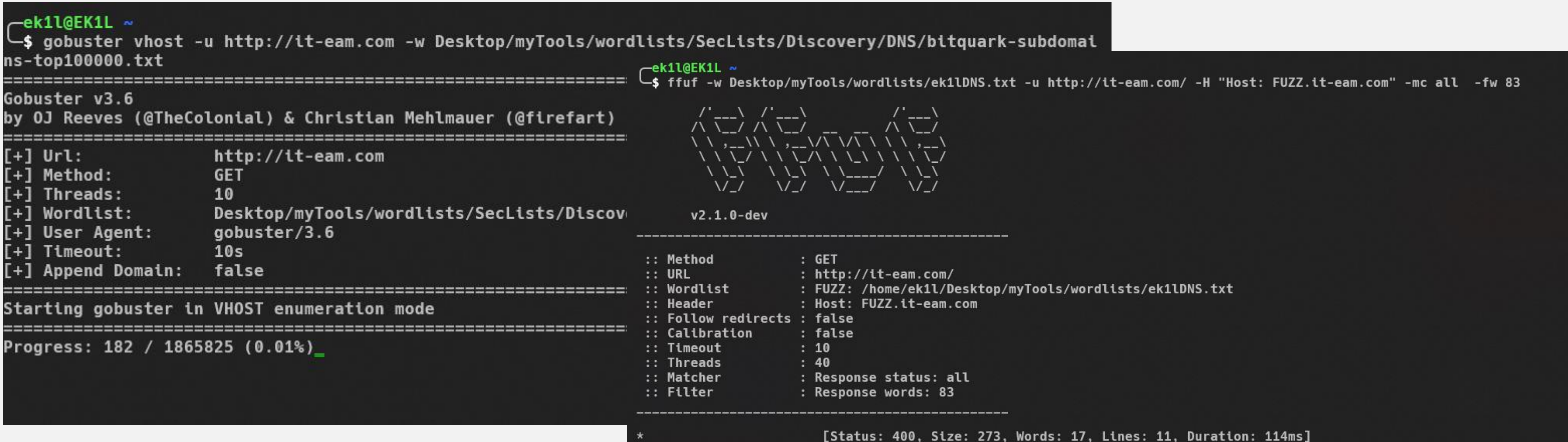
```
cat subdomains.txt | dmut -d /tmp/words-permutations.txt -w 100 \
  --dns-errorLimit 10 --use-pb --verbose -s /tmp/resolvers-trusted.txt
```

VHOST enumeration

VHost Enumeration (ou enumeração de *virtual hosts*) é uma técnica usada para descobrir **hostnames virtuais** configurados em um mesmo servidor web.

Ela é especialmente útil quando:

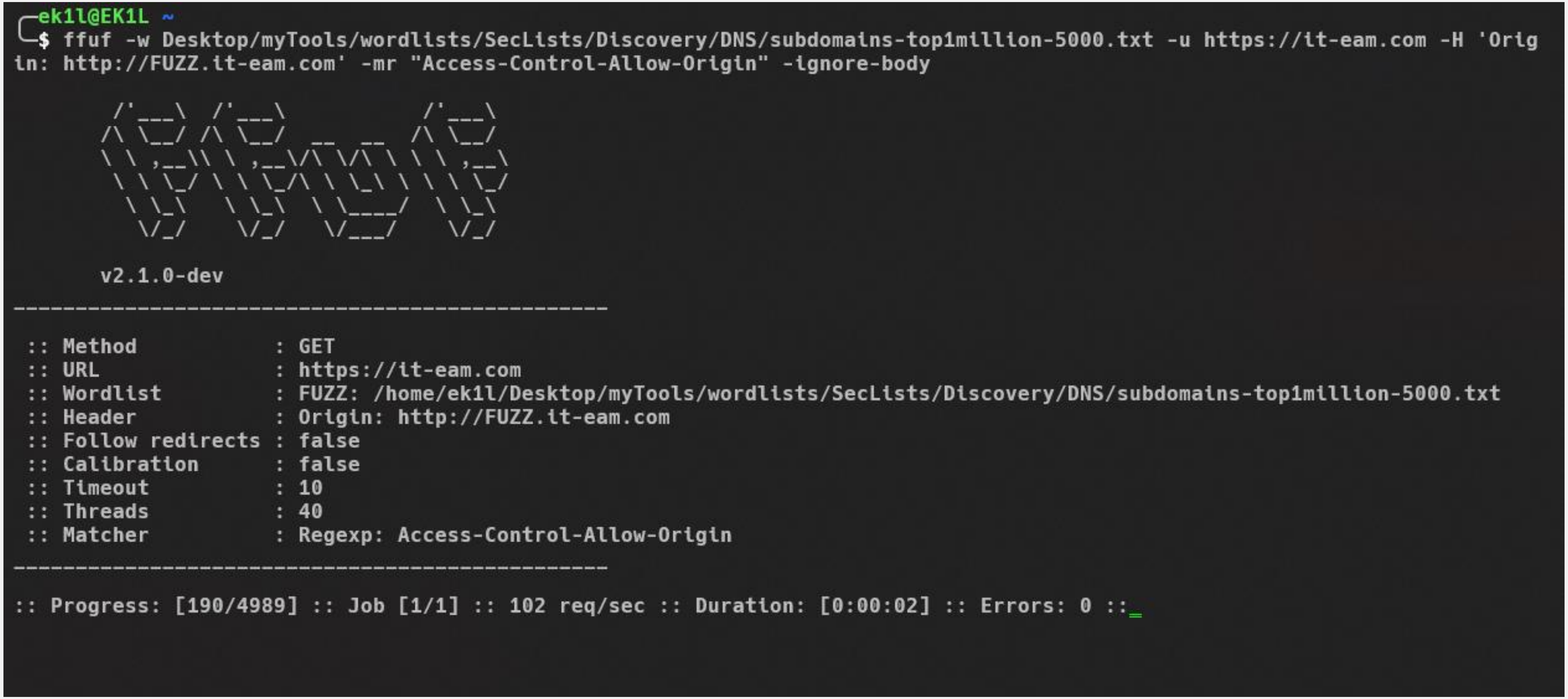
•O servidor responde com o **mesmo IP** para múltiplos domínios (*virtual hosting*).
•O site principal parece estar "limpo", mas domínios ocultos podem conter **funcionalidades restritas, vulnerabilidades ou interfaces administrativas**.



```
┌─ek1l@EK1L ~
└─$ gobuster vhost -u http://it-eam.com -w Desktop/myTools/wordlists/SecLists/Discovery/DNS/bitquark-subdomai
ns-top100000.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://it-eam.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                Desktop/myTools/wordlists/SecLists/Discov
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
[+] Append Domain:           false
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Progress: 182 / 1865825 (0.01%)_
```

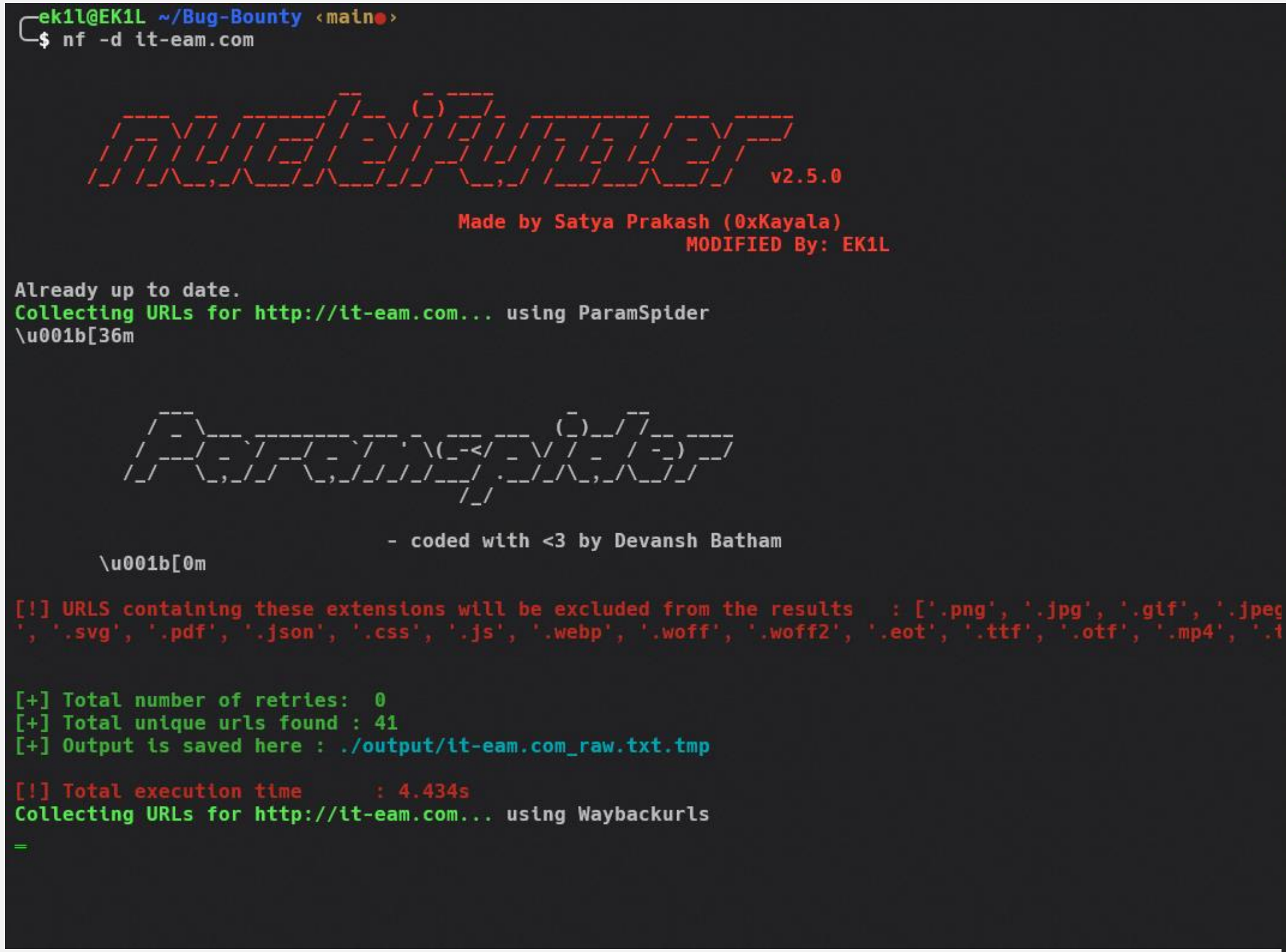
```
┌─ek1l@EK1L ~
└─$ ffuf -w Desktop/myTools/wordlists/ek1lDNS.txt -u http://it-eam.com/ -H "Host: FUZZ.it-eam.com" -mc all  -fw 83

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://it-eam.com/
 :: Wordlist         : FUZZ: /home/ek1l/Desktop/myTools/wordlists/ek1lDNS.txt
 :: Header           : Host: FUZZ.it-eam.com
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
 :: Filter           : Response words: 83
________________________________________________

*                       [Status: 400, Size: 273, Words: 17, Lines: 11, Duration: 114ms]
```

Brute Force CORS

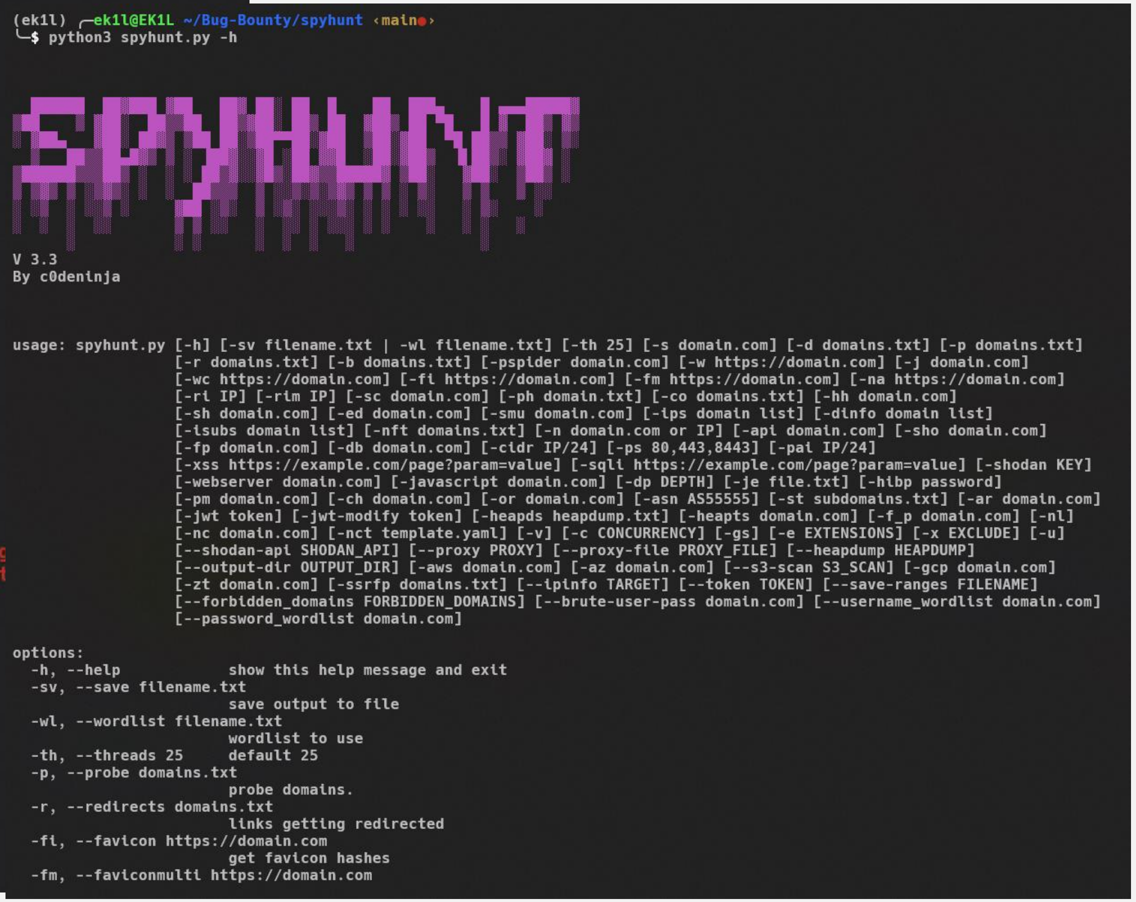


```
┌─ek1l@EK1L ~
└─$ ffuf -w Desktop/myTools/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt -u https://it-eam.com -H 'Orig
in: http://FUZZ.it-eam.com' -mr "Access-Control-Allow-Origin" -ignore-body

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://it-eam.com
 :: Wordlist         : FUZZ: /home/ek1l/Desktop/myTools/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Origin: http://FUZZ.it-eam.com
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Regexp: Access-Control-Allow-Origin
________________________________________________

:: Progress: [190/4989] :: Job [1/1] :: 102 req/sec :: Duration: [0:00:02] :: Errors: 0 ::_
```

Red Team



```
┌─ek1l@EK1L ~/Bug-Bounty ‹main●›
└─$ nf -d it-eam.com

                                                                    v2.5.0

                                        Made by Satya Prakash (0xKayala)
                                                   MODIFIED By: EK1L

Already up to date.
Collecting URLs for http://it-eam.com... using ParamSpider
\u001b[36m

                                  - coded with <3 by Devansh Batham
       \u001b[0m

[!] URLS containing these extensions will be excluded from the results   : ['.png', '.jpg', '.gif', '.jpeg
', '.svg', '.pdf', '.json', '.css', '.js', '.webp', '.woff', '.woff2', '.eot', '.ttf', '.otf', '.mp4', '.t

[+] Total number of retries:  0
[+] Total unique urls found : 41
[+] Output is saved here : ./output/it-eam.com_raw.txt.tmp

[!] Total execution time      : 4.434s
Collecting URLs for http://it-eam.com... using Waybackurls
_
```



```
(ek1l) ┌─ek1l@EK1L ~/Bug-Bounty/spyhunt ‹main●›
└─$ python3 spyhunt.py -h

V 3.3
By c0deninja


usage: spyhunt.py [-h] [-sv filename.txt | -wl filename.txt] [-th 25] [-s domain.com] [-d domains.txt] [-p domains.txt]
                  [-r domains.txt] [-b domains.txt] [-pspider domain.com] [-w https://domain.com] [-j domain.com]
                  [-wc https://domain.com] [-fi https://domain.com] [-fm https://domain.com] [-na https://domain.com]
                  [-ri IP] [-rim IP] [-sc domain.com] [-ph domain.txt] [-co domains.txt] [-hh domain.com]
                  [-sh domain.com] [-ed domain.com] [-smu domain.com] [-ips domain list] [-dinfo domain list]
                  [-isubs domain list] [-nft domains.txt] [-n domain.com or IP] [-api domain.com] [-sho domain.com]
                  [-fp domain.com] [-db domain.com] [-cidr IP/24] [-ps 80,443,8443] [-pai IP/24]
                  [-xss https://example.com/page?param=value] [-sqli https://example.com/page?param=value] [-shodan KEY]
                  [-webserver domain.com] [-javascript domain.com] [-dp DEPTH] [-je file.txt] [-hibp password]
                  [-pm domain.com] [-ch domain.com] [-or domain.com] [-asn AS55555] [-st subdomains.txt] [-ar domain.com]
                  [-jwt token] [-jwt-modify token] [-heapds heapdump.txt] [-heapts domain.com] [-f_p domain.com] [-nl]
                  [-nc domain.com] [-nct template.yaml] [-v] [-c CONCURRENCY] [-gs] [-e EXTENSIONS] [-x EXCLUDE] [-u]
                  [--shodan-api SHODAN_API] [--proxy PROXY] [--proxy-file PROXY_FILE] [--heapdump HEAPDUMP]
                  [--output-dir OUTPUT_DIR] [-aws domain.com] [-az domain.com] [--s3-scan S3_SCAN] [-gcp domain.com]
                  [-zt domain.com] [-ssrfp domains.txt] [--ipinfo TARGET] [--token TOKEN] [--save-ranges FILENAME]
                  [--forbidden_domains FORBIDDEN_DOMAINS] [--brute-user-pass domain.com] [--username_wordlist domain.com]
                  [--password_wordlist domain.com]

options:
  -h, --help            show this help message and exit
  -sv, --save filename.txt
                        save output to file
  -wl, --wordlist filename.txt
                        wordlist to use
  -th, --threads 25     default 25
  -p, --probe domains.txt
                        probe domains.
  -r, --redirects domains.txt
                        links getting redirected
  -fi, --favicon https://domain.com
                        get favicon hashes
  -fm, --faviconmulti https://domain.com
```

Bug-Bounty/spyhunt at main · Red-Team-iT-eam/Bug-Bounty

Bug-Bounty/nucleiFuzzer at main · Red-Team-iT-eam/Bug-Bounty

THE END

References

Referencias desta apresentação:

[Penetration Testing: Methodology, Scope & Types of Pentests]
External Penetration Testing Methodology | by Nairuz Abulhul | R3d Buck3T | Medium
Web Recon Made Simple: Beginner's Handbook - reNgine, Pagodo, Recon FTW, GooFuzz & More – HACKLIDO
Extensive Recon Guide For Bug Hunting – HACKLIDO
My Recon methodology and tools for bug bounty and web security – HACKLIDO
The Bug Hunter's Methodology Jason Haddix @jhaddix
Full Subdomain Discovery Using Workflows
Full Subdomain Brute Force Discovery
Theoretical Insights into Reconnaissance for External Penetration Testing | by Sevban Dönmez | Medium

TOOLS:

m4ll0k/BBTz: BBT - Bug Bounty Tools (examples 💡)