Práctica 2: Uso avanzado de Shodan y ZoomEye para reconocimiento pasivo

Objetivo

Utilizar motores de búsqueda especializados en dispositivos y servicios expuestos en Internet (**Shodan** y **Zoomeye**) para recopilar información crítica sobre una infraestructura empresarial simulada.

1. Entorno virtualizado recomendado

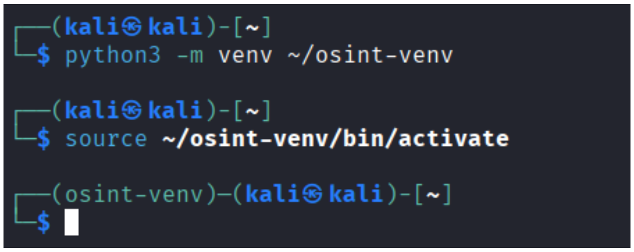
Máquina atacante

- **SO**: *Kali Linux 2025.2*
- **Requisitos**:
  - *Navegador Firefox o Chromium*
  - *Python3 y pip*
  - *Cuenta gratuita en Shodan y ZoomEye*

2. Instalación de herramientas y API

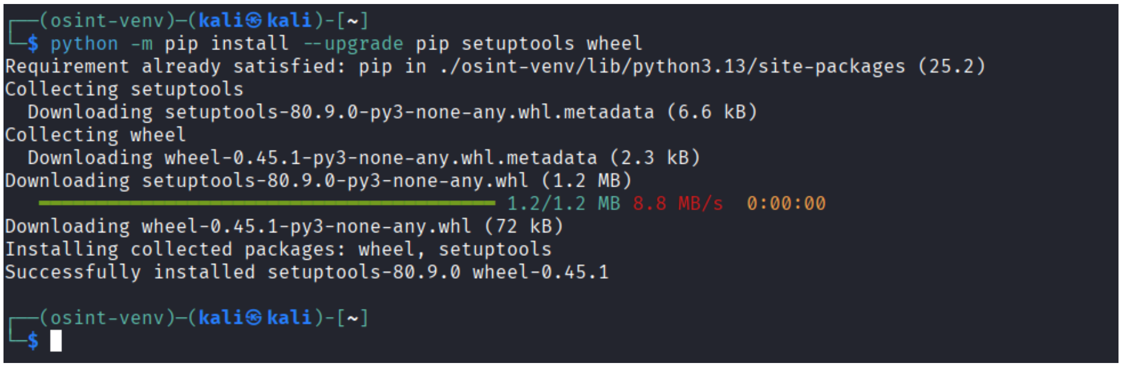
Usar un entorno virtual aislado y no ejecutar como root si se puee (mejor con un usuario normal):

```
# como usuario normal (recomendado).
python3 -m venv ~/osint-venv
source ~/osint-venv/bin/activate
```



```
┌──(kali㉿kali)-[~]
└─$ python3 -m venv ~/osint-venv

┌──(kali㉿kali)-[~]
└─$ source ~/osint-venv/bin/activate

┌──(osint-venv)─(kali㉿kali)-[~]
└─$ █
```

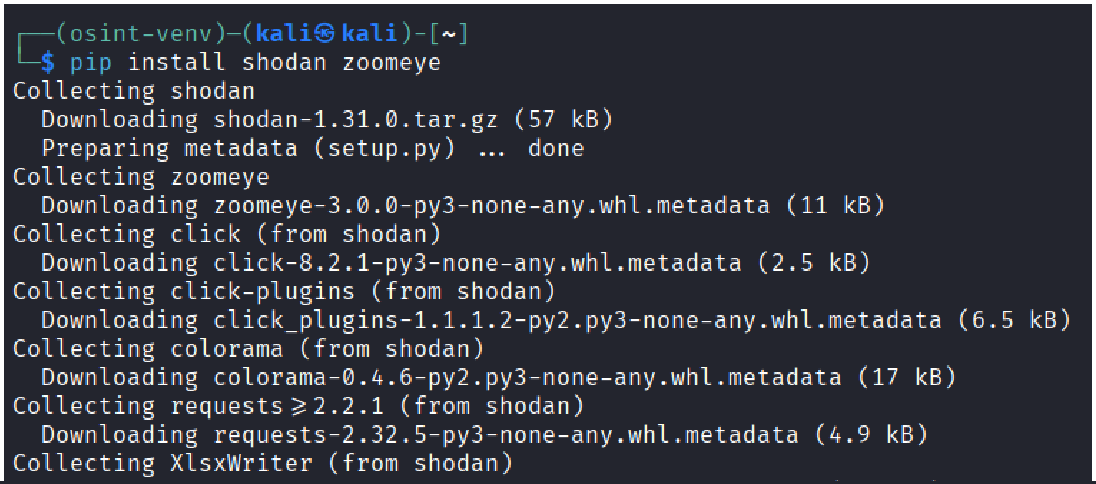
```
# actualiza herramientas del venv
python -m pip install --upgrade pip setuptools Wheel
```



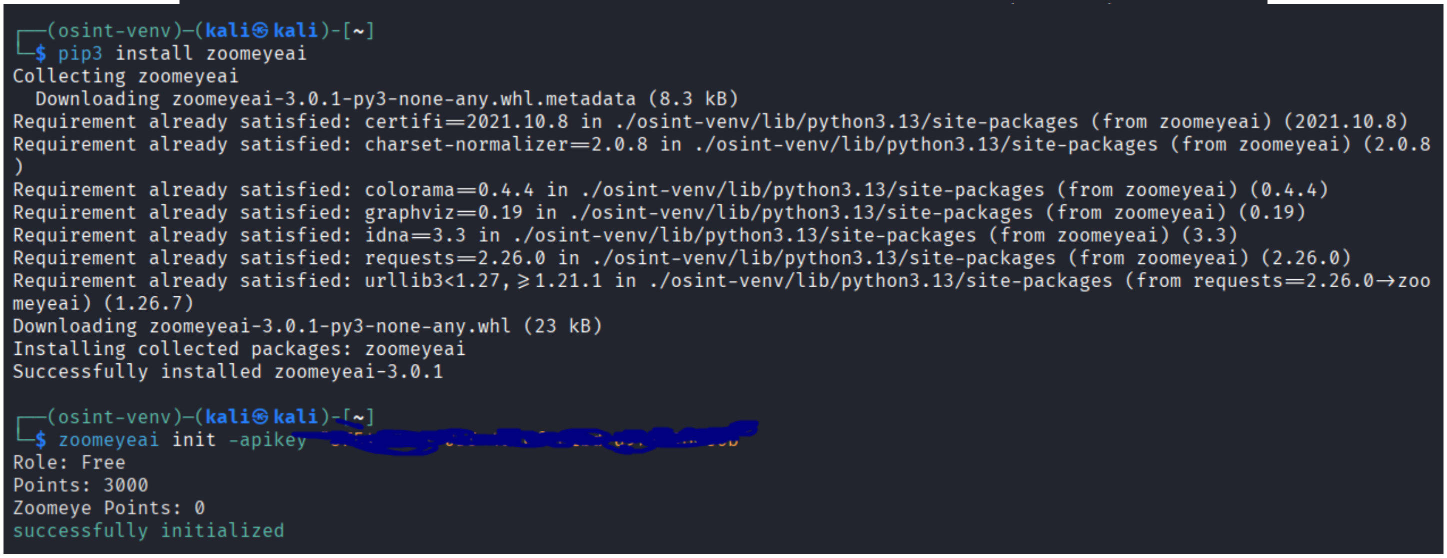
```
┌──(osint-venv)─(kali㉿kali)-[~]
└─$ python -m pip install --upgrade pip setuptools wheel
Requirement already satisfied: pip in ./osint-venv/lib/python3.13/site-packages (25.2)
Collecting setuptools
  Downloading setuptools-80.9.0-py3-none-any.whl.metadata (6.6 kB)
Collecting wheel
  Downloading wheel-0.45.1-py3-none-any.whl.metadata (2.3 kB)
Downloading setuptools-80.9.0-py3-none-any.whl (1.2 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.2/1.2 MB 8.8 MB/s  0:00:00
Downloading wheel-0.45.1-py3-none-any.whl (72 kB)
Installing collected packages: wheel, setuptools
Successfully installed setuptools-80.9.0 wheel-0.45.1

┌──(osint-venv)─(kali㉿kali)-[~]
└─$ ▮
```

3) Instala Shodan y ZoomEyeAI dentro del venv

```
pip install shodan zoomeyeai
```

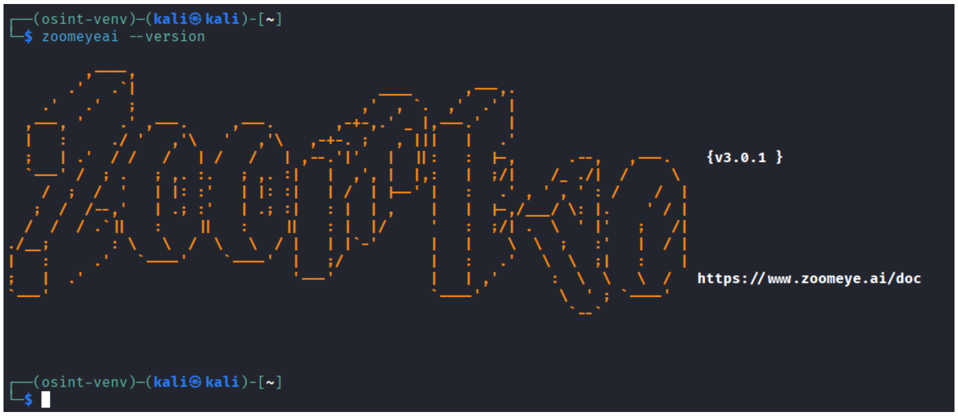


```
┌──(osint-venv)─(kali㉿kali)-[~]
└─$ pip install shodan zoomeye
Collecting shodan
  Downloading shodan-1.31.0.tar.gz (57 kB)
  Preparing metadata (setup.py) ... done
Collecting zoomeye
  Downloading zoomeye-3.0.0-py3-none-any.whl.metadata (11 kB)
Collecting click (from shodan)
  Downloading click-8.2.1-py3-none-any.whl.metadata (2.5 kB)
Collecting click-plugins (from shodan)
  Downloading click_plugins-1.1.1.2-py2.py3-none-any.whl.metadata (6.5 kB)
Collecting colorama (from shodan)
  Downloading colorama-0.4.6-py2.py3-none-any.whl.metadata (17 kB)
Collecting requests≥2.2.1 (from shodan)
  Downloading requests-2.32.5-py3-none-any.whl.metadata (4.9 kB)
Collecting XlsxWriter (from shodan)
```



```
┌──(osint-venv)─(kali㉿kali)-[~]
└─$ pip3 install zoomeyeai
Collecting zoomeyeai
  Downloading zoomeyeai-3.0.1-py3-none-any.whl.metadata (8.3 kB)
Requirement already satisfied: certifi═2021.10.8 in ./osint-venv/lib/python3.13/site-packages (from zoomeyeai) (2021.10.8)
Requirement already satisfied: charset-normalizer═2.0.8 in ./osint-venv/lib/python3.13/site-packages (from zoomeyeai) (2.0.8
)
Requirement already satisfied: colorama═0.4.4 in ./osint-venv/lib/python3.13/site-packages (from zoomeyeai) (0.4.4)
Requirement already satisfied: graphviz═0.19 in ./osint-venv/lib/python3.13/site-packages (from zoomeyeai) (0.19)
Requirement already satisfied: idna═3.3 in ./osint-venv/lib/python3.13/site-packages (from zoomeyeai) (3.3)
Requirement already satisfied: requests═2.26.0 in ./osint-venv/lib/python3.13/site-packages (from zoomeyeai) (2.26.0)
Requirement already satisfied: urllib3<1.27,≥1.21.1 in ./osint-venv/lib/python3.13/site-packages (from requests═2.26.0→zoo
meyeai) (1.26.7)
Downloading zoomeyeai-3.0.1-py3-none-any.whl (23 kB)
Installing collected packages: zoomeyeai
Successfully installed zoomeyeai-3.0.1

┌──(osint-venv)─(kali㉿kali)-[~]
└─$ zoomeyeai init -apikey [redacted]
Role: Free
Points: 3000
Zoomeye Points: 0
successfully initialized
```

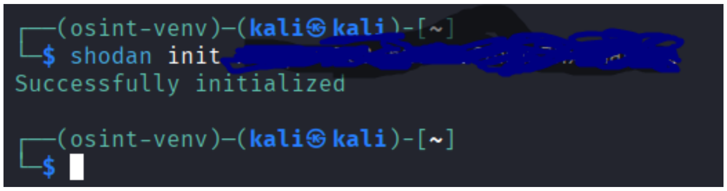
```
shodan version
zoomeyeai -help
```



```
┌──(osint-venv)─(kali㉿kali)-[~]
└─$ zoomeyeai --version

                                        {v3.0.1 }

                                        https://www.zoomeye.ai/doc

┌──(osint-venv)─(kali㉿kali)-[~]
└─$ ▌
```

Inicia sesión Shodan / configura:

```
shodan init TU_API_KEY
```



```
┌──(osint-venv)─(kali㉿kali)-[~]
└─$ shodan init [redacted]
Successfully initialized

┌──(osint-venv)─(kali㉿kali)-[~]
└─$ ▌
```

Cada vez que quieras usar estas herramientas, activa el venv:

```
source ~/osint-venv/bin/activate
```

Para salir del entorno virtual (venv):

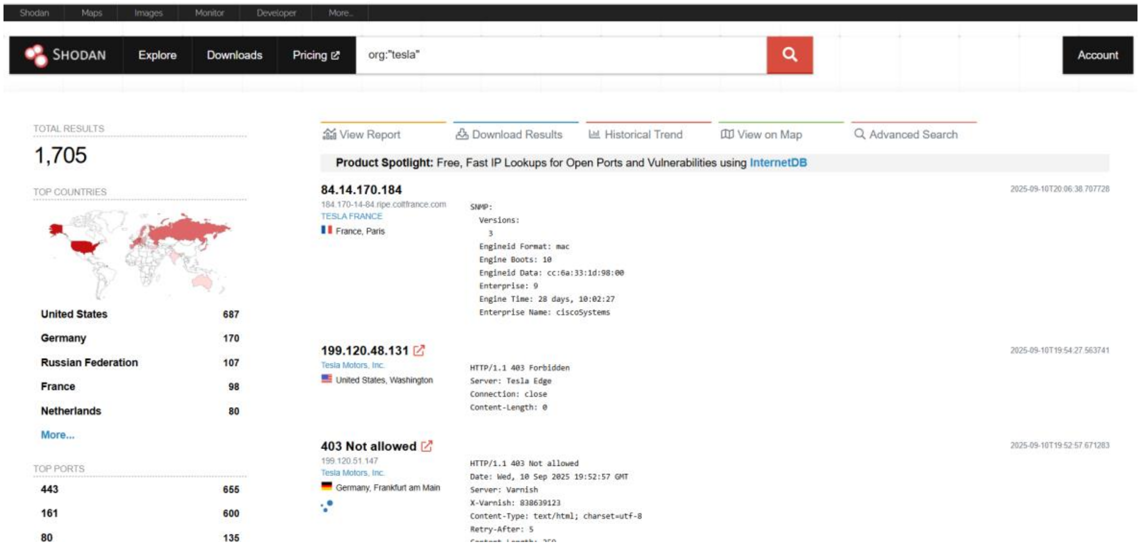
```
deactivate
```

3. SHODAN

1 - Búsqueda básica desde web

Ir a https://www.shodan.io

Buscar: `org:"tesla"` o `hostname:"vpn.tesla.com"`



org:"tesla"

TOTAL RESULTS

1,705

TOP COUNTRIES

United States	687
Germany	170
Russian Federation	107
France	98
Netherlands	80

More...

TOP PORTS

443	655
161	600
80	135

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

84.14.170.184 2025-09-10T20:06:38.707728
184.170-14-84.ripe.coltfrance.com
TESLA FRANCE
France, Paris

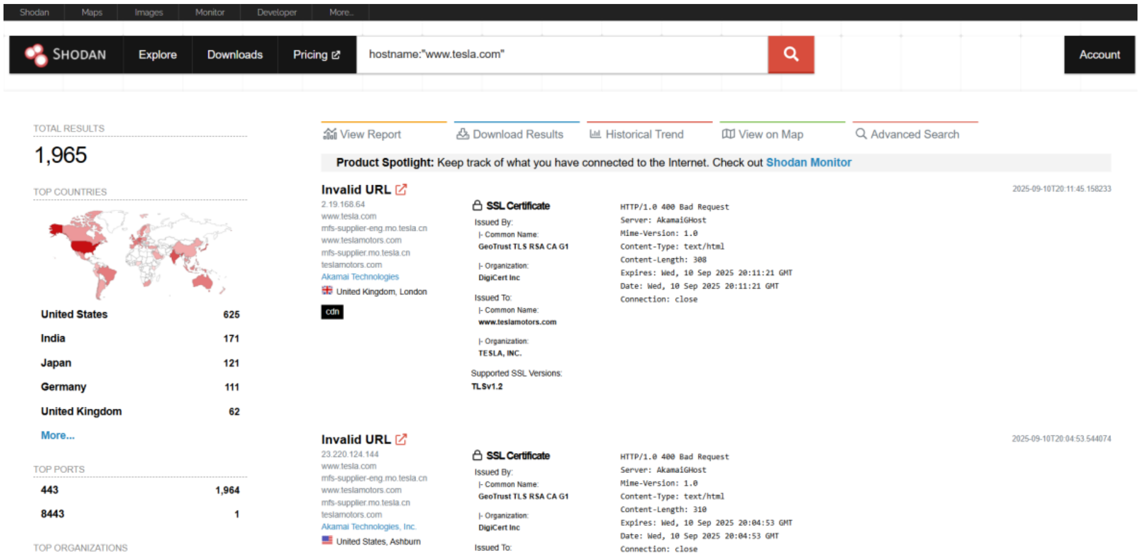
```
SNMP:
  Versions:
    3
  Engineid Format: mac
  Engine Boots: 10
  Engineid Data: cc:6a:33:1d:98:00
  Enterprise: 9
  Engine Time: 28 days, 10:02:27
  Enterprise Name: ciscoSystems
```

199.120.48.131 2025-09-10T19:54:27.563741
Tesla Motors, Inc.
United States, Washington

```
HTTP/1.1 403 Forbidden
Server: Tesla Edge
Connection: close
Content-Length: 0
```

403 Not allowed 2025-09-10T19:52:57.671283
199.120.51.147
Tesla Motors, Inc.
Germany, Frankfurt am Main

```
HTTP/1.1 403 Not allowed
Date: Wed, 10 Sep 2025 19:52:57 GMT
Server: Varnish
X-Varnish: 838639123
Content-Type: text/html; charset=utf-8
Retry-After: 5
```



hostname:"www.tesla.com"

TOTAL RESULTS

1,965

TOP COUNTRIES

United States	625
India	171
Japan	121
Germany	111
United Kingdom	62

More...

TOP PORTS

443	1,964
8443	1

TOP ORGANIZATIONS

Product Spotlight: Keep track of what you have connected to the Internet. Check out Shodan Monitor

Invalid URL 2025-09-10T20:11:45.158233
2.19.168.64
www.tesla.com
mfs-supplier-eng.mo.tesla.cn
www.teslamotors.com
mfs-supplier.mo.tesla.cn
teslamotors.com
Akamai Technologies
United Kingdom, London
cdn

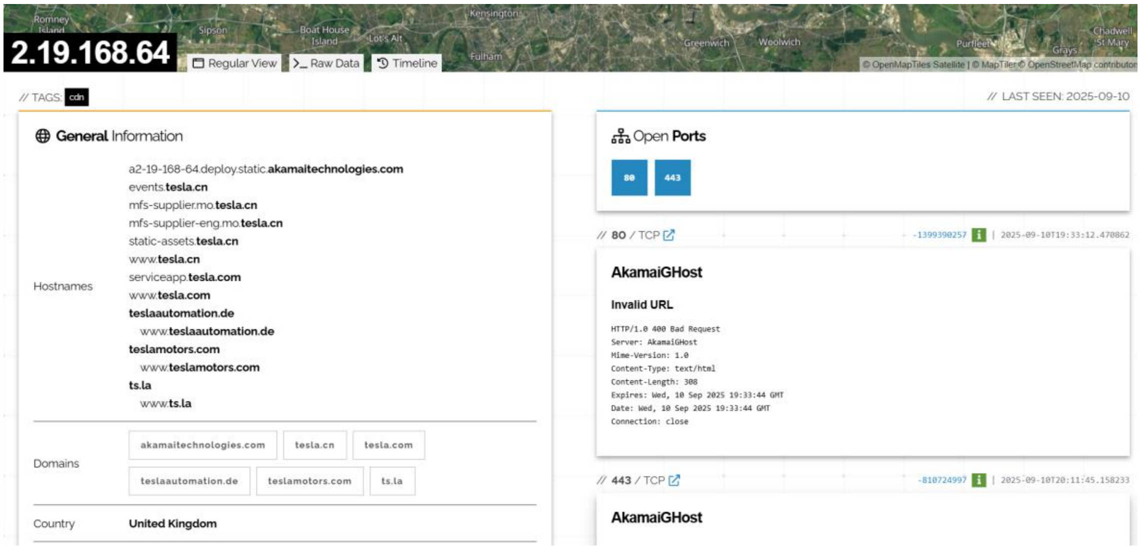
SSL Certificate
Issued By:
|- Common Name:
GeoTrust TLS RSA CA G1
|- Organization:
DigiCert Inc
Issued To:
|- Common Name:
www.teslamotors.com
|- Organization:
TESLA, INC.
Supported SSL Versions:
TLSv1.2

```
HTTP/1.0 400 Bad Request
Server: AkamaiGHost
Mime-Version: 1.0
Content-Type: text/html
Content-Length: 308
Expires: Wed, 10 Sep 2025 20:11:21 GMT
Date: Wed, 10 Sep 2025 20:11:21 GMT
Connection: close
```

Invalid URL 2025-09-10T20:04:53.544074
23.220.124.144
www.tesla.com
mfs-supplier-eng.mo.tesla.cn
www.teslamotors.com
mfs-supplier.mo.tesla.cn
teslamotors.com
Akamai Technologies, Inc.
United States, Ashburn

SSL Certificate
Issued By:
|- Common Name:
GeoTrust TLS RSA CA G1
|- Organization:
DigiCert Inc
Issued To:

```
HTTP/1.0 400 Bad Request
Server: AkamaiGHost
Mime-Version: 1.0
Content-Type: text/html
Content-Length: 310
Expires: Wed, 10 Sep 2025 20:04:53 GMT
Date: Wed, 10 Sep 2025 20:04:53 GMT
Connection: close
```



2.19.168.64

// TAGS: cdn

// LAST SEEN: 2025-09-10

General Information

Hostnames	a2-19-168-64.deploy.static.**akamaitechnologies.com** events.**tesla.cn** mfs-supplier.mo.**tesla.cn** mfs-supplier-eng.mo.**tesla.cn** static-assets.**tesla.cn** www.**tesla.cn** serviceapp.**tesla.com** www.**tesla.com** **teslaautomation.de** www.**teslaautomation.de** **teslamotors.com** www.**teslamotors.com** **ts.la** www.**ts.la**
Domains	akamaitechnologies.com tesla.cn tesla.com teslaautomation.de teslamotors.com ts.la
Country	**United Kingdom**

Open **Ports**

80 443

// **80** / TCP -1399390257 | 2025-09-10T19:33:12.470862

AkamaiGHost

Invalid URL

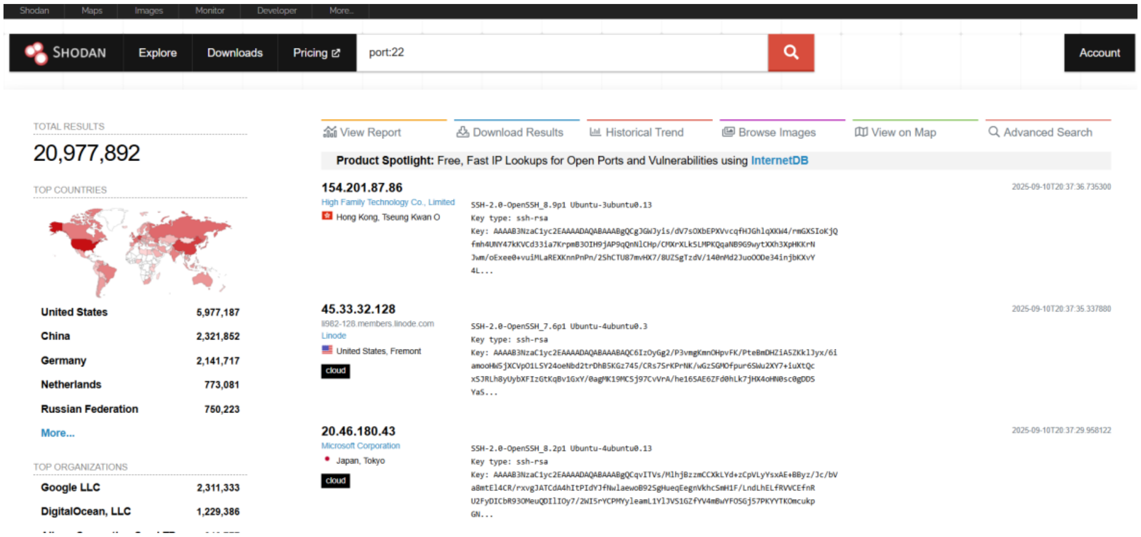
```
HTTP/1.0 400 Bad Request
Server: AkamaiGHost
Mime-Version: 1.0
Content-Type: text/html
Content-Length: 308
Expires: Wed, 10 Sep 2025 19:33:44 GMT
Date: Wed, 10 Sep 2025 19:33:44 GMT
Connection: close
```

// **443** / TCP -810724997 | 2025-09-10T20:11:45.158233

AkamaiGHost

Filtros útiles:

- `port:22`
- `country:"ES"`
- `http.title:"Login"`
- `product:"Apache"`
- `ssl:"expired"`



Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | port:22 | Account

TOTAL RESULTS

20,977,892

TOP COUNTRIES

United States	5,977,187
China	2,321,852
Germany	2,141,717
Netherlands	773,081
Russian Federation	750,223

More...

TOP ORGANIZATIONS

Google LLC	2,311,333
DigitalOcean, LLC	1,229,386

View Report | Download Results | Historical Trend | Browse Images | View on Map | Advanced Search

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

154.201.87.86
High Family Technology Co., Limited
Hong Kong, Tseung Kwan O
2025-09-10T20:37:36.735300

```
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.13
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCgJGWJyis/dV7sOXbEPXVvcqfHJGhlqXKW4/rmGXSIoKjQ
fmh4UNY47kKVCd33ia7KrpmB3OIH9jAP9qQnNlCHp/CMXrXLkSLMPKQqaNB9G9wytXXh3XpHKKrN
Jwm/oExee0+vuiMLaREXKnnPnPn/25hCTU87mvHX7/8UZSgTzdV/140nMd2JuoOODe34injbKXvY
4L...
```

45.33.32.128
li982-128.members.linode.com
Linode
United States, Fremont
cloud
2025-09-10T20:37:35.337880

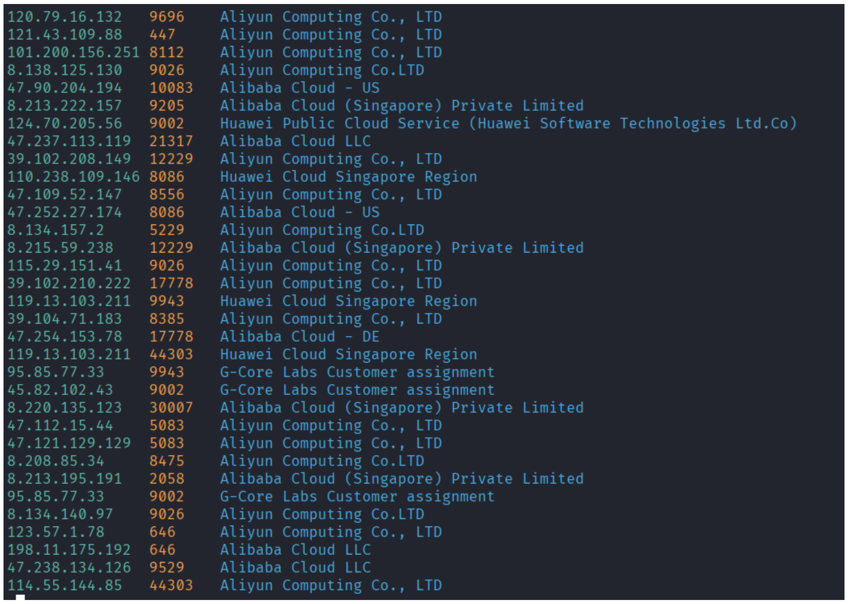
```
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC6IzOyGg2/P3vmgKmnOHpvFK/PteBmDHZiA5ZKklJyx/6i
amooHW5jXCVpO1LSY24oeNbd2trDhB5KGz745/CRs7SrKPrNK/wGzSGMOfpur6SWu2XY7+iuXtQc
x5JRLh8yUybXFIzGtKqBv1GxY/0agMK19MC5j97CvVrA/he165AE6ZFd0hLk7jHX4oHN0sc0gDDS
YaS...
```

20.46.180.43
Microsoft Corporation
Japan, Tokyo
cloud
2025-09-10T20:37:29.958122

```
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.13
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCqvITVs/MlhjBzzmCCXkLYd+zCpVLyYsxAE+BByz/Jc/bV
aBmtEl4CR/rxvgJATCdA4hItPIdYJfNwlaewoB92SgHueqEegnVkhcSmH1F/LndLhELfRVVCEfnR
U2FyDICbR93OMeuQDIlIOy7/2WI5rYCPMYyleamL1YlJVS1GZfYV4mBwYFO5Gj57PKYYTKOmcukp
GN...
```

2 - Búsqueda por CLI

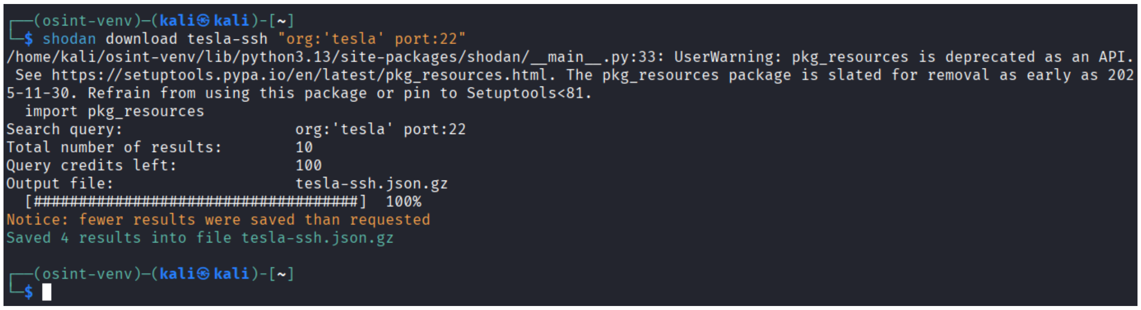
```
# Buscar servidores SSH en la red simulada
shodan search "port:22 org:'tesla'"

# Buscar cámaras IP (IoT)
shodan search "netcam" --fields ip_str,port,org,os
```



```
120.79.16.132   9696   Aliyun Computing Co., LTD
121.43.109.88   447    Aliyun Computing Co., LTD
101.200.156.251 8112   Aliyun Computing Co., LTD
8.138.125.130   9026   Aliyun Computing Co.LTD
47.90.204.194   10083  Alibaba Cloud - US
8.213.222.157   9205   Alibaba Cloud (Singapore) Private Limited
124.70.205.56   9002   Huawei Public Cloud Service (Huawei Software Technologies Ltd.Co)
47.237.113.119  21317  Alibaba Cloud LLC
39.102.208.149  12229  Aliyun Computing Co., LTD
110.238.109.146 8086   Huawei Cloud Singapore Region
47.109.52.147   8556   Aliyun Computing Co., LTD
47.252.27.174   8086   Alibaba Cloud - US
8.134.157.2     5229   Aliyun Computing Co.LTD
8.215.59.238    12229  Alibaba Cloud (Singapore) Private Limited
115.29.151.41   9026   Aliyun Computing Co., LTD
39.102.210.222  17778  Aliyun Computing Co., LTD
119.13.103.211  9943   Huawei Cloud Singapore Region
39.104.71.183   8385   Aliyun Computing Co., LTD
47.254.153.78   17778  Alibaba Cloud - DE
119.13.103.211  44303  Huawei Cloud Singapore Region
95.85.77.33     9943   G-Core Labs Customer assignment
45.82.102.43    9002   G-Core Labs Customer assignment
8.220.135.123   30007  Alibaba Cloud (Singapore) Private Limited
47.112.15.44    5083   Aliyun Computing Co., LTD
47.121.129.129  5083   Aliyun Computing Co., LTD
8.208.85.34     8475   Aliyun Computing Co.LTD
8.213.195.191   2058   Alibaba Cloud (Singapore) Private Limited
95.85.77.33     9002   G-Core Labs Customer assignment
8.134.140.97    9026   Aliyun Computing Co.LTD
123.57.1.78     646    Aliyun Computing Co., LTD
198.11.175.192  646    Alibaba Cloud LLC
47.238.134.126  9529   Alibaba Cloud LLC
114.55.144.85   44303  Aliyun Computing Co., LTD
```

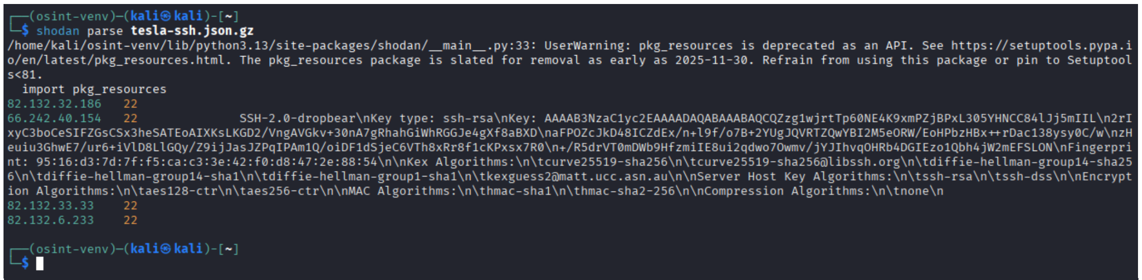
3 - Extraer resultados

```
shodan download tesla-ssh "org:'tesla' port:22"
```

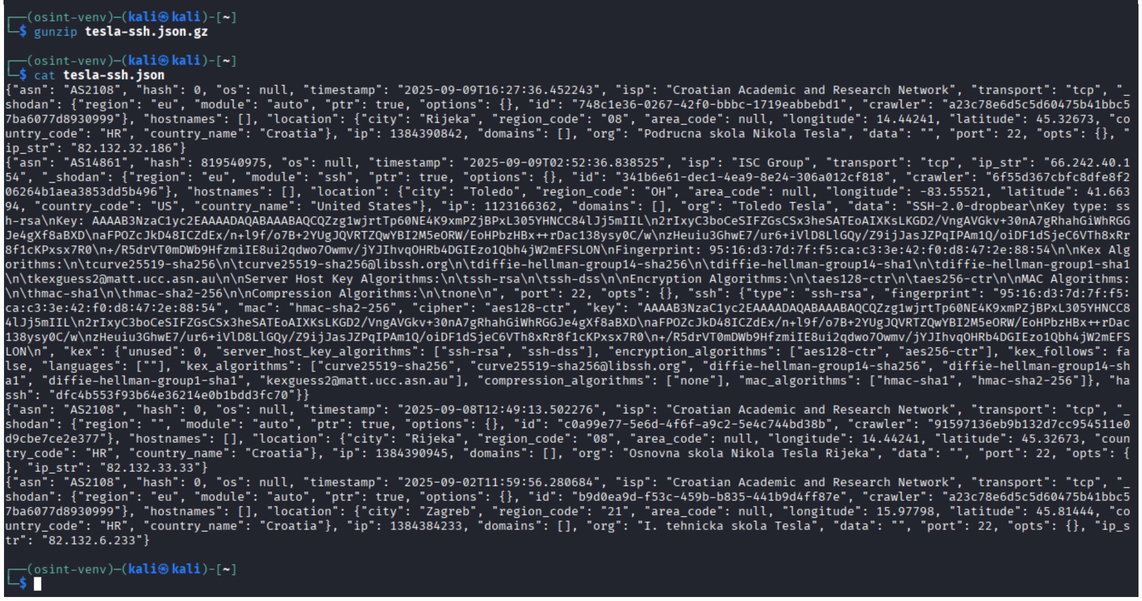


```
┌──(osint-venv)─(kali㉿kali)-[~]
└─$ shodan download tesla-ssh "org:'tesla' port:22"
/home/kali/osint-venv/lib/python3.13/site-packages/shodan/__main__.py:33: UserWarning: pkg_resources is deprecated as an API.
 See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 202
5-11-30. Refrain from using this package or pin to Setuptools<81.
  import pkg_resources
Search query:                   org:'tesla' port:22
Total number of results:        10
Query credits left:             100
Output file:                    tesla-ssh.json.gz
  [####################################]  100%
Notice: fewer results were saved than requested
Saved 4 results into file tesla-ssh.json.gz

┌──(osint-venv)─(kali㉿kali)-[~]
└─$ 
```

```
shodan parse tesla-ssh.json.gz
```



```
┌──(osint-venv)─(kali㉿kali)-[~]
└─$ shodan parse tesla-ssh.json.gz
/home/kali/osint-venv/lib/python3.13/site-packages/shodan/__main__.py:33: UserWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.i
o/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 2025-11-30. Refrain from using this package or pin to Setuptool
s<81.
  import pkg_resources
82.132.32.186   22
66.242.40.154   22              SSH-2.0-dropbear\nKey type: ssh-rsa\nKey: AAAAB3NzaC1yc2EAAAADAQABAAABAQCQZzg1wjrtTp60NE4K9xmPZjBPxL305YHNCC84lJj5mIIL\n2rI
xyC3boCeSIFZGsCSx3heSATEoAIXKsLKGD2/VngAVGkv+30nA7gRhahGiWhRGGJe4gXf8aBXD\naFPOZcJkD48ICZdEx/n+l9f/o7B+2YUgJQVRTZQwYBI2M5eORW/EoHPbzHBx++rDac138ysy0C/w\nzH
euiu3GhwE7/ur6+iVlD8LlGQy/Z9ijJasJZPqIPAm1Q/oiDF1dSjeC6VTh8xRr8f1cKPxsx7R0\n+/R5drVT0mDWb9HfzmiIE8ui2qdwo7Owmv/jYJIhvqOHRb4DGIEzo1Qbh4jW2mEFSLON\nFingerpri
nt: 95:16:d3:7d:7f:f5:ca:c3:3e:42:f0:d8:47:2e:88:54\n\nKex Algorithms:\n\tcurve25519-sha256\n\tcurve25519-sha256@libssh.org\n\tdiffie-hellman-group14-sha25
6\n\tdiffie-hellman-group14-sha1\n\tdiffie-hellman-group1-sha1\n\tkexguess2@matt.ucc.asn.au\n\nServer Host Key Algorithms:\n\tssh-rsa\n\tssh-dss\n\nEncrypt
ion Algorithms:\n\taes128-ctr\n\taes256-ctr\n\nMAC Algorithms:\n\thmac-sha1\n\thmac-sha2-256\n\nCompression Algorithms:\n\tnone\n
82.132.33.33    22
82.132.6.233    22

┌──(osint-venv)─(kali㉿kali)-[~]
└─$ 
```



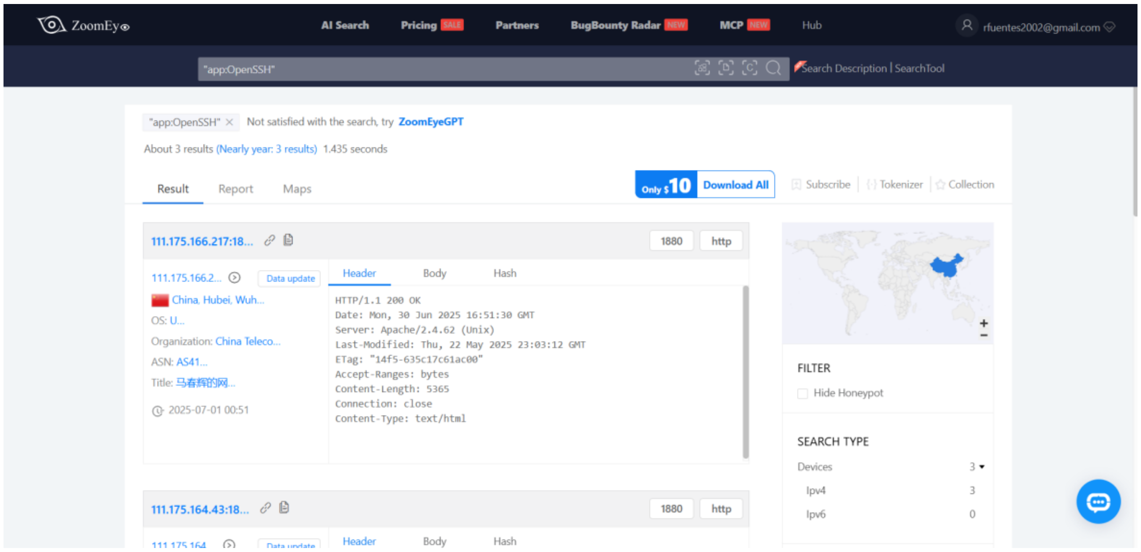
```
┌──(osint-venv)─(kali㉿kali)-[~]
└─$ gunzip tesla-ssh.json.gz

┌──(osint-venv)─(kali㉿kali)-[~]
└─$ cat tesla-ssh.json
{"asn": "AS2108", "hash": 0, "os": null, "timestamp": "2025-09-09T16:27:36.452243", "isp": "Croatian Academic and Research Network", "transport": "tcp", "_
shodan": {"region": "eu", "module": "auto", "ptr": true, "options": {}, "id": "748c1e36-0267-42f0-bbbc-1719eabbebd1", "crawler": "a23c78e6d5c5d60475b41bbc5
7ba6077d8930999"}, "hostnames": [], "location": {"city": "Rijeka", "region_code": "08", "area_code": null, "longitude": 14.44241, "latitude": 45.32673, "co
untry_code": "HR", "country_name": "Croatia"}, "ip": 1384390842, "domains": [], "org": "Podrucna skola Nikola Tesla", "data": "", "port": 22, "opts": {}, "
ip_str": "82.132.32.186"}
{"asn": "AS14861", "hash": 819540975, "os": null, "timestamp": "2025-09-09T02:52:36.838525", "isp": "ISC Group", "transport": "tcp", "ip_str": "66.242.40.1
54", "_shodan": {"region": "eu", "module": "ssh", "ptr": true, "options": {}, "id": "341b6e61-dec1-4ea9-8e24-306a012cf818", "crawler": "6f55d367cbfc8dfe8f2
06264b1aea3853dd5b496"}, "hostnames": [], "location": {"city": "Toledo", "region_code": "OH", "area_code": null, "longitude": -83.55521, "latitude": 41.663
94, "country_code": "US", "country_name": "United States"}, "ip": 1123166362, "domains": [], "org": "Toledo Tesla", "data": "SSH-2.0-dropbear\nKey type: ss
h-rsa\nKey: AAAAB3NzaC1yc2EAAAADAQABAAABAQCQZzg1wjrtTp60NE4K9xmPZjBPxL305YHNCC84lJj5mIIL\n2rIxyC3boCeSIFZGsCSx3heSATEoAIXKsLKGD2/VngAVGkv+30nA7gRhahGiWhRGG
Je4gXf8aBXD\naFPOZcJkD48ICZdEx/n+l9f/o7B+2YUgJQVRTZQwYBI2M5eORW/EoHPbzHBx++rDac138ysy0C/w\nzHeuiu3GhwE7/ur6+iVlD8LlGQy/Z9ijJasJZPqIPAm1Q/oiDF1dSjeC6VTh8xRr
8f1cKPxsx7R0\n+/R5drVT0mDWb9HfzmiIE8ui2qdwo7Owmv/jYJIhvqOHRb4DGIEzo1Qbh4jW2mEFSLON\nFingerprint: 95:16:d3:7d:7f:f5:ca:c3:3e:42:f0:d8:47:2e:88:54\n\nKex Alg
orithms:\n\tcurve25519-sha256\n\tcurve25519-sha256@libssh.org\n\tdiffie-hellman-group14-sha256\n\tdiffie-hellman-group14-sha1\n\tdiffie-hellman-group1-sha1
\n\tkexguess2@matt.ucc.asn.au\n\nServer Host Key Algorithms:\n\tssh-rsa\n\tssh-dss\n\nEncryption Algorithms:\n\taes128-ctr\n\taes256-ctr\n\nMAC Algorithms:
\n\thmac-sha1\n\thmac-sha2-256\n\nCompression Algorithms:\n\tnone\n", "port": 22, "opts": {}, "ssh": {"type": "ssh-rsa", "fingerprint": "95:16:d3:7d:7f:f5:
ca:c3:3e:42:f0:d8:47:2e:88:54", "mac": "hmac-sha2-256", "cipher": "aes128-ctr", "key": "AAAAB3NzaC1yc2EAAAADAQABAAABAQCQZzg1wjrtTp60NE4K9xmPZjBPxL305YHNCC8
4lJj5mIIL\n2rIxyC3boCeSIFZGsCSx3heSATEoAIXKsLKGD2/VngAVGkv+30nA7gRhahGiWhRGGJe4gXf8aBXD\naFPOZcJkD48ICZdEx/n+l9f/o7B+2YUgJQVRTZQwYBI2M5eORW/EoHPbzHBx++rDac
138ysy0C/w\nzHeuiu3GhwE7/ur6+iVlD8LlGQy/Z9ijJasJZPqIPAm1Q/oiDF1dSjeC6VTh8xRr8f1cKPxsx7R0\n+/R5drVT0mDWb9HfzmiIE8ui2qdwo7Owmv/jYJIhvqOHRb4DGIEzo1Qbh4jW2mEFS
LON\n", "kex": {"unused": 0, "server_host_key_algorithms": ["ssh-rsa", "ssh-dss"], "encryption_algorithms": ["aes128-ctr", "aes256-ctr"], "kex_follows": fa
lse, "languages": [""], "kex_algorithms": ["curve25519-sha256", "curve25519-sha256@libssh.org", "diffie-hellman-group14-sha256", "diffie-hellman-group14-sh
a1", "diffie-hellman-group1-sha1", "kexguess2@matt.ucc.asn.au"], "compression_algorithms": ["none"], "mac_algorithms": ["hmac-sha1", "hmac-sha2-256"]}, "ha
ssh": "dfc4b553f93b64e36214e0b1bdd3fc70"}}
{"asn": "AS2108", "hash": 0, "os": null, "timestamp": "2025-09-08T12:49:13.502276", "isp": "Croatian Academic and Research Network", "transport": "tcp", "_
shodan": {"region": "", "module": "auto", "ptr": true, "options": {}, "id": "c0a99e77-5e6d-4f6f-a9c2-5e4c744bd38b", "crawler": "91597136eb9b132d7cc954511e0
d9cbe7ce2e377"}, "hostnames": [], "location": {"city": "Rijeka", "region_code": "08", "area_code": null, "longitude": 14.44241, "latitude": 45.32673, "coun
try_code": "HR", "country_name": "Croatia"}, "ip": 1384390945, "domains": [], "org": "Osnovna skola Nikola Tesla Rijeka", "data": "", "port": 22, "opts": {
}, "ip_str": "82.132.33.33"}
{"asn": "AS2108", "hash": 0, "os": null, "timestamp": "2025-09-02T11:59:56.280684", "isp": "Croatian Academic and Research Network", "transport": "tcp", "_
shodan": {"region": "eu", "module": "auto", "ptr": true, "options": {}, "id": "b9d0ea9d-f53c-459b-b835-441b9d4ff87e", "crawler": "a23c78e6d5c5d60475b41bbc5
7ba6077d8930999"}, "hostnames": [], "location": {"city": "Zagreb", "region_code": "21", "area_code": null, "longitude": 15.97798, "latitude": 45.81444, "co
untry_code": "HR", "country_name": "Croatia"}, "ip": 1384384233, "domains": [], "org": "I. tehnicka skola Tesla", "data": "", "port": 22, "opts": {}, "ip_s
tr": "82.132.6.233"}

┌──(osint-venv)─(kali㉿kali)-[~]
└─$ 
```

4. ZOOMEYE

1 - Web UI

Ir a https://www.zoomeye.org/ y probar estas queries:

- "app:OpenSSH"
- port=80 && country="ES"
- service:ftp



"app:OpenSSH"

"app:OpenSSH" × Not satisfied with the search, try ZoomEyeGPT

About 3 results (Nearly year: 3 results) 1.435 seconds

111.175.166.217:18...

111.175.166.2...

China, Hubei, Wuh...

OS: U...

Organization: China Teleco...

ASN: AS41...

Title: 马春辉的网...

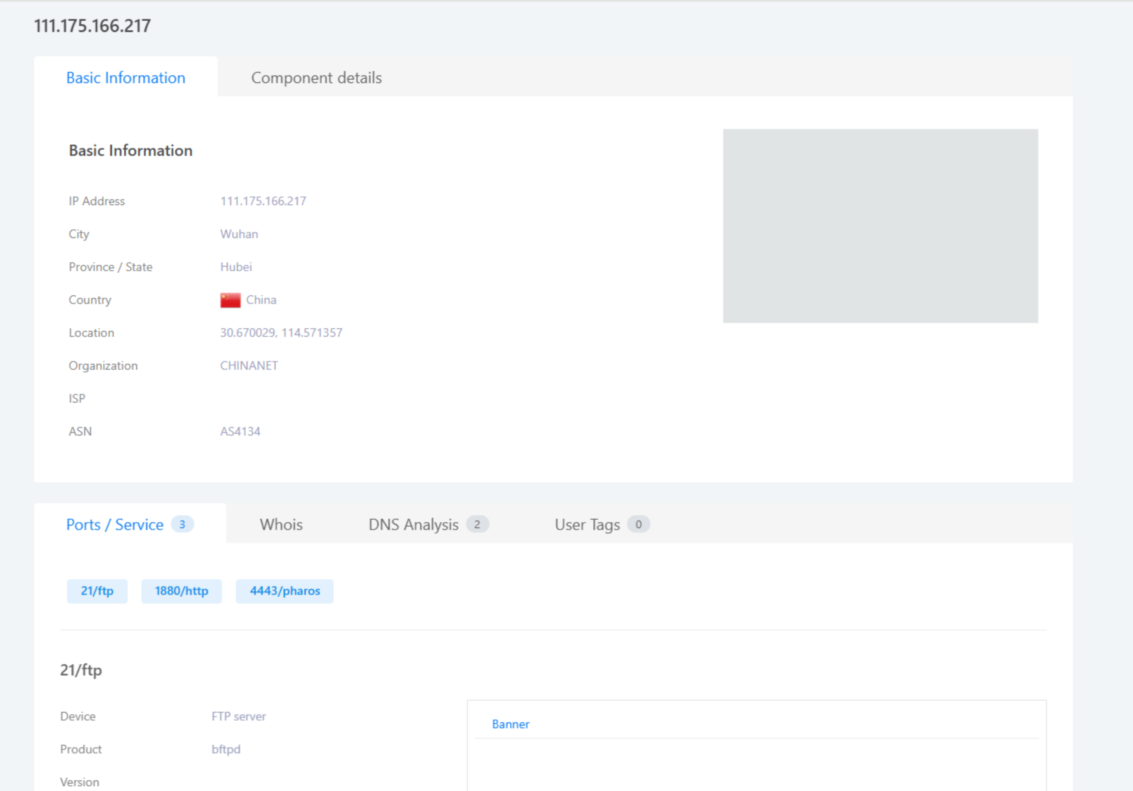
2025-07-01 00:51

```
HTTP/1.1 200 OK
Date: Mon, 30 Jun 2025 16:51:30 GMT
Server: Apache/2.4.62 (Unix)
Last-Modified: Thu, 22 May 2025 23:03:12 GMT
ETag: "14f5-635c17c61ac00"
Accept-Ranges: bytes
Content-Length: 5365
Connection: close
Content-Type: text/html
```

Devices	3
Ipv4	3
Ipv6	0

111.175.164.43:18...

111.175.164...



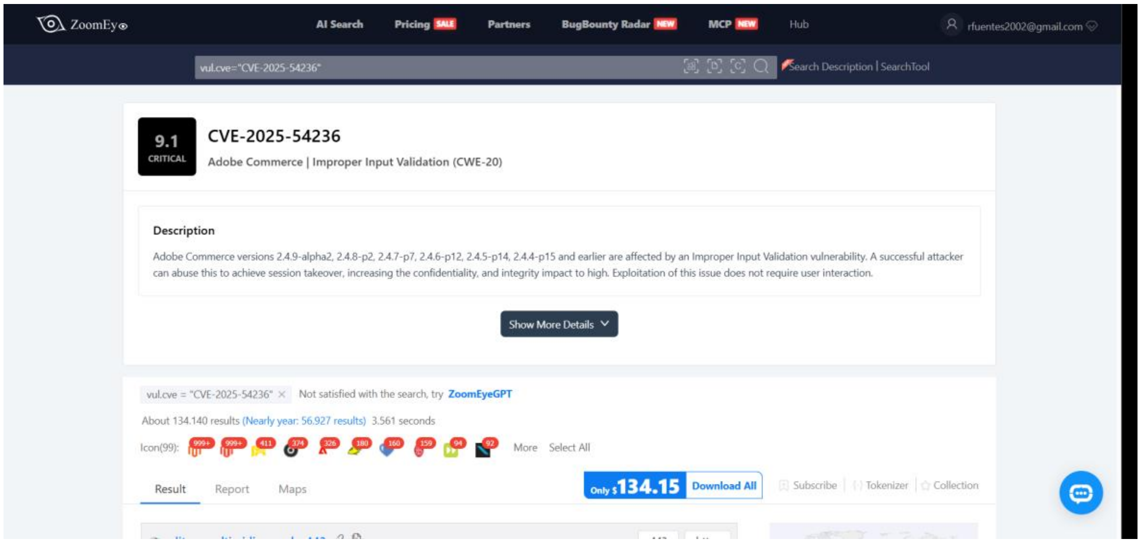
111.175.166.217

Basic Information

IP Address	111.175.166.217
City	Wuhan
Province / State	Hubei
Country	China
Location	30.670029, 114.571357
Organization	CHINANET
ISP	
ASN	AS4134

21/ftp

Device	FTP server
Product	bftpd
Version	



vul.cve="CVE-2025-54236"

9.1 CRITICAL

CVE-2025-54236

Adobe Commerce | Improper Input Validation (CWE-20)

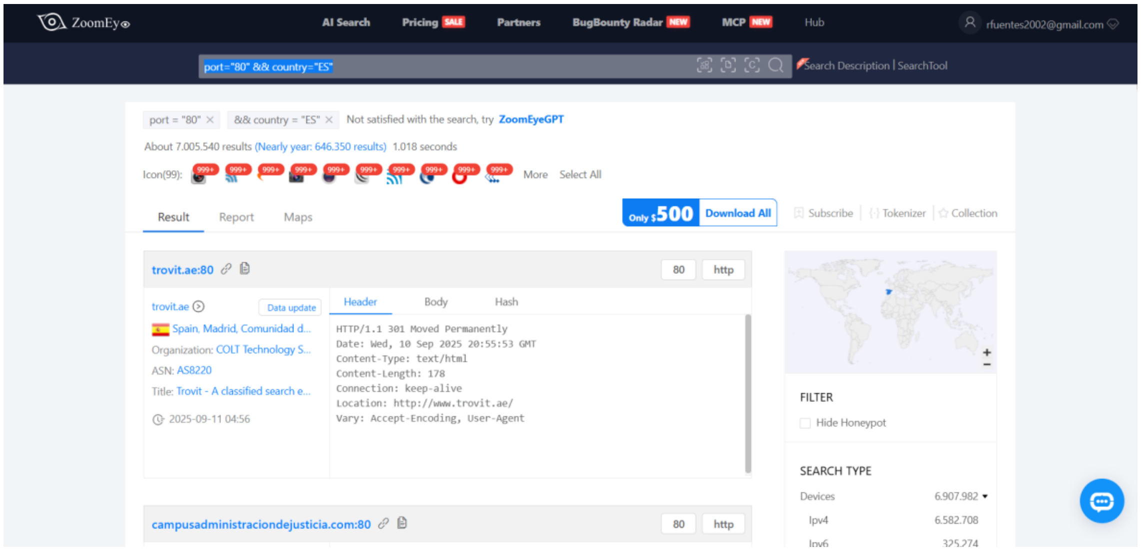
Description

Adobe Commerce versions 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14, 2.4.4-p15 and earlier are affected by an Improper Input Validation vulnerability. A successful attacker can abuse this to achieve session takeover, increasing the confidentiality, and integrity impact to high. Exploitation of this issue does not require user interaction.

vul.cve = "CVE-2025-54236" Not satisfied with the search, try ZoomEyeGPT

About 134.140 results (Nearly year: 56.927 results) 3.561 seconds

Icon(99): 999+ 999+ 411 374 326 180 160 159 94 92



port="80" && country="ES"

port = "80" && country = "ES" Not satisfied with the search, try ZoomEyeGPT

About 7.005.540 results (Nearly year: 646.350 results) 1.018 seconds

Icon(99): 999+ 999+ 999+ 999+ 999+ 999+ 999+ 999+ 999+ 999+

trovit.ae:80 80 http

trovit.ae
Spain, Madrid, Comunidad d...
Organization: COLT Technology S...
ASN: AS8220
Title: Trovit - A classified search e...
2025-09-11 04:56

```
HTTP/1.1 301 Moved Permanently
Date: Wed, 10 Sep 2025 20:55:53 GMT
Content-Type: text/html
Content-Length: 178
Connection: keep-alive
Location: http://www.trovit.ae/
Vary: Accept-Encoding, User-Agent
```

FILTER
□ Hide Honeypot

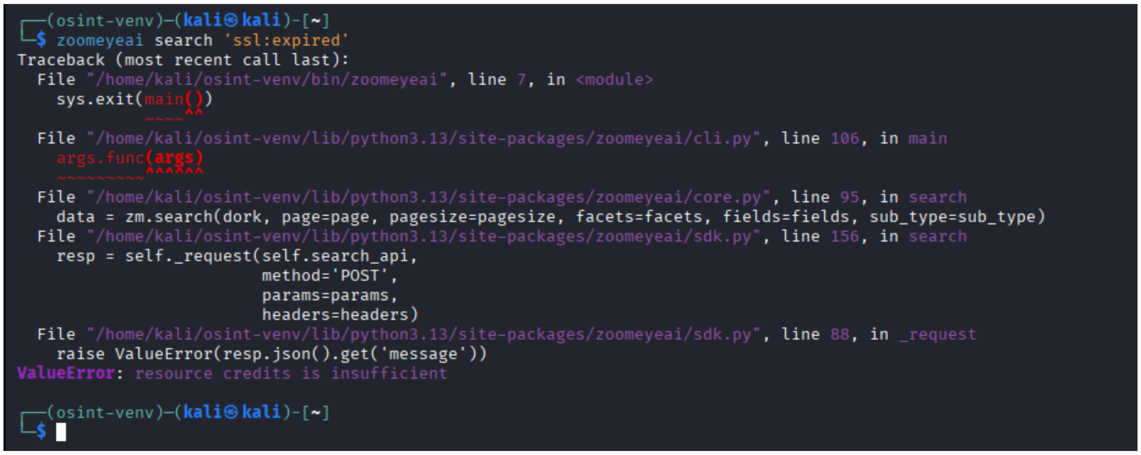
SEARCH TYPE

Devices	6.907.982
Ipv4	6.582.708
Ipv6	325.274

campusadministraciondejusticia.com:80 80 http

2 - CLI

```
# Buscar hosts en España con HTTP
zoomeyeai search 'port:80 && country:ES'

# Buscar dispositivos con SSL expuesto
zoomeyeai search 'ssl:expired'
```



```
┌──(osint-venv)─(kali㉿kali)-[~]
└─$ zoomeyeai search 'ssl:expired'
Traceback (most recent call last):
  File "/home/kali/osint-venv/bin/zoomeyeai", line 7, in <module>
    sys.exit(main())
             ~~~~^^
  File "/home/kali/osint-venv/lib/python3.13/site-packages/zoomeyeai/cli.py", line 106, in main
    args.func(args)
    ~~~~~~~~~^^^^^^
  File "/home/kali/osint-venv/lib/python3.13/site-packages/zoomeyeai/core.py", line 95, in search
    data = zm.search(dork, page=page, pagesize=pagesize, facets=facets, fields=fields, sub_type=sub_type)
  File "/home/kali/osint-venv/lib/python3.13/site-packages/zoomeyeai/sdk.py", line 156, in search
    resp = self._request(self.search_api,
                         method='POST',
                         params=params,
                         headers=headers)
  File "/home/kali/osint-venv/lib/python3.13/site-packages/zoomeyeai/sdk.py", line 88, in _request
    raise ValueError(resp.json().get('message'))
ValueError: resource credits is insufficient

┌──(osint-venv)─(kali㉿kali)-[~]
└─$ █
```

Es posible que si no disponemos de créditos (plan Free) sólo podamos utilizar las búsquedas a través de la web

5. Actividades de evaluación

Actividad	Detalle
Captura de datos de Shodan	Lista de IPs, servicios, versiones
Captura de datos de Zoomeye	Certificados, metadatos SSL/TLS
Informe de riesgos	Análisis de posibles vectores de ataque
Recomendaciones	Qué servicios deberían ocultarse o reforzarse

6. Dominio simulado sugerido

- `vpn.example-corp.com`
- `mail.example-corp.com`
- `camera.example-corp.com` (IoT simulado)

Puedes simular IPs o configurar máquinas locales y exponer servicios en una red controlada (por ejemplo, con **VirtualBox Host-only Adapter**), aunque para búsquedas reales se usará el entorno público.