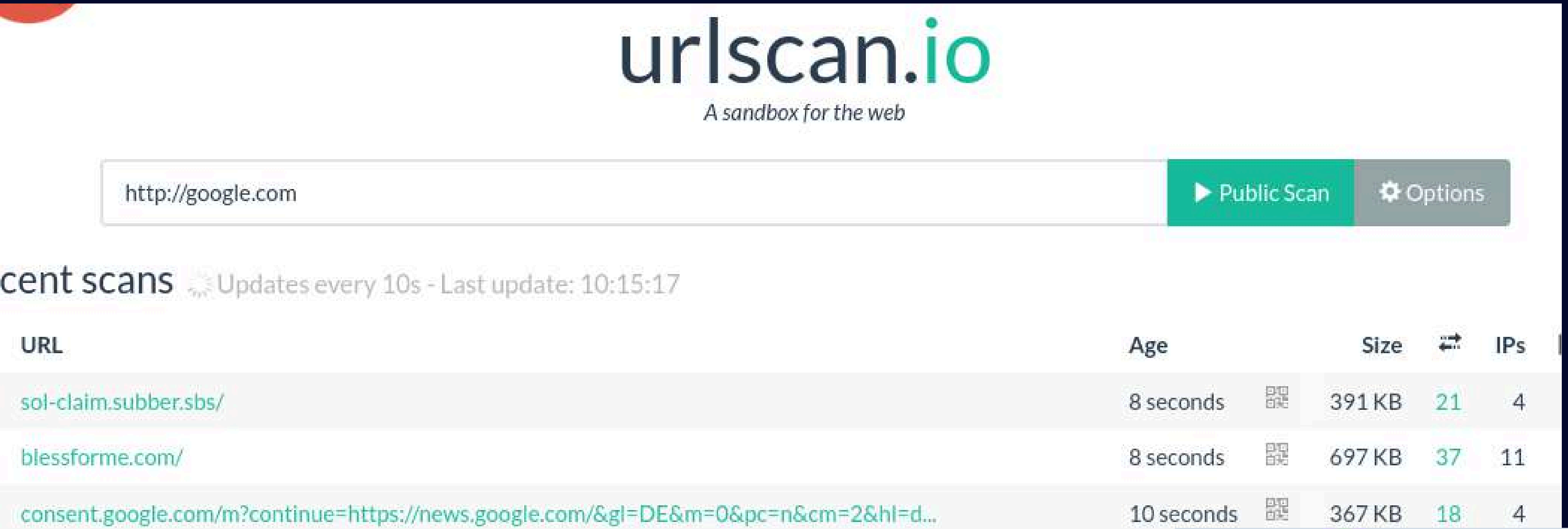
HACKING TOOLKITS

SANTIAGO MARTINEZ
MIGUEL ENRIQUE
DORIAN SANTIAGO
GONZALO LOPEZ

URLSCAN

Sandbox | **Analizar** | **Scripts** | **Detectar phishing**

USO



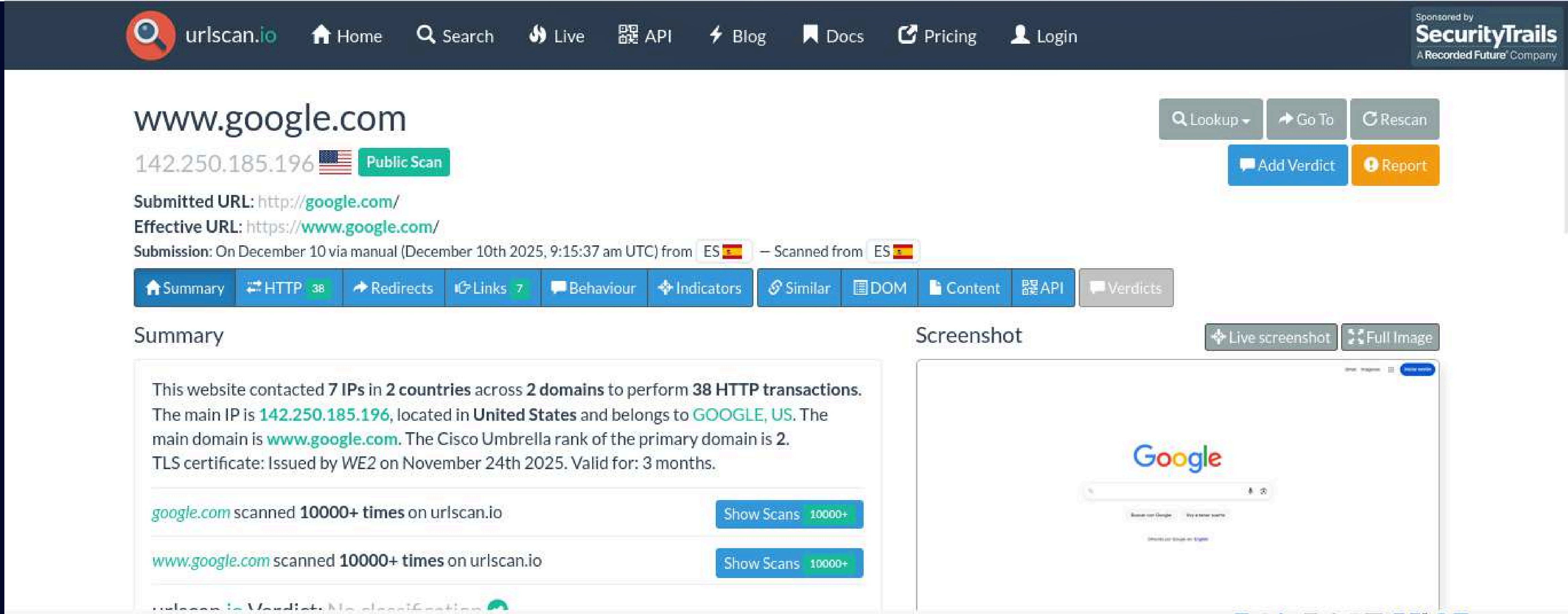
urlscan.io

A sandbox for the web

http://google.com

cent scans Updates every 10s - Last update: 10:15:17

URL	Age		Size	⇄	IPs
sol-claim.subber.sbs/	8 seconds		391 KB	21	4
blessforme.com/	8 seconds		697 KB	37	11
consent.google.com/m?continue=https://news.google.com/&gl=DE&m=0&pc=n&cm=2&hl=d...	10 seconds		367 KB	18	4



www.google.com

142.250.185.196 Public Scan

Submitted URL: http://google.com/

Effective URL: https://www.google.com/

Submission: On December 10 via manual (December 10th 2025, 9:15:37 am UTC) from ES — Scanned from ES

Summary

This website contacted **7 IPs** in **2 countries** across **2 domains** to perform **38 HTTP transactions**. The main IP is 142.250.185.196, located in **United States** and belongs to GOOGLE, US. The main domain is www.google.com. The Cisco Umbrella rank of the primary domain is **2**. TLS certificate: Issued by *WE2* on November 24th 2025. Valid for: 3 months.

google.com scanned **10000+ times** on urlscan.io Show Scans 10000+

www.google.com scanned **10000+ times** on urlscan.io Show Scans 10000+

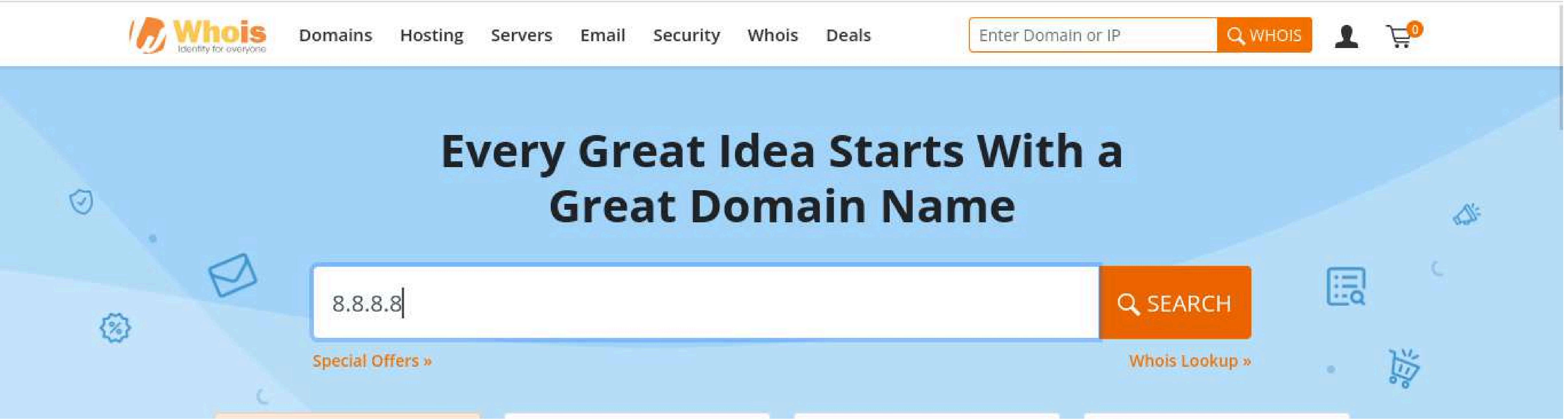
urlscan.io Verdict: No classification

Screenshot

WHOISCOM

dirección IP

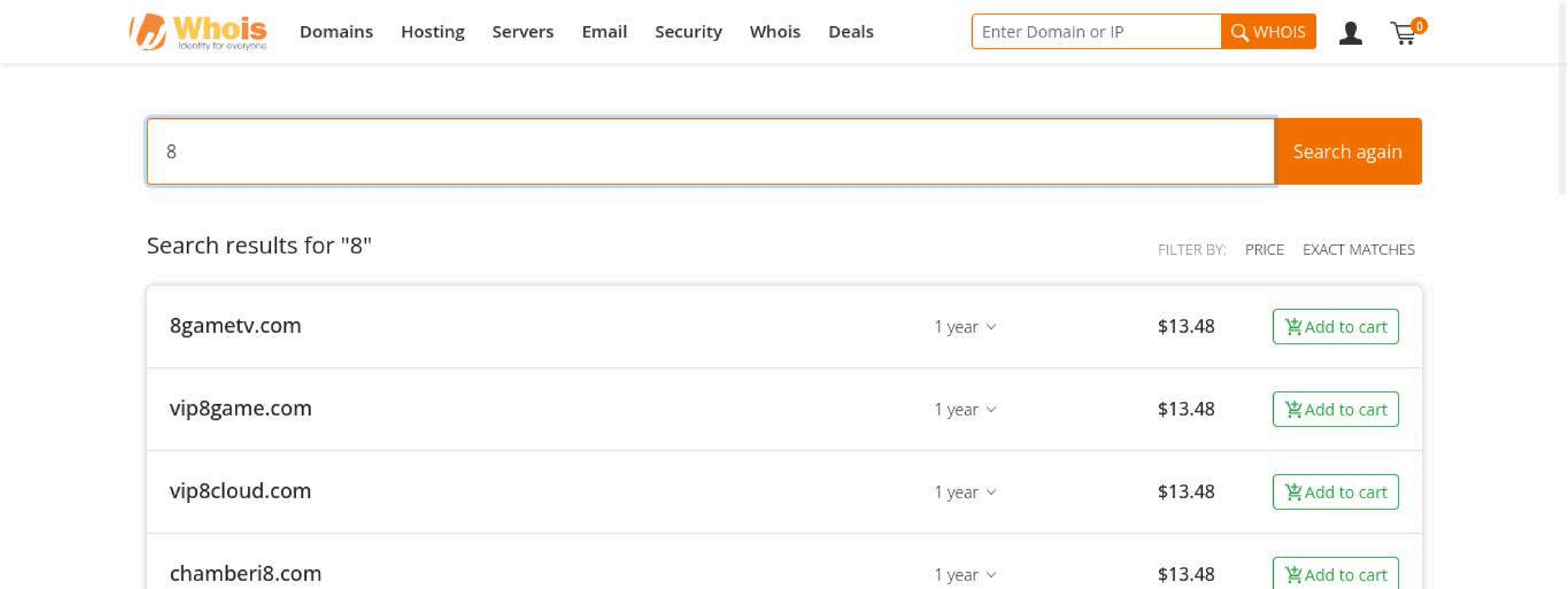
Dominios



Every Great Idea Starts With a Great Domain Name

8.8.8.8

USO



8

Search results for "8"

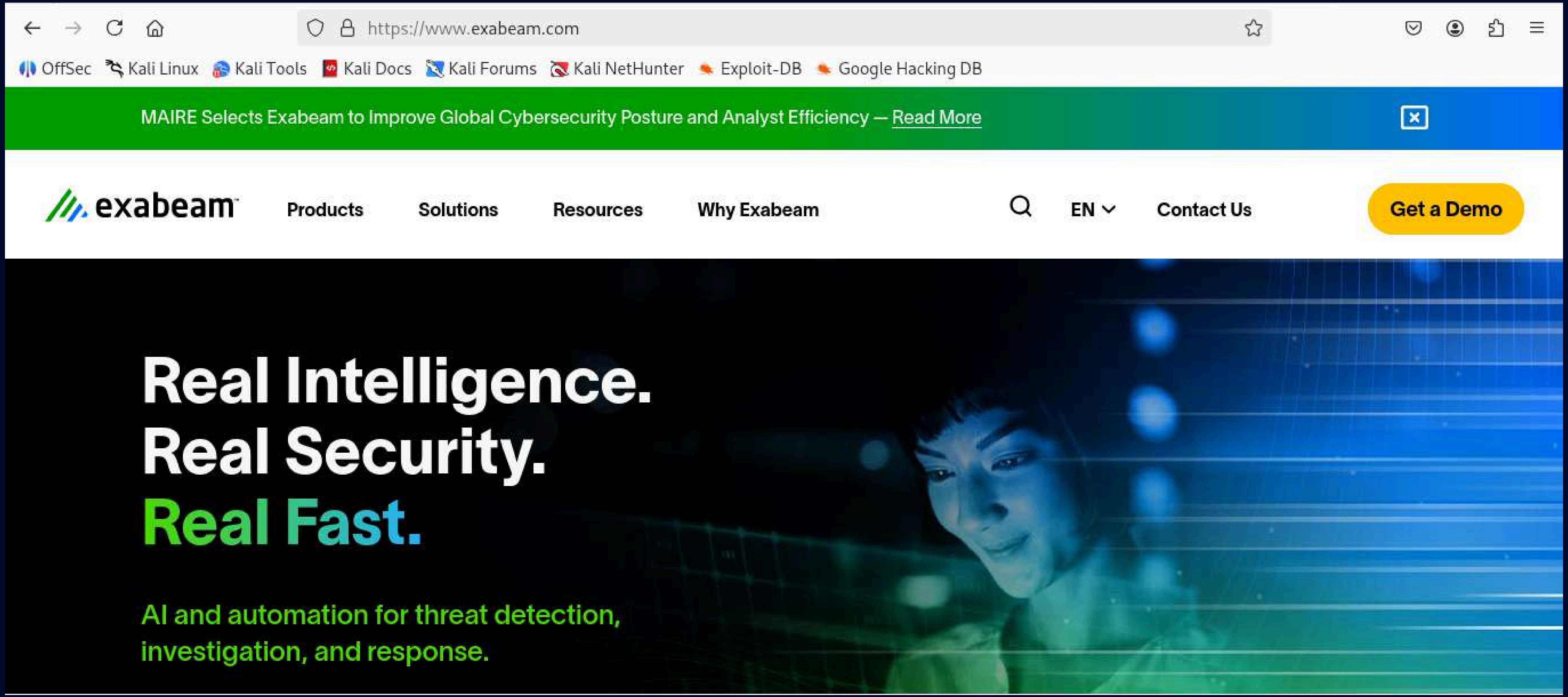
8gametv.com	1 year	$13.48	Add to cart
vip8game.com	1 year	$13.48	Add to cart
vip8cloud.com	1 year	$13.48	Add to cart
chamberi8.com	1 year	$13.48	Add to cart

LOGRHYTHM SIEM

Recolección Logs

Detección Amenazas

Cumplimiento Normativo



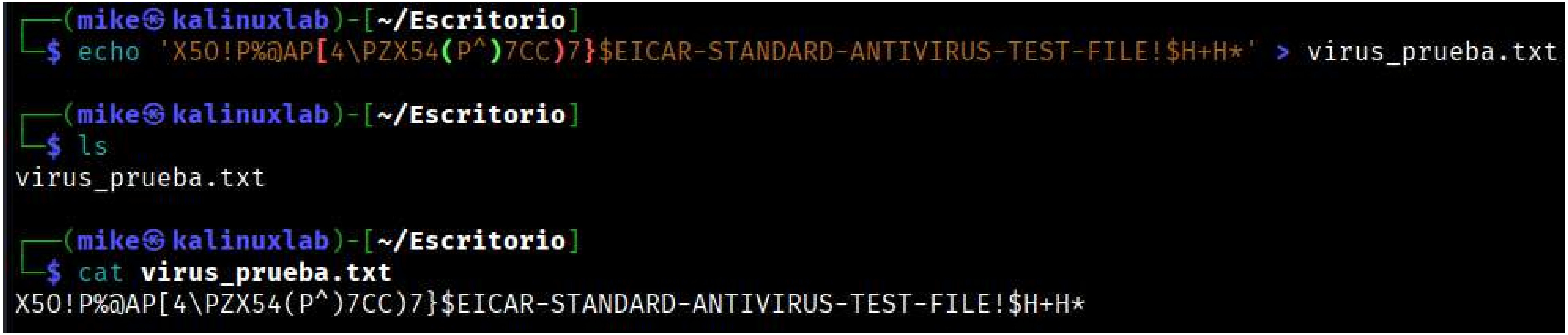
https://www.exabeam.com

MAIRE Selects Exabeam to Improve Global Cybersecurity Posture and Analyst Efficiency — Read More

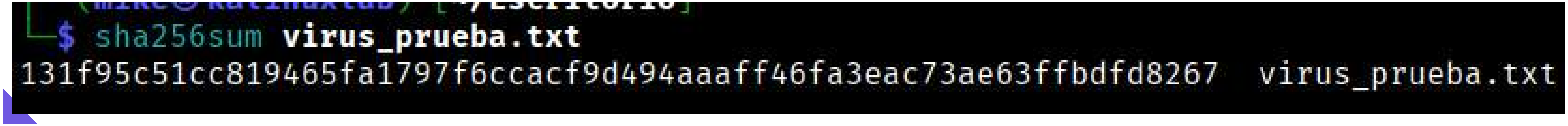
Real Intelligence.
Real Security.
Real Fast.

AI and automation for threat detection, investigation, and response.

PRUEBA

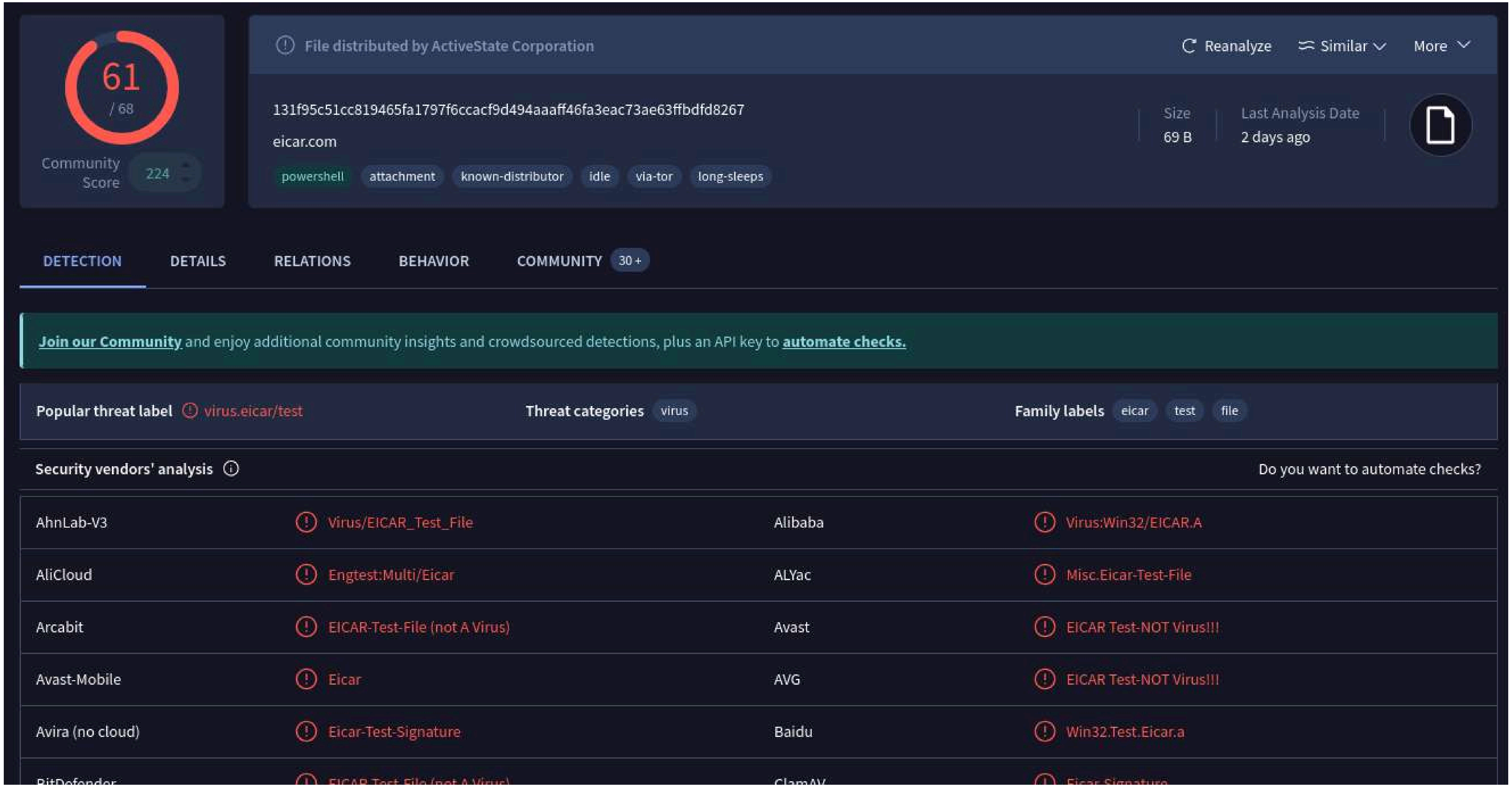


```
┌──(mike㉿kalinuxlab)-[~/Escritorio]
└─$ echo 'X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*' > virus_prueba.txt

┌──(mike㉿kalinuxlab)-[~/Escritorio]
└─$ ls
virus_prueba.txt

┌──(mike㉿kalinuxlab)-[~/Escritorio]
└─$ cat virus_prueba.txt
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```



```
┌──(mike㉿kalinuxlab)-[~/Escritorio]
└─$ sha256sum virus_prueba.txt
131f95c51cc819465fa1797f6ccacf9d494aaff46fa3eac73ae63ffbdfd8267  virus_prueba.txt
```

VIRUSTOTAL



61
/ 68

Community Score 224

File distributed by ActiveState Corporation

Reanalyze Similar More

131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267

eicar.com

powershell attachment known-distributor idle via-tor long-sleeps

Size
69 B

Last Analysis Date
2 days ago

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label virus.eicar/test Threat categories virus Family labels eicar test file

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Virus/EICAR_Test_File	Alibaba	Virus:Win32/EICAR.A
AliCloud	Engtest:Multi/Eicar	ALYac	Misc.Eicar-Test-File
Arcabit	EICAR-Test-File (not A Virus)	Avast	EICAR Test-NOT Virus!!!
Avast-Mobile	Eicar	AVG	EICAR Test-NOT Virus!!!
Avira (no cloud)	Eicar-Test-Signature	Baidu	Win32.Test.Eicar.a
BitDefender	EICAR-Test-File (not A Virus)	ClamAV	Eicar-Signature

VIRUSTOTAL

DEHASHED

Motor de Busqueda

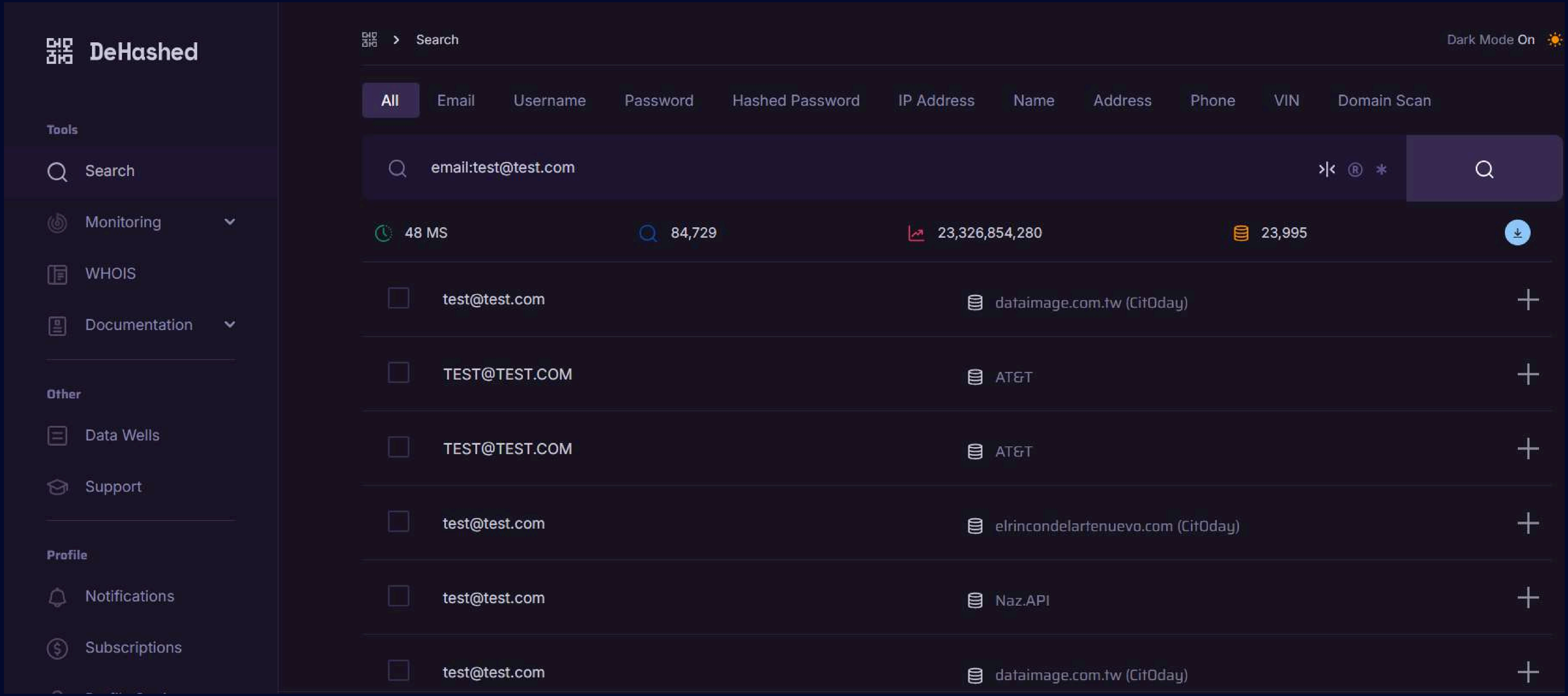
BD Filtradas

Correo, IP, Telefono

Brechas de Seguridad

PRUEBA

https://www.dehashed.com/



email:test@test.com

48 MS | 84,729 | 23,326,854,280 | 23,995

test@test.com	dataimage.com.tw (Cit0day)
TEST@TEST.COM	AT&T
TEST@TEST.COM	AT&T
test@test.com	elrincondelartenuevo.com (Cit0day)
test@test.com	Naz.API
test@test.com	dataimage.com.tw (Cit0day)

OPENVAS / GVM

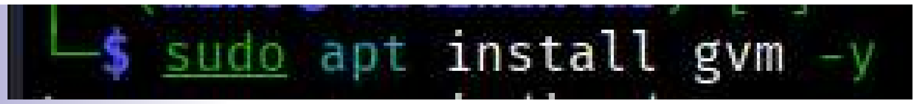
Vulnerabilidades

Auditor Automatizado

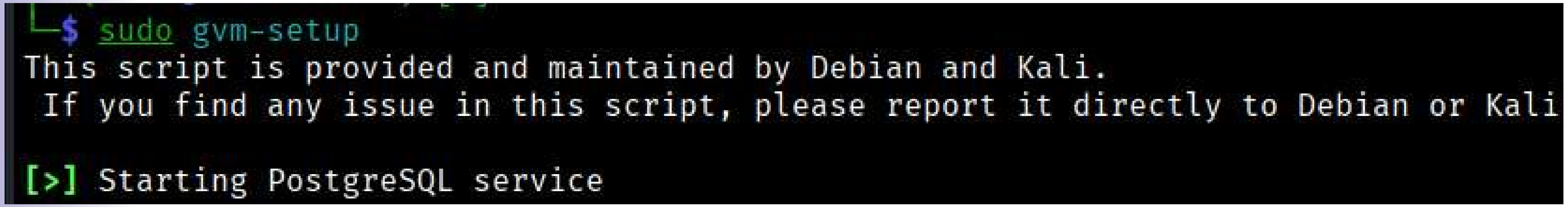
Red

“Puertas” Abiertas

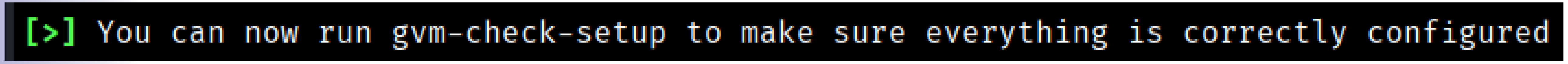
INSTALACIÓN Y PRUEBA



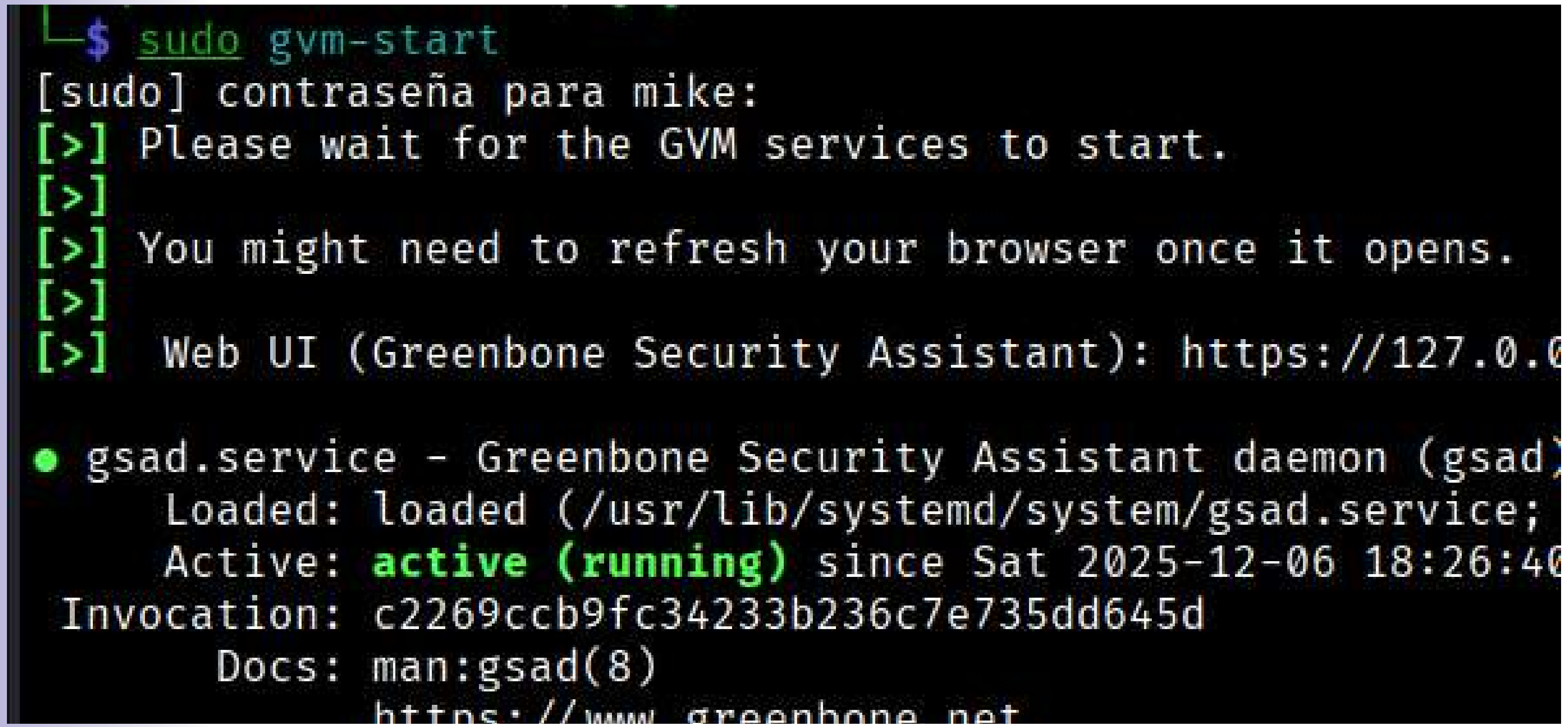
```
└─$ sudo apt install gvm -y
```



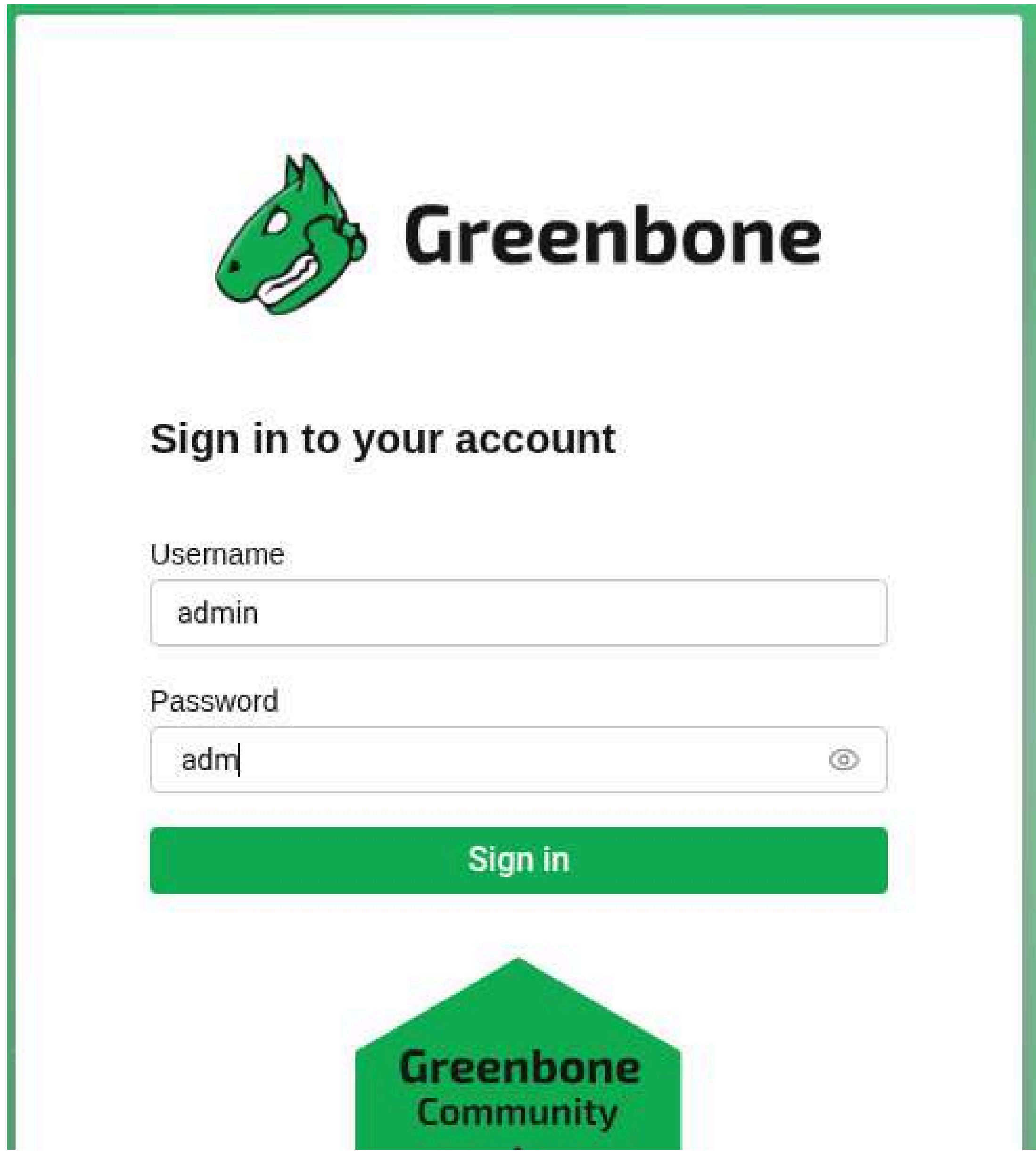
```
└─$ sudo gvm-setup
This script is provided and maintained by Debian and Kali.
 If you find any issue in this script, please report it directly to Debian or Kali

[>] Starting PostgreSQL service
```



```
[>] You can now run gvm-check-setup to make sure everything is correctly configured
```



```
└─$ sudo gvm-start
[sudo] contraseña para mike:
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>]  Web UI (Greenbone Security Assistant): https://127.0.0

● gsad.service - Greenbone Security Assistant daemon (gsad)
     Loaded: loaded (/usr/lib/systemd/system/gsad.service;
     Active: active (running) since Sat 2025-12-06 18:26:40
 Invocation: c2269ccb9fc34233b236c7e735dd645d
       Docs: man:gsad(8)
             https://www.greenbone.net
```



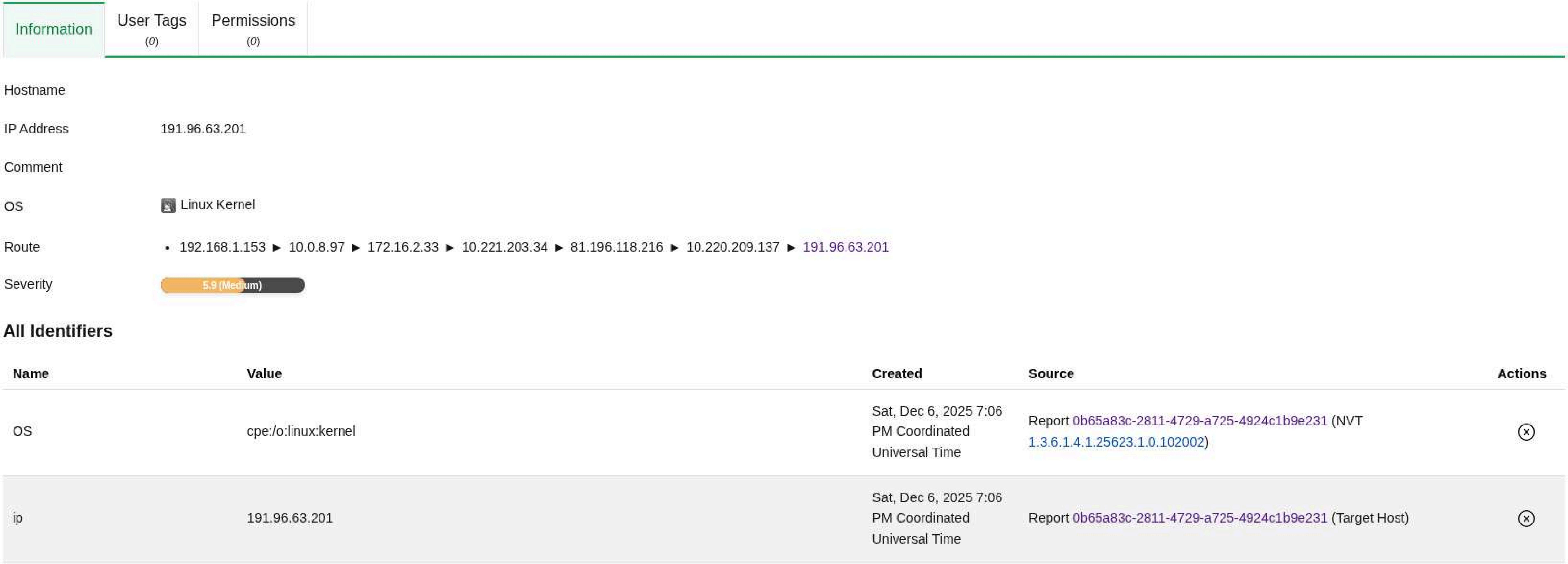
Sign in to your account

Username: admin

Password: adm

```
sudo -u _gvm gvmd --user=admin --new-password=admin
```

OPENVAS / GVM

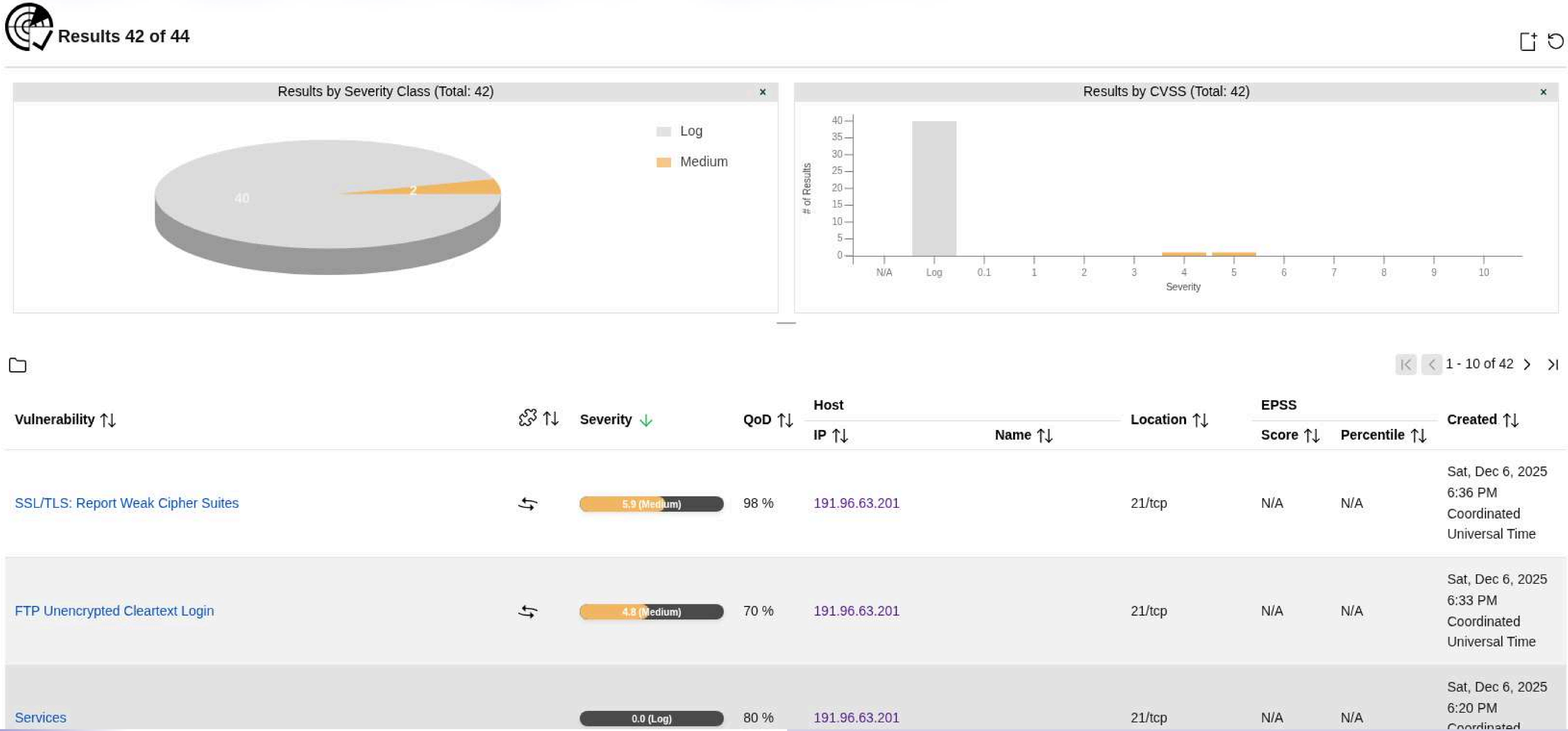


Hostname	
IP Address	191.96.63.201
Comment	
OS	Linux Kernel
Route	192.168.1.153 ► 10.0.8.97 ► 172.16.2.33 ► 10.221.203.34 ► 81.196.118.216 ► 10.220.209.137 ► 191.96.63.201
Severity	5.9 (Medium)

All Identifiers

Name	Value	Created	Source	Actions
OS	cpe:/o:linux:kernel	Sat, Dec 6, 2025 7:06 PM Coordinated Universal Time	Report 0b65a83c-2811-4729-a725-4924c1b9e231 (NVT 1.3.6.1.4.1.25623.1.0.102002)	⊗
ip	191.96.63.201	Sat, Dec 6, 2025 7:06 PM Coordinated Universal Time	Report 0b65a83c-2811-4729-a725-4924c1b9e231 (Target Host)	⊗

OPENVAS / GVM



Results 42 of 44

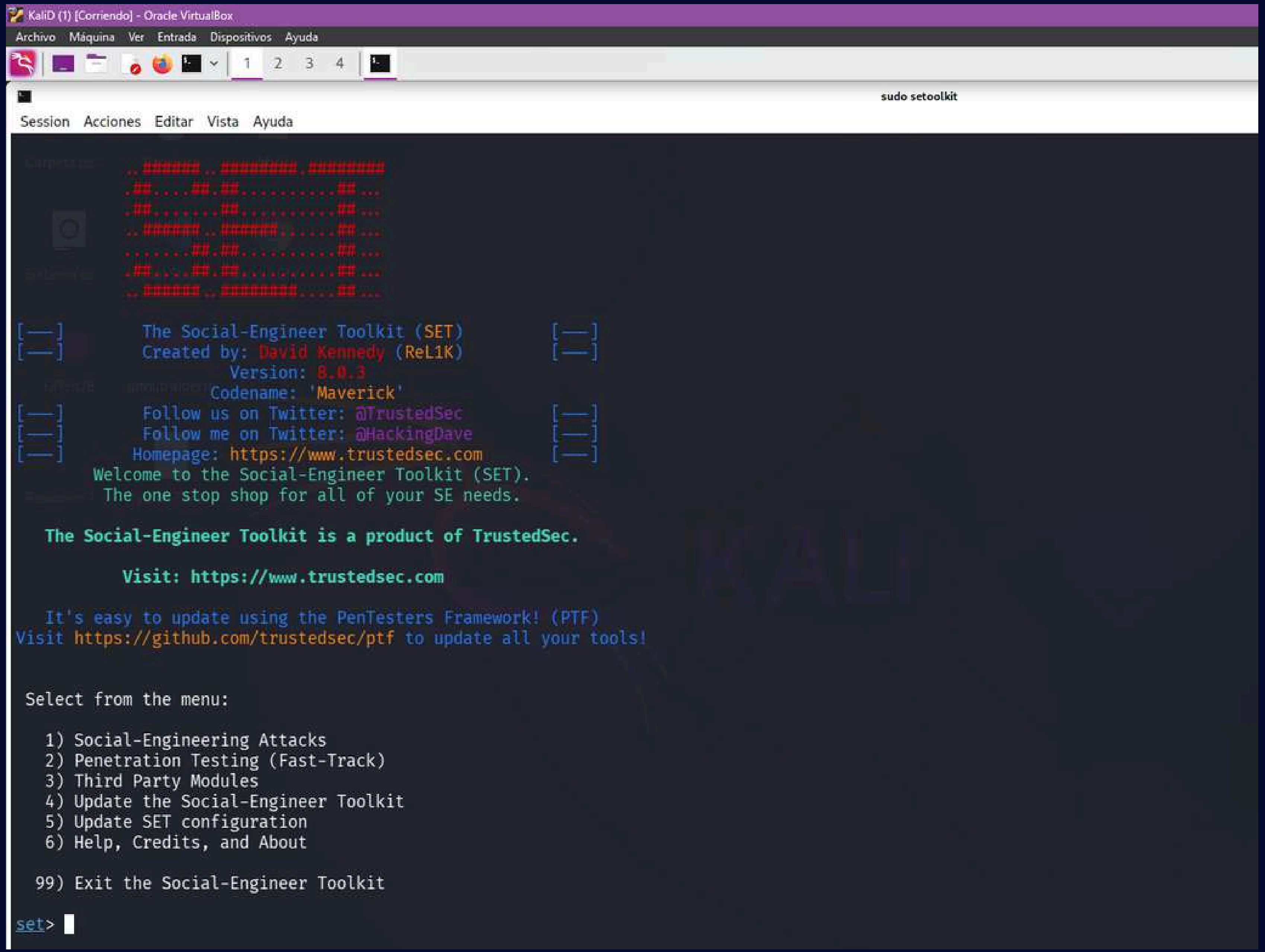
Vulnerability		Severity	QoD	Host		Location	EPSS		Created
				IP	Name		Score	Percentile	
SSL/TLS: Report Weak Cipher Suites	⇆	5.9 (Medium)	98 %	191.96.63.201		21/tcp	N/A	N/A	Sat, Dec 6, 2025 6:36 PM Coordinated Universal Time
FTP Unencrypted Cleartext Login	⇆	4.8 (Medium)	70 %	191.96.63.201		21/tcp	N/A	N/A	Sat, Dec 6, 2025 6:33 PM Coordinated Universal Time
Services		0.0 (Log)	80 %	191.96.63.201		21/tcp	N/A	N/A	Sat, Dec 6, 2025 6:20 PM Coordinated

SOCIAL ENGINEERING TOOLKIT - SET

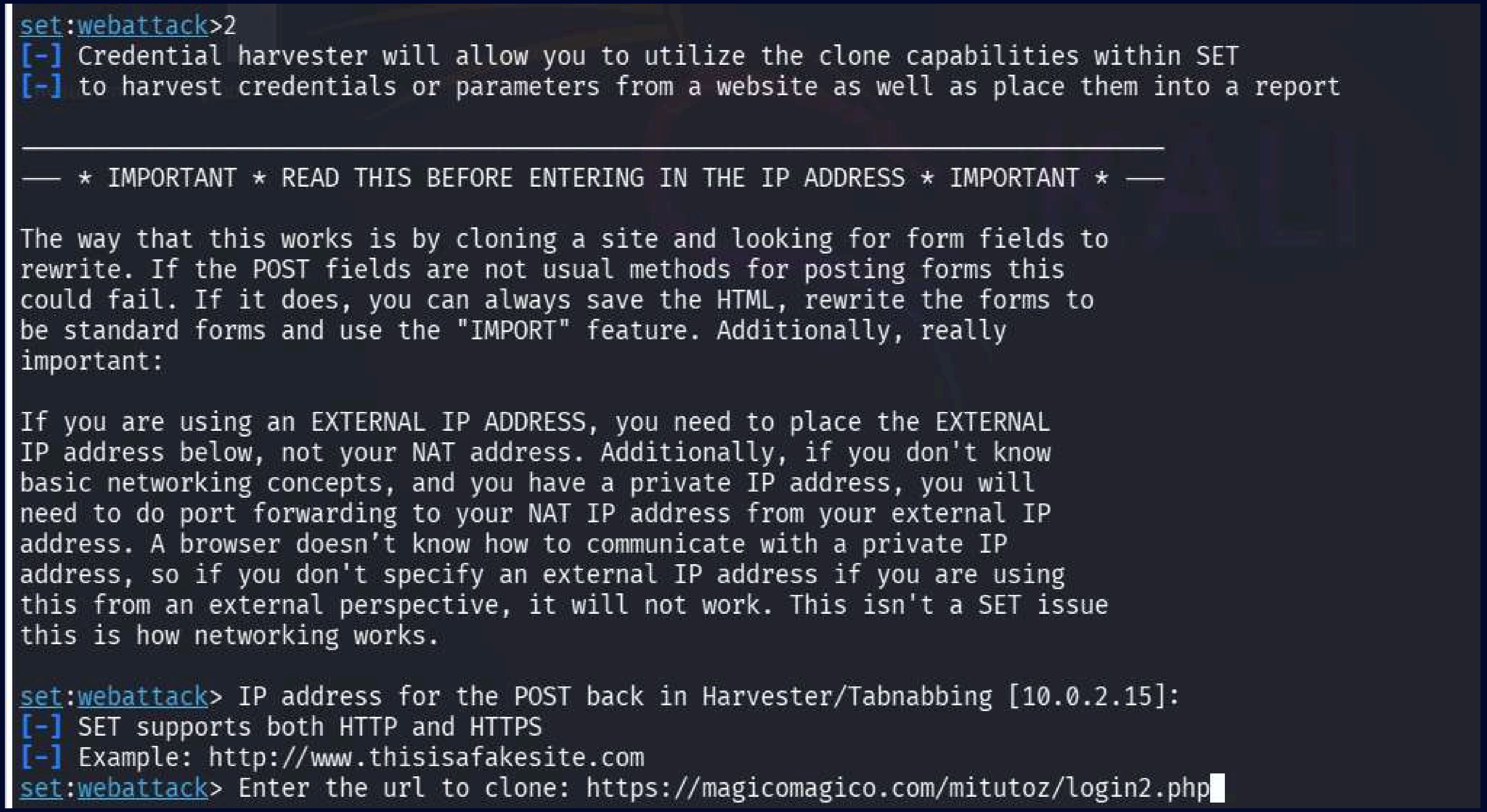
INSTALACIÓN

```
git clone https://github.com/trustedsec/social-engineer-toolkit/ setoolkit/
cd setoolkit
pip3 install -r requirements.txt
python setup.py
```

PRUEBA



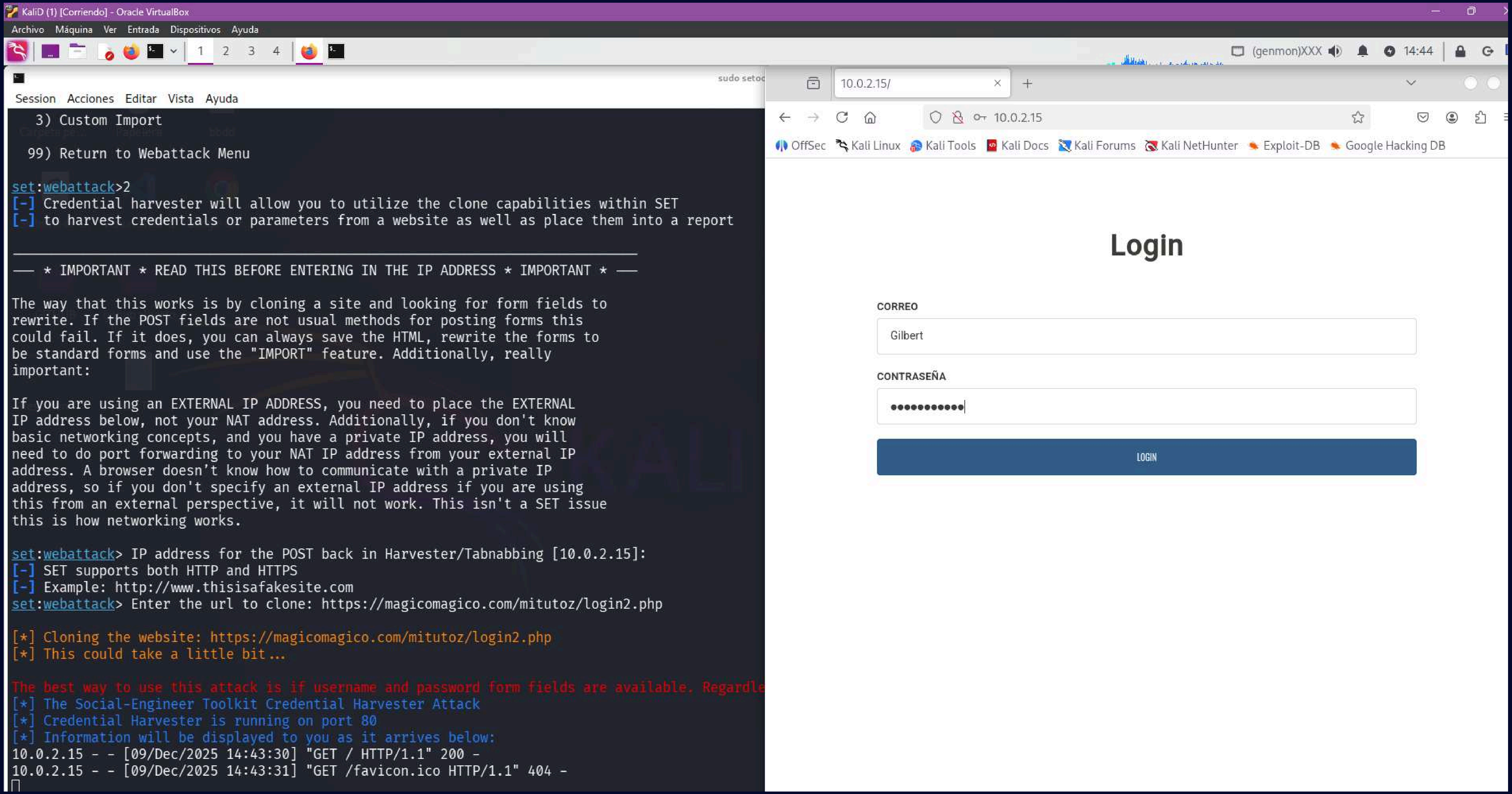
```
          ..######..########.########
          .##....##.##..........##...
          .##.......##..........##...
          ..######..######......##...
          .......##.##..........##...
          .##....##.##..........##...
          ..######..########....##...

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 
```



```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://magicomagico.com/mitutoz/login2.php
```

- **Menú Principal** → opción 1(Social-Engineering Attacks)
- **Vector de Ataque** → opción 2 (Website Attack Vectors).
- **Método** → opción 3 (Credential Harvester Attack Method).
- **Técnica** → opción 2 (Site Cloner)

SOCIAL ENGINEERING TOOLKIT - SET


KaliD (1) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
(genmon)XXX 14:44
sudo setoo
Session Acciones Editar Vista Ayuda
10.0.2.15/
10.0.2.15
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

```
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

───────────────────────────────────────────────────────────────────────────────
─── * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ───

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://magicomagico.com/mitutoz/login2.php

[*] Cloning the website: https://magicomagico.com/mitutoz/login2.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardle
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [09/Dec/2025 14:43:30] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [09/Dec/2025 14:43:31] "GET /favicon.ico HTTP/1.1" 404 -
```

Login

CORREO

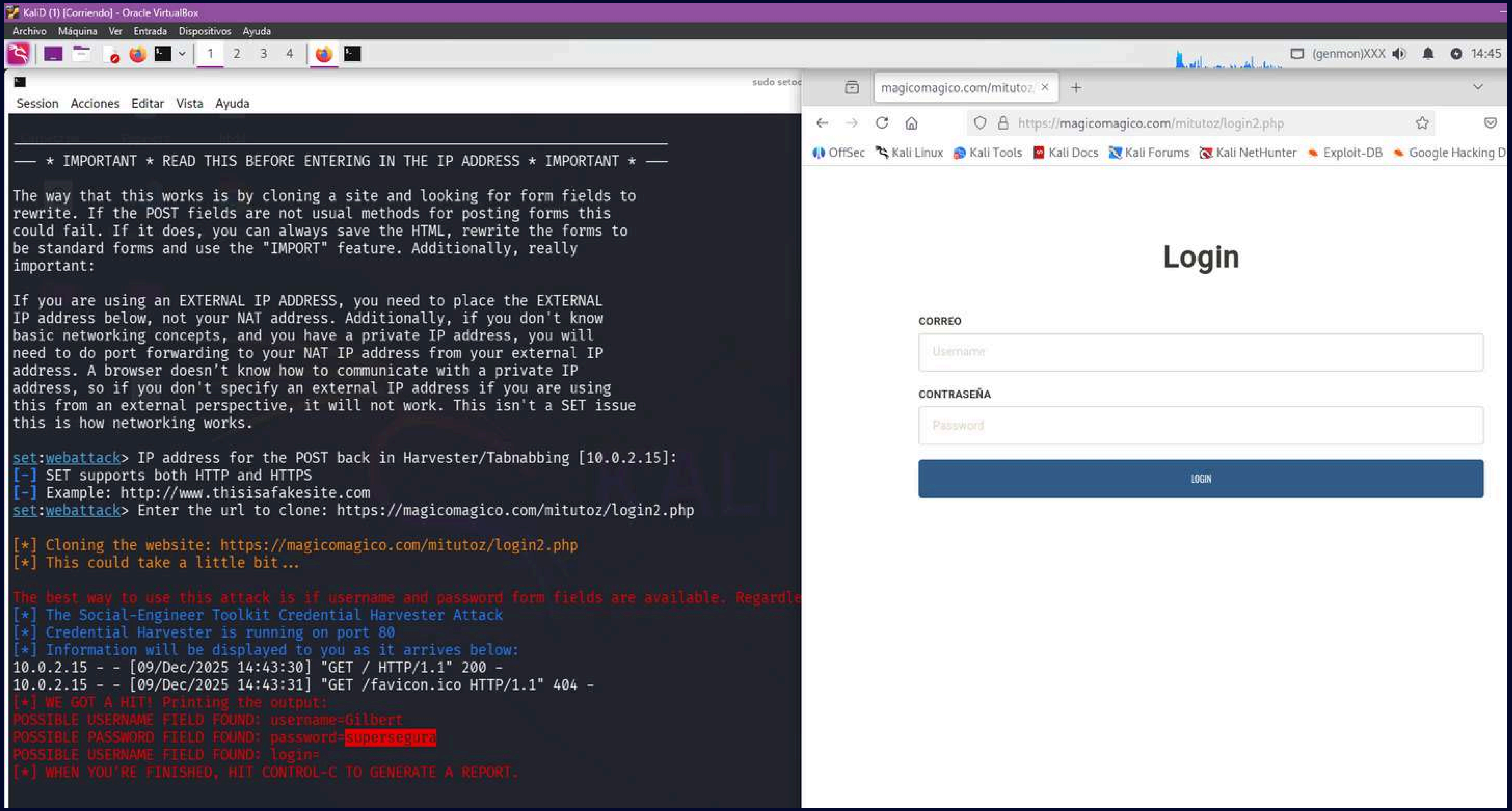
Gilbert

CONTRASEÑA

●●●●●●●●●●●

LOGIN

SOCIAL ENGINEERING TOOLKIT - SET

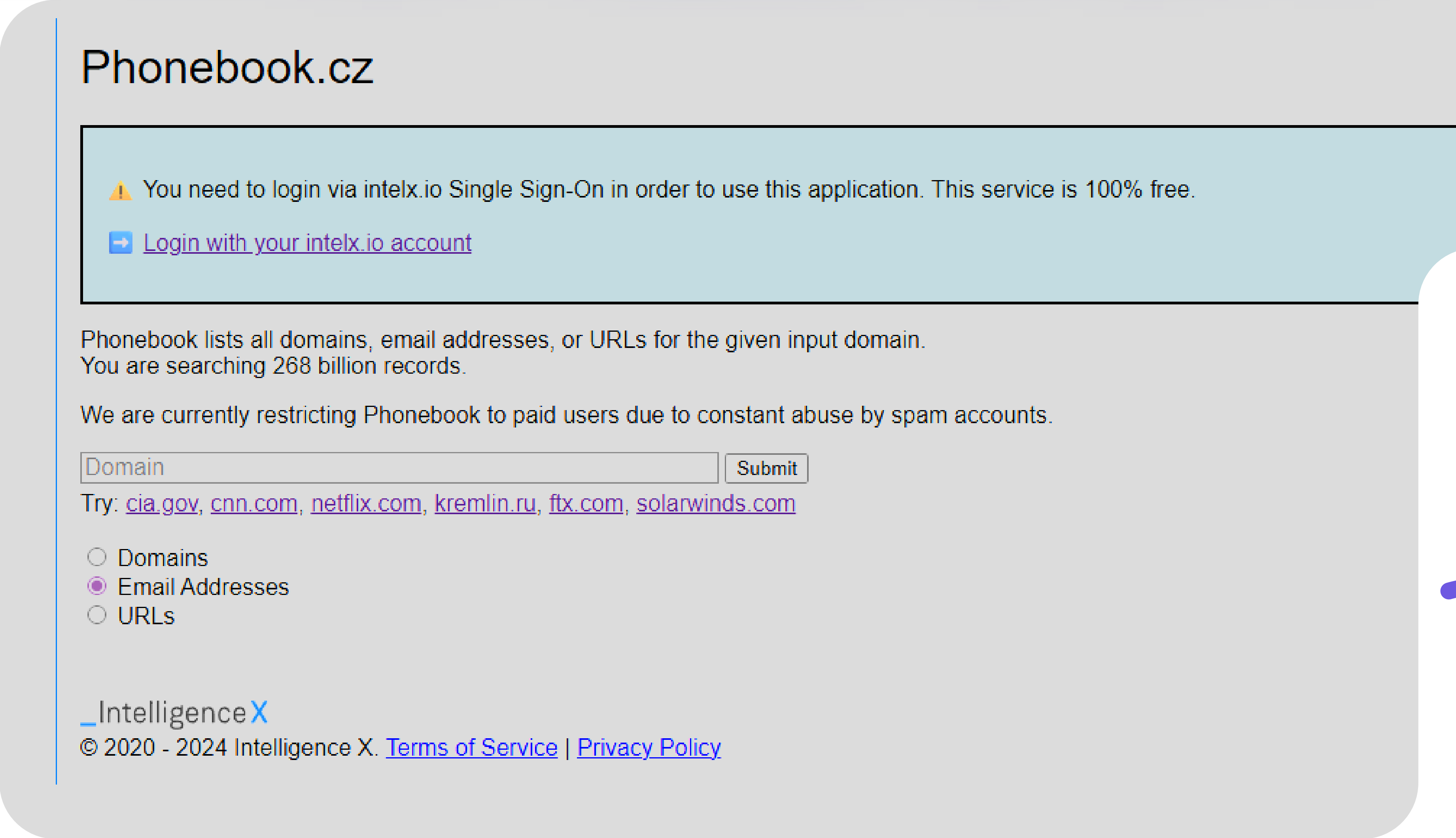


```
── * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ──

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://magicomagico.com/mitutoz/login2.php

[*] Cloning the website: https://magicomagico.com/mitutoz/login2.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardle
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [09/Dec/2025 14:43:30] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [09/Dec/2025 14:43:31] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=Gilbert
POSSIBLE PASSWORD FIELD FOUND: password=supersegura
POSSIBLE USERNAME FIELD FOUND: login=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

OTRAS FUNCIONES

- **Infectious Media Generator (USB)**
- **Mass Mailer Attack (Email)**
- **PowerShell Attack Vectors (Control)**
- **QRCode Generator (Móvil)**

PHONEBOOK



Phonebook.cz

⚠ You need to login via intelx.io Single Sign-On in order to use this application. This service is 100% free.

➡ Login with your intelx.io account

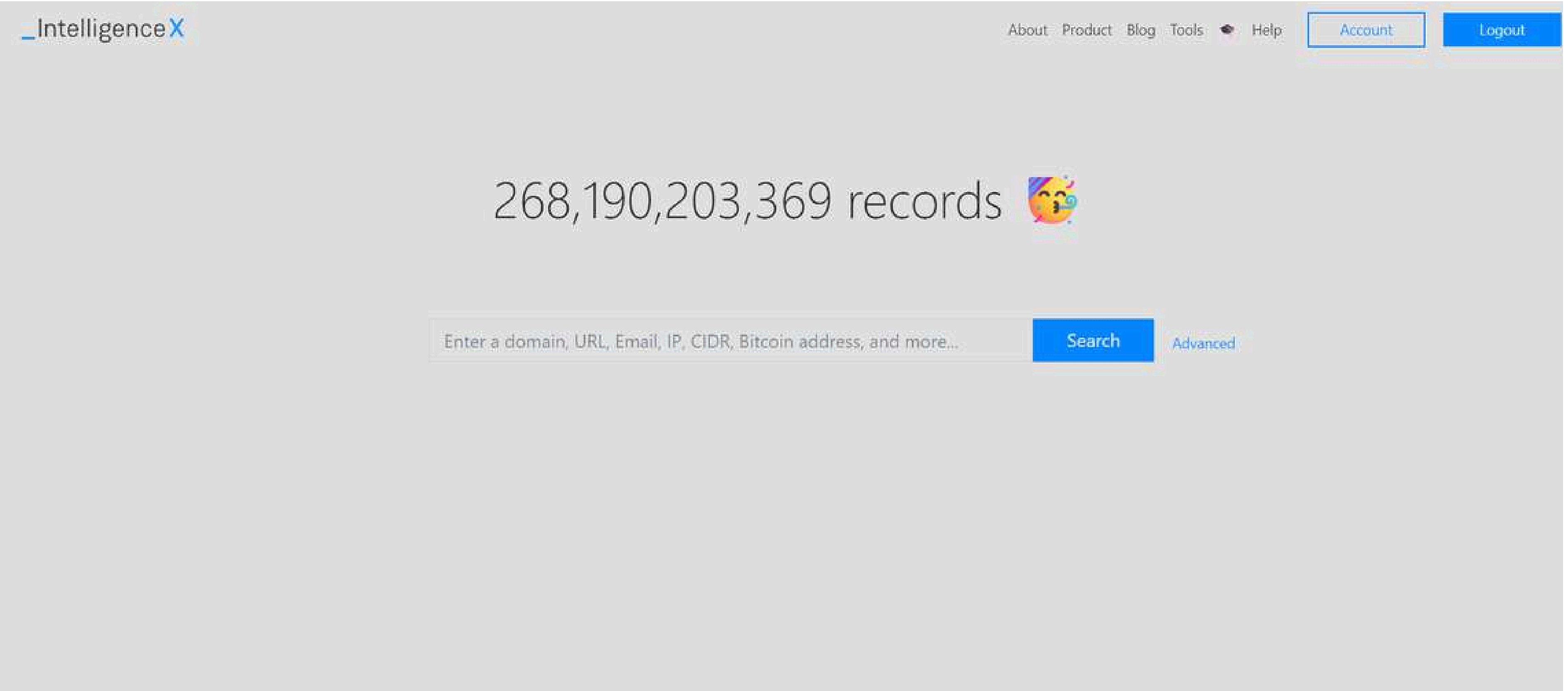
Phonebook lists all domains, email addresses, or URLs for the given input domain.
You are searching 268 billion records.

We are currently restricting Phonebook to paid users due to constant abuse by spam accounts.

Try: cia.gov, cnn.com, netflix.com, kremlin.ru, ftx.com, solarwinds.com

○ Domains
● Email Addresses
○ URLs

_IntelligenceX
© 2020 - 2024 Intelligence X. Terms of Service | Privacy Policy

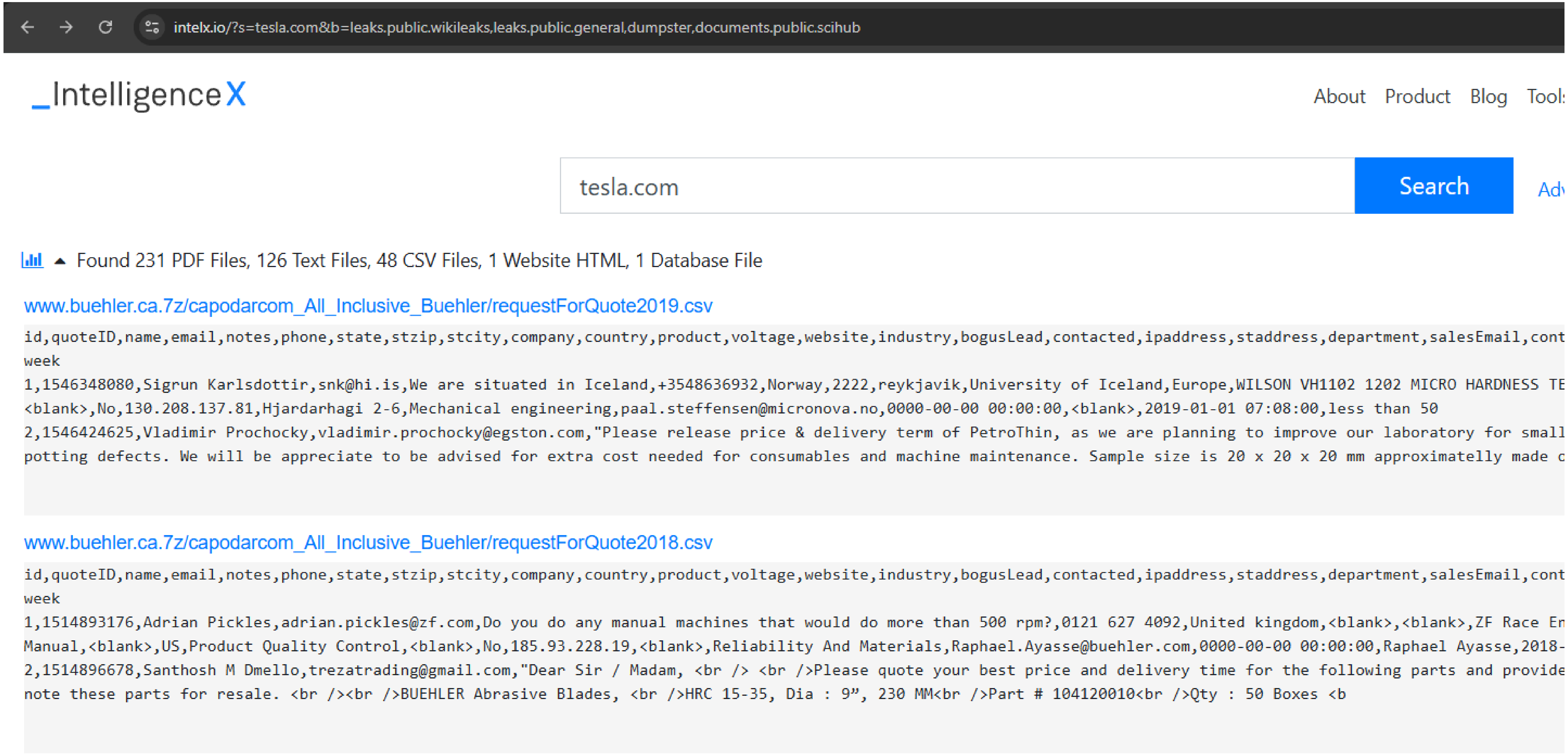


_IntelligenceX
About
Product
Blog
Tools
Help
Account
Logout

268,190,203,369 records

Enter a domain, URL, Email, IP, CIDR, Bitcoin address, and more...
Search
Advanced

PHONEBOOK



intelx.io/?s=tesla.com&b=leaks.public.wikileaks,leaks.public.general,dumpster,documents.public.scihub

Found 231 PDF Files, 126 Text Files, 48 CSV Files, 1 Website HTML, 1 Database File

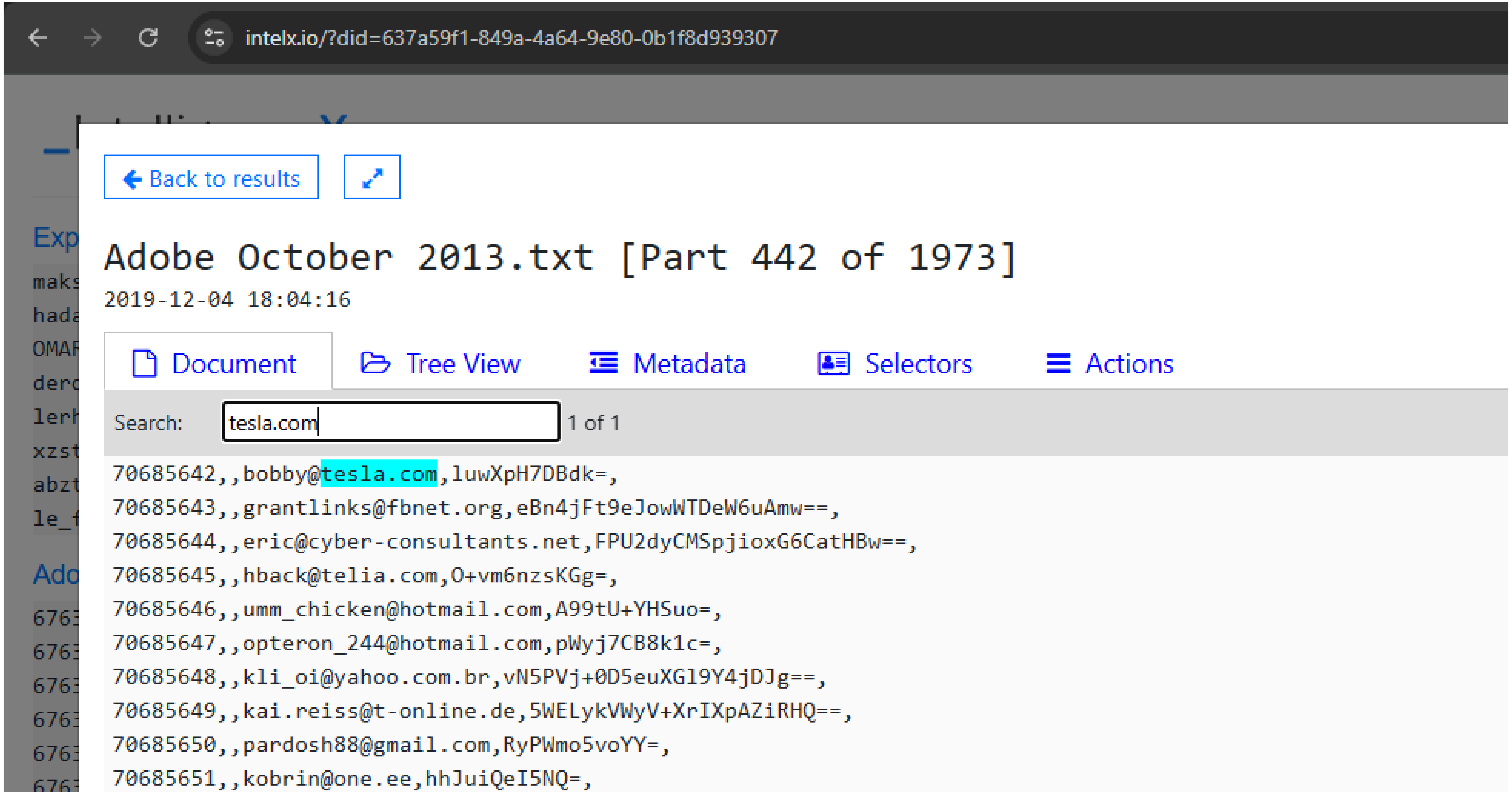
www.buehler.ca.7z/capodarcom_All_Inclusive_Buehler/requestForQuote2019.csv

```
id,quoteID,name,email,notes,phone,state,stzip,stcity,company,country,product,voltage,website,industry,bogusLead,contacted,ipaddress,staddress,department,salesEmail,cont
week
1,1546348080,Sigrun Karlsdottir,snk@hi.is,We are situated in Iceland,+3548636932,Norway,2222,reykjavik,University of Iceland,Europe,WILSON VH1102 1202 MICRO HARDNESS TE
<blank>,No,130.208.137.81,Hjardarhagi 2-6,Mechanical engineering,paal.steffensen@micronova.no,0000-00-00 00:00:00,<blank>,2019-01-01 07:08:00,less than 50
2,1546424625,Vladimir Prochocky,vladimir.prochocky@egston.com,"Please release price & delivery term of PetroThin, as we are planning to improve our laboratory for small
potting defects. We will be appreciate to be advised for extra cost needed for consumables and machine maintenance. Sample size is 20 x 20 x 20 mm approximatelly made c
```

www.buehler.ca.7z/capodarcom_All_Inclusive_Buehler/requestForQuote2018.csv

```
id,quoteID,name,email,notes,phone,state,stzip,stcity,company,country,product,voltage,website,industry,bogusLead,contacted,ipaddress,staddress,department,salesEmail,cont
week
1,1514893176,Adrian Pickles,adrian.pickles@zf.com,Do you do any manual machines that would do more than 500 rpm?,0121 627 4092,United kingdom,<blank>,<blank>,ZF Race En
Manual,<blank>,US,Product Quality Control,<blank>,No,185.93.228.19,<blank>,Reliability And Materials,Raphael.Ayasse@buehler.com,0000-00-00 00:00:00,Raphael Ayasse,2018-
2,1514896678,Santhosh M Dmello,trezatrading@gmail.com,"Dear Sir / Madam, <br /> <br />Please quote your best price and delivery time for the following parts and provide
note these parts for resale. <br /><br />BUEHLER Abrasive Blades, <br />HRC 15-35, Dia : 9”, 230 MM<br />Part # 104120010<br />Qty : 50 Boxes <b
```

PHONEBOOK



Adobe October 2013.txt [Part 442 of 1973]

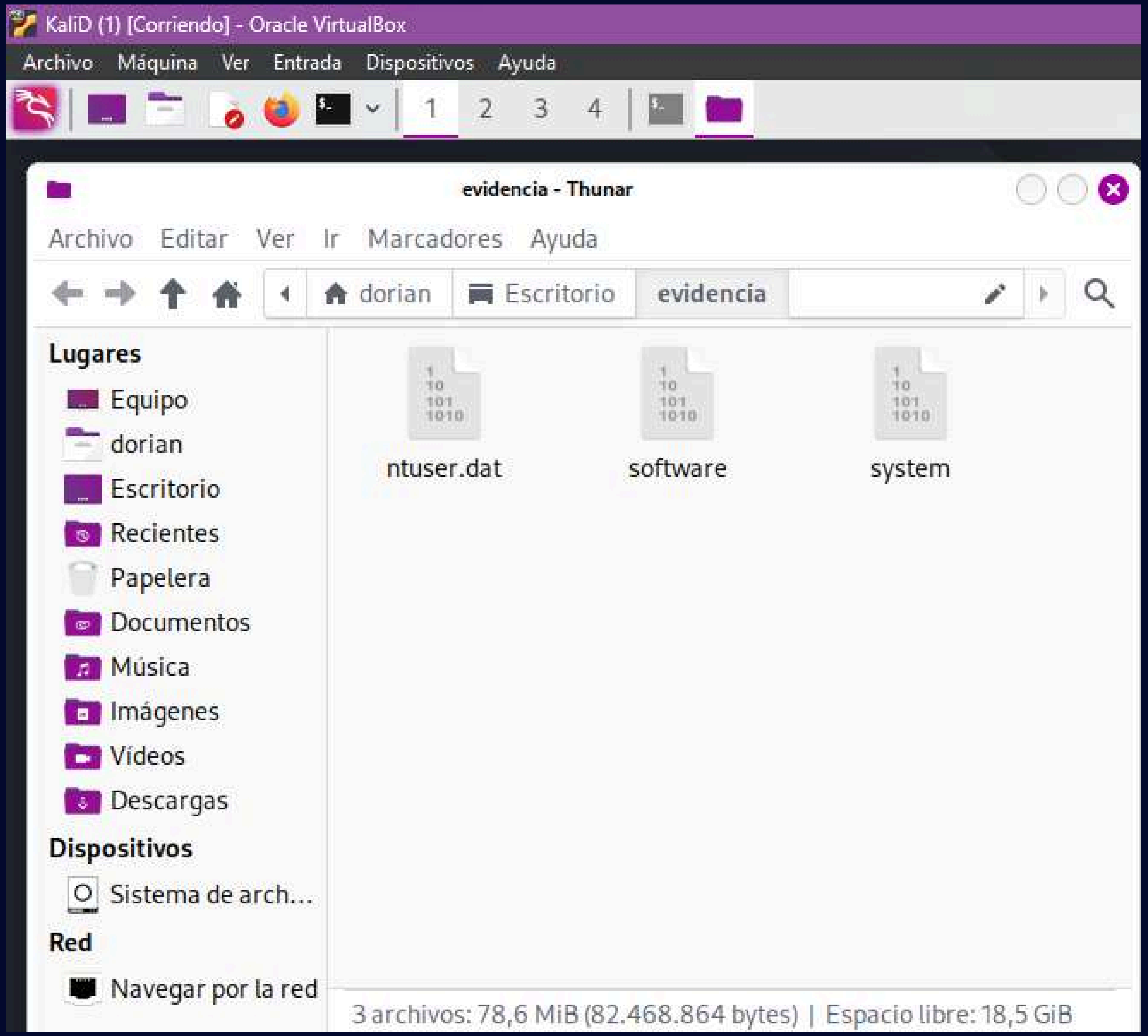
2019-12-04 18:04:16

```
70685642,,bobby@tesla.com,luwXpH7DBdk=,
70685643,,grantlinks@fbnet.org,eBn4jFt9eJowWTDeW6uAmw==,
70685644,,eric@cyber-consultants.net,FPU2dyCMSpjioxG6CatHBw==,
70685645,,hback@telia.com,O+vm6nzsKGg=,
70685646,,umm_chicken@hotmail.com,A99tU+YHSuo=,
70685647,,opteron_244@hotmail.com,pWyj7CB8k1c=,
70685648,,kli_oi@yahoo.com.br,vN5PVj+0D5euXGl9Y4jDJg==,
70685649,,kai.reiss@t-online.de,5WELykVWyV+XrIXpAZiRHQ==,
70685650,,pardosh88@gmail.com,RyPWmo5voYY=,
70685651,,kobrin@one.ee,hhJuiQeI5NQ=,
```

REGRIPPER

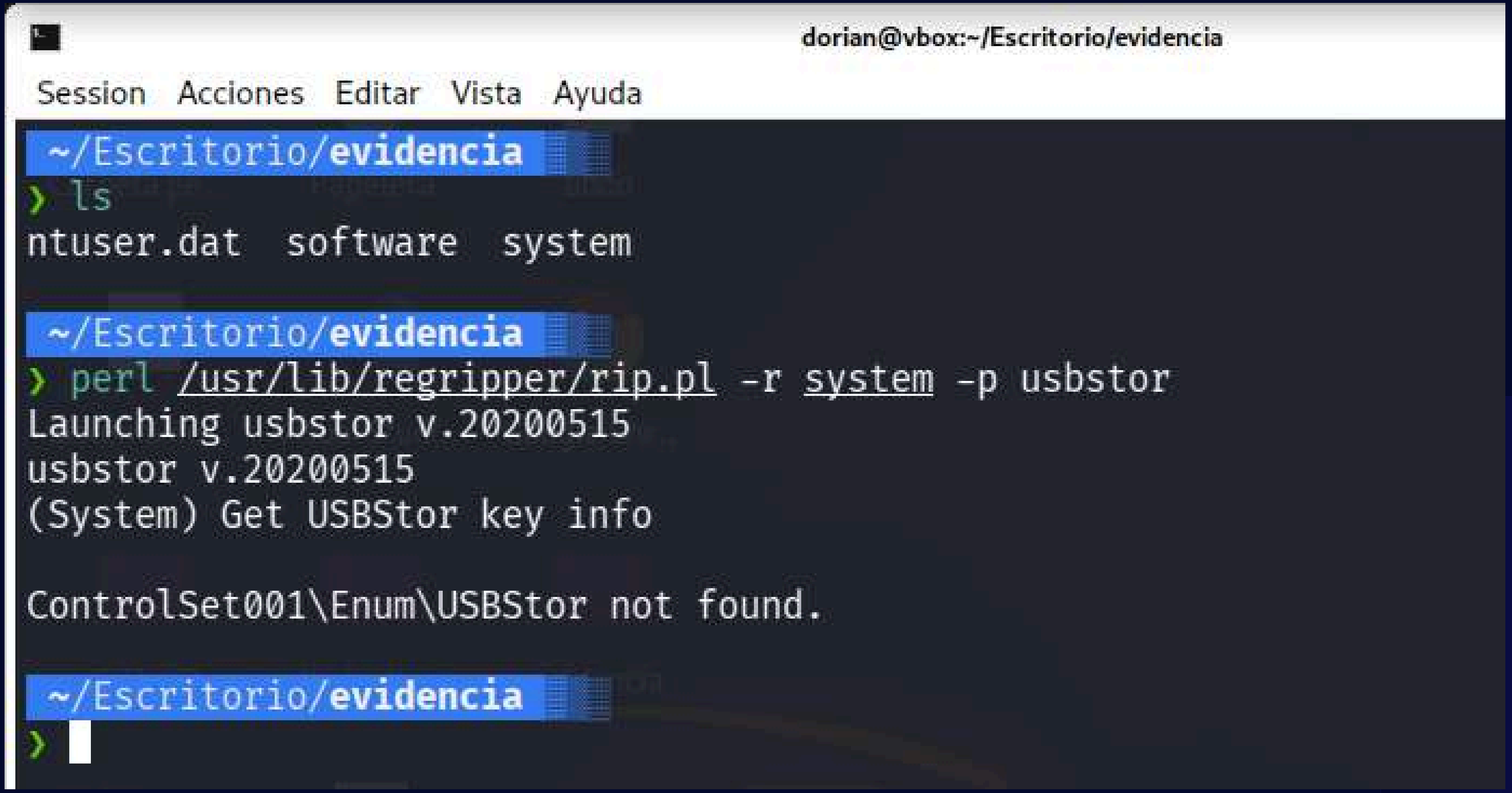
Análisis Forense

PRUEBA



3 archivos: 78,6 MiB (82.468.864 bytes) | Espacio libre: 18,5 GiB

LISTAR USB CONECTADOS



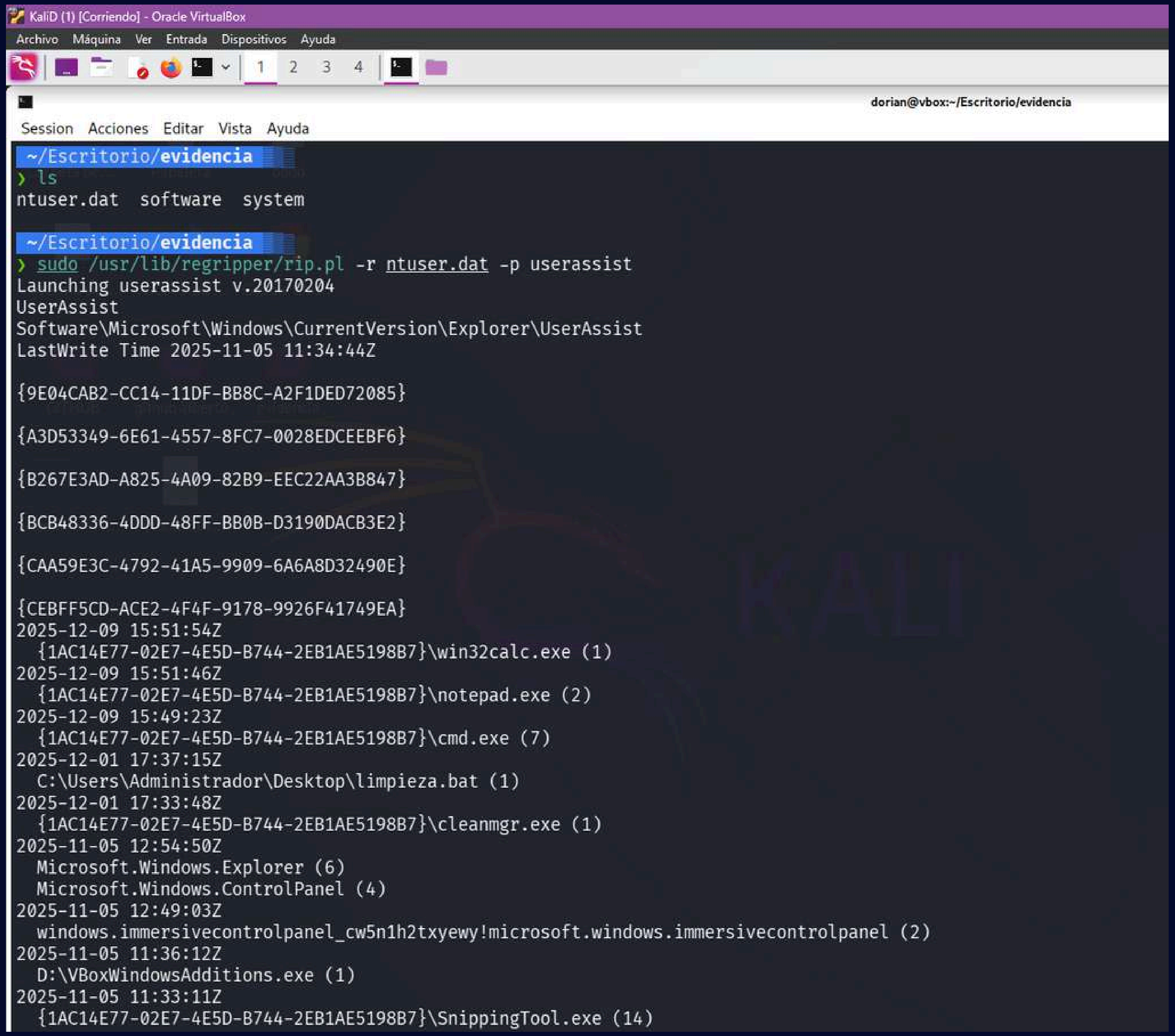
dorian@vbox:~/Escritorio/evidencia
Session Acciones Editar Vista Ayuda

```
~/Escritorio/evidencia
❯ ls
ntuser.dat  software  system

~/Escritorio/evidencia
❯ perl /usr/lib/regripper/rip.pl -r system -p usbstor
Launching usbstor v.20200515
usbstor v.20200515
(System) Get USBStor key info

ControlSet001\Enum\USBStor not found.

~/Escritorio/evidencia
❯
```

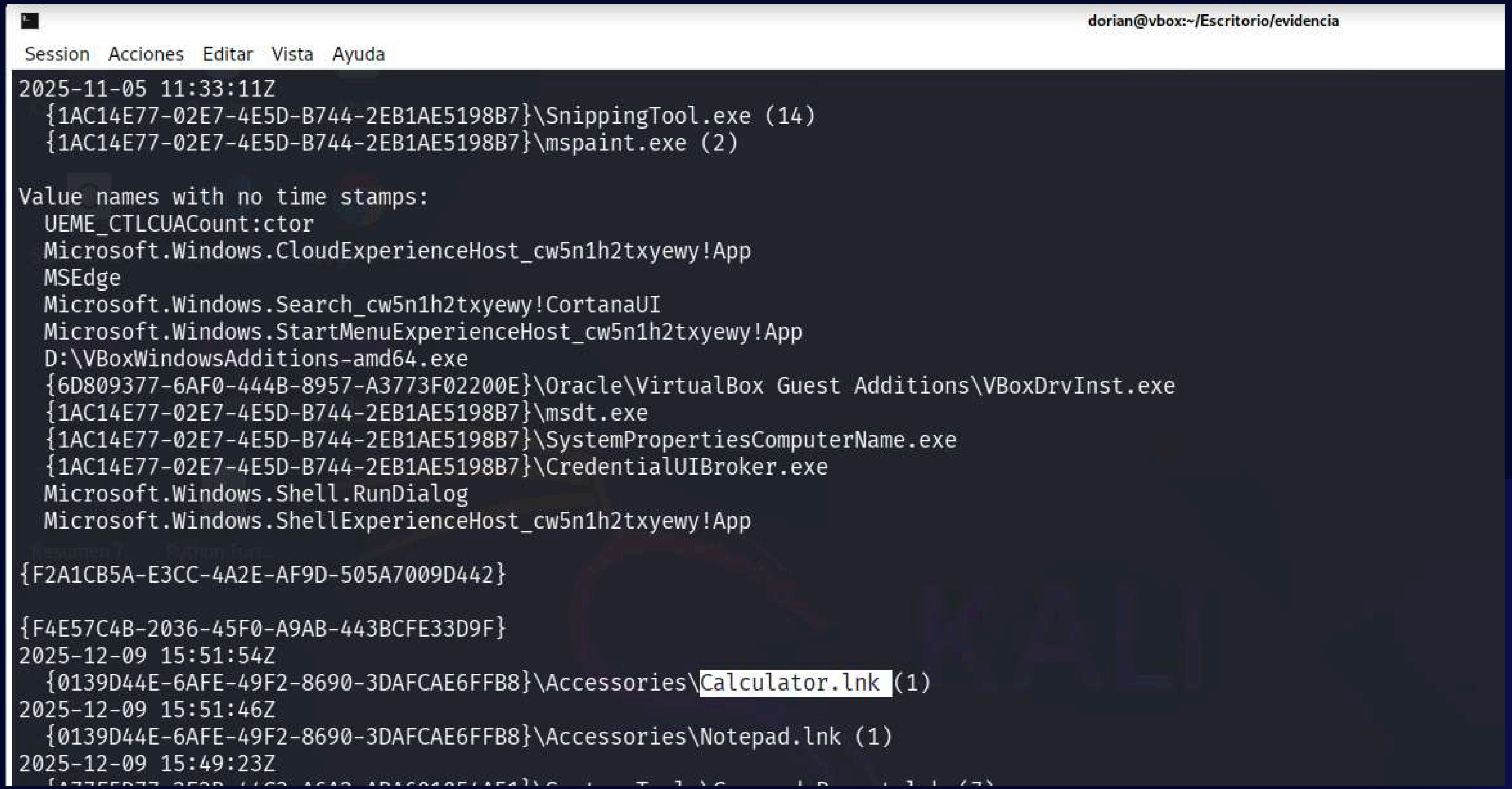
REGRIPPER

PRUEBA

LISTAR PROGRAMAS EJECUTADOS


KaliD (1) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
dorian@vbox:~/Escritorio/evidencia
Session Acciones Editar Vista Ayuda

```
 ~/Escritorio/evidencia
❯ ls
ntuser.dat  software  system

 ~/Escritorio/evidencia
❯ sudo /usr/lib/regripper/rip.pl -r ntuser.dat -p userassist
Launching userassist v.20170204
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time 2025-11-05 11:34:44Z

{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}

{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}

{B267E3AD-A825-4A09-82B9-EEC22AA3B847}

{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}

{CAA59E3C-4792-41A5-9909-6A6A8D32490E}

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
2025-12-09 15:51:54Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\win32calc.exe (1)
2025-12-09 15:51:46Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (2)
2025-12-09 15:49:23Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (7)
2025-12-01 17:37:15Z
  C:\Users\Administrador\Desktop\limpieza.bat (1)
2025-12-01 17:33:48Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cleanmgr.exe (1)
2025-11-05 12:54:50Z
  Microsoft.Windows.Explorer (6)
  Microsoft.Windows.ControlPanel (4)
2025-11-05 12:49:03Z
  windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel (2)
2025-11-05 11:36:12Z
  D:\VBoxWindowsAdditions.exe (1)
2025-11-05 11:33:11Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (14)
```

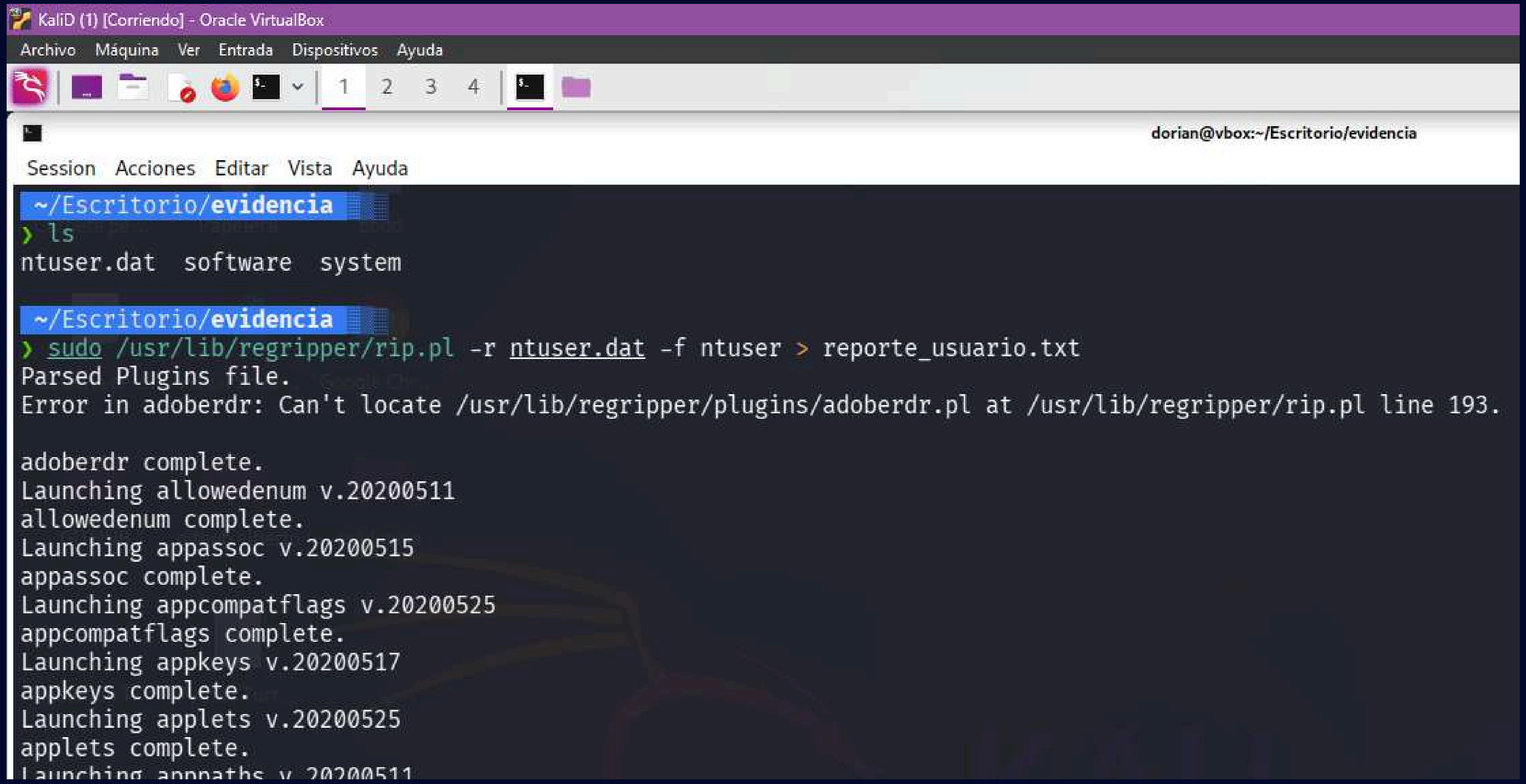

dorian@vbox:~/Escritorio/evidencia
Session Acciones Editar Vista Ayuda

```
2025-11-05 11:33:11Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (14)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (2)

Value names with no time stamps:
  UEME_CTLCUACount:ctor
  Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy!App
  MSEdge
  Microsoft.Windows.Search_cw5n1h2txyewy!CortanaUI
  Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy!App
  D:\VBoxWindowsAdditions-amd64.exe
  {6D809377-6AF0-444B-8957-A3773F02200E}\Oracle\VirtualBox Guest Additions\VBoxDrvInst.exe
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\msdt.exe
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SystemPropertiesComputerName.exe
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\CredentialUIBroker.exe
  Microsoft.Windows.Shell.RunDialog
  Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy!App

{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}

{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
2025-12-09 15:51:54Z
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Calculator.lnk (1)
2025-12-09 15:51:46Z
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Notepad.lnk (1)
2025-12-09 15:49:23Z
```

REGRIPPER

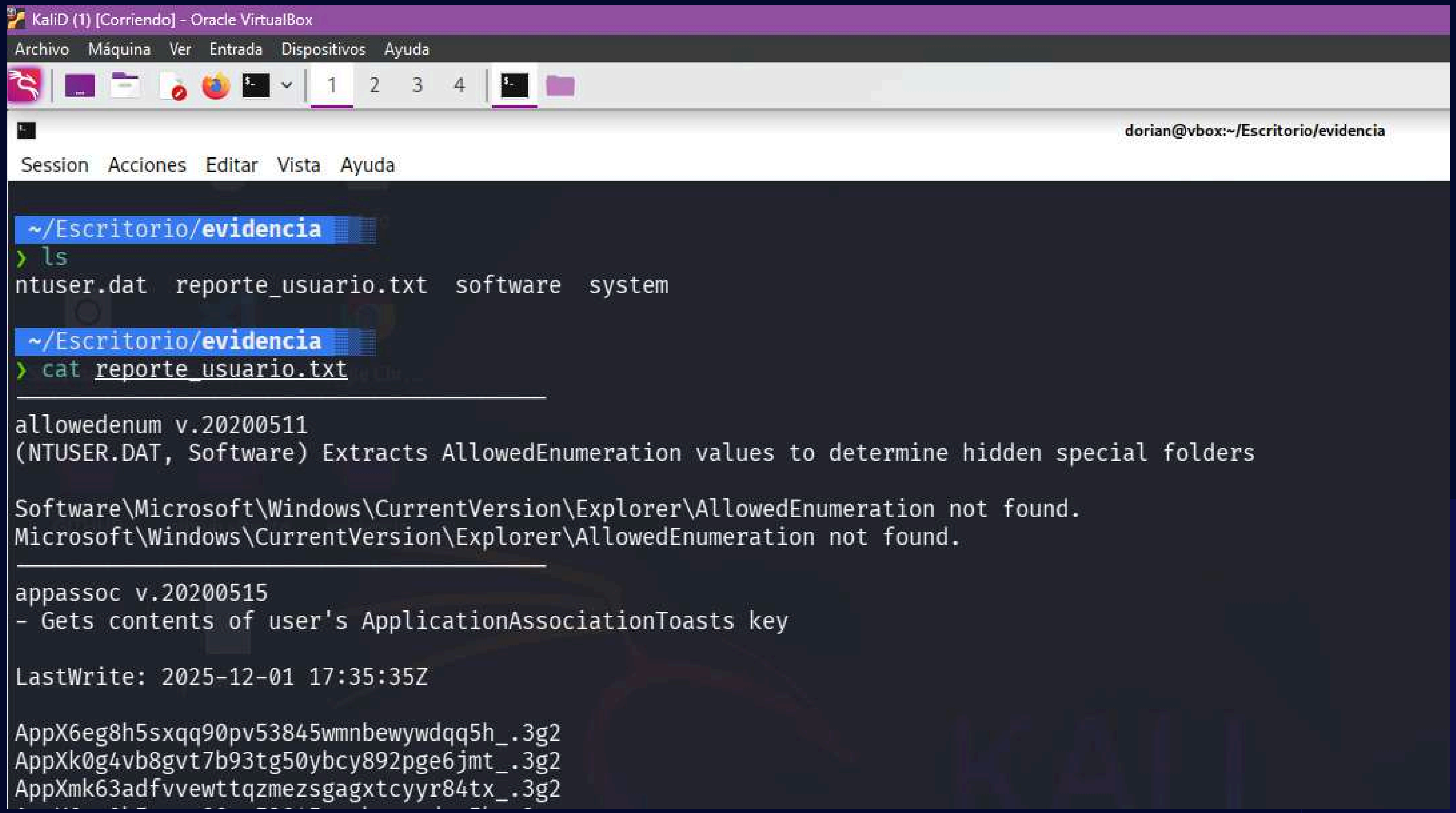
PRUEBA

REPORTE COMPLETO



KaliD (1) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
dorian@vbox:~/Escritorio/evidencia
Session Acciones Editar Vista Ayuda

```
 ~/Escritorio/evidencia
❯ ls
ntuser.dat  software  system

 ~/Escritorio/evidencia
❯ sudo /usr/lib/regripper/rip.pl -r ntuser.dat -f ntuser > reporte_usuario.txt
Parsed Plugins file.
Error in adoberdr: Can't locate /usr/lib/regripper/plugins/adoberdr.pl at /usr/lib/regripper/rip.pl line 193.

adoberdr complete.
Launching allowedenum v.20200511
allowedenum complete.
Launching appassoc v.20200515
appassoc complete.
Launching appcompatflags v.20200525
appcompatflags complete.
Launching appkeys v.20200517
appkeys complete.
Launching applets v.20200525
applets complete.
Launching apppaths v.20200511
```



KaliD (1) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
dorian@vbox:~/Escritorio/evidencia
Session Acciones Editar Vista Ayuda

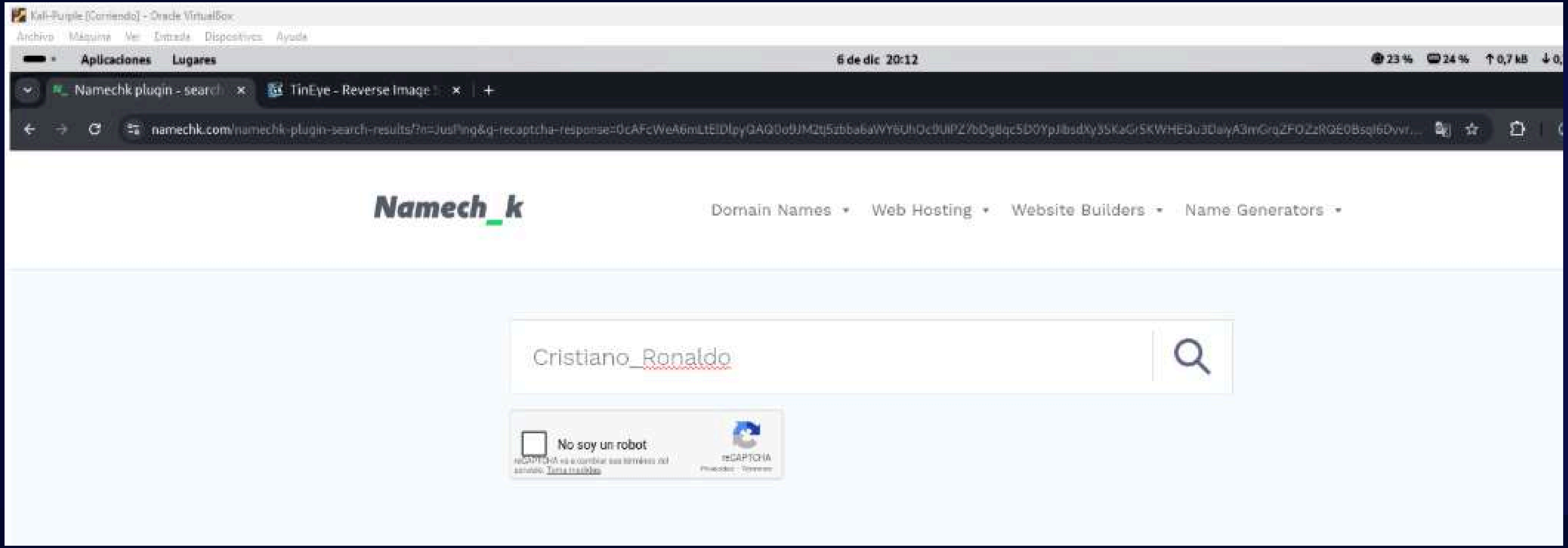
```
 ~/Escritorio/evidencia
❯ ls
ntuser.dat  reporte_usuario.txt  software  system

 ~/Escritorio/evidencia
❯ cat reporte_usuario.txt
----------------------------------------
allowedenum v.20200511
(NTUSER.DAT, Software) Extracts AllowedEnumeration values to determine hidden special folders

Software\Microsoft\Windows\CurrentVersion\Explorer\AllowedEnumeration not found.
Microsoft\Windows\CurrentVersion\Explorer\AllowedEnumeration not found.
----------------------------------------
appassoc v.20200515
- Gets contents of user's ApplicationAssociationToasts key

LastWrite: 2025-12-01 17:35:35Z

AppX6eg8h5sxqq90pv53845wmnbewywdqq5h_.3g2
AppXk0g4vb8gvt7b93tg50ybcy892pge6jmt_.3g2
AppXmk63adfvvewttqzmezsgagxtcyyr84tx_.3g2
```

+ NAMECHK

Disponibilidad

Uso Nombres

Identidad



namechk.com/namechk-plugin-search-results/?n=JusPing&g-recaptcha-response=0cAFcWeA6mLtEIDlpyQAQ0o9JM2tj5zbba6aWY6UhOc9UlPZ7bDg8qc5D0YpJbsdXy3SKaGr5KWHEQu3DaiyA3mGrqZFOZzRGE0Bsql6Dvvr...

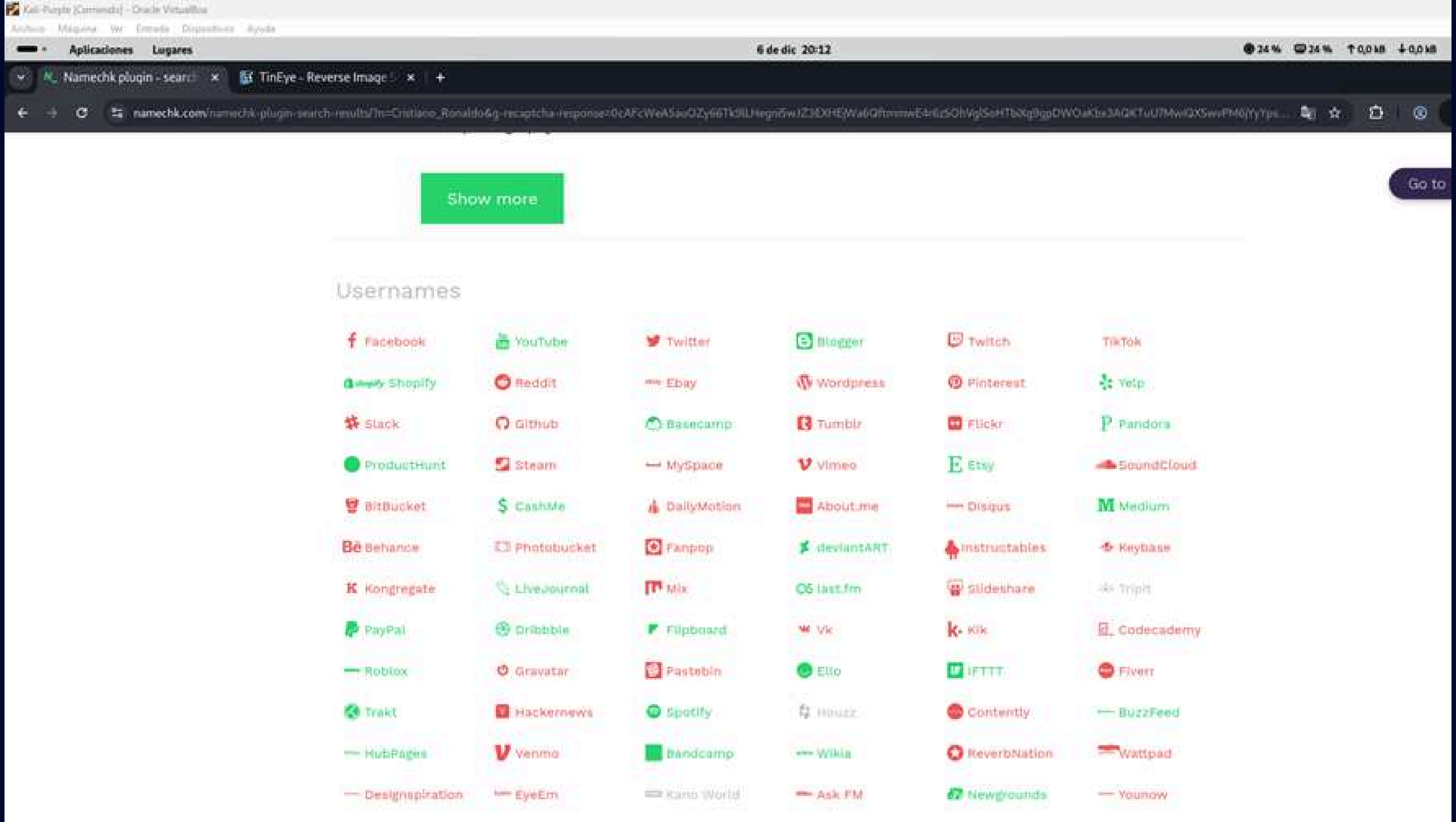
Cristiano_Ronaldo

□ No soy un robot

+ NAMECHK

Verde: No existe

Rojo: Existe.


Kali-Purple [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Lugares
6 de dic 20:12
Namechk plugin - search
TinEye - Reverse Image
namechk.com/namechk-plugin-search-results/?n=Cristiano_Ronaldo&g-recaptcha-response=0cAFcWeA5aoOZy66TkRLHegn
Show more
Go to

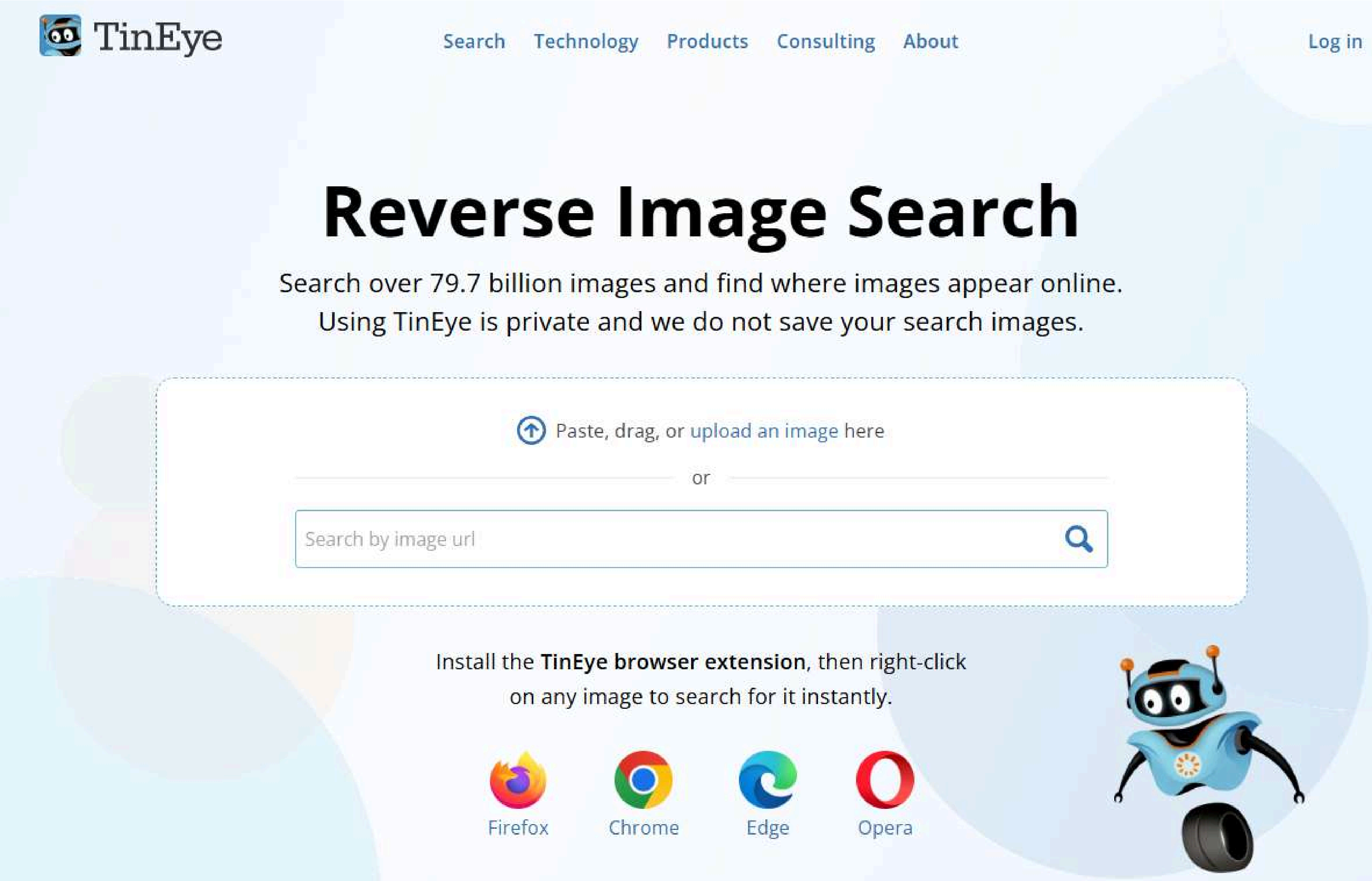
Usernames

Facebook	YouTube	Twitter	Blogger	Twitch	TikTok
Shopify	Reddit	Ebay	Wordpress	Pinterest	Yelp
Slack	Github	Basecamp	Tumblr	Flickr	Pandora
ProductHunt	Steam	MySpace	Vimeo	Etsy	SoundCloud
BitBucket	CashMe	DailyMotion	About.me	Disqus	Medium
Behance	Photobucket	Fanpop	devianART	Instructables	Keybase
Kongregate	LiveJournal	Mix	last.fm	Slideshare	Tripit
PayPal	Dribbble	Flipboard	Vk	Kik	Codecademy
Roblox	Gravatar	Pastebin	Ello	IFTTT	Fiverr
Trakt	Hackernews	Spotify	Houzz	Contently	BuzzFeed
HubPages	Venmo	Bandcamp	Wikia	ReverbNation	Wattpad
Designspiration	EyeEm	Kano World	Ask FM	Newgrounds	Younow

Busqueda

Rastreo

Fakes



TinEye

Reverse Image Search

Search over 79.7 billion images and find where images appear online.
Using TinEye is private and we do not save your search images.

Paste, drag, or upload an image here

or

Search by image url

Install the **TinEye browser extension**, then right-click on any image to search for it instantly.

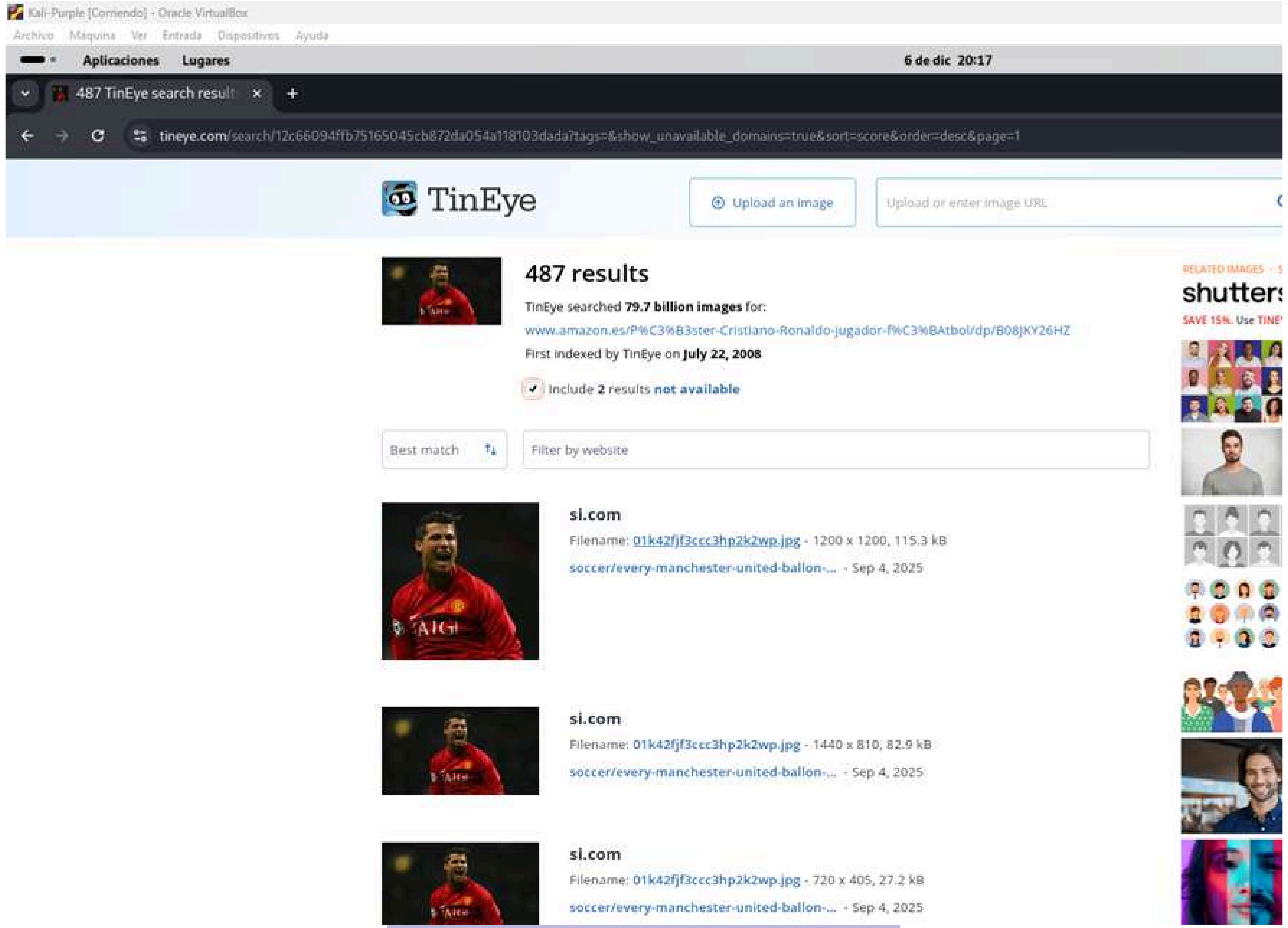
TINEYE

Busqueda

Rastreo

Fakes

TINEYE


Kali-Purple [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Lugares
6 de dic 20:17
487 TinEye search result
tineye.com/search/12c66094ffb75165045cb872da054a118103dada?tags=&show_unavailable_domains=true&sort=score&order=desc&page=1
TinEye
Upload an image
Upload or enter image URL
Best match
Filter by website
RELATED IMAGES
shutters
SAVE 15%. Use TINE

487 results

TinEye searched **79.7 billion images** for:

www.amazon.es/P%C3%B3ster-Cristiano-Ronaldo-Jugador-f%C3%BAtbol/dp/B08JKY26HZ

First indexed by TinEye on **July 22, 2008**

☑ Include **2** results **not available**

si.com
Filename: 01k42fjf3ccc3hp2k2wp.jpg - 1200 x 1200, 115.3 kB
soccer/every-manchester-united-ballon-... - Sep 4, 2025

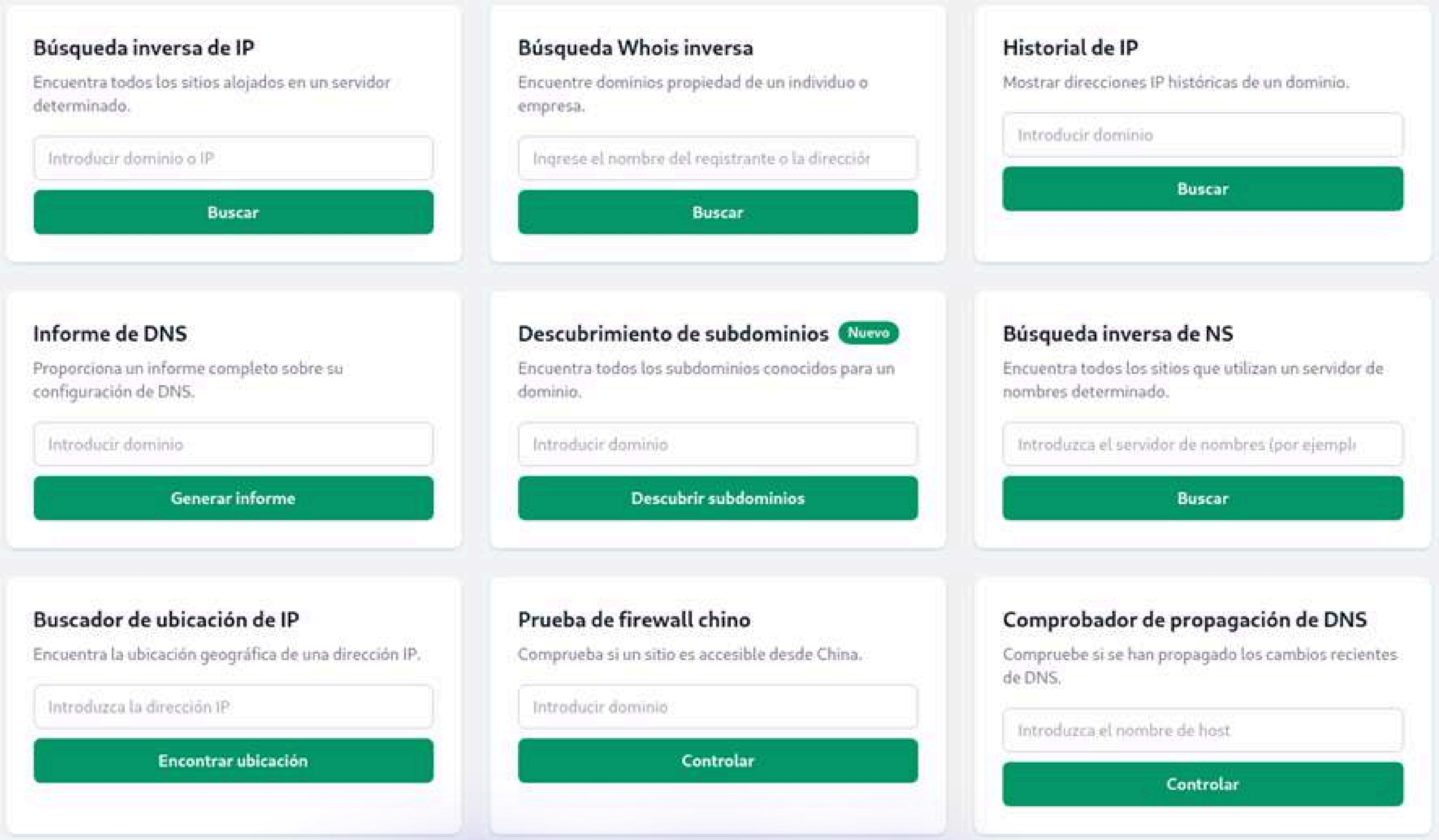
si.com
Filename: 01k42fjf3ccc3hp2k2wp.jpg - 1440 x 810, 82.9 kB
soccer/every-manchester-united-ballon-... - Sep 4, 2025

si.com
Filename: 01k42fjf3ccc3hp2k2wp.jpg - 720 x 405, 27.2 kB
soccer/every-manchester-united-ballon-... - Sep 4, 2025

Redes

DNS

IPs



Búsqueda inversa de IP

Encuentra todos los sitios alojados en un servidor determinado.

Introducir dominio o IP

Buscar

Búsqueda Whois inversa

Encuentre dominios propiedad de un individuo o empresa.

Ingrese el nombre del registrante o la direcciór

Buscar

Historial de IP

Mostrar direcciones IP históricas de un dominio.

Introducir dominio

Buscar

Informe de DNS

Proporciona un informe completo sobre su configuración de DNS.

Introducir dominio

Generar informe

Descubrimiento de subdominios Nuevo

Encuentra todos los subdominios conocidos para un dominio.

Introducir dominio

Descubrir subdominios

Búsqueda inversa de NS

Encuentra todos los sitios que utilizan un servidor de nombres determinado.

Introduzca el servidor de nombres (por ejempl

Buscar

Buscador de ubicación de IP

Encuentra la ubicación geográfica de una dirección IP.

Introduzca la dirección IP

Encontrar ubicación

Prueba de firewall chino

Comprueba si un sitio es accesible desde China.

Introducir dominio

Controlar

Comprobador de propagación de DNS

Compruebe si se han propagado los cambios recientes de DNS.

Introduzca el nombre de host

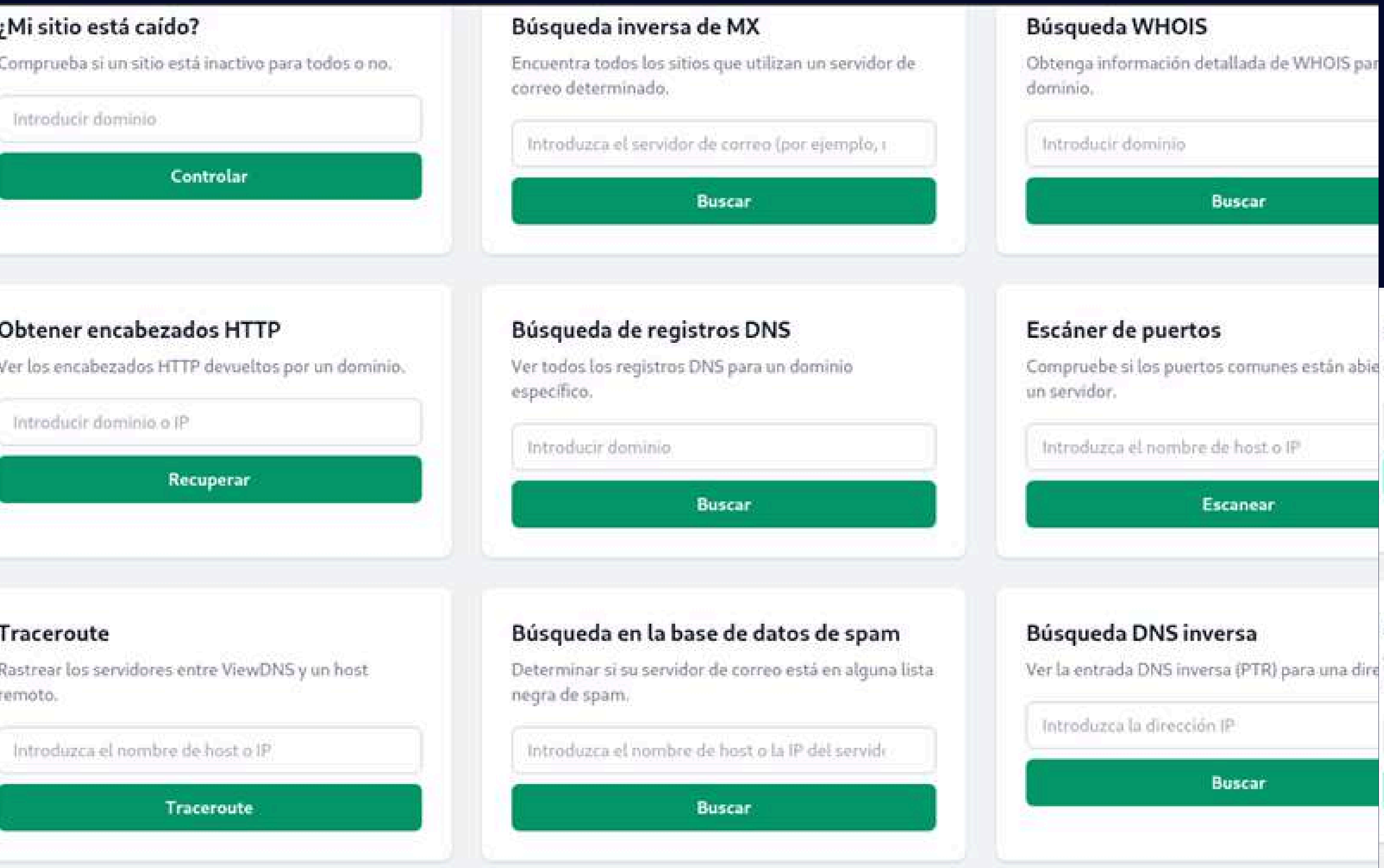
Controlar

+ VIEWDNS

Redes

DNS

IPs



¿Mi sitio está caído?

Comprueba si un sitio está inactivo para todos o no.

Introducir dominio

Controlar

Búsqueda inversa de MX

Encuentra todos los sitios que utilizan un servidor de correo determinado.

Introduzca el servidor de correo (por ejemplo, ı

Buscar

Búsqueda WHOIS

Obtenga información detallada de WHOIS par dominio.

Introducir dominio

Buscar

Obtener encabezados HTTP

Ver los encabezados HTTP devueltos por un dominio.

Introducir dominio o IP

Recuperar

Búsqueda de registros DNS

Ver todos los registros DNS para un dominio específico.

Introducir dominio

Buscar

Escáner de puertos

Compruebe si los puertos comunes están abie un servidor.

Introduzca el nombre de host o IP

Escanear

Traceroute

Rastrear los servidores entre ViewDNS y un host remoto.

Introduzca el nombre de host o IP

Traceroute

Búsqueda en la base de datos de spam

Determinar si su servidor de correo está en alguna lista negra de spam.

Introduzca el nombre de host o la IP del servid

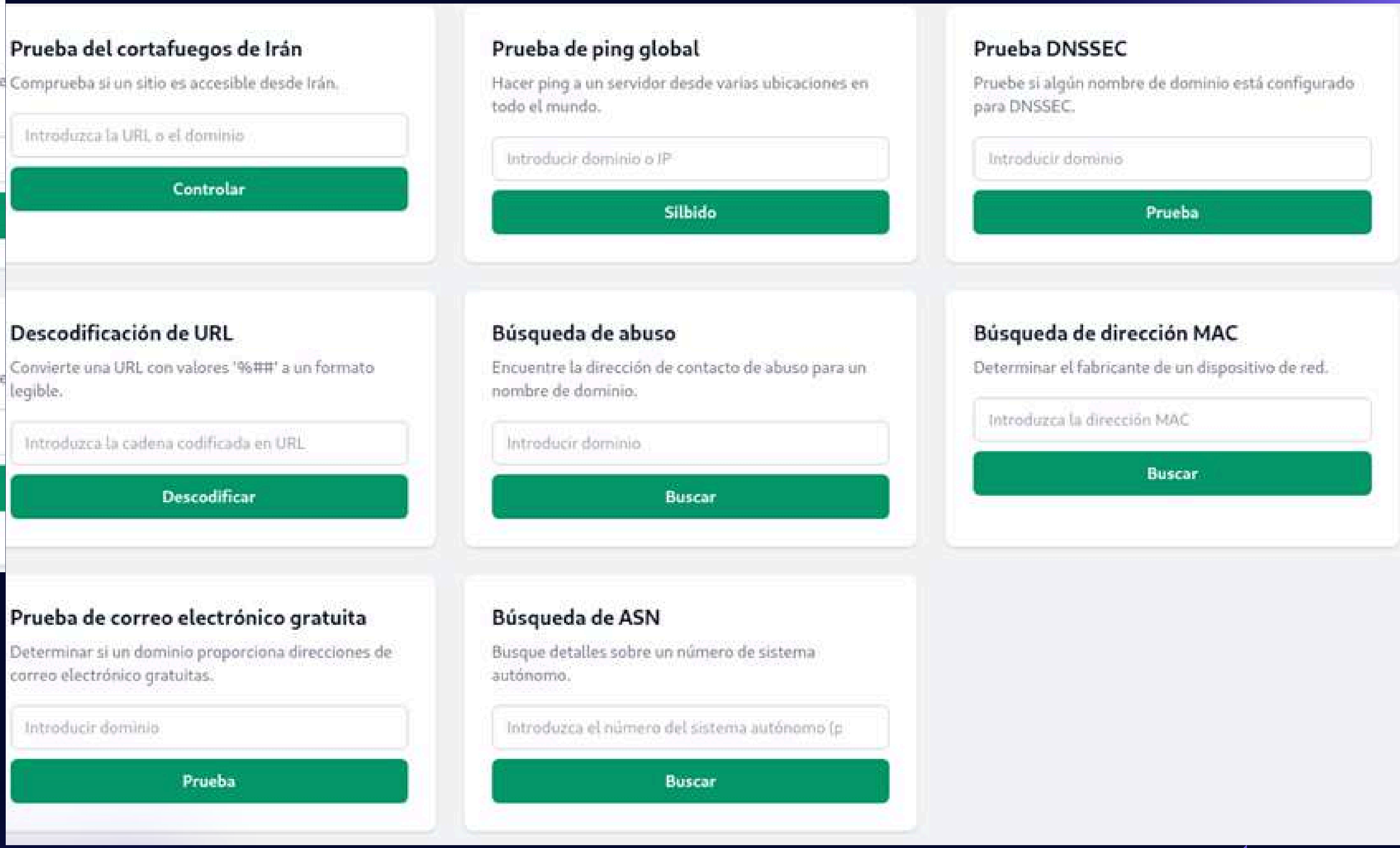
Buscar

Búsqueda DNS inversa

Ver la entrada DNS inversa (PTR) para una dire

Introduzca la dirección IP

Buscar



Prueba del cortafuegos de Irán

Comprueba si un sitio es accesible desde Irán.

Introduzca la URL o el dominio

Controlar

Prueba de ping global

Hacer ping a un servidor desde varias ubicaciones en todo el mundo.

Introducir dominio o IP

Silbido

Prueba DNSSEC

Pruebe si algún nombre de dominio está configurado para DNSSEC.

Introducir dominio

Prueba

Descodificación de URL

Convierte una URL con valores '%##' a un formato legible.

Introduzca la cadena codificada en URL

Descodificar

Búsqueda de abuso

Encuentre la dirección de contacto de abuso para un nombre de dominio.

Introducir dominio

Buscar

Búsqueda de dirección MAC

Determinar el fabricante de un dispositivo de red.

Introduzca la dirección MAC

Buscar

Prueba de correo electrónico gratuita

Determinar si un dominio proporciona direcciones de correo electrónico gratuitas.

Introducir dominio

Prueba

Búsqueda de ASN

Busque detalles sobre un número de sistema autónomo.

Introduzca el número del sistema autónomo (p

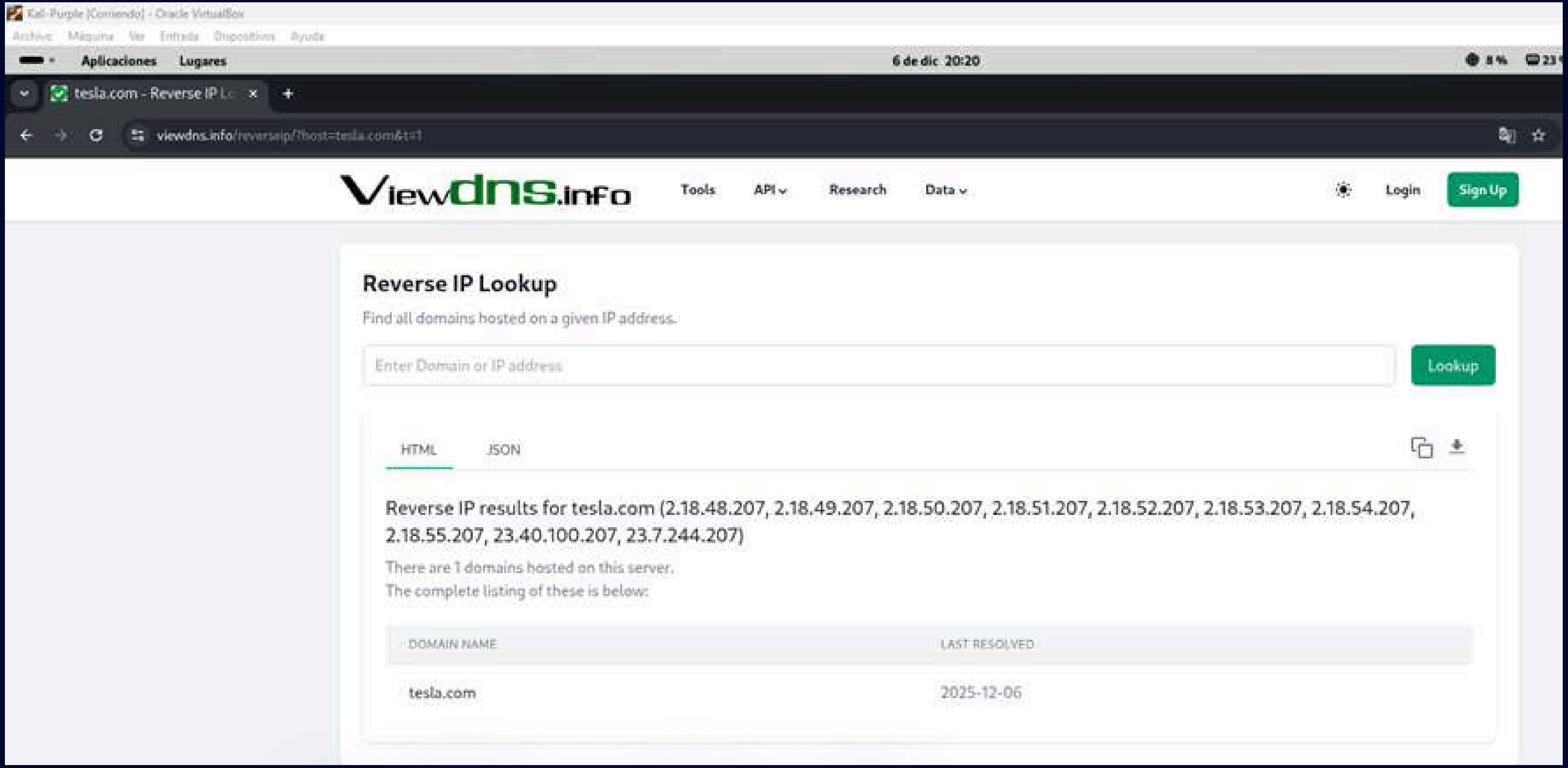
Buscar

+ VIEWDNS

Redes

DNS

IPs


Kali-Purple [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Lugares
6 de dic 20:20
tesla.com - Reverse IP Lo
viewdns.info/reverseip/?host=tesla.com&t=1
ViewDNS.info
Tools
API
Research
Data
Login
Sign Up
Enter Domain or IP address
Lookup
HTML
JSON

Reverse IP Lookup

Find all domains hosted on a given IP address.

Reverse IP results for tesla.com (2.18.48.207, 2.18.49.207, 2.18.50.207, 2.18.51.207, 2.18.52.207, 2.18.53.207, 2.18.54.207, 2.18.55.207, 23.40.100.207, 23.7.244.207)

There are 1 domains hosted on this server.
The complete listing of these is below:

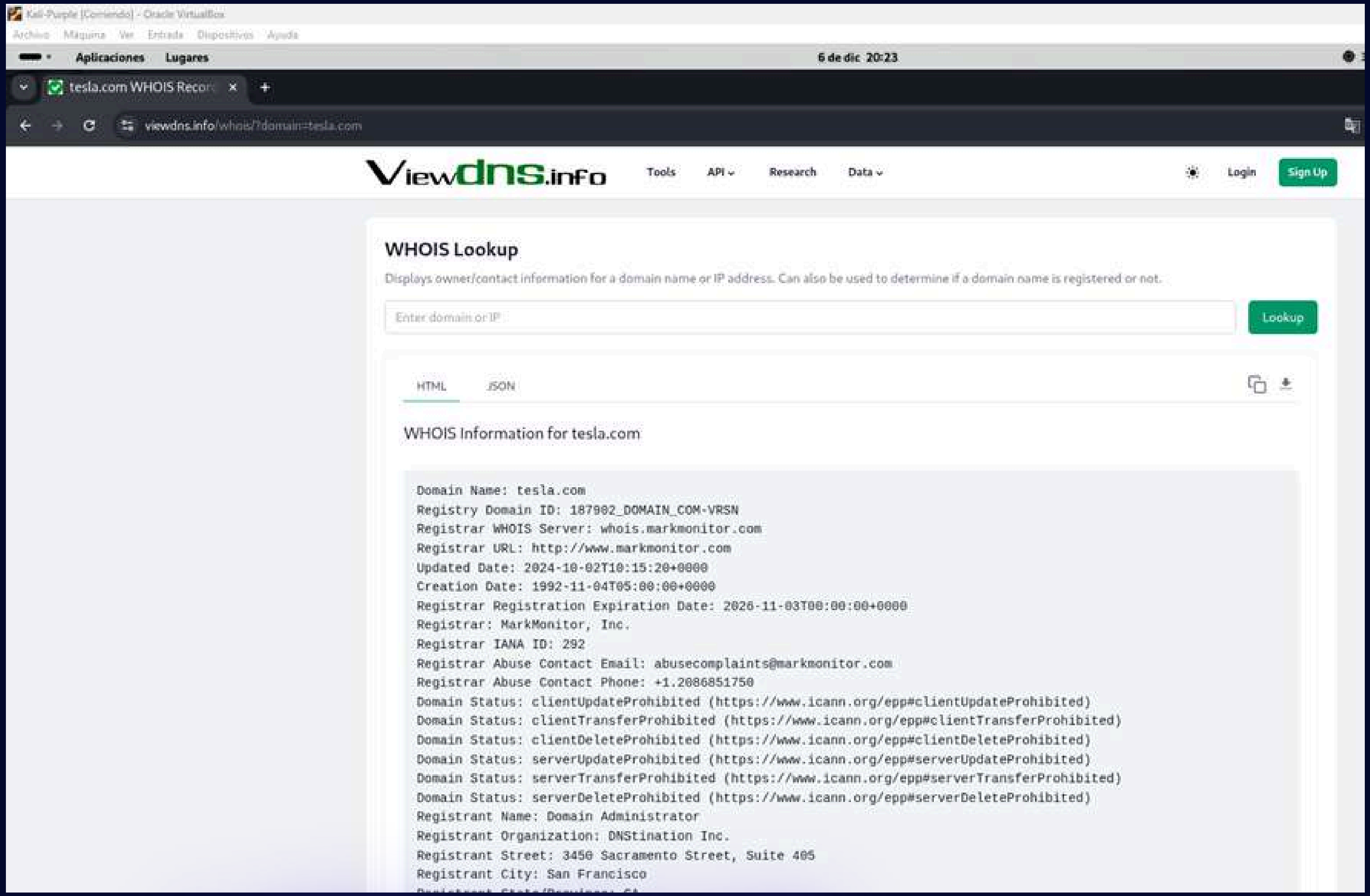
DOMAIN NAME	LAST RESOLVED
tesla.com	2025-12-06

+ VIEWDNS

Redes

DNS

IPs


Kali-Purple [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Lugares
6 de dic 20:23
tesla.com WHOIS Recor
viewdns.info/whois/?domain=tesla.com
ViewDNS.info
Tools
API
Research
Data
Login
Sign Up

WHOIS Lookup

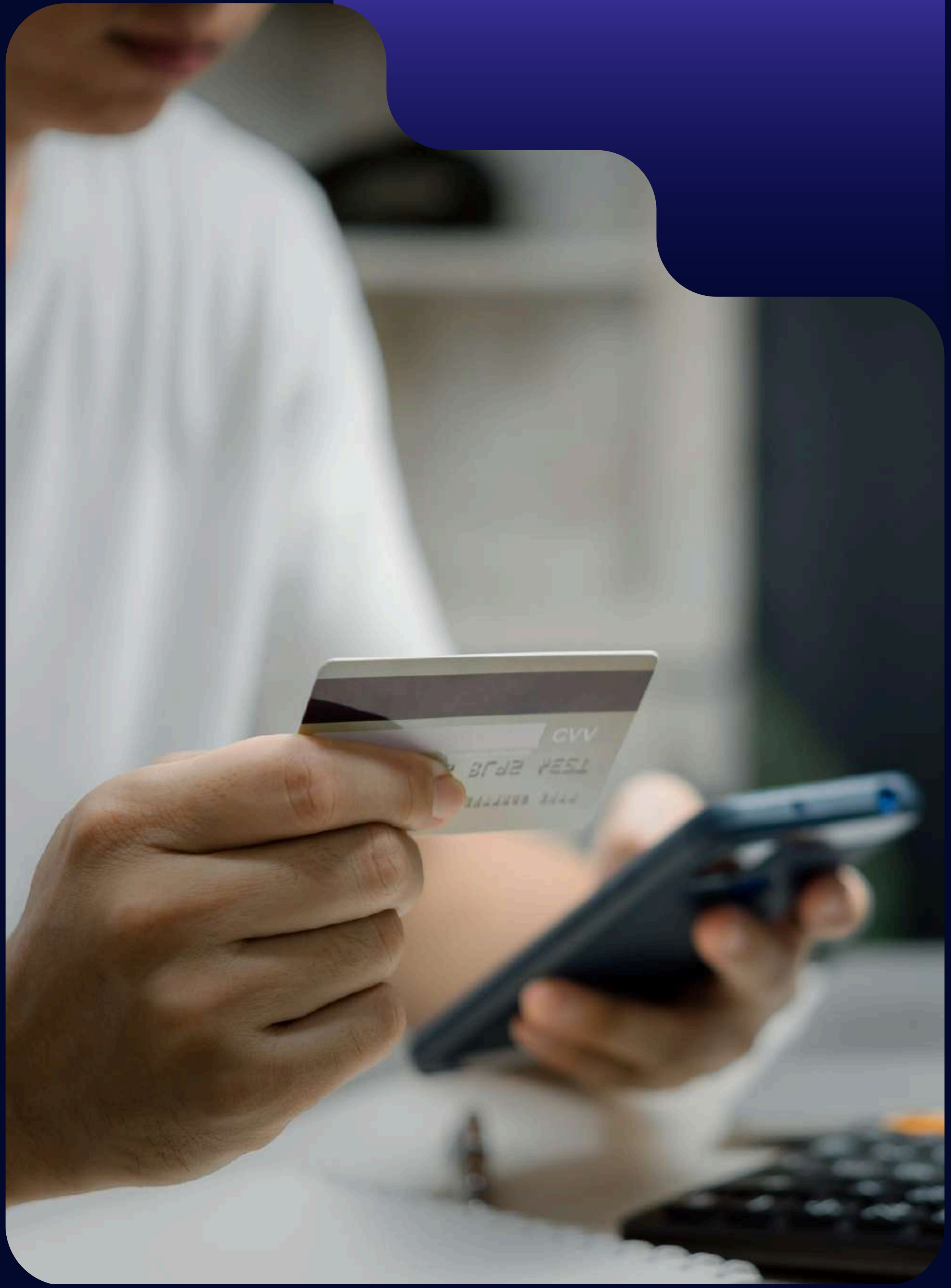
Displays owner/contact information for a domain name or IP address. Can also be used to determine if a domain name is registered or not.

Enter domain or IP — Lookup

WHOIS Information for tesla.com

```
Domain Name: tesla.com
Registry Domain ID: 187902_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2024-10-02T10:15:20+0000
Creation Date: 1992-11-04T05:00:00+0000
Registrar Registration Expiration Date: 2026-11-03T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Name: Domain Administrator
Registrant Organization: DNStination Inc.
Registrant Street: 3450 Sacramento Street, Suite 405
Registrant City: San Francisco
Registrant State/Province: CA
```

+ VIEWDNS



¡MUCHAS GRACIAS!