



# Penetration Testing & Ethical Hacking

## Enumerating Target e Port Scanning

Parte 3

Arcangelo Castiglione  
arcastiglione@unisa.it

# Outline

---

- Concetti Introduttivi
- Suite Protocollare TCP/IP
- Formato dei Messaggi TCP e UDP
- Active Enumeration
  - Network Scanner Nmap
  - Zenmap
  - Unicornscan
  - Masscan
- Passive Enumeration
  - Shodan
  - ZoomEye
  - FOFA
  - Censys

# Outline

---

- Concetti Introduttivi
- Suite Protocollare TCP/IP
- Formato dei Messaggi TCP e UDP
- Active Enumeration
  - Network Scanner Nmap
  - Zenmap
  - Unicornscan
  - Masscan
- Passive Enumeration
  - Shodan
  - ZoomEye
  - FOFA
  - Censys

# Shodan

## Caratteristiche

---

- <https://www.shodan.io/>
  - Motore di ricerca che consente di trovare (tramite opportuni filtri) vari tipi di **dispositivi connessi ad Internet**
  - Noto per essere il più importante motore di ricerca per **dispositivi connessi ad Internet**
    - Computer
    - Webcam
    - Server
    - Router
    - Dispositivi IoT
    - Etc
  - Introdotto nel 2009 da John Matherly



# Shodan

## Caratteristiche

---

➤ <https://www.shodan.io/>

- Anche definito come **motore di ricerca di service banner**
  - Metadati che il Server invia al Client
  - I *service banner* potrebbero contenere informazioni interessanti sui software di rete in esecuzione sul Server
    - Messaggio di benvenuto
    - Eventuali opzioni supportate dal software
    - Qualsiasi altra cosa che potrebbe essere utile al Client prima di interagire con il Server



# Shodan

## Caratteristiche

---

- Shodan raccoglie dati su vari servizi di rete
  - *Web Server* (HTTP/HTTPS - porte 80, 8080, 443, 8443)
  - *FTP* (porta 21)
  - *SSH* (porta 22)
  - *Telnet* (porta 23)
  - *IMAP* (porte 143 o 993)
  - *SMTP* (porta 25)
  - *Real Time Streaming Protocol (RTSP)*, porta 554
    - Utilizzato per accedere alle webcam ed ai loro flussi video
  - Etc



# Shodan

## Caratteristiche

---

- Shodan fornisce inoltre
  - Una propria interfaccia a linea di comando (*Shodan Command-Line Interface*) utilizzabile online
    - <https://cli.shodan.io/>
  - API per scrivere programmi basati su Shodan
- Interessante strumento basato sulle API di Shodan
  - *SearchDiggity*
  - <https://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/>



# Shodan

## Caratteristiche

---

- Consente di scoprire
  - Quali sistemi sono presenti in un asset
  - I servizi attivi in tali sistemi (ed i relativi *banner*)
  - Le versioni di tali servizi
  - Etc
- **N.B.** Le **informazioni** fornite da tale strumento **potrebbero non essere allineate** con lo stato corrente dell'asset
  - Prima di proseguire con le fasi successive del processo di penetration testing sarebbe opportuno condurre anche una fase di *Active Target Enumeration*
  - Un host potrebbe non essere più attivo o lo stato/versione delle sue porte/servizi potrebbe essere cambiato



# Shodan

## Caratteristiche

---

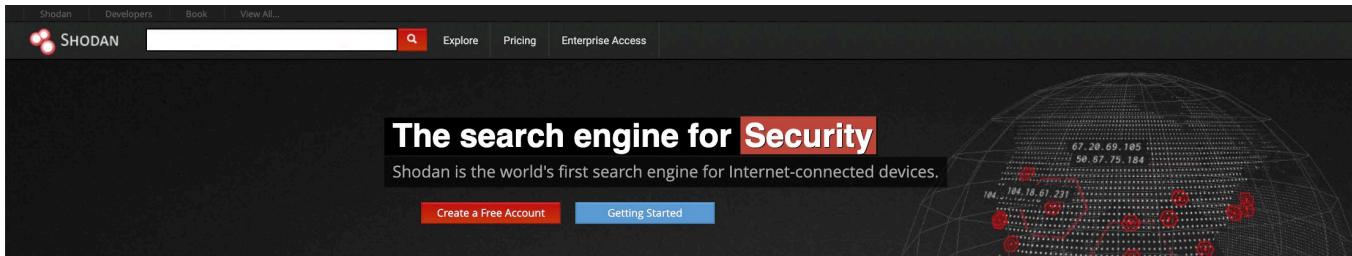
- Shodan è uno strumento utile per ottenere in maniera «discreta» ed affidabile numerose informazioni
  
- Il suo *timestamp* permette di avere un'idea su quanto siano recenti i risultati mostrati
  
- La versione «free» fornisce funzionalità molto limitate
  - Numero limitato di pagine come risultato per ciascuna query
  - Numero limitato di filtri da applicare
  - Etc



# Shodan

## Interfaccia

➤ <https://www.shodan.io/>



The screenshot shows several sections of the Shodan homepage:

- Explore the Internet of Things**: Includes a blue cloud icon and text about discovering connected devices.
- Monitor Network Security**: Includes an eye icon and text about tracking accessible computers on a network.
- See the Big Picture**: Includes a globe icon and text about finding power plants, Smart TVs, and refrigerators.
- Get a Competitive Advantage**: Includes a dollar sign icon and text about performing empirical market intelligence.
- 56% of Fortune 100**: Shows a bar chart with the text '56% of Fortune 100' and a graduation cap icon.
- 1,000+ Universities**: Shows a bar chart with the text '1,000+ Universities' and a graduation cap icon.

A central message at the bottom of this section reads: 'Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.'



Analyze the Internet in Seconds

Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest Internet intelligence. Who buys Smart TVs? Which countries are building the most wind farms? What companies are affected by Heartbleed? Shodan provides the tools to answer questions at the Internet-scale.

[Sample Report on Heartbleed](#)

Istantanea sche

Enumerating Target e Port Scanning

# Shodan

## Dorks – Query Shodan Predefinite

➤ <https://www.shodan.io/explore>

The screenshot shows the Shodan Explore page with several sections:

- CATEGORIES:** Industrial Control Systems, Databases, Network Infrastructure, Video Games.
- RESEARCH:**
  - Shodan 2000:** Explore the Internet in style using an 80's retro-futuristic interface to synthwave music. [2000.SHODAN.IO](http://2000.SHODAN.IO)
  - Internet Observatory:** How exposed to the Internet is your country? What is the most common vulnerability? Get a high-level view of the Internet using our Observatory. [EXPOSURE.SHODAN.IO](http://EXPOSURE.SHODAN.IO)
  - Favicon Map:** Favicons are the small icons you see in your browser tab at the top. See the most common favicons across the Internet. [FAVICONMAP.SHODAN.IO](http://FAVICONMAP.SHODAN.IO)
- BROWSE SEARCH DIRECTORY:** A search bar for "Search shared queries..." and a list of popular tags: webcam, cam, camera, ip, router, scada, ftp, server, http, telnet, test, password, cisco, web, default, login, ssh, i, nas, ipcam.
- Popular Tags:** A list of tags: webcam, cam, camera, ip, router, scada, ftp, server, http, telnet, test, password, cisco, web, default, login, ssh, i, nas, ipcam.
- What is the search directory?** Shodan lets users share their search queries with the community by saving them to the search directory. Shodan doesn't otherwise store or share your search queries. The queries in the search directory were explicitly shared by our users for the benefit of the community.
- Note:** The current Shodan website doesn't yet let you submit search queries to the directory.
- Webcam:** best ip cam search I have found yet. ▲ 12.519 [webcam](#) [surveillance](#) [cams](#)
- Cams:** admin admin. ▲ 5.290 [cam](#) [webcam](#)
- Netcam:** Netcam. ▲ 2.697 [netcam](#)
- default password:** Finds results with "default password" in the ban.. ▲ 2.111 [router](#) [default](#) [password](#)
- ufanet:** '80;:8080; ▲ 1.413 [ufanet](#)
- MORE:** ...

# Shodan

## Registrazione

- **N.B.** Prima di utilizzare Shodan è **fortemente consigliata** la registrazione e l'accesso ad esso
- **Altrimenti non possono essere usati i suoi filtri di ricerca**

The screenshot shows the Shodan homepage with a dark background. At the top right, there is a green button labeled "Login or Register". A red box and a red arrow point to this button, indicating where to click to register. The main content area features a large globe with various IP addresses marked on it. Below the globe, there are several sections with icons and text:

- Explore the Internet of Things**: Includes a blue cloud icon and text about discovering connected devices.
- Monitor Network Security**: Includes a red eye icon and text about tracking network accessibility.
- See the Big Picture**: Includes a green globe icon and text about finding power plants, Smart TVs, refrigerators, etc.
- Get a Competitive Advantage**: Includes a dollar sign icon and text about performing empirical market intelligence.

At the bottom, there are two statistics: "56% of Fortune 100" with a building icon, and "1,000+ Universities" with a graduation cap icon. A small note at the bottom states: "Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between."

# Shodan

## Registrazione

➤ <https://account.shodan.io/register>

[Create Account](#)

Username

Password

Confirm Password

Email

Subscribe to the newsletter

By creating an account you are agreeing to our [Privacy Policy](#) and [Terms of Use](#)

[CREATE](#)



# Shodan

## Billing

➤ <https://account.shodan.io/billing>

**Choose Your Plan**

No contracts. No setup fees. Cancel anytime.

**Freelancer**  
**\$69/month**

**CHOOSE THIS PLAN**

- ✓ Up to 1 million results per month \*
- ✓ Scan up to 5,120 IPs per month
- ✓ Network Monitoring for 5,120 IPs

---

- ✓ Access to most filters
- ✓ Allows paging through search results
- ✓ Basic access to the Streaming API
- ✓ Commercial Use

---

- ✓ E-Mail support

**Small Business**  
**\$359/month**

**CHOOSE THIS PLAN**

- ✓ Up to 20 million results per month \*
- ✓ Scan up to 65,536 IPs per month
- ✓ Network Monitoring for 65,536 IPs

---

- ✓ Access to most filters
- ✓ Allows paging through search results
- ✓ Basic access to the Streaming API
- ✓ Commercial Use

---

- ✓ E-Mail support
- ✓ Vulnerability search filter

**Corporate**  
**\$1099/month**

**CHOOSE THIS PLAN**

- ✓ Unlimited results per month \*
- ✓ Scan up to 327,680 IPs per month
- ✓ Network Monitoring for 327,680 IPs

---

- ✓ Access to all filters
- ✓ Allows paging through search results
- ✓ Basic access to the Streaming API
- ✓ Commercial Use

---

- ✉ Premium Support
- ⌚ Vulnerability search filter
- ✓ Batch IP Lookups
- ⌚ Tag Search Filter
- 👤 Complementary Membership Upgrades



# Shodan

## Filtri di Ricerca

---

- Shodan fornisce numerosi filtri di ricerca, raggruppati nelle seguenti categorie
  - General
  - HTTP
  - SSL
  - Bitcoin
  - Restricted
  - NTP
  - Screenshots
  - SNMP
  - Telnet
  - Cloud
  - SSH



# Shodan

## Filtri di Ricerca

---

- Alcuni tra i filtri di Shodan più utilizzati sono
  - **city**: cerca i dispositivi in una determinata città
  - **country**: cerca i dispositivi in un determinato paese
  - **geo**: cerca i dispositivi in base alle coordinate geografiche
  - **hostname**: cerca i dispositivi che corrispondono al nome di host
  - **net**: ricerca basata su un IP o CIDR
  - **os**: ricerca basata sul Sistema Operativo
  - **port**: cerca dispositivi che hanno determinate porte aperte
  - **before/after**: cerca risultati appartenenti ad un determinato intervallo temporale

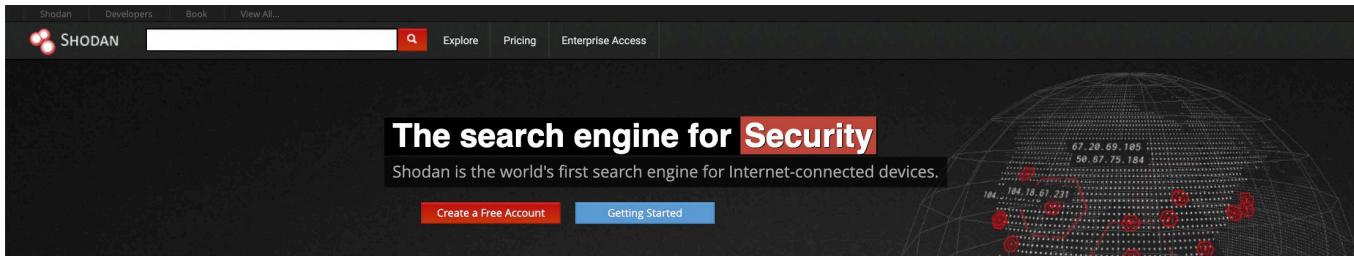


<https://www.shodan.io/search/filters>

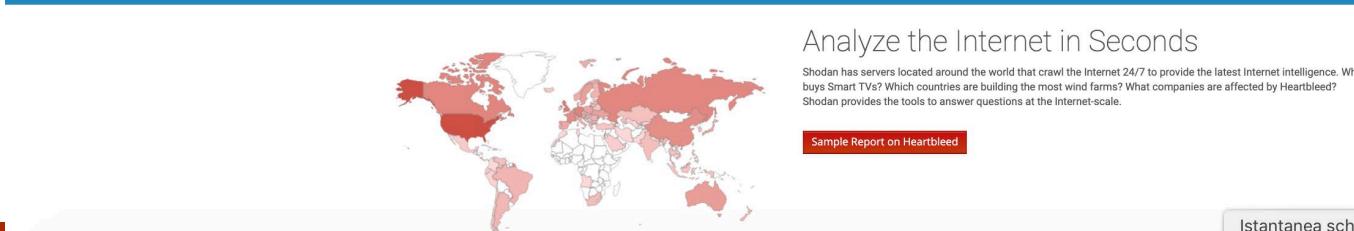
# Shodan

## Esempio 1

➤ <https://www.shodan.io/>



This part of the screenshot highlights several features of Shodan. On the left, there's a section titled 'Explore the Internet of Things' with a blue cloud icon, explaining how to discover connected devices. Next to it is 'Monitor Network Security' with an eye icon, detailing how to track accessible computers. On the right, there's a section titled 'See the Big Picture' with a globe icon, discussing various types of connected devices. Below these are two more sections: 'Get a Competitive Advantage' with a dollar sign icon, and a large blue banner at the bottom stating '56% of Fortune 100' with a building icon. The banner also mentions that Shodan is used by researchers, security professionals, and enterprises.



Enumerating Target e Port Scanning

# Shodan

## Esempio 1

- Effettuiamo una ricerca per Autonomous System Network (**asn:as137**)

The screenshot shows the Shodan search interface. At the top, there is a navigation bar with 'Developer' and 'More...' options. Below it is a search bar with a placeholder 'Search...', a red search button with a magnifying glass icon, and a 'Pricing' link. The main area is titled 'Dashboard'. It features two main sections: 'Getting Started' on the left and 'ASCII Videos' on the right. The 'Getting Started' section includes links to 'What is Shodan?', 'Search Query Fundamentals', and 'Working with Shodan Data Files', along with a 'LEARN MORE' button. The 'ASCII Videos' section includes links to 'Setting up Real-Time Network Monitoring', 'Measuring Public SMB Exposure', and 'Analyzing the Vulnerabilities for a Network', along with a 'VISIT THE CHANNEL' button.

# Shodan

## Esempio 1

- Effettuiamo una ricerca per Autonomous System Network (**asn:as137**)

The screenshot shows the Shodan search interface with the query **asn:as137** entered in the search bar. The results page displays 119,275 total results. A world map highlights Italy in pink, indicating the location of most findings. The top countries section lists Italy (119,241), Brazil (13), France (9), and Belgium (5). Two specific results are detailed: one for IP 157.138.174.18 located at UNI-Venezia, Italy, Venice, and another for IP 193.205.148.175 located at leonard.ino.it, CNR - INO Firenze, Italy, Florence. The 193.205.148.175 entry includes an SSL Certificate section with details about the certificate issuer and organization.

TOTAL RESULTS  
119,275

TOP COUNTRIES

Country	Count
Italy	119,241
Brazil	13
France	9
Belgium	5

157.138.174.18  
UNI-Venezia  
Italy, Venice

193.205.148.175  
leonard.ino.it  
CNR - INO Firenze  
Italy, Florence

SSL Certificate  
Issued By:  
J- Common Name:  
R3  
I- Organization:  
Let's Encrypt  
Issued To:  
J- Common Name:

# Shodan

## Esempio 1

- Effettuiamo una ricerca per Autonomous System Network (**asn:as137**)

Porte più utilizzate

TOP PORTS	
2000	18,456
8008	17,868
80	15,891
443	14,235
8010	10,134
<a href="#">More...</a>	

TOP ORGANIZATIONS	
Universita' degli Studi di Udine	18,892
UNI-Venezia	10,052
INFN - LNF - Frascati	5,913
UNI-Padova	4,385
POLI-Torino	4,207
<a href="#">More...</a>	

Organizzazioni con il maggior numero di dispositivi censiti

# Shodan

## Esempio 1

- Effettuiamo una ricerca per Autonomous System Network (**asn:as137**)

Software più utilizzati

TOP PRODUCTS	
Apache httpd	12,474
OpenSSH	7,187
nginx	4,361
Fortinet FortiGate-600E	1,851
ciscoSystems	1,321
<a href="#">More...</a>	

Sistemi Operativi  
più utilizzati

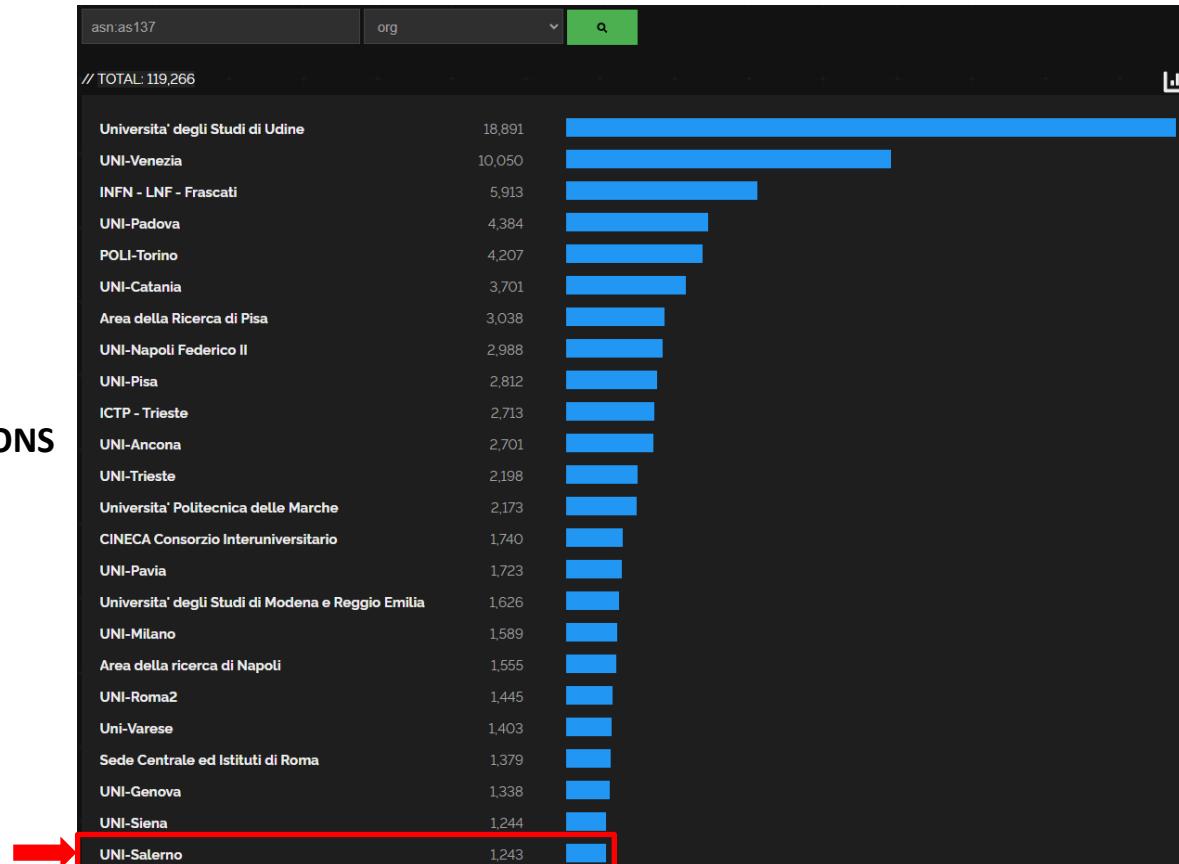
TOP OPERATING SYSTEMS	
Windows	2,114
Ubuntu	1,895
Linux	940
Debian	474
Windows (build 10.0.19041)	201
<a href="#">More...</a>	

# Shodan

## Esempio 1

- Selezioniamo l'organizzazione **UNI-Salerno**

### TOP ORGANIZATIONS



Enumerating Target e Port Scanning

# Shodan

## Esempio 1

### ➤ Information freshness

The screenshot shows a Shodan search interface with three results listed:

- 193.205.186.112** (highlighted with a red box)
  - UNI-Salerno
  - Italy, Rome
  - HTTP/1.1 400 Bad Request
  - Date: Mon, 22 Apr 2024 08:50:53 GMT
  - Server: Apache/2.4.46 (Unix) OpenSSL/1.1.1i PHP/8.0.2 mod\_perl/2.0.11 Perl/v5.32.1
  - Vary: accept-language,accept-charset
  - Accept-Ranges: bytes
  - Connection: close
  - Content-Type: text/html; charset=utf-8
  - Content-Language: en
  - Expires: ...
- 193.205.162.176**
  - UNI-Salerno
  - Italy, Lancusi-Penta-Bolano
  - No data returned
- 193.205.184.221**
  - dev2.unisa.it
  - UNI-Salerno
  - Italy, Rome
  - No data returned

A red callout box labeled "Information freshness" points to the timestamp "2024-04-22T08:51:52.196107" in the first result's details.

# Shodan

## Esempio 1

- Selezioniamo l'indirizzo IP 193.205.186.112

The screenshot shows the Shodan search interface with the following details:

- View Report**, **Browse Images**, **View on Map** buttons.
- Partner Spotlight:** Looking for a Splunk alternative to store all the Shodan data? Check out [Gravwell](#).
- IP Address:** 193.205.186.112 (highlighted with a red box).
- Date:** 2024-04-22T08:51:52.196107
- Location:** UNI-Salerno, Italy, Rome.
- HTTP Response Headers:**

```
HTTP/1.1 400 Bad Request
Date: Mon, 22 Apr 2024 08:50:53 GMT
Server: Apache/2.4.46 (Unix) OpenSSL/1.1.1i PHP/8.0.2 mod_perl/2.0.11 Perl/v5.32.1
Vary: accept-language,accept-charset
Accept-Ranges: bytes
Connection: close
Content-Type: text/html; charset=utf-8
Content-Language: en
Expires: ...
```
- IP Address:** 193.205.162.176
- Location:** UNI-Salerno, Italy, Lancusi-Penta-Bolano.
- Date:** 2024-04-22T08:45:29.839106
- IP Address:** 193.205.184.221
- Location:** dev2.unisa.it, UNI-Salerno, Italy, Rome.
- Date:** 2024-04-22T08:18:16.481011

# Shodan

## Esempio 1

➤ Informazioni relative all'indirizzo IP 193.205.186.112 (Informazioni Generali)

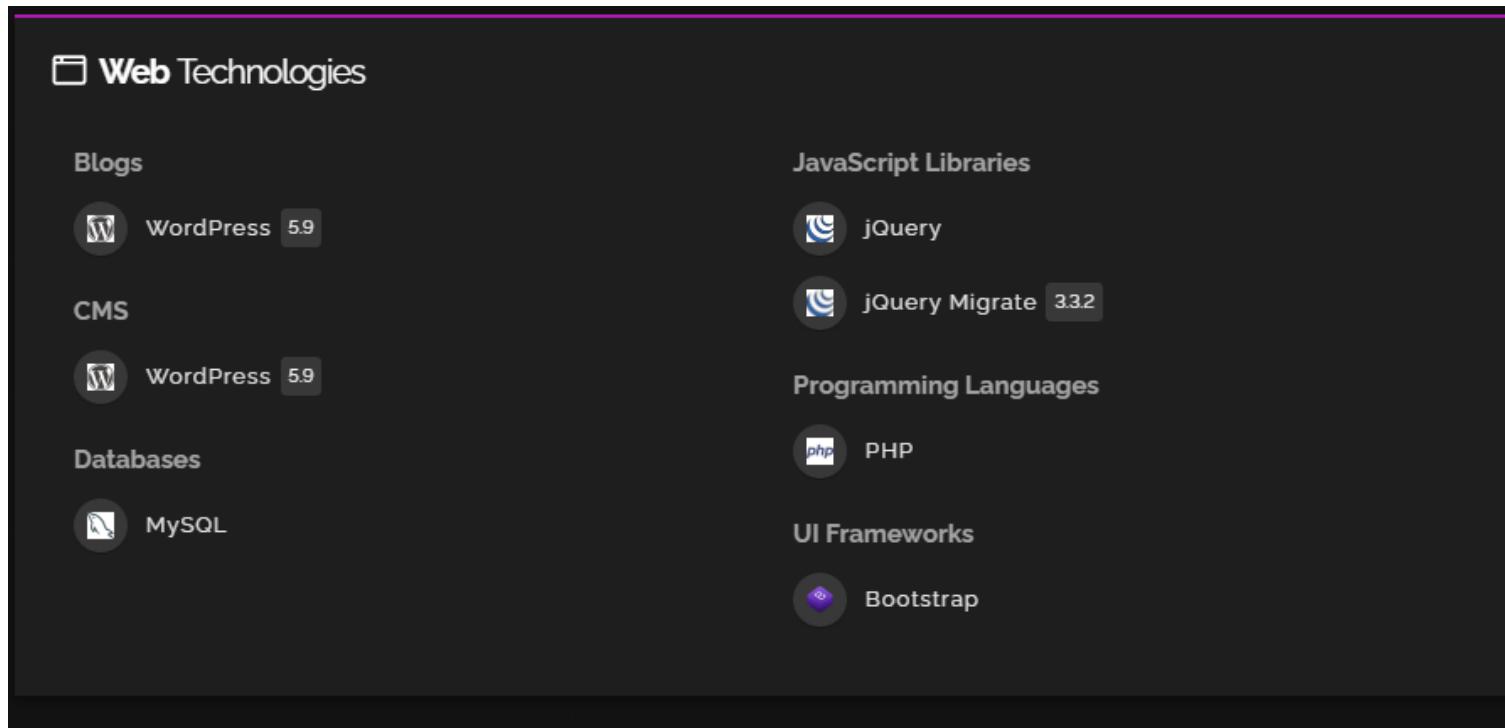
The screenshot shows the Shodan search results for the IP address 193.205.186.112. At the top, the IP is displayed in large white text. Below it are two buttons: "Regular View" and "Raw Data". A small map of Italy is visible in the background. The main content area is titled "General Information" and contains the following data:

Hostnames	[REDACTED]
Domains	UNISA.IT
Country	Italy
City	Rome
Organization	UNI-Salerno
ISP	Consortium GARR
ASN	AS137

# Shodan

## Esempio 1

➤ Informazioni relative all'indirizzo IP 193.205.186.112 (Tecnologie Web)



# Shodan

## Esempio 1

➤ Informazioni relative all'indirizzo IP 193.205.186.112 (Porte Aperte)

Open Ports

21 25 80 110 137 143 443 445 2000 3306 8010

// 80 / TCP ↗ 1534238299 | 2024-04-03T08:29:28.496073

**Apache httpd 2.4.46**

```
HTTP/1.1 200 OK
Date: Wed, 03 Apr 2024 08:28:36 GMT
Server: Apache/2.4.46 (Unix) OpenSSL/1.1.1i PHP/8.0.2 mod_perl/2.0.11 Perl/v5.32.1
X-Powered-By: PHP/8.0.2
X-Pingback: http://www.biopl.it/home/xmlrpc.php
Link: <http://www.biopl.it/home/wp-json/>; rel="https://api.w.org/"
Link: <http://www.biopl.it/home/wp-json/wp/v2/pages/2>; rel="alternate"; type="application/json"
Link: <http://www.biopl.it/home/>; rel=shortlink
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

Eventuali banner relativi alle porte aperte

# Shodan

## Esempio 1

### ➤ Informazioni relative all'indirizzo IP 193.205.186.112 (Vulnerabilità)

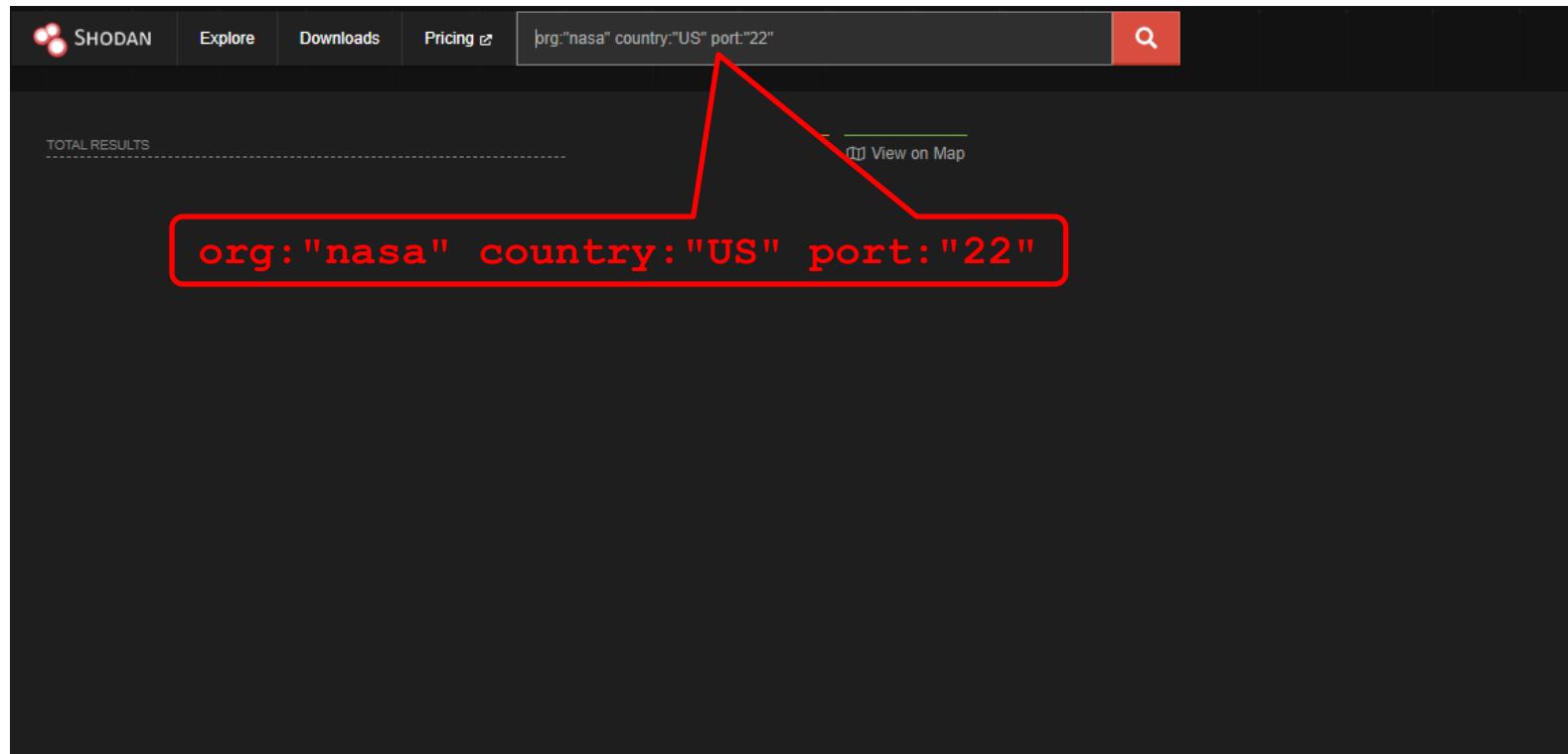
#### ⚠ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

<b>CVE-2024-0727</b>	Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.
<b>CVE-2023-5678</b>	Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions

# Shodan

## Esempio 2



# Shodan

## Esempio 2

The screenshot shows the Shodan search interface with the query `port:22` entered in the search bar. The results page displays three findings:

- 169.154.198.34**  
g5874-kona.cmc.gsfc.nasa.gov  
NASA Goddard Space Flight Center  
United States, Greenbelt  
SSH-2\_0-OpenSSH\_7.4  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAQABAAQDc2OIYmsGdd4Gdmaf11GQ02g8zEfws53CL26kucIy2EDqLUv2ap+92gB523JjX16C48st1gIby796PsCLIPYsT9AEEv3jXdkm@roAhkwCE21KKAA3usM9LghxQtin5hbInnEVlQayYeG4CCcgKC7g2eA12v/RyV1vHx5jPxmXZuoSHaNsdxXLbfMcvY/k1/yHNfkPc4PF8VsSukw1RaN+OIf+c5INZ8...
- 169.154.198.66**  
g5874-kona2.cmc.gsfc.nasa.gov  
NASA Goddard Space Flight Center  
United States, Greenbelt  
SSH-2\_0-OpenSSH\_7.4  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAQABAAQc2OIYmsGdd4Gdmaf11GQ02g8zEfws53CL26kucIy2EDqLU5K1EqihDBw/kFRWk9TbejdRaDnuQpuv3RMPhqcSnOKEC13Py74DHdRxTopaCQVa2Zk4Qnx6aE1F0P9ATa+CKV8tfuE2BhlgGU8xswhCJYwS9f7G7aMb5ZQEfkwQ9BD2MSbpA31aKF7rbdSs7SUzeZz43TQY/f3d5tuMpJ2Rv+Y1...
- 169.154.128.58**  
odist5.sci.gsfc.nasa.gov  
NASA Goddard Space Flight Center  
United States, Greenbelt  
SSH-2\_0-OpenSSH\_8.2p1 Ubuntu-4ubuntu0.4  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAQABAAQDhInTj210I/V1azvM8Np1101955XBzVwqbpb5sT8yruCzq2tW5suOrS7F487V40ghhkQP2TXl.lcA4Z7mrP685G158eAAKNQ5QyR4yyBdUvvtcbqPeab6hme3p31tmw0j10zZqgPkw4w5mTOe0KQm1WTtxg5RMJ112UmaoqnRZt160gYIKzmKvOdrnHnr11Vp03eE...

Enumerating Target e Port Scanning

# Shodan

## Esempio 2

"port:22"  Account

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

**169.154.198.34**

gsl74-kona2.comc.gsfc.nasa.gov  
NASA Goddard Space Flight Center  
United States, Greenbelt

SSH-2.0-OpenSSH\_7.4  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAQABAAAQABzBF5Bwspcu5UhjaIQuuAwI17n7n3yJloCwTT3ClrDvZv2ap+92g85233JX16C48st1gby796PscLUPYsT9AEEv3jXoK8roAhkwCE21KA3usM9Lgi0Qtn5hBm0nVPtQdYg44CCgx7ge2eAIZv/RyV1vhX5\_jPxcmXzuo5hawNsuxXLbfmcV//k1/yHnfkPc4PFBVsSuKv1RnN+0f+c5Nz8...

**169.154.198.66**

gsl74-kona2.comc.gsfc.nasa.gov  
NASA Goddard Space Flight Center  
United States, Greenbelt

SSH-2.0-OpenSSH\_7.4  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAQABAAAQABzBF5Bwspcu5UhjaIQuuAwI17n7n3yJloCwTT3ClrDvZ5K1EqnhdBW/+xRMK0tBMedirAnQpuv30RPhqSMjKEC13Fy74DHURxTopaCVA14Qnx6ElF8P9ATa0+CV8BfufE2BNMgQIBX+swhCJy59P7G7aMbS2QEerfvQ9B02NmSbpA31akF7rbd5s7sUzce2z43T0V/F3dStulp2l2RvY1...

**169.154.128.58**

occlif5.sci.gsfc.nasa.gov  
NASA Goddard Space Flight Center  
United States, Greenbelt

SSH-2.0-OpenSSH\_8.2p1 Ubuntu-4ubuntu0.4  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAQABAAAQABzBF5Bwspcu5UhjaIQuuAwI17n7n3yJloCwTT3ClrDvZ2IM5suOr57f483V4OglnhQP2TX01cA4Z7mrP6B56158eAAKNQ5Qy#4y8DxVuvt:8qVpEaBb6hne3P31tm0j10zZegPkwuSeTOe8KQh1Wtxg5RM0J11z1maoqeRZt168gYTKzmkV0drn#Hnr11Vp03e...

2022-04-07T09:54:23.87599

2022-04-07T03:09:27.36421

2022-03-28T06:37:20.67239

**Information freshness**

# Shodan

## Esempio 2

The screenshot shows the Shodan search interface with the query "port:22" entered in the search bar. The results section displays three findings:

- 169.154.198.34**  
g5874-kona2.cmc.gsfc.nasa.gov  
NASA Goddard Space Flight Center  
United States, Greenbelt  
SSH-2\_0-OpenSSH\_7.4  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAQABAAQDzBBf50wspcu5Uwja1QauLwd17N7m3yUoWTT3CUrDvZV2ap+92gB523JjX16C48st1gIby796PsCLIPYsT9AEEv3jXdkm@roAhkwCE21KKAA3usM9LghxQtin5hbinEVlQayYeG4CCcgKC7g2eA12v/RyV1vHx5jPxmXZuoSHaNs0XLbfMcvY/k1/yHNfkPc4PF8VsSukw1RaN+OIf+c5INZ8...  
An arrow points to this result.
- 169.154.198.66**  
g5874-kona2.cmc.gsfc.nasa.gov  
NASA Goddard Space Flight Center  
United States, Greenbelt  
SSH-2\_0-OpenSSH\_7.4  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAQABAAQDzBBf50wspcu5Uwja1QauLwd17N7m3yUoWTT3CUrDvZV2ap+92gB523JjX16C48st1gIby796PsCLIPYsT9AEEv3jXdkm@roAhkwCE21KKAA3usM9LghxQtin5hbinEVlQayYeG4CCcgKC7g2eA12v/RyV1vHx5jPxmXZuoSHaNs0XLbfMcvY/k1/yHNfkPc4PF8VsSukw1RaN+OIf+c5INZ8...  
This result is identical to the first one.
- 169.154.128.58**  
odist5.sci.gsfc.nasa.gov  
NASA Goddard Space Flight Center  
United States, Greenbelt  
SSH-2\_0-OpenSSH\_8.2p1 Ubuntu-4ubuntu0.4  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAQABAAQDzBBf50wspcu5Uwja1QauLwd17N7m3yUoWTT3CUrDvZV2ap+92gB523JjX16C48st1gIby796PsCLIPYsT9AEEv3jXdkm@roAhkwCE21KKAA3usM9LghxQtin5hbinEVlQayYeG4CCcgKC7g2eA12v/RyV1vHx5jPxmXZuoSHaNs0XLbfMcvY/k1/yHNfkPc4PF8VsSukw1RaN+OIf+c5INZ8...  
This result is identical to the first two.

Enumerating Target e Port Scanning

# Shodan

## Esempio 2

The screenshot shows the Shodan search results for the IP address 169.154.198.34. At the top, there is a map of the Washington, D.C. area with several locations labeled. A red arrow points from the text "Geolocalizzazione dell'host selezionato" to the map. Below the map, the search results are displayed in a table format:

General Information	
Hostnames	gs674-kona.ccmc.gsfc.nasa.gov
Domains	NASA.GOV
Country	United States
City	Greenbelt
Organization	NASA Goddard Space Flight Center
ISP	NASA Goddard Space Flight Center
ASN	AS7847

Below the general information, there is a section titled "Vulnerabilities" with two entries:

- CVE-2018-15919**: Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'
- CVE-2017-15906**: The process\_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

Enumerating Target e Port Scanning

# Shodan

## Esempio 2

SHODAN Explore Downloads Pricing Search... 🔍

169.154.198.34 Regular View Raw Data History

**General Information**

Hostnames	gs674-kona.ccmc.gsfc.nasa.gov
Domains	NASA.GOV
Country	United States
City	Greenbelt
Organization	NASA Goddard Space Flight Center
ISP	NASA Goddard Space Flight Center
ASN	AS7847

**Vulnerabilities**

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

**CVE-2018-15919** Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'

**CVE-2017-15906** The process\_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

**Informazioni generali sull'host selezionato**

Enumerating Target e Port Scanning

# Shodan

## Esempio 2

The screenshot shows the Shodan search results for the IP address 169.154.198.34. The top navigation bar includes links for SHODAN, Explore, Downloads, Pricing, and a search bar. The main content area starts with a map of the Washington D.C. area, with the IP address 169.154.198.34 highlighted in red. Below the map is a table of general information:

General Information	
Hostnames	gs674-kona.ccmc.gsfc.nasa.gov
Domains	NASA.GOV
Country	United States
City	Greenbelt
Organization	NASA Goddard Space Flight Center
ISP	NASA Goddard Space Flight Center
ASN	AS7847

A red callout box points to the "Vulnerabilities" section at the bottom of the page, which contains two entries:

- CVE-2018-15919**: Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'
- CVE-2017-15906**: The process\_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

**Eventuali vulnerabilità dell'host selezionato**

# Shodan

## Esempio 2

Open Ports  
22

// 22 / TCP 2004830606 | 2022-04-08T22:10:59.661749

**OpenSSH 7.4**

```
SSH-2.0-OpenSSH_7.4
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAADQABAAAQOczBBf8wspcuSiWjalQauAwI7m3yUoCwTTJCUrDvZ
v2apewZgB523jXj6C48stlgby796PsCUPYsT9AEv3jXdkm8roAhkwE2lKKAA3usM9LghxQtNS
hBcJnEVp0AyYe4CCcpXC7gcaA1Zv/YyVivH5jPXcmZuo5HaNsdxLbfMcV/k1/yHNfkPc4
PFBVsSuKw1RaN+Olfc+c5NZ88zEUpb/YT6JWmzLqjvp4tMOvUnN0/2jM7ylu9RC/x6wI4Ng01et
SzMy8V0rgV1dCCEuHW/1bc19YxiduSebchsuad1hMF1vebZza10A30ZFHP180qv
Fingerprint: fc:c9:36:25:00:ae:d6:df:5c:42:9c:b8:11:89:b7:b5

Kex Algorithms:
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp512
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha1
diffie-hellman-group18-sha512
diffie-hellman-group-exchange-sha1
diffie-hellman-group14-sha256
diffie-hellman-group14-sha1
diffie-hellman-group1-sha1
diffie-hellman-group1-sha1

Server Host Key Algorithms:
ssh-rsa
rsa-sha2-512
rsa-sha2-256
ecdsa-sha2-nistp256

Encryption Algorithms:
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com

MAC Algorithms:
hmac-sha2-256
hmac-sha2-512

Compression Algorithms:
none
zlib@openssh.com
```

Ulteriori informazioni (banner)  
sui servizi erogati dall'host

# Shodan

## Esempio 3

TOTAL RESULTS  
17,867

TOP CITIES

Milan	3,820
Rome	2,488
Turin	640
Naples	517
Bologna	434

More...

TOP ORGANIZATIONS

Fastweb SpA	3,413
Telecom Italia S.p.A.	3,204
Vodafone Italia S.p.A.	1,575
Telecom Italia S.p.A. TIN EASY LITE	1,488
Tiscali Italia S.p.A.	686

More...

TOP PRODUCTS

Samba	5,995
smbx	375
NQE 2.0	300
NO 6.2	6
YNQ 1.4.6	5

More...

TOP OPERATING SYSTEMS

Windows 6.1	2,334
Unix	2,316
QTS	1,353
Windows Server 2012 R2 Standard 9600	555
Darwin	375

More...

country:"IT" port:"445"

View Results | View on Map

93.42.154.234  
host-93-42-154-234.qb67.infowebnet.it  
Fastweb SpA  
Italy, Milano

185.251.124.23  
host-185-251-124-23.ipv4.inflibrasil.com  
Unguanti Claudia trading as Micro Servizi  
Italy, Grammichele

31.198.27.98  
host-31-198-27-98.business.telecomitalia.it  
TROTTA BUS SERVICES SPA  
Italy, Milan

87.26.8.236  
host-87-26-8-236.business.telecomitalia.it  
Telecom Italia S.p.A. IPTV  
Italy, Palazzo sulOglio

**country:"IT" port:"445"**

SMB Version: 1  
OS: Windows 6.1  
Software: Samba 4.7.1  
Capabilities: dfs, extended-security, infolevel-passthru, large-files, large-reads, large-writes, level2-locks, lock-and-read, nt-find, nt-smb, nt-status, raw-mode, rpc-remote-api, unicode, unix

Shares

Name	Type	Comments
print\$	Disk	Printer Drivers
GCORE_Windows_Server_2016 Disk	Disk	
IPC\$	IPC	IPC Service (Samba 4.7.1)
ISPsystem_Windows_Server_2019 Disk	Disk	

SMB Status:  
Authentication: enabled  
SMB Version: 1  
OS: Windows Server 2016 Standard 14393  
Software: Windows Server 2016 Standard 4.3  
Capabilities: extended-security, infolevel-passthru, large-files, large-reads, large-writes, level2-locks, lock-and-read, lwo, nt-find, nt-smb, nt-status, rpc-remote-api, unicode

SMB Status:  
Authentication: enabled  
SMB Version: 1  
OS: Windows Server 2016 Datacenter 14393  
Software: Windows Server 2016 Datacenter 4.3  
Capabilities: extended-security, infolevel-passthru, large-files, large-reads, large-writes, level2-locks, lock-and-read, lwo, nt-find, nt-smb, nt-status, rpc-remote-api, unicode

SMB Status:  
Authentication: enabled  
SMB Version: 1  
OS: Windows 6.1  
Software: Samba 4.1.11-Ubuntu  
Capabilities: dfs, extended-security, infolevel-passthru, large-files, large-reads, large-writes, level2-locks, lock-and-read, nt-find, nt-smb, nt-status, rpc-remote-api, unicode, unix

SMB Status:  
Authentication: enabled  
SMB Version: 1  
OS: QTS  
Software: Samba 4.13.17  
Capabilities: dfs, extended-security, infolevel-passthru, large-files, large-reads, large-writes, level2-locks, lock-and-read, nt-find, nt-smb, nt-status, raw-mode, rpc-remote-api, unicode

# Shodan

## Esempio 3

**TOTAL RESULTS**  
17,867

**TOP CITIES**

City	Count
Milan	3,820
Rome	2,488
Turin	640
Naples	517
Bologna	434

**TOP ORGANIZATIONS**

Organization	Count
Fastweb SpA	3,413
Telecom Italia S.p.A.	3,204
Vodafone Italia S.p.A.	1,575
Telecom Italia S.p.A. TIM EASY LITE	1,488
Tiscali Italia S.p.A.	686

**TOP PRODUCTS**

Product	Count
Samba	5,995
smbx	375
NQE 2.0	300
NO 6.2	6
YNQ 1.4.6	5

**TOP OPERATING SYSTEMS**

OS	Count
Windows 6.1	2,334
Unix	2,316
QTS	1,353
Windows Server 2012 R2 Standard 9600	555
Darwin	375

**New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor**

**92.38.174.4**  
do-muz.gicore.it  
G-Core Labs S.A.  
Italy, Milano

**93.42.154.234**  
93-42-154-234.q87.infowebnet.it  
Fastweb SpA  
Italy, Milano

**185.251.124.23**  
host-185-251-124-23.ipv4.inflibrasil.com  
Unguanti Claudia trading as Micro Servizi  
Italy, Grammichele

**31.198.27.98**  
host-31-198-27-98.business.telecomitalia.it  
TROTTA BUS SERVICES SPA  
Italy, Milan

**87.26.8.236**  
host-87-26-8-236.business.telecomitalia.it  
Telecom Italia S.p.A. IPTV  
Italy, Palazzo dello Stato

**92.38.174.4**  
SMB Status:  
Authentication: disabled  
SMB Version: 1  
OS: Windows 6.1  
Software: Samba 4.7.1  
Capabilities: dfs, extended-security, infolevel-passthru, large-files, large-reads, large-writes, level2-locks, lock-and-read, nt-find, nt-smb, nt-status, raw-mode, rpc-remote-api, unicode, unix

**93.42.154.234**  
SMB Status:  
Authentication: enabled  
SMB Version: 1  
OS: Windows Server 2016 Standard 14393  
Software: Windows Server 2016 Standard 4.3  
Capabilities: extended-security, infolevel-passthru, large-files, large-reads, large-writes, level2-locks, lock-and-read, lwo, nt-find, nt-smb, nt-status, rpc-remote-api, unicode

**185.251.124.23**  
SMB Status:  
Authentication: enabled  
SMB Version: 1  
OS: Windows Server 2016 Datacenter 14393  
Software: Windows Server 2016 Datacenter 6.3  
Capabilities: extended-security, infolevel-passthru, large-files, large-reads, large-writes, level2-locks, lock-and-read, lwo, nt-find, nt-smb, nt-status, rpc-remote-api, unicode

**31.198.27.98**  
SMB Status:  
Authentication: enabled  
SMB Version: 1  
OS: Windows 6.1  
Software: Samba 4.3.11-Ubuntu  
Capabilities: dfs, extended-security, infolevel-passthru, large-files, large-reads, large-writes, level2-locks, lock-and-read, nt-find, nt-smb, nt-status, rpc-remote-api, unicode, unix

**87.26.8.236**  
SMB Status:  
Authentication: enabled  
SMB Version: 1  
OS: QTS  
Software: Samba 4.13.17  
Capabilities: dfs, extended-security, infolevel-passthru, large-files, large-reads, large-writes, level2-locks, lock-and-read, nt-find, nt-smb, nt-status, raw-mode, rpc-remote-api, unicode

Enumerating Target e Port Scanning

# Shodan

## Esempio 3

Informazioni sulle altre porte aperte presenti sull'host selezionato

The screenshot shows the Shodan search results for the IP address 92.38.174.4. At the top, there's a map of Milan with various locations labeled. Below the map, the IP address is displayed as 92.38.174.4 with options for Regular View, Row Data, and History. A red box highlights the "Open Ports" section on the right.

**General Information**

- Hostnames: dci-mi2.gcorelabs.com, gcorelabs.com
- Domains: GCORELABS.COM
- Country: Italy
- City: Milano
- Organization: G-Core Labs S.A.
- ISP: G-Core Labs S.A.
- ASN: AS199524
- Operating System: Windows 6.1

**Web Technologies**

- JQUERY

**Open Ports**

Ports: 80, 111, 443, 445

**// 80 / TCP**

```
HTTP/1.1 301 Moved Permanently
Content-Length: 9
Connection: close
Location: https://92.38.174.4/
Date: Sat, 09 Apr 2022 04:14:44 GMT
```

**// 111 / TCP**

Portmap	Program Version	Protocol	Port
portscanner	4	tcp	111
portscanner	2	tcp	111
portscanner	2	tcp	1111
portscanner	4	udp	111
portscanner	3	udp	1111
portscanner	4	udp	1111
status	1	udp	52237
status	1	tcp	59978
mountd	1	udp	20048
mountd	2	tcp	20048
mountd	2	udp	20048
mountd	2	tcp	20048
mountd	3	udp	20048
mountd	3	tcp	20048
mountd	3	tcp	20048
nfs	4	tcp	2049
180227	3	tcp	2049
nfs	3	udp	2049
180227	3	udp	2049
clockmgr	1	udp	33489
clockmgr	3	udp	33489
clockmgr	4	udp	33489
clockmgr	1	tcp	33899
clockmgr	3	tcp	33899
clockmgr	4	tcp	33899

**// 443 / TCP**

# Shodan

## Esempio 4

**vsftpd 2.3.4 country:"US" port:"21"**

TOTAL RESULTS  
393

TOP CITIES

New York City	137
Newark	15
Ashburn	11
San Jose	11
Los Angeles	10
More...	

TOP ORGANIZATIONS

Techie Hosting, Inc.	137
Comcast Cable Communications, LLC	27
T-Mobile USA, Inc.	19
Charter Communications Inc	17
Charter Communications	10
More...	

TOP PRODUCTS

vsftpd	1
vsftpd (before 2.0.8) or WU-FTPD	1

**66.211.130.34**  
Techie Hosting, Inc.  
United States, Portland

220 (vsftpd 2.3.4)  
530 Login incorrect.  
530 Please login with USER and PASS.  
211-Features:  
EPRT  
EPSV  
MDTM  
PASV  
REST STREAM  
SIZE  
TVFS  
UTF8  
211 End

**208.71.131.16**  
Techie Hosting, Inc.  
United States, New York City

220 (vsftpd 2.3.4)  
530 Login incorrect.  
530 Please login with USER and PASS.  
211-Features:  
EPRT  
EPSV  
MDTM  
PASV  
REST STREAM  
SIZE  
TVFS  
UTF8  
211 End

**208.71.130.44**  
Techie Hosting, Inc.  
United States, New York City

220 (vsftpd 2.3.4)  
530 Login incorrect.  
530 Please login with USER and PASS.  
211-Features:  
EPRT  
EPSV  
MDTM

Enumerating Target e Port Scanning

# Shodan

## Esempio 4

TOTAL RESULTS  
393

TOP CITIES  
New York City  
Newark  
Ashburn

TOP PRODUCTS  
vsftpd  
vsftpd (before 2.0.8) or WU-FTPd

**69.85.203.196**  
Crown Management, LLC  
United States, New Orleans

220 (vsFTPD 2.3.4)  
530 Login incorrect.  
530 Please login with USER and PASS.  
211-Features:  
EPRT  
EPSV  
MDTM  
PASV  
REST STREAM  
SIZE  
TVFS  
UTF8  
211 End

**66.211.130.34**  
FirstLight Fiber  
United States, Portland

220 (vsFTPD 2.3.4)  
530 Login incorrect.  
530 Please login with USER and PASS.  
211-Features:  
EPRT  
EPSV  
MDTM  
PASV  
REST STREAM  
SIZE  
TVFS  
UTF8  
211 End

**208.71.131.16**  
Techie Hosting, Inc.  
United States, New York City

220 (vsFTPD 2.3.4)  
530 Login incorrect.  
530 Please login with USER and PASS.  
211-Features:  
EPRT  
EPSV  
MDTM  
PASV  
REST STREAM  
SIZE  
TVFS  
UTF8  
211 End

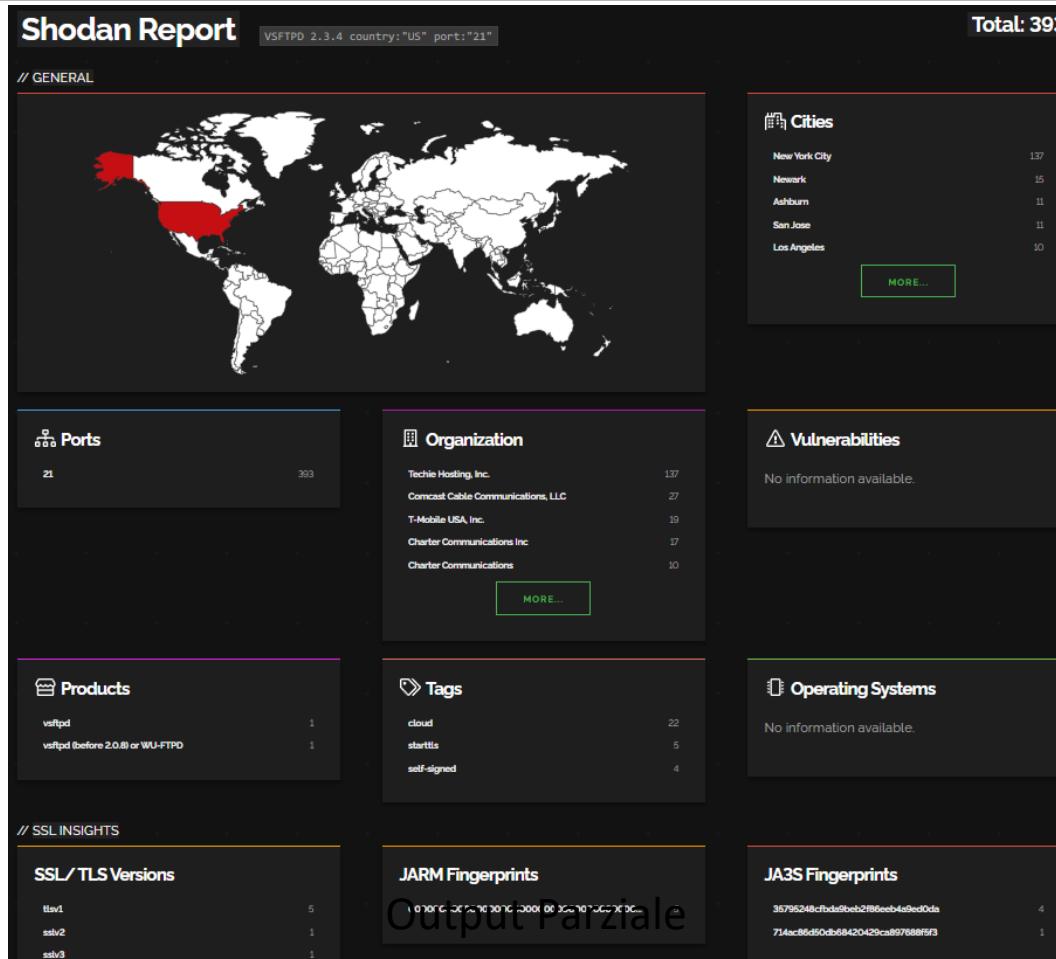
**208.71.130.44**  
Techie Hosting, Inc.  
United States, New York City

220 (vsFTPD 2.3.4)  
530 Login incorrect.  
530 Please login with USER and PASS.  
211-Features:  
EPRT  
EPSV  
MDTM

Enumerating Target e Port Scanning

# Shodan

## Esempio 4



Enumerating Target e Port Scanning

# Shodan

## Esempio 5

The screenshot shows the Shodan search interface with the query `rfb 003.007 authentication country:"ru"` entered in the search bar. A red box highlights the search term `rfb 003.007 authentication country:"ru"`. The results page displays 157 total results. The top section includes links for `View` and `Map`. Below this, there are sections for `TOP CITIES`, `TOP PORTS`, and `TOP ORGANIZATIONS`. The main results area lists four IP addresses with their details:

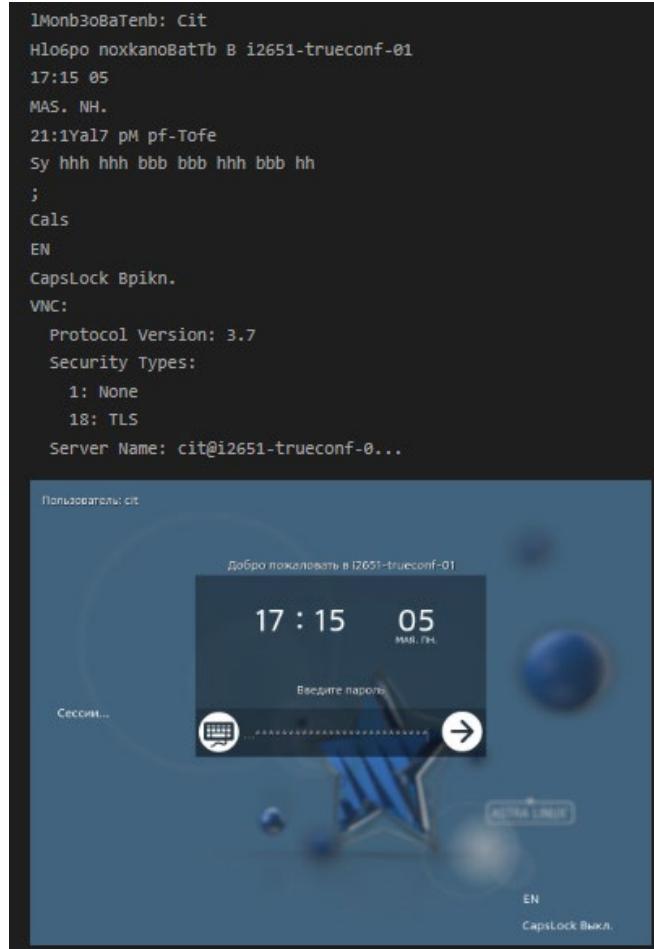
- 79.172.36.66**  
Protocol: RFB 003.007  
Authentication: disabled  
Country: Russian Federation, Yekaterinburg  
Organization: JSC ER-Telecom Holding  
Port: 79.172.36.66.usat.ru
- 87.251.183.194**  
Protocol: RFB 003.007  
Authentication: disabled  
Country: Russian Federation, Yekaterinburg  
Organization: PJSC Rostelecom  
Port: 87.251.183.194.rnsat.ru
- 188.235.160.190**  
Protocol: RFB 003.007  
Authentication: disabled  
Country: Russian Federation, Saratov  
Organization: CJSC ER-Telecom Holding Saratov branch  
Port: dynamicip.188.235.160.190.pppoe.saratov.ertelecom.ru
- 83.171.73.101**  
Protocol: RFB 003.007  
Authentication: disabled  
Country: Russian Federation, Krasnogorsk  
Organization: PJSC Rostelecom  
Port: 83.171.73.101.rnsat.ru

Each result entry includes a small flag icon representing the country and a link to the detailed view.

Enumerating Target e Port Scanning

# Shodan

## Esempio 5



Enumerating Target e Port Scanning

# Shodan

## Esempio 6

The screenshot shows the Shodan search interface with the query 'netcam' entered in the search bar. A red box highlights the search term 'netcam'. The results page displays a map of the world with red dots indicating found devices. Below the map are sections for 'TOP COUNTRIES' and 'TOP PORTS'. The 'TOP COUNTRIES' section lists the United States (570), Germany (398), Hong Kong (381), Russian Federation (335), and France (318). The 'TOP PORTS' section lists port 80 (600), port 81 (297), port 82 (219), port 8080 (163), and port 8000 (147). The main search results are shown in a grid format, with each result including the IP address, organization name, location, and a detailed technical panel. The first result is 113.253.233.239, which belongs to HGC Global Communications Limited in Hong Kong, Hong Kong. The second result is 193.252.194.239, which belongs to Orange S.A. in France, Cambrai. The third result is 149.28.168.149, which belongs to Vultr Holdings, LLC in Australia, Sydney. The fourth result is 129.28.171.180, which belongs to Tencent Cloud Computing (Beijing) Co., Ltd in China, Guangzhou. The fifth result is 37.143.130.93, which belongs to Oneprovider.com - Madrid Infrastructure in Spain, Madrid.

IP Address	Organization	Location
113.253.233.239	HGC Global Communications Limited	Hong Kong, Hong Kong
193.252.194.239	Orange S.A.	France, Cambrai
149.28.168.149	Vultr Holdings, LLC	Australia, Sydney
129.28.171.180	Tencent Cloud Computing (Beijing) Co., Ltd	China, Guangzhou
37.143.130.93	Oneprovider.com - Madrid Infrastructure	Spain, Madrid

Enumerating Target e Port Scanning

# Shodan

## Esempio 7

The screenshot shows the Shodan search interface with the query "Axis M1013" entered into the search bar. The results page displays 48 findings across various countries and organizations. Each result entry includes the IP address or host name, organization name, location, and a snippet of the device's configuration or log output.

TOP COUNTRIES	COUNT
Mexico	20
Russian Federation	9
United States	8
Nicaragua	3
Brazil	2
<a href="#">More...</a>	

TOP ORGANIZATIONS	COUNT
Gestión de direccionamiento UniNet	12
Uninet S.A. de C.V.	8
EQUIPOS Y SISTEMAS S.A.	3
Novgorod Datacom	3
Purdue University	3
<a href="#">More...</a>	

**Axis M1013**

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

**189.190.91.168**  
ds1-189-190-91-168-dyn.prod-infinium.com.mx  
Gestión de direccionamiento UniNet  
Mexico, Puebla

220 AXIS M1013 Fixed Network Camera 5.51.7.3 (2020) ready.  
538 Login incorrect.  
214-The following commands are implemented.  
USER QUIT PASS SYST HELP PORT PASV LIST  
NLST RETR STOR TYPE MKD RMD DELE PWD  
CWD SITE COUP RNFR RNTO NOOP...

**128.46.190.92**  
shincam-me38.ecn.purdue.edu  
Purdue University  
United States, West Lafayette

220 AXIS M1013 Fixed Network Camera 5.50.5.1 (2014) ready.  
538 Login incorrect.  
214-The following commands are implemented.  
USER QUIT PASS SYST HELP PORT PASV LIST  
NLST RETR STOR TYPE MKD RMD DELE PWD  
CWD SITE COUP RNFR RNTO NOOP...

**67.215.107.37**  
Nusbeam Communications  
Puerto Rico, San Juan

220 AXIS M1013 Fixed Network Camera 5.40.5.3 (2013) ready.  
538 Login incorrect.  
214-The following commands are implemented.  
USER QUIT PASS SYST HELP PORT PASV LIST  
NLST RETR STOR TYPE MKD RMD DELE PWD  
CWD SITE COUP RNFR RNTO NOOP...

**200.145.110.201**  
host10201.fcav.unesp.br  
UNIVERSIDADE ESTADUAL PAULISTA  
Brazil, Jaboticabal

220 AXIS M1013 Fixed Network Camera 5.40.5.2 (2013) ready.  
538 Login incorrect.  
214-The following commands are implemented.  
USER QUIT PASS SYST HELP PORT PASV LIST  
NLST RETR STOR TYPE MKD RMD DELE PWD  
CWD SITE COUP RNFR RNTO NOOP...

**84.242.195.42**  
Novgorod Datacom  
Russian Federation, Veliky Novgorod

220 AXIS M1013 Fixed Network Camera 5.40.5.3 (2013) ready.  
538 Login incorrect.  
214-The following commands are implemented.  
USER QUIT PASS SYST HELP PORT PASV LIST  
NLST RETR STOR TYPE MKD RMD DELE PWD  
CWD SITE COUP RNFR RNTO NOOP...

Enumerating Target e Port Scanning

# Shodan

## Esempio 8

A screenshot of the Shodan search interface. The search bar at the top contains the query `"default password"`. A red arrow points from the text `"default password"` to the search bar. The search results page shows various findings across different sections: TOP COUNTRIES, TOP PORTS, TOP ORGANIZATIONS, and TOP PRODUCTS. A red box highlights the first result in the main list:

**85.287.247.18**  
Ubiquiti Networks Device:  
IP Address: 85.287.247.18  
MAC Address: 00:15:60:89:11:05  
Alternate IP Address: 169.254.17.213  
Alternate MAC Address: 00:15:60:BA:11:D5  
Hostname: HACKED-ROUTER-HELP-SOS-HAD-**DEFAULT-PASSWORD**  
Product: NS5  
Version: X55.ar2313.v4.0.4.5074.150724.1344

Below this, there are two more results listed:

**88.8.205.34**  
Ubiquiti Networks Device:  
IP Address: 88.8.205.34  
MAC Address: 00:15:60:89:11:05  
Alternate IP Address: 169.254.17.213  
Alternate MAC Address: 00:15:60:BA:11:D5  
Hostname: HACKED-ROUTER-HELP-SOS-HAD-**DEFAULT-PASSWORD**  
Product: NS5  
Version: X55.ar2313.v4.0.4.5074.150724.1344

**37.114.229.53**  
Ubiquiti Networks Device:  
IP Address: 37.114.229.53  
MAC Address: 44:09:E7:C8:F8:8F  
Alternate IP Address: 192.168.1.1  
Alternate MAC Address: 44:09:E7:C8:F8:8F  
Hostname: HACKED-ROUTER-HELP-SOS-HAD-**DEFAULT-PASSWORD**  
Product: LMS  
Version: XW.ar934x.v5.6.2\_licensed.28182.150805.1456

**106.75.45.110**  
Ubiquiti Networks Device:  
IP Address: 106.75.45.110  
MAC Address: 44:09:E7:C8:F8:8F  
Alternate IP Address: 192.168.1.1  
Alternate MAC Address: 44:09:E7:C8:F8:8F  
Hostname: HACKED-ROUTER-HELP-SOS-HAD-**DEFAULT-PASSWORD**  
Product: LMS  
Version: XW.ar934x.v5.6.2\_licensed.28182.150805.1456

**147.78.3.206**  
Ubiquiti Networks Device:  
IP Address: 147.78.3.206  
MAC Address: 44:09:E7:C8:F8:8F  
Alternate IP Address: 192.168.1.1  
Alternate MAC Address: 44:09:E7:C8:F8:8F  
Hostname: HACKED-ROUTER-HELP-SOS-HAD-**DEFAULT-PASSWORD**  
Product: LMS  
Version: XW.ar934x.v5.6.2\_licensed.28182.150805.1456

Enumerating Target e Port Scanning

# Shodan

## Esempio 9

SHODAN | Explore | Downloads | Pricing | Server: SQ-WEBCAM |

TOTAL RESULTS: 320

TOP COUNTRIES:

Russian Federation 84  
Ukraine 43  
United Kingdom 35  
United States 35  
India 24  
[More...](#)

TOP PORTS:

Port	Count
80	30
81	29
52869	29
7547	28
37215	27
<a href="#">More...</a>	

TOP ORGANIZATIONS:

Organization	Count
Softline Trade JSC	84
Linode	80
139.162.0.0/16	26
LTD HOSTPRO LAB	24
Linode, LLC	22
<a href="#">More...</a>	

Server: SQ-WEBCAM

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

172.104.47.64   
http://162.76-64.members.linode.com  
Linode  
Singapore, Singapore  
   
HTTP/1.1 200 OK  
Server: 368 web server, 792/71644 HTTP Server version 2.0 - TELDAT S.A., A10wS/1.00, ADB Broadband HTTP Server, ADH-Web, AR, ASUSTeK UPnP/1.0 MiniUPnPd/1.4,

139.59.56.96   
DigitalOcean, LLC  
India, Doddaballapur  
   
HTTP/1.1 200 OK  
Server: 368 web server, 792/71644 HTTP Server version 2.0 - TELDAT S.A., A10wS/1.00, ADB Broadband HTTP Server, ADH-Web, AR, ASUSTeK UPnP/1.0 MiniUPnPd/1.4,

139.162.119.9   
http://1603.9-members.linode.com  
139.162.0.0/16  
Japan, Tokyo  
   
HTTP/1.1 200 OK  
Server: 368 web server, 792/71644 HTTP Server version 2.0 - TELDAT S.A., A10wS/1.00, ADB Broadband HTTP Server, ADH-Web, AR, ASUSTeK UPnP/1.0 MiniUPnPd/1.4,

93.90.222.17   
Softline Trade JSC  
Russia, Federation, Moscow  
   
HTTP/1.1 200 OK  
Server: 368 web server, 792/71644 HTTP Server version 2.0 - TELDAT S.A., A10wS/1.00, ADB Broadband HTTP Server, ADH-Web, AR, ASUSTeK UPnP/1.0 MiniUPnPd/1.4,

139.162.119.9   
http://1603.9-members.linode.com  
139.162.0.0/16  
Japan, Tokyo  
   
HTTP/1.1 200 OK  
Server: 368 web server, 792/71644 HTTP Server version 2.0 - TELDAT S.A., A10wS/1.00, ADB Broadband HTTP Server, ADH-Web, AR, ASUSTeK UPnP/1.0 MiniUPnPd/1.4,

93.90.222.28   
Softline Trade JSC  
Russia, Federation, Moscow  
   
HTTP/1.1 200 OK  
Server: 368 web server, 792/71644 HTTP Server version 2.0 - TELDAT S.A., A10wS/1.00, ADB Broadband HTTP Server, ADH-Web, AR, ASUSTeK UPnP/1.0 MiniUPnPd/1.4,

Enumerating Target e Port Scanning

# Shodan

## Esempio 10

SHODAN | Explore | Downloads | Pricing | linux upnp avtech

TOTAL RESULTS  
231,376

TOP COUNTRIES

Country	Count
Malaysia	48,428
Thailand	39,224
Indonesia	16,746
Taiwan	14,441
China	12,371
More...	

TOP PORTS

Port	Count
80	18,695
88	5,297
8080	4,081
81	3,839
8000	2,773
More...	

TOP ORGANIZATIONS

Organization	Count
Triple T Broadband Public Company Limited	24,563
TMN ST	23,773
Maxis Broadband Sdn Bhd	12,862
Internet Service Provider in Sri Lanka.	10,910
Chunghwa Telecom Co.,Ltd.	10,714
More...	

TOP PRODUCTS

Product	Count
Avtech AVN801 network camera	58,476
lighttpd	74
Apache httpd	63
Teradici PCoIP Management Console	59
CherryPy httpd	34
More...	

linux upnp avtech

View Report

123-195-224-17.dynamic.kbronet.com.tw  
Kbr CO., Ltd.  
Taiwan, Taoyuan City

Date: Mon, 11 Apr 2022 04:05:12 GMT  
Server: Linux/2.x UPnP/1.0 Avtech/1.0  
Connection: close  
Last-Modified: Tue, 26 Nov 2019 07:36:01 GMT  
Content-Type: text/html  
ETag: 238-54171-1574753761  
Content-Length: 54171

HTTP/1.1 200 OK  
Date: Mon, 11 Apr 2022 04:05:03 GMT  
Server: Linux/2.x UPnP/1.0 Avtech/1.0  
Connection: close  
Last-Modified: Wed, 27 Jun 2018 03:19:35 GMT  
Content-Type: text/html  
ETag: 388-15858-1530069575  
Content-Length: 15858

::: Login :::  
115.111.101.201  
STREAMY-BIZ-CENTRAL  
Malaysia, George Town

HTTP/1.1 200 OK  
Date: Mon, 11 Apr 2022 04:44:42 GMT  
Server: Linux/2.x UPnP/1.0 Avtech/1.0  
Connection: close  
Last-Modified: Thu, 30 Mar 2017 06:47:43 GMT  
Content-Type: text/html  
ETag: 268-16695-1498856463  
Content-Length: 16695

::: Login :::  
115.132.1.244  
TMNST  
Malaysia, Kuala Lumpur

HTTP/1.1 200 OK  
Date: Sun, 18 April 2022 21:04:16 GMT  
Server: Linux/2.x UPnP/1.0 Avtech/1.0  
Connection: close  
Last-Modified: Thu, 29 Nov 2018 15:04:28 GMT  
Content-Type: text/html  
ETag: 383-15858-1543503368  
Content-Length: 15858

Remote Surveillance, Any time & Any where

114.35.8.116  
114-35-8-116.hinet-ip.hinet.net  
Chunghwa Telecom Co.,Ltd.  
Taiwan, Miaoli

HTTP/1.1 200 OK  
Date: Mon, 11 Apr 2022 04:04:08 GMT  
Server: Linux/2.x UPnP/1.0 Avtech/1.0  
Connection: keep-alive  
Last-Modified: Fri, 28 May 2021 12:21:22 GMT  
Content-Type: text/html  
ETag: 238-54171-1622204482  
Content-Length: 54171

Enumerating Target e Port Scanning

# Outline

---

- Concetti Introduttivi
- Suite Protocollare TCP/IP
- Formato dei Messaggi TCP e UDP
- Active Enumeration
  - Network Scanner Nmap
  - Zenmap
  - Unicornscan
  - Masscan
- Passive Enumeration
  - Shodan
  - ZoomEye
  - FOFA
  - Censys

# ZoomEye

## Caratteristiche

---

- Motore di ricerca che permette di ottenere informazioni su
  - Dispositivi
  - Siti Web
  - Servizi di rete
  - Componenti di rete
  - Etc
- Prima di utilizzare ZoomEye è fortemente consigliata la registrazione
- Talvolta per l'accesso a ZoomEye potrebbe essere necessario l'utilizzo di VPN
  - A causa di filtri su indirizzi IP provenienti dall'Unione Europea



# ZoomEye

## Pricing

<https://www.zoomeye.ai/pricing>

		Registered User	Personal (Security enthusiasts) \$796 <b>\$190/Year</b>	Professional (Security teams and analysts) \$1,906 <b>\$1,090/Year</b>	Business (Medium to large enterprises) \$19,166 <b>\$10,990/Year</b>	Corporate (Tailored enterprise solutions)
Features & Price			<b>Buy Now</b>	<b>Buy Now</b>	<b>Buy Now</b>	<b>Contact Now</b>
New Explore+	ZoomEye Hub <small>NEW</small>	✗	✓	✓	✓	✓
	ZoomEyeGPT(AI Search) <small>NEW</small>	5 results/Day	30 results/Day	100 results/Day	1000 results/Day	Custom
	Monthly Maximum Results	3,000	100,000	800,000	10,000,000	Custom
	Maximum Result Pages	5	50	50	100	Custom
Primary	API Access Available	Use ZoomEye-Point	✓	✓	✓	✓
	API Request Rate Limit (requests/second)	0.5	1	1	2	Custom
	Number of Result Fields Available	46	71	74	78	78
	Web-based Results Download	Use ZoomEye-Point	✓	✓	✓	✓
	Honeypot Filtering	50 Points	10 Points	10 Points	✓	✓
Ability	Aggregated Results Data	20	50	50	100	100
	Historical Data Access	✗	✗	✗	✓	✓



# ZoomEye

## Interfaccia

➤ <https://www.zoomeye.ai/>

The screenshot shows the ZoomEye search interface. At the top, there is a navigation bar with links for Home, Pricing (which has a red "SALE" badge), Solutions, Explore, Tools, and Support. Below the navigation bar is a large blue globe graphic with a network of lines and dots. In the center of the globe is the ZoomEye logo, which consists of a stylized eye icon above the word "ZoomEye". Below the globe is a search bar with a placeholder "Search..." and a button with a magnifying glass icon. To the right of the search bar are icons for IP, domain, file, and collapse. Underneath the search bar is a section titled "HOT Popular Searches" with a list of 10 items. The items are numbered 1 through 10 and include: 1 app:"Starlink", 2 app:"Cisco WebUI", 3 app:"Openfire", 4 app:"Pentaho", 5 app:"EasyN webcam httpd", 6 app:"MinIO", 7 app:"Citrix ADC", 8 app:"Metabase", 9 app:"Fortigate SSL VPN", and 10 title:"Cisco ASDM". There is also a "Collapse" button next to the search results.

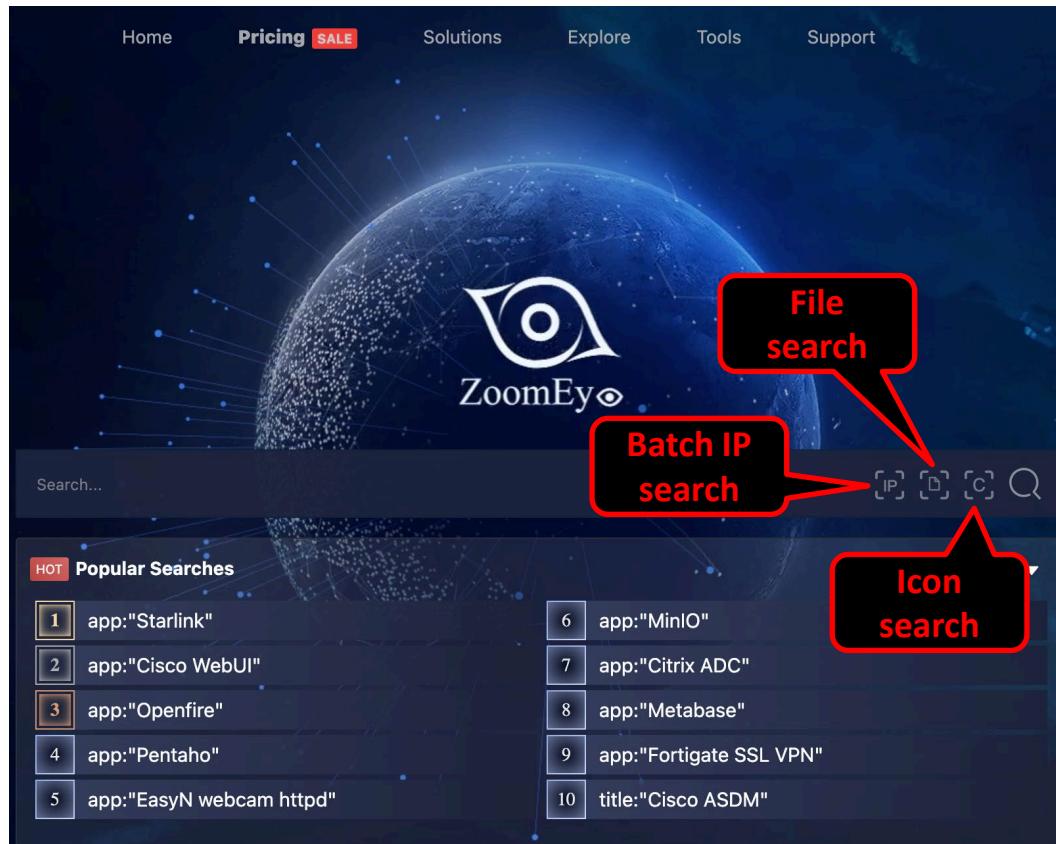
Rank	Query
1	app:"Starlink"
2	app:"Cisco WebUI"
3	app:"Openfire"
4	app:"Pentaho"
5	app:"EasyN webcam httpd"
6	app:"MinIO"
7	app:"Citrix ADC"
8	app:"Metabase"
9	app:"Fortigate SSL VPN"
10	title:"Cisco ASDM"

Enumerating Target e Port Scanning

# ZoomEye

## Interfaccia

➤ <https://www.zoomeye.ai/>



# ZoomEye

## API

- ZoomEye offre agli utenti la possibilità di utilizzare API
  - <https://github.com/knownsec/ZoomEye>

ZoomEye API SDK <https://www.zoomeye.org/api>

The screenshot shows a GitHub repository page for the 'ZoomEye API SDK'. At the top, there are tabs for 'zoomeye', 'zoomeye-api', and 'zoomeye-sdk', with 'zoomeye-api' being the active tab. Below the tabs, the repository statistics are displayed: 23 commits, 2 branches, 1 release, 5 contributors, and a license of GPL-2.0. A progress bar indicates the repository is 100% complete. The main area shows a list of commits. The first commit is a merge pull request from 'hysia' (commit e06afc5) on Nov 29, 2018. Other commits include 'Initial commit' for '.gitignore' and 'LICENSE', 'add unittest script' for 'tests', 'add setup.py', 'Update Readme.md', 'run a tests shell script', 'remove requires - getpass', and 'python3 (raw\_input -> input)' for 'zoomeye.py'. The commits are dated from 3 years ago to 11 months ago.

File / Commit Message	Date
tests add unittest script	3 years ago
.gitignore Initial commit	4 years ago
LICENSE Initial commit	4 years ago
MANIFEST.in add setup.py	3 years ago
README.md Update Readme.md	11 months ago
run_tests.sh run a tests shell script	3 years ago
setup.py remove requires - getpass	3 years ago
zoomeye.py python3 (raw_input -> input)	3 years ago

# ZoomEye

## Topics

➤ <https://www.zoomeye.ai/topics>



Power automation topics



Git platform topics



Blockchain topics



Industrial topics



Certificate topics



Firewall topics



Router topics



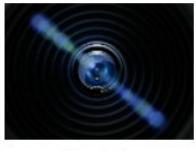
Printer topics



WAF topics



DNS topics



Camera topics



Network storage topics



Database topics

Enumerating Target e Port Scanning

# ZoomEye

## Filtri di Ricerca

➤ <https://www.zoomeye.ai/>

The screenshot shows the Zoomeye search interface. At the top, there is a search bar labeled "Search..." and several filter icons: IP, Domain, Certificate, and a magnifying glass. To the right of the magnifying glass icon are two buttons: "Search Description" and "SearchTool". A red box highlights the "Search Description" button. Below the search bar, there is a section titled "HOT Popular Searches" with a list of 10 items. Each item has a small numbered icon (1 through 10) and a corresponding search term. A red callout bubble points to the "Search Description" button with the text: "È possibile visualizzare tutti i filtri offerti da Zoomeye".

Rank	Search Term
1	app="pgAdmin4"
2	app="OpenVPN"
3	app="CrushFTP"
4	app="Next.js"
5	app="Vite"
6	app="Zabbix Monitoring System"
7	app="Kubernetes Ingress Nginx"
8	app="MongoDB"
9	app="MinIO Browser"
10	app="Jenkins"

# ZoomEye

## Filtri di Ricerca

➤ <https://www.zoomeye.ai/>

The screenshot shows two sections of the ZoomEye search documentation:

### Search Description

- Search scope covers devices (IPv4, IPv6) and websites (domain names)
- When entering a search string, the system will match the keywords in "global" mode, covering content from various protocols such as HTTP, SSH, FTP, etc. (e.g., HTTP/HTTPS protocol headers, body, SSL, title, and other protocol banners)
- The search string is case-insensitive and will be matched after segmentation (the search results page provides a "segmentation" test function). Use == for precise matching and strict restriction of search syntax case sensitivity.
- Please use quotation marks for search strings (e.g., "Cisco System" or 'Cisco System'). If there are quotation marks in the search string, use \ for escape, e.g., "a\"b". If there are brackets in the search string, use \ for escape, e.g., portinfo\()

### Search Logic Operations

SearchLogic	Description	Example
=	Search for assets containing keywords	<code>title="knownsec"</code> Search for websites with titles containing Knowsec's assets
==	Accurate search, indicating a strict match	<code>title=="knownsec"</code> Precise search, which means exact match of

# ZoomEye

## Filtri di Ricerca

---

### ➤ Alcuni tra i principali filtri di ricerca

- **app**: nome dell'applicazione
- **country**: country code (ad es., **UK**, **IT**, **ES**, **FR**, **CN**, **JP**)
- **city**: nome della città
- **port**: numero di porta
- **os**: nome del Sistema Operativo (ad es., **os:linux**)
- **service**: nome del servizio
- **hostname**: hostname (ad es., **hostname:google.com**)
- **ip**: indirizzo IP (ad ed., **ip:8.8.8.8**)
- **cidr**: segmento CIDR (ad es., **cidr:8.8.8.0/24**)

# ZoomEye

---

## ➤ Operatori Logici

Simbolo	Descrizione
=	Ricerca asset che abbiano una corrispondenza rispetto alle keyword
==	Ricerca accurata, che richiede una corrispondenza esatta rispetto alle keyword (case sensitive)
	OR Logico
&&	AND Logico
!=	NOT Logico
()	Forniscono prioritizzazione delle operazioni
*	Fuzzy search, use * for search

# ZoomEye

## Dorks

➤ <https://www.zoomeye.ai/>

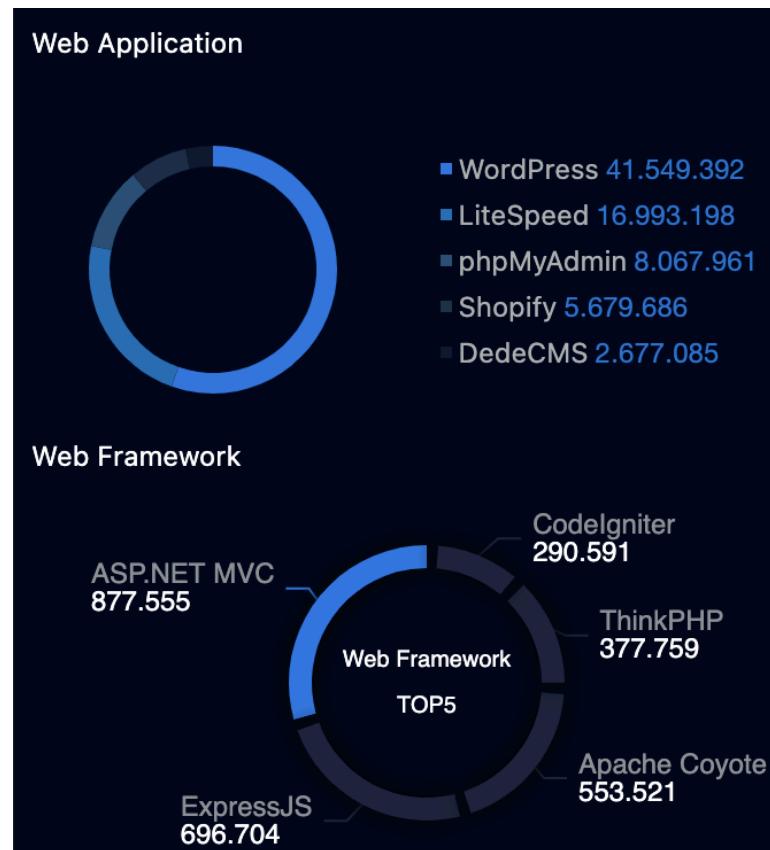


Enumerating Target e Port Scanning

# ZoomEye

## Statistiche

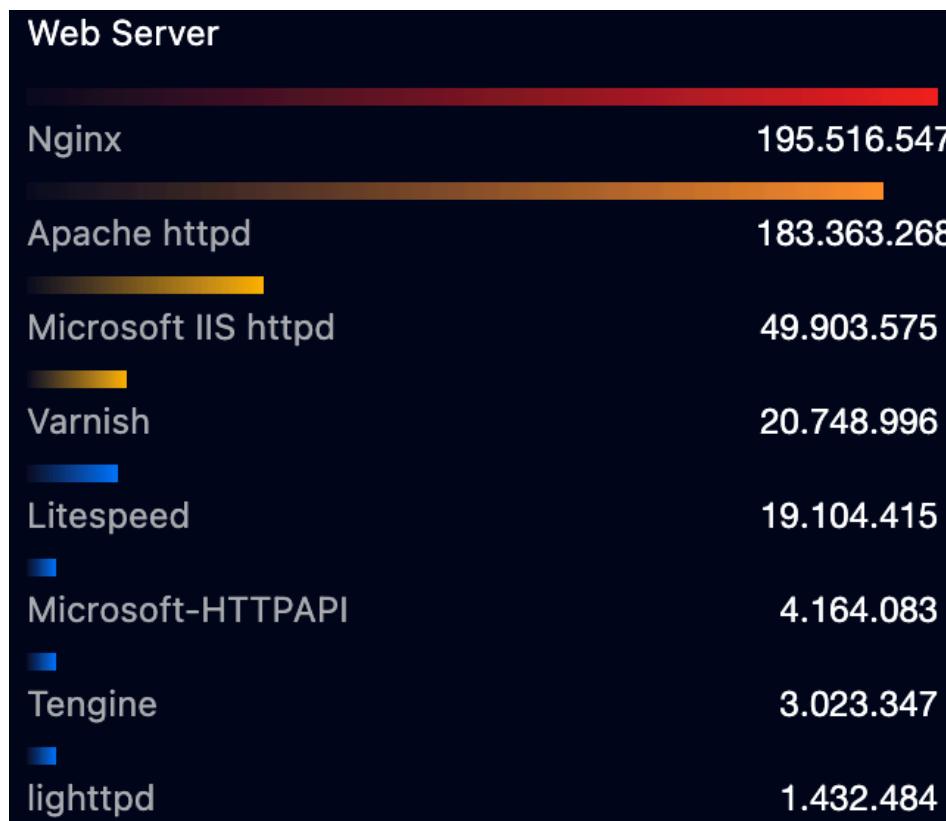
➤ <https://www.zoomeye.ai/statistics>



# ZoomEye

## Statistiche

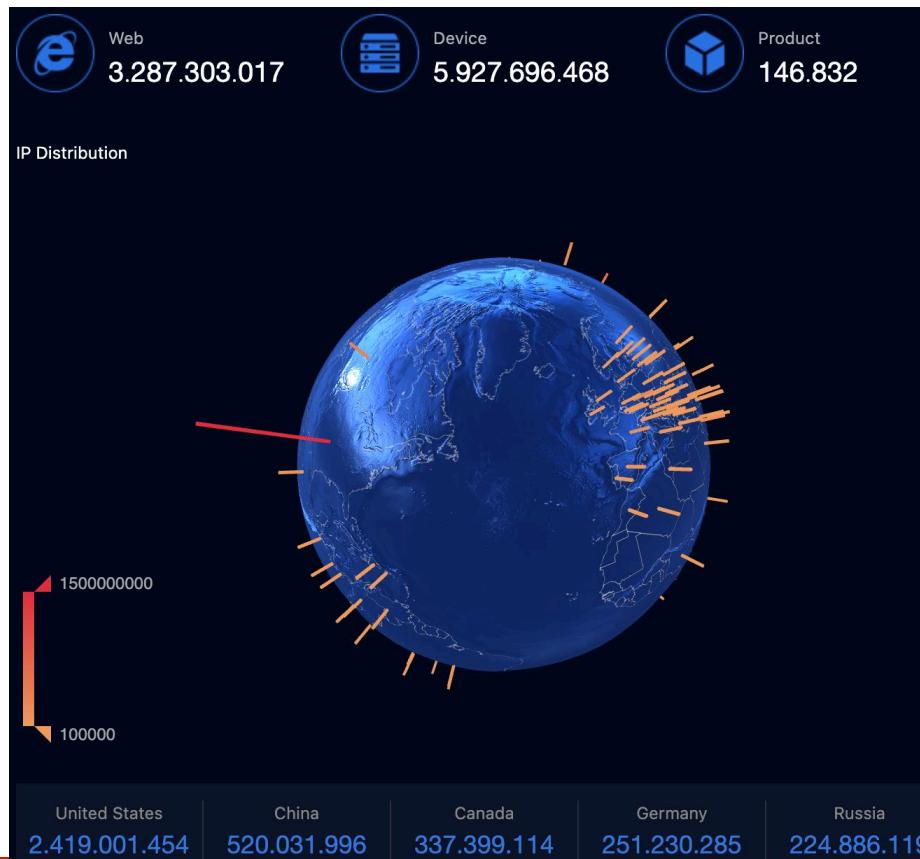
➤ <https://www.zoomeye.ai/statistics>



# ZoomEye

## Statistiche

➤ <https://www.zoomeye.ai/statistics>

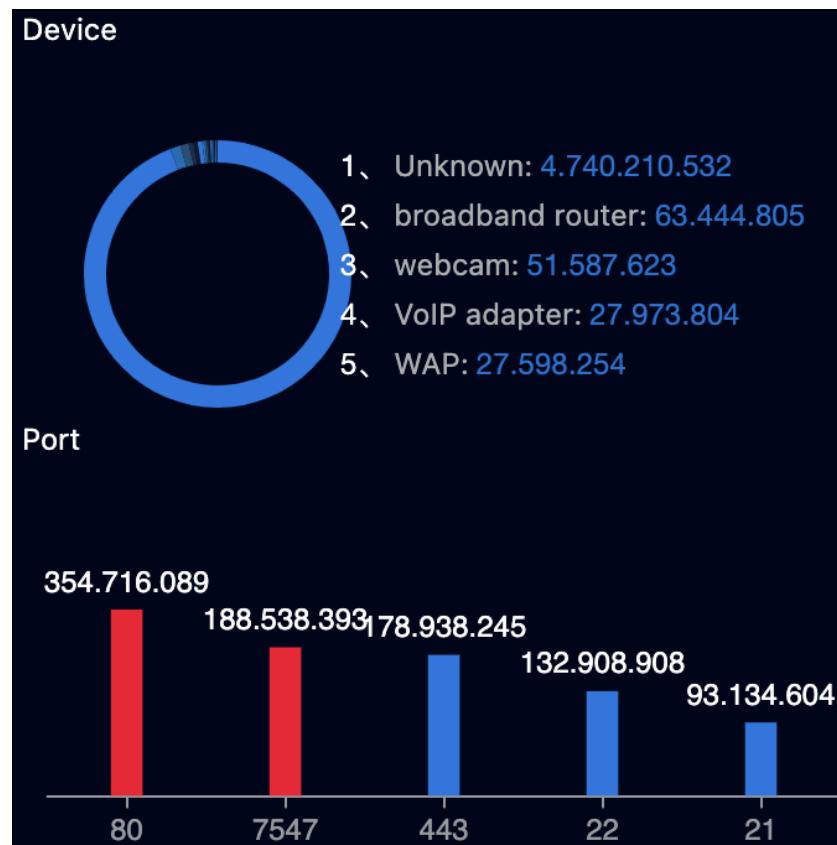


Enumerating Target e Port Scanning

# ZoomEye

## Statistiche

➤ <https://www.zoomeye.ai/statistics>



Enumerating Target e Port Scanning

# ZoomEye

## Statistiche

➤ <https://www.zoomeye.ai/statistics>



# ZoomEye

## ZoomEyeGPT Beta

➤ <https://www.zoomeye.ai/gpt>

The screenshot shows the ZoomEyeGPT Beta web application. At the top, there's a dark header bar with the title "ZoomEyeGPT Beta". Below it, a sub-header explains the tool's purpose: "ZoomEyeGPT is an AI-powered tool specifically designed to enhance cyberspace asset searches. It addresses the challenges users face when navigating ZoomEye's search syntax. Whether you're a system administrator, an academic researcher, a network technology enthusiast, or a cybersecurity beginner, ZoomEyeGPT provides tailored syntax recommendations based on your needs. By reducing the learning curve, streamlining complex operations, and simplifying the search process, it makes powerful network exploration accessible to all." The main area is a search form titled "ZoomEyeGPT Search Query:" with a placeholder text: "Enter your target asset, and we'll auto-generate the search syntax. For example: Find Nginx assets in Los Angeles, USA." Below the input field, a note says "(Daily limit: 5)". To the right of the input field is a blue button with a white upward-pointing arrow icon. Underneath the search form, there's a section titled "Examples" with four buttons: "Search for Starlink devices in Ukraine.", "Search for publicly accessible security cameras in Russia.", "Search for data on port 22 or port 3306 in the United States.", and "Search for assets containing Arabic payment keywords.". A final button at the bottom says "Please help me convert the Censys query 'services.http.response.body: \"index of/\" into a ZoomEye query."

# ZoomEye

## Componenti

➤ <https://www.zoomeye.ai/component>

The screenshot shows the ZoomEye Components search interface. On the left, a sidebar lists 'Equipment type' categories with their counts: Gateway(395), PBX(391), Manager Platform(505), Industrial Equipment(79), CDN(43), Big Data(13), CMS(100), Web Framework(70), IP Camera(395), Video Recorder(156), IDS(15), Software Platfoem(61), Office Anywhere System(55), and Management Software(113). The main area displays search results for 'Gateway'. Under 'Gateway', there are five items: Cisco SIP Gateway, Cisco Expressway E, zyxel AAM1212, Cisco TANDBERG ..., and Cisco Application ... . Below this section is a downward-pointing arrow. The next section, 'PBX', contains five items: Samsung PBX teln..., Asterisk PBX 11.20..., Asterisk PBX 1.6.2...., Asterisk PBX 1.8.1..., and Asterisk PBX 1.6.2... . Below this section is another downward-pointing arrow.

Enumerating Target e Port Scanning

# ZoomEye

## Esempio 1

- Effettuiamo una ricerca per Autonomous System Network (**asn=as137**)

asn = "as137" Not satisfied with the search, try [ZoomEyeGPT](#)

About 1.025.461 results (Nearly year: 86.541 results) 0.204 seconds

Icon(99):  More Select All

[Result](#) **Report** [Maps](#)

**Only \$500** [Download All](#)

[Subscribe](#) | [Tokenizer](#) | [Collection](#)

**150.145.38.62:8787** 

150.145.38.62	Data update	Banner	Hash
 Italy, Sardegna, Sassari Organization: Consiglio Nazionale...		HTTP/1.1 200 OK Content-Type: text/html X-Content-Type-Options: nosniff Server: RStudio Set-Cookie: rs-csrf-token=d5dc1d03-733f-415b-bb83-2c55d0af790; path=/; csrf-token=d5dc1d03-733f-415b-bb83-2c55d0af790; path=/; HttpOnly Pragma: no-cache Cache-Control: no-cache, no-store, max-age=0, must-revalidate Date: Mon, 05 May 2025 14:34:00 GMT X-Frame-Options: DENY	
		See All Text	

**infophd.disi.unitn.it:80** 

infophd.disi.u...	Data update	Header	Body	Hash
 Italy, Trentino-Alto Adige		HTTP/1.1 302 Found		

FILTER  Hide Honeypot

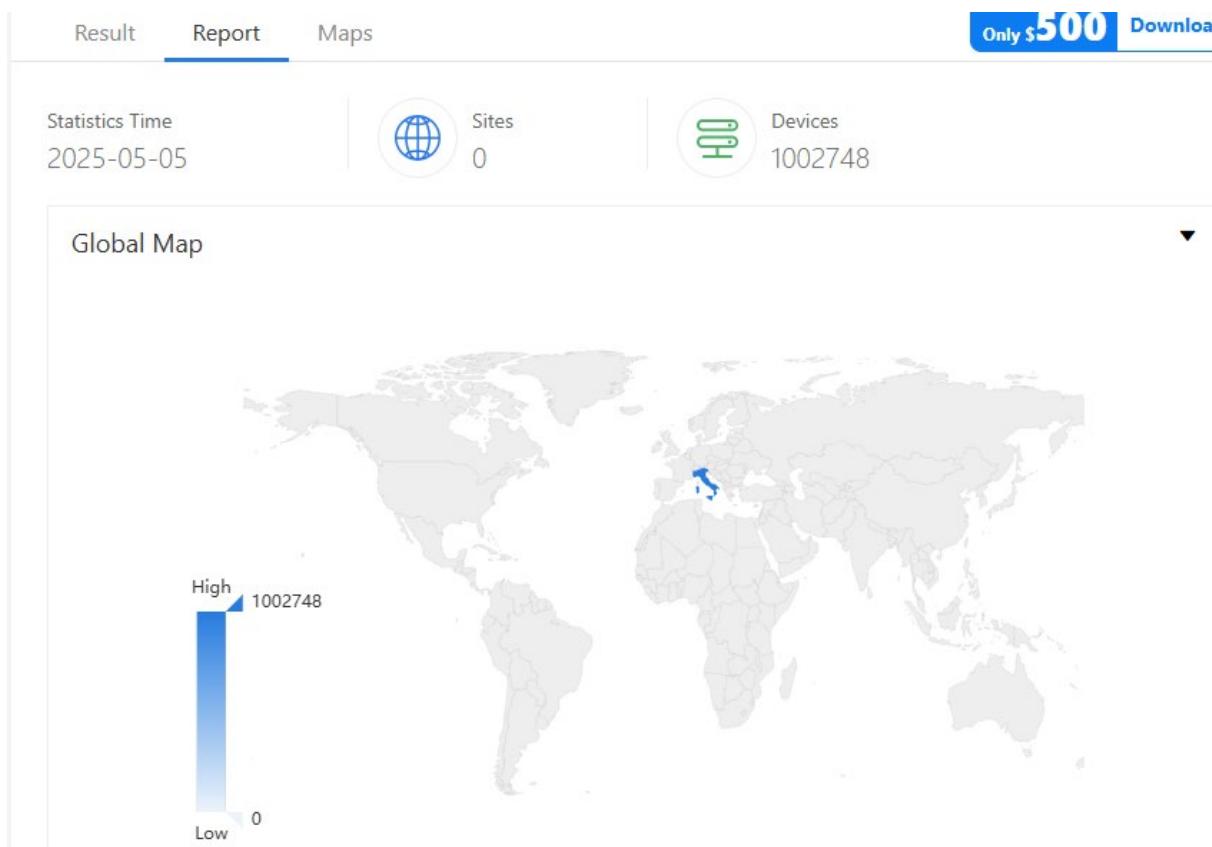
SEARCH TYPE

Devices	1.003.004
Ipv4	1.002.748
Ipv6	256
Websites	22.457

# ZoomEye

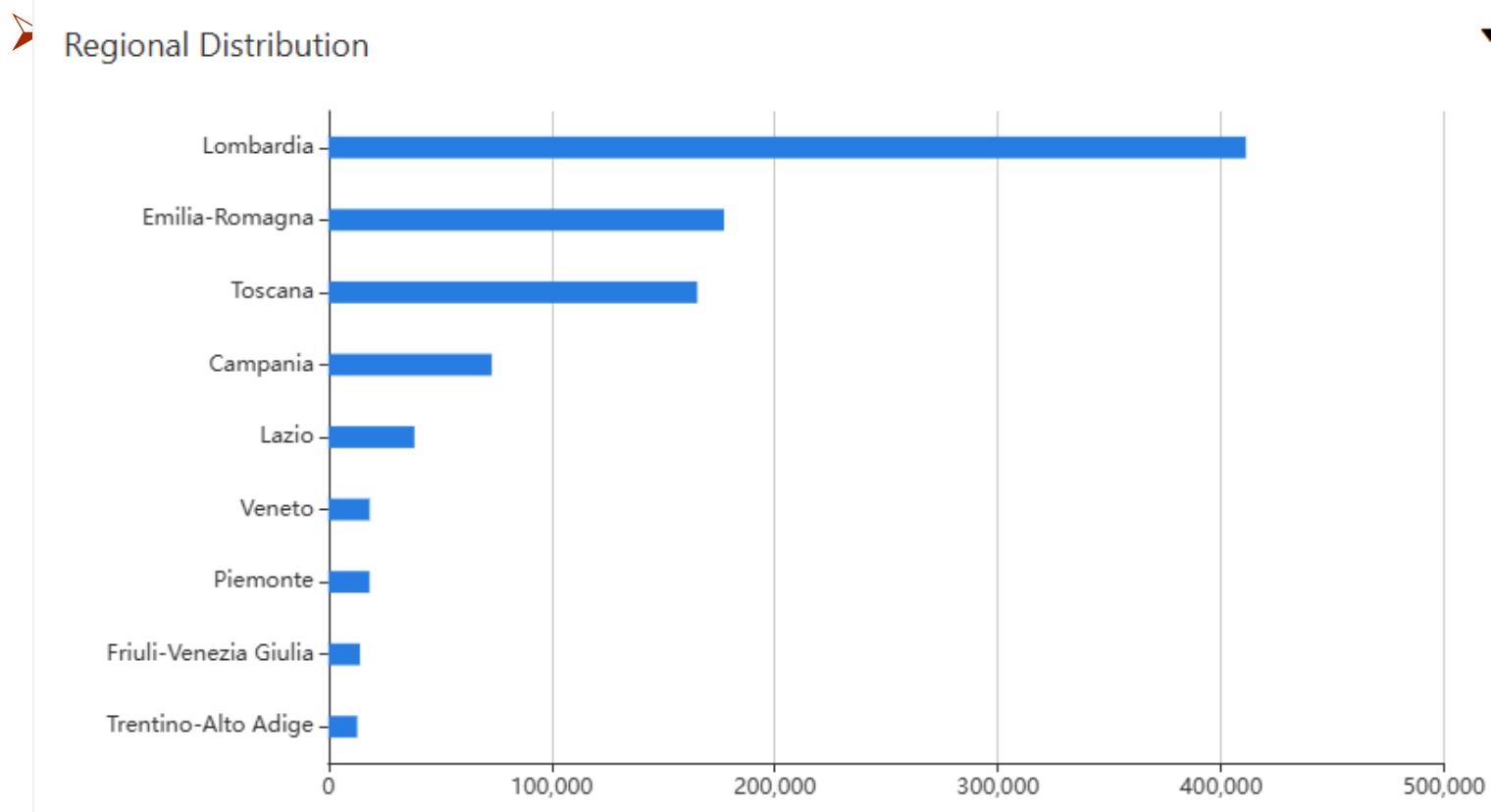
## Esempio 1

- Possiamo visualizzare numerose statistiche relative all'AS AS137



# ZoomEye

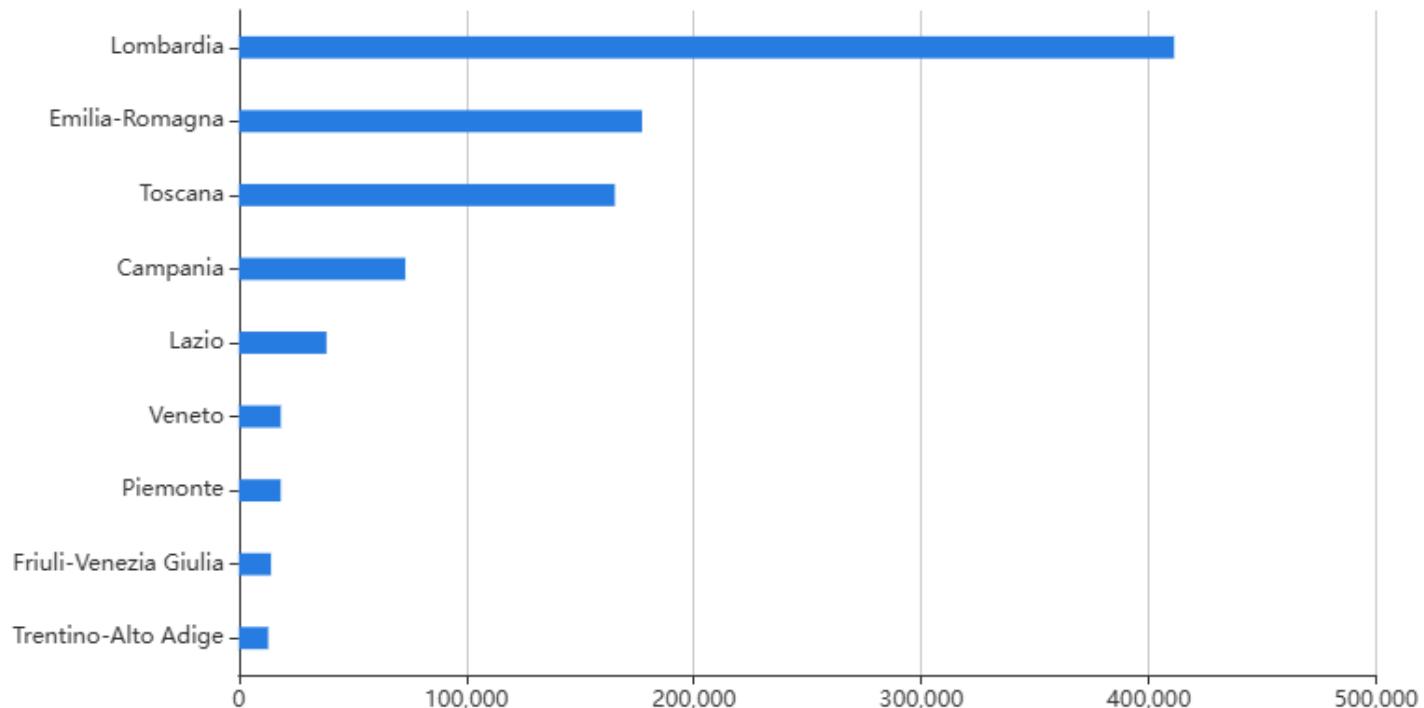
## Esempio 1



# ZoomEye

## Esempio 1

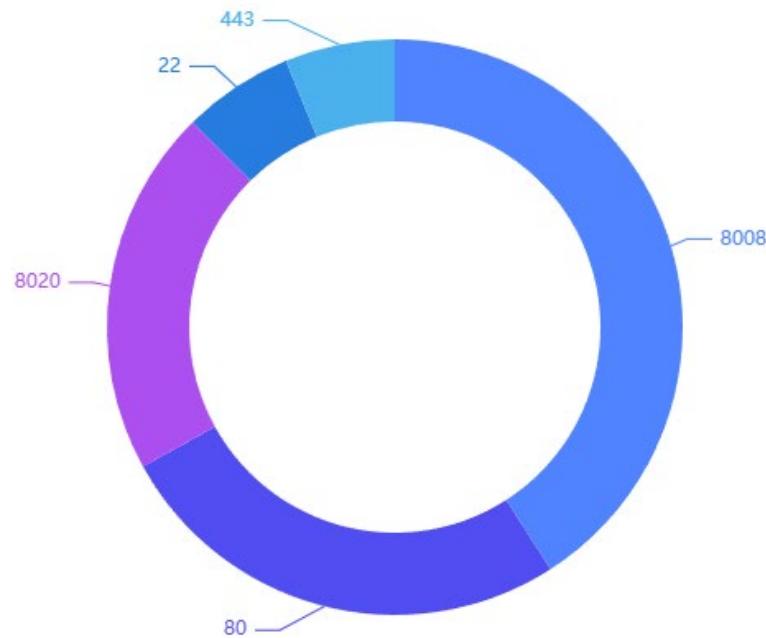
Regional Distribution



# ZoomEye

## Esempio 1

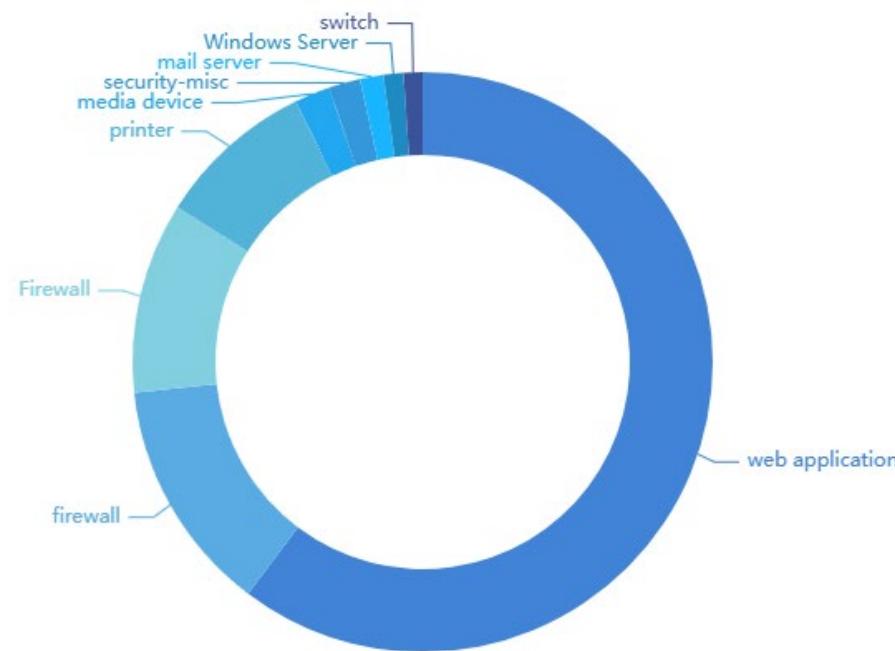
Port Statistics



# ZoomEye

## Esempio 1

Device



# ZoomEye

## Esempio 2

- Specifichiamo l'organizzazione «Università degli Studi di Salerno»

The screenshot shows the ZoomEye search results page. At the top, there is a search bar with the query "asn=as137 && org='Università degli Studi di Salerno'". Below the search bar, there is a "Popular Searches" section with a red box highlighting the search query. The results list includes:

Rank	Search Query	Result Description
1	app="pgAdmin4"	app="Zabbix Monitoring System"
2	app="OpenVPN"	app="Kubernetes Ingress Nginx"
3	app="CrushFTP"	app="MongoDB"
4	app="Next.js"	app="MinIO Browser"
5	app="Vite"	app="Jenkins"
7		
8		
9		
10		

# ZoomEye

## Esempio 2

- Vengono mostrati tutti i dispositivi appartenenti all'organizzazione

The screenshot shows the ZoomEye search interface with two search results displayed.

**Result 1: 193.205.161.7:9000**

- IP: 193.205.161.7
- Country: Italy, Campania, Salerno
- Organization: Università degli Stu...
- ASN: AS137
- Date: 2025-05-04 03:57
- Banner: HTTP/1.1 303 See Other
- Hash: Set-Cookie: PLAY\_SESSION=; Max-Age=0; Expires=Thu, 01 Jan 1970 00:00:00  
X-Frame-Options: SAMEORIGIN  
X-Xss-Protection: 1; mode=block  
X-Content-Type-Options: nosniff  
Location: /jatos/login  
X-Permitted-Cross-Domain-Policies: master-only  
Date: Sat, 03 May 2025 21:13:16 GMT  
Content-Length: 0  
Referrer-Policy: origin-when-cross-origin, strict-origin-when-cross-orig
- See All Text

**Result 2: 193.205.161.136:9000**

- IP: 193.205.161.136
- Country: Italy, Campania, Salerno
- Hostname: music.di.unisa.it
- Organization: Università degli Stu...
- ASN: AS137
- Title: Page not found at /
- Date: 2025-05-04 03:57
- Banner: HTTP/1.1 404 Not Found
- Hash: Date: Sat, 03 May 2025 20:19:17 GMT  
Server: WSGIServer/0.2 CPython/3.11.0  
Content-Type: text/html; charset=utf-8  
X-Frame-Options: DENY  
Content-Length: 4851  
X-Content-Type-Options: nosniff  
Referrer-Policy: same-origin  
Cross-Origin-Opener-Policy: same-origin  
Vary: Origin
- See All Text

**Right Panel Statistics:**

- FILTER: Hide Honeypot
- SEARCH TYPE:
  - Devices: 1.993
  - Ipv4: 1.993
  - Ipv6: 0
  - Websites: 17
- YEAR:
  - 2025: 75
  - 2024: 50
  - 2023: 304
- ITALY:
  - Campania: 1.085

# ZoomEye

## Esempio 2

- Possiamo controllare i dettagli relativi a ciascun dispositivo

The screenshot shows the ZoomEye web interface with two device details panels and various search filters.

**Device 1:** IP 193.205.161.7:9000

- Banner: HTTP/1.1 303 See Other
- Hash: Set-Cookie: PLAY\_SESSION=; Max-Age=0; Expires=Thu, 01 Jan 1970 00:00:00
- Header: X-Frame-Options: SAMEORIGIN
- Header: X-Xss-Protection: 1; mode=block
- Header: X-Content-Type-Options: nosniff
- Header: Location: /jatos/login
- Header: X-Permitted-Cross-Domain-Policies: master-only
- Date: Sat, 03 May 2025 21:13:16 GMT
- Content-Length: 0
- Referrer-Policy: origin-when-cross-origin, strict-origin-when-cross-origin

**Device 2:** IP 193.205.161.136:9000

- Banner: HTTP/1.1 404 Not Found
- Header: Date: Sat, 03 May 2025 20:19:17 GMT
- Header: Server: WSGIServer/0.2 CPython/3.11.0
- Header: Content-Type: text/html; charset=utf-8
- Header: X-Frame-Options: DENY
- Header: Content-Length: 4851
- Header: X-Content-Type-Options: nosniff
- Header: Referrer-Policy: same-origin
- Header: Cross-Origin-Opener-Policy: same-origin
- Header: Vary: Origin

**Search Filters (Right Side):**

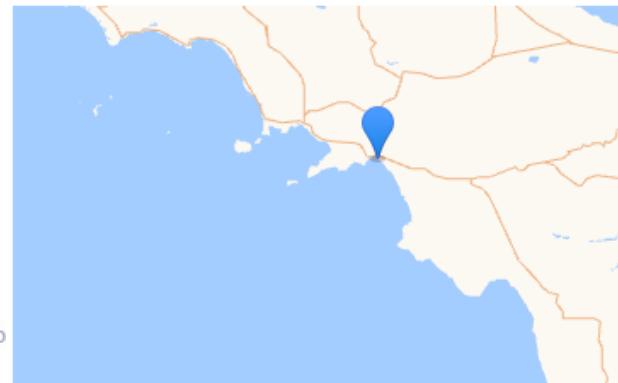
- FILTER**: Hide Honeypot
- SEARCH TYPE**: Devices (1.993), Ipv4 (1.993), Ipv6 (0), Websites (17)
- YEAR**: 2025 (75), 2024 (50), 2023 (304), More
- ITALY**: Campania (1.085)

# ZoomEye

## Esempio 2

### ➤ Informazioni di Base

Basic Information	Component details
IP Address	193.205.161.7
City	Salerno
Province / State	Campania
Country	 Italy
Location	40.673361, 14.769705
Organization	Università degli Studi di Salerno
ISP	
Hostnames	ISIS-PC
ASN	AS137



# ZoomEye

## Esempio 2

### ➤ Dettagli relativi al dispositivo

The screenshot shows a summary of device components:

- Application (1)**: VMware ESXi Web UI
- Support**
- Server (3)**: Apache, FileZilla, Microsoft Windows 7 - 10 microsoft-ds
- OS (1)**: Microsoft Windows NT netbios-ssn
- Hardware (1)**: DD-WRT

# ZoomEye

## Esempio 2

- Informazioni sulle porte aperte ed i relativi servizi e banner

The screenshot shows the ZoomEye search interface with the following details:

- Ports / Service**: 11 (selected)
- Whois**: 0
- DNS Analysis**: 2
- User Tags**: 0

Below the tabs, a list of open ports and services is shown:

- 21/ftp
- 22/ssh
- 80/http
- 137/netbios-ns
- 443/https
- 445/microsoft-ds
- 3389/ms-wbt-server
- 8008/http
- 8080/http
- 9000/http
- 9080/http

For each port/service, there is a detailed table of information:

### 21/ftp

Device	
Product	FileZilla ftpd
Version	0.9.44
Service	ftp
ProtType	TCP
OS	
Updated	2020-02-02 03:14

### 22/ssh

Device	
Product	dropbear
Version	0.52
Service	ssh
ProtType	TCP

# ZoomEye

## Esempio 3

➤ <https://www.zoomeye.ai/>



# ZoomEye

## Esempio 3

➤ <https://www.zoomeye.ai/>

app = "openssh" && banner = "4.7p1" && country = "it" Not satisfied with the search, try [ZoomEyeGPT](#)

About 1.775 results (Nearly year: 35 results) 0.584 seconds

Result Report Maps Only \$10 Download All Subscribe Tokenizer Collection

188.14.169.244:2222

188.14.169.244 Data update Banner Hash

SSH-2.0-OpenSSH\_4.7p1 Debian-8ubuntu1.2

Country: Italy, Lombardia, Milan  
OS: Linux  
Hostname: host-188-14-169-244...  
Organization: Telecom Italia S.p.A.  
ASN: A53269  
IDC  
2025-05-05 13:07

213.212.143.63:2223

213.212.143.63 Data update Banner Hash

SSH-2.0-OpenSSH\_4.7p1 Debian-8ubuntu3

Country: Italy, Lombardia, Milan  
OS: Linux  
Hostname: 63.143.212.213.static.a...  
Organization: Aries Srl  
ISP: IT.Gate S.p.A.



FILTER  Hide Honeypot

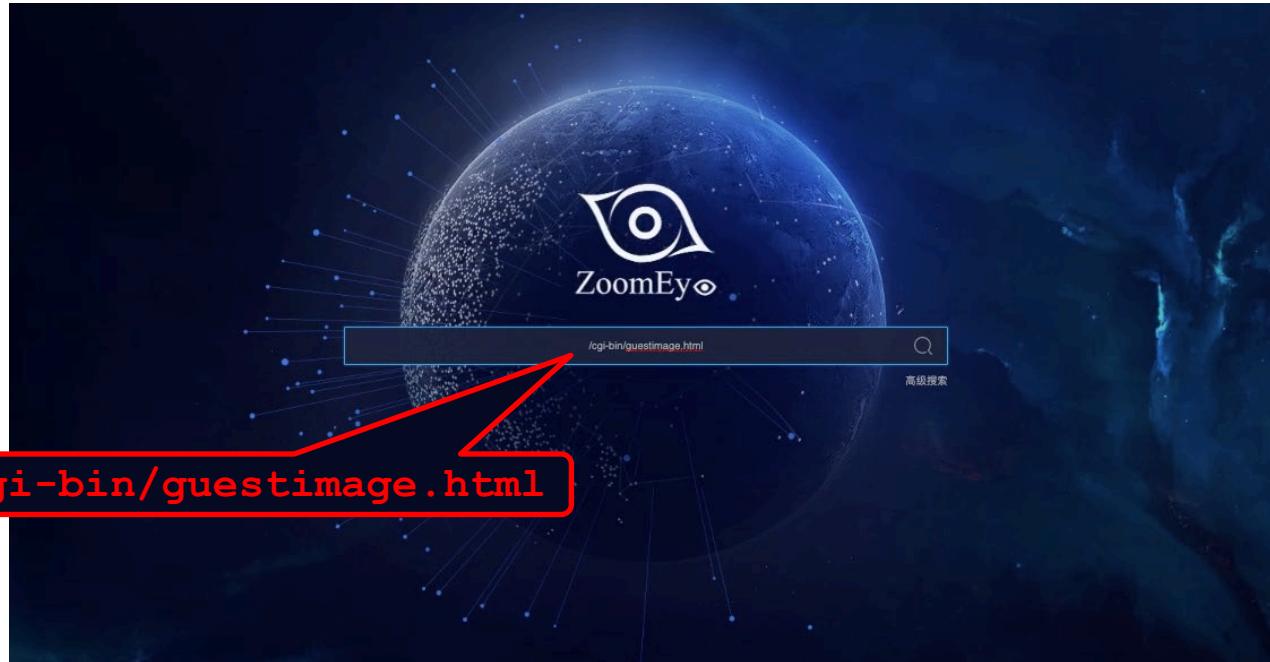
SEARCH TYPE Devices 1.775 ▾  
IPv4 1.774  
IPv6 1

YEAR 2025 4  
2024 42

# ZoomEye

## Esempio 4

➤ <https://www.zoomeye.ai/>



# ZoomEye

## Esempio 4

➤ <https://www.zoomeye.ai/>

<p>82.226.203.114 ➤</p> <p>ble59-3-82-226-203-114.fbx.pro...</p> <p>3000/http</p> <p>France, Lille</p> <p>⌚ 2019-11-02 06:29</p>	<pre>HTTP/1.0 302 Found Location: /cgi-bin/guestimage.html Content-type: text/html; charset=utf-8 Cache-Control: no-cache  &lt;!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"&gt; &lt;html&gt; &lt;head&gt;p &lt;title&gt; Redirect to guestimage: /cgi-bin/guestimage.html &lt;/title&gt; &lt;meta http-equiv="Content-Type" content="text/html; charset=utf-8"&gt; &lt;/head&gt; &lt;body&gt; &lt;br&gt;</pre>	<p>Singapore 1./U1 ▲</p> <p>Australia 1.696 ▲</p> <p>Austria 1.451 ▲</p> <p>Spain 1.407 ▲</p> <p>Switzerland 1.405 ▲</p> <p>Belgium 913 ▲</p>
<p>50.199.221.101 ➤</p> <p>mail.masslaborers.org</p> <p>8888/http</p> <p>United States, Milford</p> <p>⌚ 2019-11-02 06:17</p>	<pre>HTTP/1.0 302 Found Location: /cgi-bin/guestimage.html Content-type: text/html; charset=ISO-8859-1 Cache-Control: no-cache  &lt;!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"&gt; &lt;html&gt; &lt;head&gt; &lt;title&gt; Redirect to guestimage: /cgi-bin/guestimage.html &lt;/title&gt; &lt;meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1"&gt; &lt;/head&gt; &lt;body&gt; &lt;br&gt;</pre>	<p>组件</p> <p>MOBOTIX webcam... 21.380</p> <p>Mobotix M10 PRIS... 10.576</p> <p>thttpd 3.182</p> <p>Unknown 1.487</p> <p>Mobotix Camera ht... 1.038</p> <p>Apache httpd 40</p> <p>nginx 2</p> <p>LANDesk remote ... 1</p> <p>QNAP NAS storage... 1</p> <p>服务</p> <p>http 36.270</p>

# ZoomEye

## Esempio 4 (Caso 1)

➤ <https://www.zoomeye.ai/>

The screenshot shows the Zoomeye search interface. On the left, two search results are displayed:

- 82.226.203.114** (highlighted with a red arrow and a magnifying glass icon)
  - ble59-3-82-226-203-114.fbx.pro...
  - 3000/http
  - France, Lille
  - 2019-11-02 06:29
- 50.199.221.101**
  - mail.masslaborers.org
  - 8888/http
  - United States, Milford
  - 2019-11-02 06:17

To the right, there is a sidebar with a table of countries and their scores:

Country	Score
Singapore	1./U1 ▲
Australia	1.696 ▲
Austria	1.451 ▲
Spain	1.407 ▲
Switzerland	1.405 ▲
Belgium	913 ▲

Below the table, there are sections for "组件" (Components) and "服务" (Services), each with a list of items and their counts.

**组件**

MOBOTIX webcam...	21.380
Mobotix M10 PRIS...	10.576
thttpd	3.182
Unknown	1.487
Mobotix Camera ht...	1.038
Apache httpd	40
nginx	2
LANDesk remote ...	1
QNAP NAS storage...	1

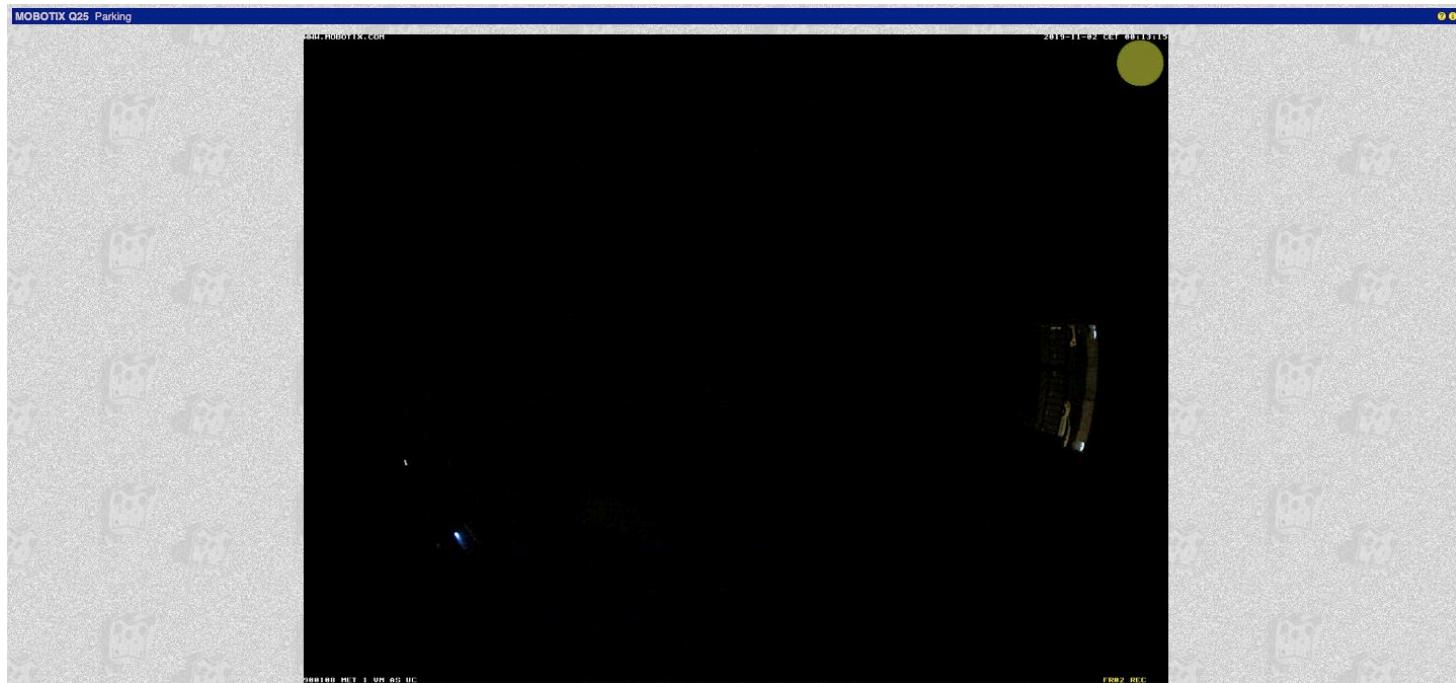
**服务**

http	36.270
------	--------

# ZoomEye

## Esempio 4 (Caso 1)

➤ <https://www.zoomeye.ai/>



# ZoomEye

## Esempio 4 (Caso 2)

➤ <https://www.zoomeye.ai/>

82.226.203.114 ⓘ  
ble59-3-82-226-203-114.fbx.pro...  
3000/http  
France, Lille  
2019-11-02 06:29

HTTP/1.0 302 Found  
Location: /cgi-bin/guestimage.html  
Content-type: text/html; charset=utf-8  
Cache-Control: no-cache

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">  
<html>  
<head>p  
<title>  
Redirect to guestimage: /cgi-bin/guestimage.html  
</title>  
<meta http-equiv="Content-Type" content="text/html; charset=utf-8":  
</head>  
<body>  
<br>

50.199.221.101 ⓘ  
mail.masslaborers.org...  
8888/http  
United States, Milford  
2019-11-02 06:17

HTTP/1.0 302 Found  
Location: /cgi-bin/guestimage.html  
Content-type: text/html; charset=ISO-8859-1  
Cache-Control: no-cache

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">  
<html>  
<head>  
<title>  
Redirect to guestimage: /cgi-bin/guestimage.html  
</title>  
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1":  
</head>  
<body>  
<br>

组件	数量
Singapore	1./U1 ▲
Australia	1.696 ▲
Austria	1.451 ▲
Spain	1.407 ▲
Switzerland	1.405 ▲
Belgium	913 ▲

服务	数量
MOBOTIX webcam...	21.380
Mobotix M10 PRIS...	10.576
thttpd	3.182
Unknown	1.487
Mobotix Camera ht...	1.038
Apache httpd	40
nginx	2
LANDesk remote ...	1
QNAP NAS storage...	1

# ZoomEye

## Esempio 4 (Caso 2)

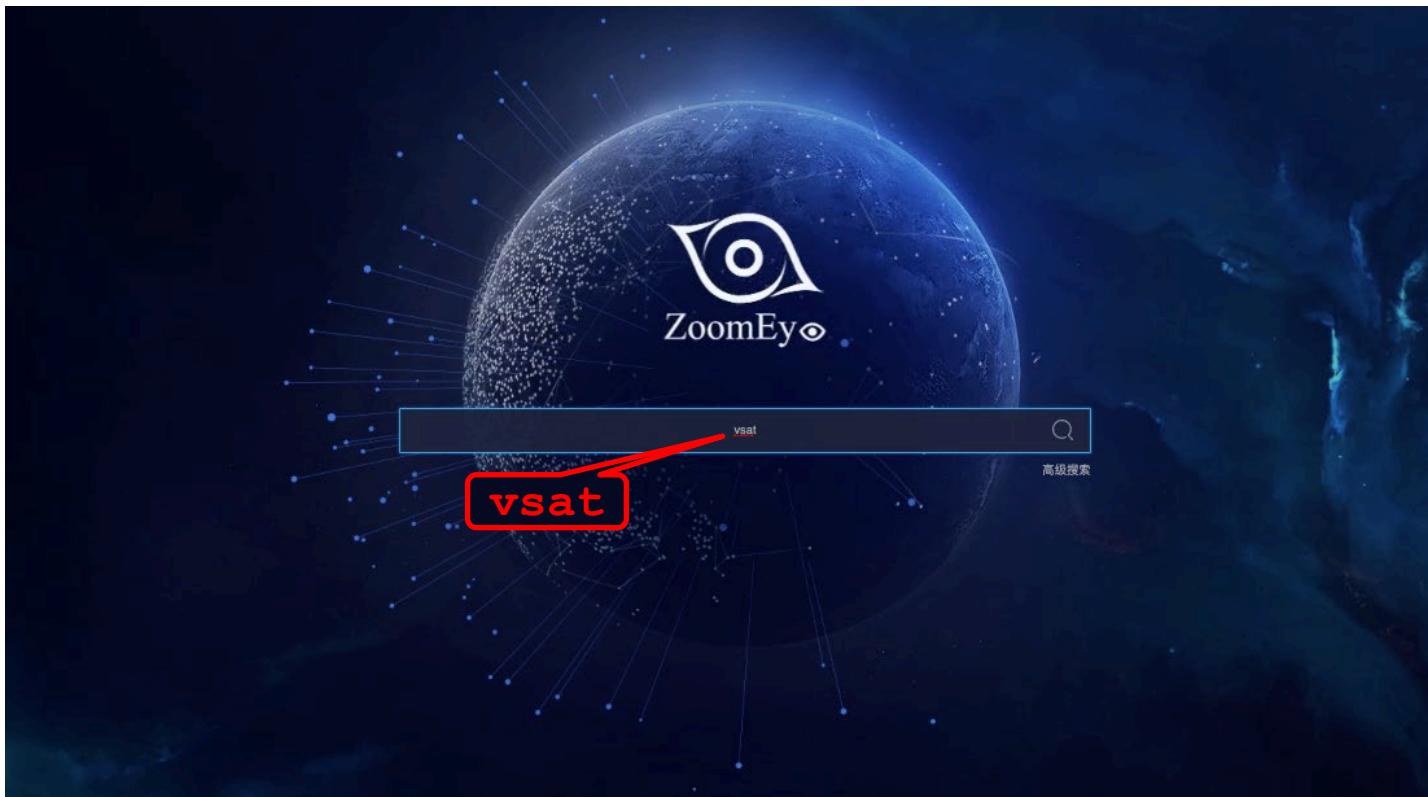
➤ <https://www.zoomeye.ai/>



# ZoomEye

## Esempio 5

➤ <https://www.zoomeye.ai/>



# ZoomEye

## Esempio 5

➤ <https://www.zoomeye.ai/>



- VSAT (*Very-Small-Aperture Terminal*)
  - Sistema usato per comunicazioni satellitari
  - VSAT utilizza IPv4 per la comunicazione

# ZoomEye

## Esempio 5

➤ <https://www.zoomeye.ai/>

Result Report Maps Vulnerability

About 137.887 results (Nearly year: 57.164 results) 2.196 seconds

Value ranking

avisho.r... Banner SSL Data update

HTTP/1.1 200 OK  
Date: Wed, 19 Apr 2023 16:08:13 GMT  
Content-Type: text/html; charset=utf-8  
Transfer-Encoding: chunked  
Connection: keep-alive  
expires: Thu, 19 Nov 1981 08:52:00 GMT  
cache-control: no-store, no-cache, must-revalidate  
pragma: no-cache  
content-language: fa  
vary: Accept-Encoding,User-Agent  
strict-transport-security: max-age=0  
x-turbo-charged-by: LiteSpeed  
CF-Cache-Status: DYNAMIC  
Report-To: {"endpoints": [{"url": "https://a.nel.cloudflare.com/report"}]}

Universi... Banner SSL Data update

HTTP/1.1 301 Moved Permanently  
Location: https://gobisons.ca/  
Server: Microsoft-IIS/10.0  
Strict-Transport-Security: max-age=0;  
X-Content-Type-Options: nosniff  
X-XSS-Protection: 1; mode=block  
Referrer-Policy: no-referrer-when-downgrade  
Date: Wed, 19 Apr 2023 16:07:06 GMT  
Content-Length: 0

<!doctype html>  
<html id="ct100\_html" lang="en" class=" index homepage">

Subscribe Collection download share tokenizer

Value ranking

World map showing search results distribution.

SEARCH TYPE

Devices	113.778 ▲
IPv4	113.749
IPv6	29
Websites	24.108

YEAR

2023	37.407
2022	23.992
2021	21.718
More	

COUNTRY

United States	29.697 ▲
China	19.653 ▲
Viet Nam	17.682 ▲
Indonesia	6.566 ▲
Ivory Coast	6.565 ▲
More	

Enumerating Target e Port Scanning

# ZoomEye

## Esempio 5

➤ <https://www.zoomeye.ai/>

Result Report Maps Vulnerability

About 137.887 results (Nearly year: 57.164 results) 2.196 seconds

Value ranking

avisho.r... SSL Data update

HTTP/1.1 200 OK  
Date: Wed, 19 Apr 2023 16:08:13 GMT  
Content-Type: text/html; charset=utf-8  
Transfer-Encoding: chunked  
Connection: keep-alive  
expires: Thu, 19 Nov 1981 08:52:00 GMT  
cache-control: no-store, no-cache, must-revalidate  
pragma: no-cache  
content-language: fa  
vary: Accept-Encoding,User-Agent  
strict-transport-security: max-age=0  
x-turbo-charged-by: LiteSpeed  
CF-Cache-Status: DYNAMIC  
Report-To: {"endpoints": [{"url": "https://a.nel.cloudflare.com/report"}]}

Universi... SSL Data update

HTTP/1.1 301 Moved Permanently  
Location: https://gobissons.ca/  
Server: Microsoft-IIS/10.0  
Strict-Transport-Security: max-age=0;  
X-Content-Type-Options: nosniff  
X-XSS-Protection: 1; mode=block  
Referrer-Policy: no-referrer-when-downgrade  
Date: Wed, 19 Apr 2023 16:07:06 GMT  
Content-Length: 0

<!doctype html>  
<html id="ct100\_html" lang="en" class=" index homepage">

Value ranking

World map showing search results distribution.

SEARCH TYPE

Devices	113.778 ▾
IPv4	113.749
IPv6	29
Websites	24.108

YEAR

2023	37.407
2022	23.992
2021	21.718
More	

COUNTRY

United States	29.697 ▾
China	19.653 ▾
Viet Nam	17.682 ▾
Indonesia	6.566 ▾
Ivory Coast	6.565 ▾
More	

Universi... SSL Data update

HTTP/1.1 200 OK  
Date: Wed, 19 Apr 2023 16:08:13 GMT  
Content-Type: text/html; charset=utf-8  
Transfer-Encoding: chunked  
Connection: keep-alive  
expires: Thu, 19 Nov 1981 08:52:00 GMT  
cache-control: no-store, no-cache, must-revalidate  
pragma: no-cache  
content-language: fa  
vary: Accept-Encoding,User-Agent  
strict-transport-security: max-age=0  
x-turbo-charged-by: LiteSpeed  
CF-Cache-Status: DYNAMIC  
Report-To: {"endpoints": [{"url": "https://a.nel.cloudflare.com/report"}]}

www.gobissons.ca SSL Data update

HTTP/1.1 301 Moved Permanently  
Location: https://gobissons.ca/  
Server: Microsoft-IIS/10.0  
Strict-Transport-Security: max-age=0;  
X-Content-Type-Options: nosniff  
X-XSS-Protection: 1; mode=block  
Referrer-Policy: no-referrer-when-downgrade  
Date: Wed, 19 Apr 2023 16:07:06 GMT  
Content-Length: 0

<!doctype html>  
<html id="ct100\_html" lang="en" class=" index homepage">

Enumerating Target e Port Scanning

# ZoomEye

## Esempio 5

➤ <https://www.zoomeye.ai/>

The official athletics website for the University of Manitoba Bisons

Basic Information	Component details
Website	www.gobisons.ca
IP Address	174.143.104.95
City	Dallas
Province / State	Texas
Country	United States
Location	32.78183, -96.79586
Organization	Rackspace Hosting
ISP	rackspace.com
ASN	AS33070



A map of Dallas, Texas, highlighting several locations. Labeled points include: 达拉斯斯通 菲利艾美酒店 (Le Méridien Dallas, The Stoneleigh), 雷米顿酒店(达拉斯店) (Remington(Dallas)), Exall Park, Fresenius Kidney Care Swiss Avenue, Buckner F, Divcon EK, 约翰F肯尼迪纪念广场 (John F Kennedy Memorial Plaza), 47B, 蒙特酒店 (Mont Hotel), 洛伦佐酒店 - 同桑德连锁酒店成员 (Lorenzo Hotel), 达拉斯南区NYLO酒店 (NYLO-Dallas South Side), and Irma Levin Young W Leadership.

# ZoomEye

## Esempio 5

➤ <https://www.zoomeye.ai/>

The official athletics website for the University of Manitoba Bisons

Basic Information	Component details
Website	www.gobisons.ca
IP Address	174.143.104.95
City	Dallas
Province / State	Texas
Country	United States
Location	32.78183, -96.79586
Organization	Rackspace Hosting
ISP	rackspace.com
ASN	AS33070

32.78183, -96.79586

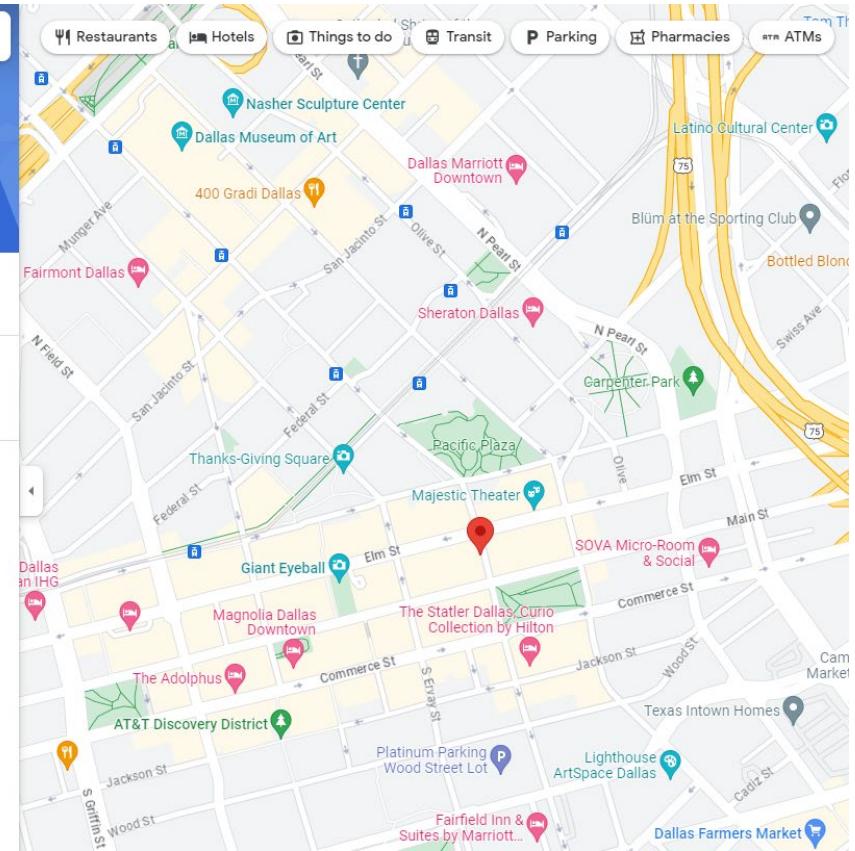
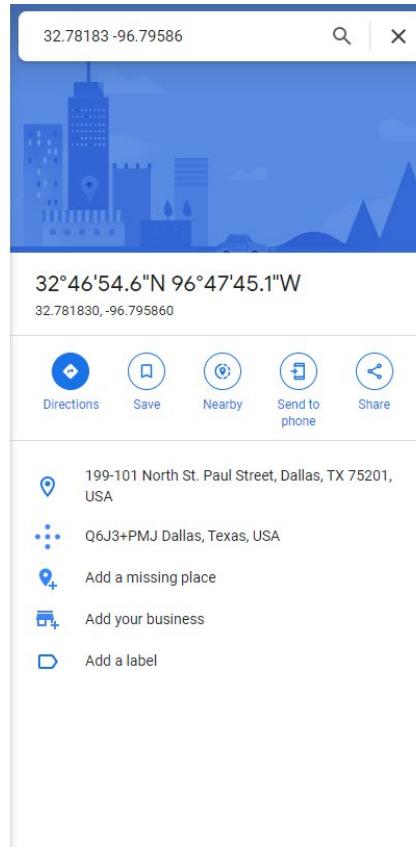
➤ Cercando le seguenti coordinate tramite Google Maps possiamo geolocalizzare l'imbarcazione  
➤ 32.78183, -96.79586

# ZoomEye

## Esempio 5

➤ <https://www.zoomeye.ai/>

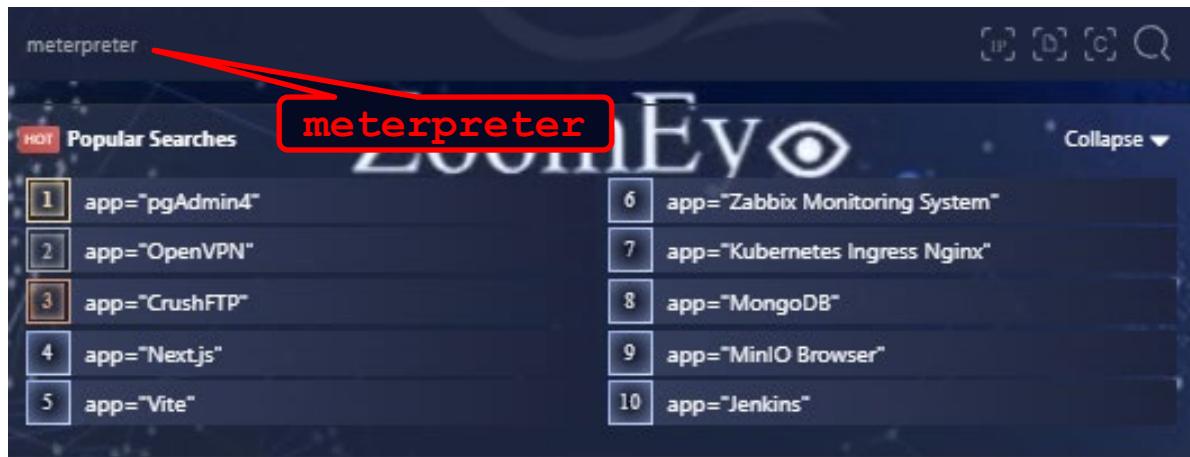
Possiamo inserire le coordinate geografiche su Google Maps



# ZoomEye

## Esempio 6

➤ <https://www.zoomeye.ai/>



➤ **Meterpreter**

- **Payload avanzato, appartiene alla suite Metasploit**
- **Consente l'accesso remoto ad una macchina target**

# ZoomEye

## Esempio 6

➤ <https://www.zoomeye.ai/>

Result   Report   Maps   Only \$10   Download All    Subscribe |  Tokenizer |  Collection

**charge.elastic.co:80**

Header	Body	Hash
HTTP/1.1 308 Permanent Redirect Cache-Control: private Location: https://charge.elastic.co:443/ Content-Length: 0 Date: Mon, 05 May 2025 11:59:50 GMT Content-Type: text/html; charset=UTF-8		

charge.elastic...  Data update  
United States  
Organization: Google LLC  
ASN: AS15169  
Title: Billing Information for Elasti...  
⌚ 2025-05-05 20:14

**prelert-info.elastic.co:80**

Header	Body	Hash
HTTP/1.1 308 Permanent Redirect Cache-Control: private Location: https://prelert-info.elastic.co:443/ Content-Length: 0 Date: Mon, 05 May 2025 11:44:12 GMT Content-Type: text/html; charset=UTF-8		

prelert-info.elastic...  Data update  
United States  
Organization: Google LLC  
ASN: AS15169  
Title: Machine Learning for Elasti...  
⌚ 2025-05-05 20:00

**artifacts.elastic.co:80**

Header	Body	Hash
HTTP/1.1 308 Permanent Redirect Cache-Control: private Location: https://artifacts.elastic.co:443/ Content-Length: 0 Date: Mon, 05 May 2025 11:36:24 GMT Content-Type: text/html; charset=UTF-8		

artifacts.elastic...  Data update  
United States  
Organization: Google LLC  
ASN: AS396982  
Title: Download and provision Elasti...  
⌚ 2025-05-05 19:51

**MAP**

**FILTER**  Hide Honeypot

**SEARCH TYPE**

Devices	2,860
Ipv4	2,860
Ipv6	0
Websites	71

**YEAR**

2025	121
2024	195
2023	183
More	

**COUNTRY**

United States	923 ▲
China	353 ▲
Germany	260 ▲
The Netherlands	163 ▲
India	129 ▲

# ZoomEye

## Esempio 6

➤ <https://www.zoomeye.ai/>

Result Report Maps Only \$10 Download All

charge.elastic.co:80

Header	Body	Hash
HTTP/1.1 308 Permanent Redirect Cache-Control: private Location: https://charge.elastic.co:443/ Content-Length: 0 Date: Mon, 05 May 2025 11:59:50 GMT Content-Type: text/html; charset=UTF-8		

prelert-info.elastic.co:80

Header	Body	Hash
HTTP/1.1 308 Permanent Redirect Cache-Control: private Location: https://prelert-info.elastic.co:443/ Content-Length: 0 Date: Mon, 05 May 2025 11:44:12 GMT Content-Type: text/html; charset=UTF-8		

artifacts.elastic.co:80

Header	Body	Hash
HTTP/1.1 308 Permanent Redirect Cache-Control: private Location: https://artifacts.elastic.co:443/ Content-Length: 0 Date: Mon, 05 May 2025 11:44:12 GMT Content-Type: text/html; charset=UTF-8		

Subscribe | Tokenizer | Collection

MAP

FILTER

Hide Honeypot

SEARCH TYPE

Devices	2,860
Ipv4	2,860
Ipv6	0
Websites	71

YEAR

2025	121
2024	195
2023	183
More	

COUNTRY

United States	923
China	353

India 129

La suite Meterpreter verrà mostrata in dettaglio durante le fasi di *Exploitation e Post Exploitation*

# Outline

---

- Concetti Introduttivi
- Suite Protocollare TCP/IP
- Formato dei Messaggi TCP e UDP
- Active Enumeration
  - Network Scanner Nmap
  - Zenmap
  - Unicornscan
  - Masscan
- Passive Enumeration
  - Shodan
  - ZoomEye
  - **FOFA**
  - Censys

# FOFA

---

- Motore di ricerca cinese per dispositivi e servizi esposti su Internet, simile a Shodan o ZoomEye
- Effettua ricerche passive su IP, domini, certificati SSL, header HTTP ed altri metadati di rete
- Usato in ambito:
  - OSINT
  - Security assessment
  - Threat hunting
  - Bug bounty e pentest

# FOFA

## Pricing

➤ <https://en.fofa.info/vip>

The image shows the FOFA Pricing page with five subscription plans:

- Registered User (Non-commercial only)**: Free to Use. Includes: ✓ Query Credits 300/month, ✓ 3k Results/month, ✓ Access 58 Syntaxes ⓘ, ✓ Web Download Feature, ✓ 1 User, ✓ FOFA Fingerprint Rule, ✓ Website Feature ID (FID), ✓ Cloud Assets Tag.
- Personal**: \$250/year. Includes: ✓ Query Credits 10,000/month, ✓ Up to 100k Results/month, ✓ Access 65 Syntaxes ⓘ, ✓ Web Download Feature, ✓ 1 User, ✓ Access 36 fields in Query API, ✓ 1 Request/second in Query API, ✓ HOST Aggregation API.
- Professional**: \$1,190/year. Includes: ✓ Query Credits 80,000/month, ✓ Up to 800k Results/month, ✓ Access 70 Syntaxes ⓘ, ✓ Web Download Feature, ✓ 1 User, ✓ Access 41 fields in Query API, ✓ 1 Request/second in Query API, ✓ HOST Aggregation API, ✓ Statistic Aggregation API.
- Business**: \$11,990/year. Includes: ✓ Query Credits 900,000/month, ✓ Up to 9million Results/month, ✓ Access All Syntaxes ⓘ, ✓ Web Download Feature, ✓ 5 Users ⓘ, ✓ Access 47 fields in Query API, ✓ 2 Request/second in Query API, ✓ HOST Aggregation API, ✓ Statistic Aggregation API, ✓ FOFA Fingerprint Rule, ✓ Website Feature ID (FID), ✓ Cloud Assets Tag, ✓ Fuzzy Search ⓘ, ✓ Product Tag, ✓ Category Tag, ✓ Third Party SDK Tag.
- Corporate**: \$64,800/year. Includes: ✓ Query Credits Custom, ✓ Custom Results/month, ✓ Access All Syntaxes ⓘ, ✓ Web Download Feature, ✓ Custom Users ⓘ, ✓ Access all fields in Query API, ✓ 5 Request/second in Query API, ✓ HOST Aggregation API, ✓ Statistic Aggregation API, ✓ FOFA Fingerprint Rule, ✓ Website Feature ID (FID), ✓ Cloud Assets Tag, ✓ Fuzzy Search ⓘ, ✓ Product Tag, ✓ Category Tag, ✓ Third Party SDK Tag, ✓ Asset Refresh, ✓ Statistical Visualization.

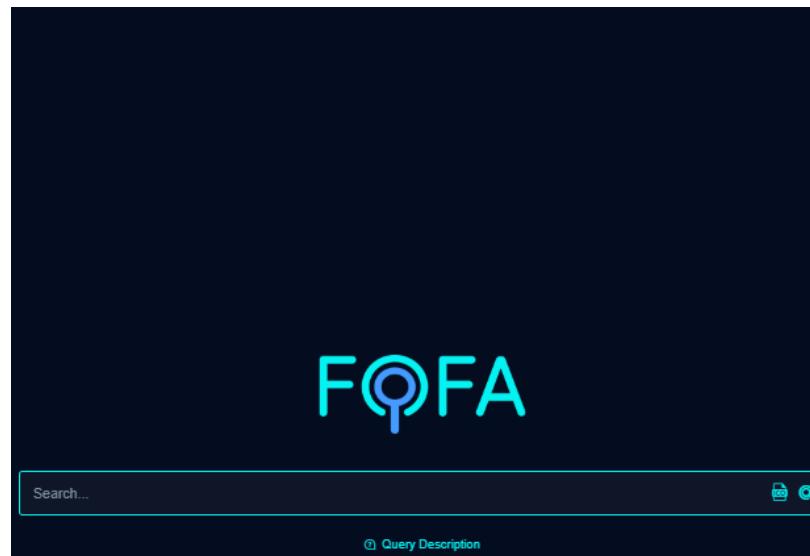
Each plan has a "Subscribe" button and a "Purchase Activation Code" link.

# FOFA

## Interfaccia

---

➤ <https://en.fofa.info/>

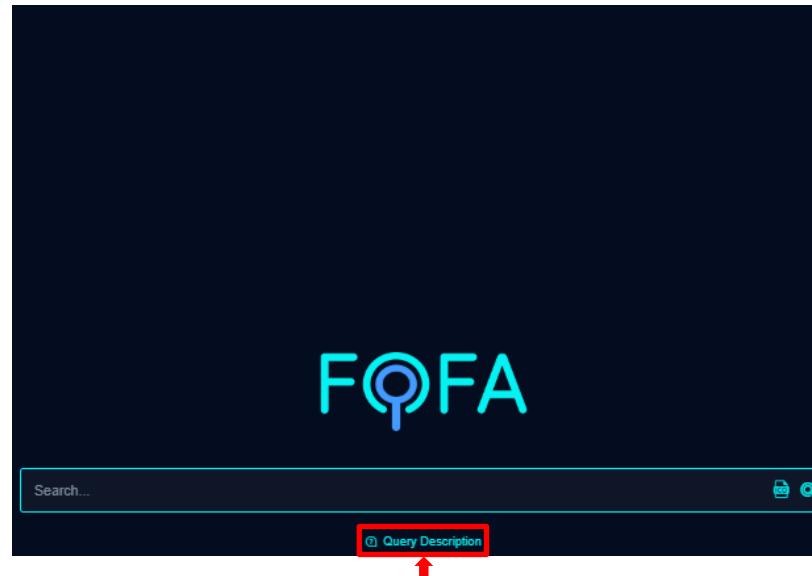


# FOFA

## Query Syntax

---

- Offre funzionalità molto simili a quelle fornite da Shodan e ZoomEye, accessibili mediante opportuni «filtrri»



# FOFA

## Query Description

➤ <https://en.fofa.info/>

Query Description X

If the query keyword has no syntax or filter, it will default to search from HTML, HTTP header and URL;  
If the query syntax has multiple AND & OR relationships, try including it with ();  
Add "==" to complete the match, such as finding all hosts of qq.com. It can be domain=="qq.com".

+ Advanced Search

Filter Example (Click to search)	Description	Tips
<code>title="bing"</code>	Query the "bing" from the title.	-
<code>header="elastic"</code>	Query "elastic" from the header.	-
<code>body="google"</code>	Query the "google" assets from HTML.	-
<code>fid="SXXGNUO2FefBTcCLIT/2Q=="</code>	Search the same fingerprint results by fid.	Type is subdomain.
<code>domain="bing.com"</code>	Query the "bing.com" by the domain name.	-
<code>icp="京ICP证030173号"</code>	Query the website record number.	Type is subdomain.
<code>js_name="js/jquery.js"</code>	Query " js/jquery.js" from the website body.	Type is subdomain.
<code>js_md5="82ac3f14327a8b7ba49baa208d4eaa15"</code>	Query the related results by js_md5.	-
<code>cname="ap21.inst.siteforce.com"</code>	Query "ap21.inst.siteforce.com" assets from Cname	-

## Output Parziale

# FOFA

## Featured Categories

➤ <https://en.fofa.info/subject>

**Rule Search Subject**

Include Databases, Industrial Control Systems, etc.

[Databases](#)   [Industrial Control Systems](#)   [Blockchain](#)   [Mining](#)



MySQL

Mysql



SQL

PostgreSQL



mongoDB

MongoDB



Riak

Riak



elastic

Elastic



redis

Redis



memcached

Memcached



Cassandra

Cassandra



CouchDB

CouchDB

Enumerating Target e Port Scanning

# FOFA

## API

- FOFA offre delle proprie API
- <https://en.fofa.info/api>

The screenshot shows the FOFA API Reference page with the 'Query Interface' section highlighted. The left sidebar contains navigation links for API Introduction, Limits, Request Structure, SDK, and various interface sections like Aggregation & Statistics and Basic Interface. The main content area has a heading 'Query Interface' with a sub-instruction: 'It provides a way to search for hosts and get detailed information to make development easier.' Below this is a 'GET' button followed by the URL 'https://fofa.info/api/v1/search/all'. To the right is a table detailing the parameters for the search query:

No.	Field	Necessary	Type	Description	Example
1	qbase64	Yes	string	The query syntax after base 64 encoding is your query content.	aXA0lJewMy4zNS4xNjguMzgi
2	fields	No	string	FOFA API can select the fields; the default is host, IP, and port. See Appendix 1 for more details.	host,ip,port
3	page	No	int	Turn the page; the default is page 1, sorted by update time.	1
4	size	No	int	The number of results per page; the default size is 100, and the maximum size per page is 10,000.	100
5	full	No	boolean	Results within one year are displayed. Specify true to search all results.	false

# FOFA

## Registrazione

- Prima di utilizzare FOFA è opportuno registrarsi su  
➤ [https://i.nosec.org/register?locale=en&service=https://en.fofa.info/f\\_login](https://i.nosec.org/register?locale=en&service=https://en.fofa.info/f_login)

Register

Email address, need activate account.

Password

Confirm your password

Username

Click the image to change.

I agree to the [Service & User Agreement](#)

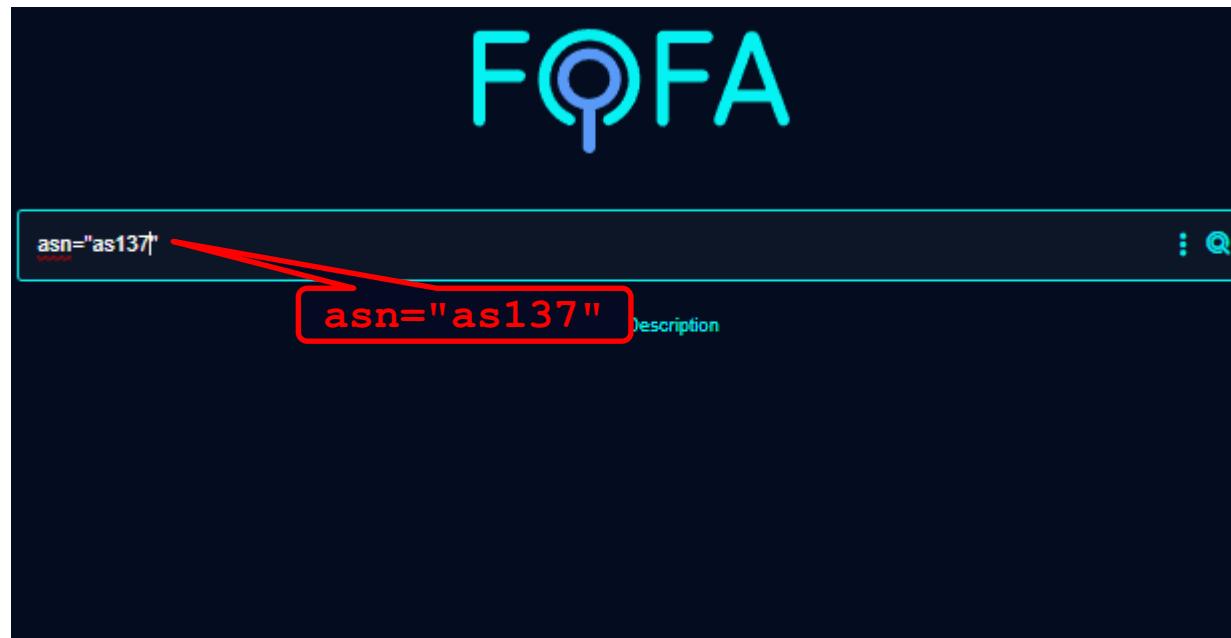
**Register**

[Already have an account?](#) [Didn't receive the email?](#)

# FOFA

## Esempio 1

- Effettuiamo una ricerca per Autonomous System Network (**asn=as137**)



# FOFA

## Esempio 1

- Effettuiamo una ricerca per Autonomous System Network (**asn=as137**)

The screenshot shows the FOFA search results for the query **asn=as137**. At the top, it displays **628,225 results ( 185,052 unique IP ) ,806 ms** and provides links for **Keyword Search**, **Nearly year results**, and **all results**. It also notes the exclusion of **8 Honeypot/Fraud Datas**.

The main search results are presented in two sections:

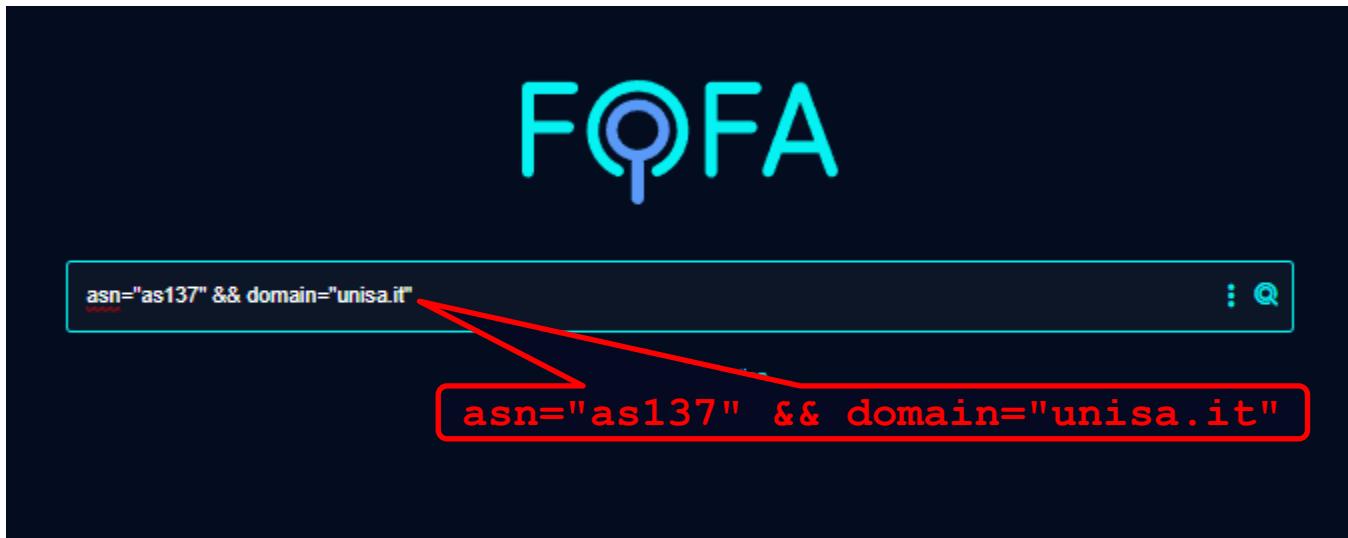
- 140.105.52.3:8020**: This entry shows the banner for the IP 140.105.52.3 at port 8020. The banner content includes:
  - HTTP/1.1 200 OK
  - Content-Length: 4503
  - Connection: close
  - Cache-Control: no-cache
  - Content-Type: text/html; charset=utf-8
  - X-Frame-Options: SAMEORIGIN
  - X-XSS-Protection: 1; mode=block
  - X-Content-Type-Options: nosniff
  - Content-Security-Policy: frame-ancestors 'self'
- https://193.204.65.141:8443**: This entry shows the banner for the IP 193.204.65.141 at port 8443. The banner content includes:
  - HTTP/1.1 404 Not Found
  - X-Frame-Options: SAMEORIGIN
  - Content-Security-Policy: frame-ancestors 'self'
  - Strict-Transport-Security: max-age=31536000; includeSubdomains
  - Content-Type: text/html;charset=iso-8859-1
  - Content-Length: 827
  - Server: Jetty(9.4.12.v20180830)

Each result page includes standard FOFA navigation and search controls.

# FOFA

## Esempio 2

- Effettuiamo una ricerca per Autonomous System Network (**asn=as137**) e dominio **unisa.it**



# FOFA

## Esempio 2

- Effettuiamo una ricerca per Autonomous System Network (**asn=as137**) e dominio **unisa.it**

The screenshot shows two search results from the FOFA search interface. Both results are for the domain `unisa.it`.

**Result 1:** `https://centroictbc.unisa.it` (443)

- IP: 193.205.185.18
- Country: Italy / Campania / Salerno
- ASN: 137
- Organization: Consortium GARR
- Date: 2024-02-13
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16

**Result 2:** `unisa-api.dev.unisa.it` (80)

- IP: 193.205.186.35
- Country: Italy / Campania / Salerno
- ASN: 137
- Organization: Consortium GARR
- Date: 2024-02-13
- Server: Apache/2.4.54 (Debian) / debian

Both results show detailed header information, including the HTTP response code (200 OK), connection type (close), transfer encoding (chunked), cache control (no-store, no-cache, must-revalidate, post-check=0, pre-check=0), content type (text/html; charset=UTF-8), date (Tue, 13 Feb 2024 15:46:19 GMT), expires (Thu, 19 Nov 1981 08:52:00 GMT), pragma (no-cache), and server details (Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 for the first result, and Apache/2.4.54 (Debian) for the second). The results also mention a cookie named XSRF-TOKEN.

# FOFA

## Esempio 2

- Effettuiamo una ricerca per Autonomous System Network (**asn=as137**) e dominio **unisa.it**

829 results ( 117 unique IP ), 1416 ms. Keyword Search.  
Nearly year results, click to view all results.  
Pure resolution domain asset detected, click to view.

**centroictbc.unisa.it** (443)

Header Products

HTTP/1.1 200 OK  
Connection: close  
Transfer-Encoding: chunked  
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
Content-Type: text/html; charset=UTF-8  
Date: Tue, 13 Feb 2024 15:45:19 GMT  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Pragma: no-cache  
Server: Apache/2.4.8 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 / centos

**unisa-api.dev.unisa.it** (80)

Header Products

HTTP/1.1 200 OK  
Connection: close  
Transfer-Encoding: chunked  
Cache-Control: no-cache, private  
Content-Type: text/html; charset=UTF-8  
Date: Tue, 13 Feb 2024 15:44:21 GMT  
Server: Apache/2.4.54 (Debian) / debian

**Porte Aperte**

# FOFA

## Esempio 2

- Effettuiamo una ricerca per Autonomous System Network (**asn=as137**) e dominio **unisa.it**



TOP SERVERS

Apache	313
nginx/1.18.0 (Ubuntu)	72
Apache/2.4.7 (Ubuntu)	45
Apache/2.4.41 (Ubuntu)	30

TOP PROTOCOLS

http	58
https	32
ssh	7
dns	5
netbios-ssn	4

# Outline

---

- Concetti Introduttivi
- Suite Protocollare TCP/IP
- Formato dei Messaggi TCP e UDP
- Active Enumeration
  - Network Scanner Nmap
  - Zenmap
  - Unicornscan
  - Masscan
- Passive Enumeration
  - Shodan
  - ZoomEye
  - FOFA
  - Censys

# Censys

## Caratteristiche

---

- Piattaforma open-source e commerciale per l'analisi della superficie d'attacco online
- Ricerca dispositivi, domini e certificati digitali esposti
- Individua anche vulnerabilità note, configurazioni errate, ed asset non registrati
- Scannerizza continuamente IPv4, IPv6, HTTP, HTTPS, SMTP, SSH, etc.
- Integra feed CVE, Shodan-like query, API, dashboard di analisi
- Supporta filtri avanzati, JSON search e tagging automatico

# Censys

## Progetto GitHub

➤ <https://github.com/censys>

The screenshot shows the GitHub profile for the organization "Censys". The profile includes a logo of two overlapping orange circles, a brief description stating "Censys is a platform that helps information security practitioners discover, monitor, and analyze devices that are accessible from the Internet.", and social links for 98 followers, Ann Arbor, the website https://www.censys.com, Twitter (@censysio), and email support@censys.com. The navigation bar includes tabs for Overview (selected), Repositories (29), Packages, and People (7). The "Pinned" section features two repositories: "censys-cloud-connector" (Python, 8 stars, 6 forks) and "censys-python" (Python, 435 stars, 97 forks). Below this is a "Repositories" section with a search bar and filters for Type, Language, and Sort. A red horizontal bar at the bottom contains the repository "censys-sdk-python" (Public).

Censys

Censys is a platform that helps information security practitioners discover, monitor, and analyze devices that are accessible from the Internet.

98 followers Ann Arbor https://www.censys.com @censysio support@censys.com

Overview Repositories 29 Packages People 7

Pinned

censys-cloud-connector Public

The Censys Unified Cloud Connector is a standalone connector that gathers assets from various cloud providers and stores them in Censys ASM. This Connector offers users the ability to supercharge o...

Python 8 6

censys-python Public

An easy-to-use and lightweight API wrapper for Censys APIs.

Python 435 97

Repositories

Find a repository... Type Language Sort

censys-sdk-python Public

Top lan Go TypeS

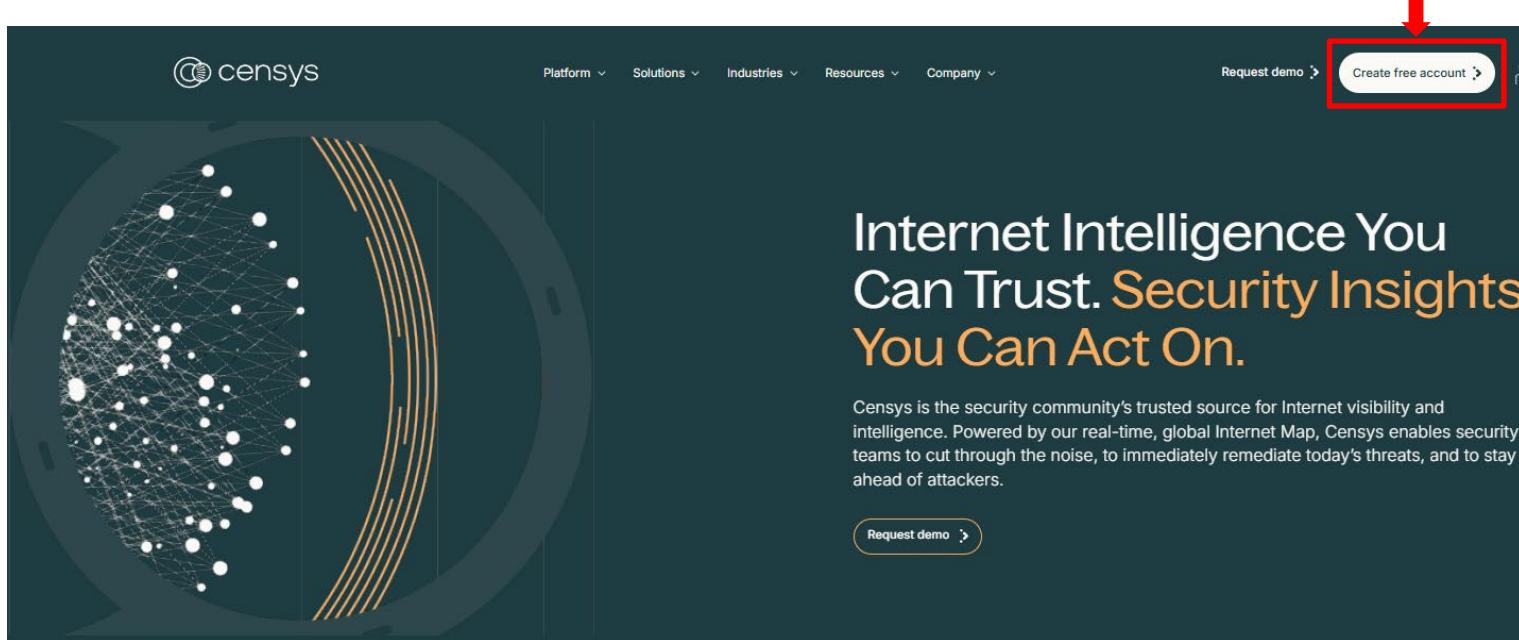
Most u censys python

Enumerating Target e Port Scanning

# Censys

## Interfaccia Web

➤ <https://censys.com/>

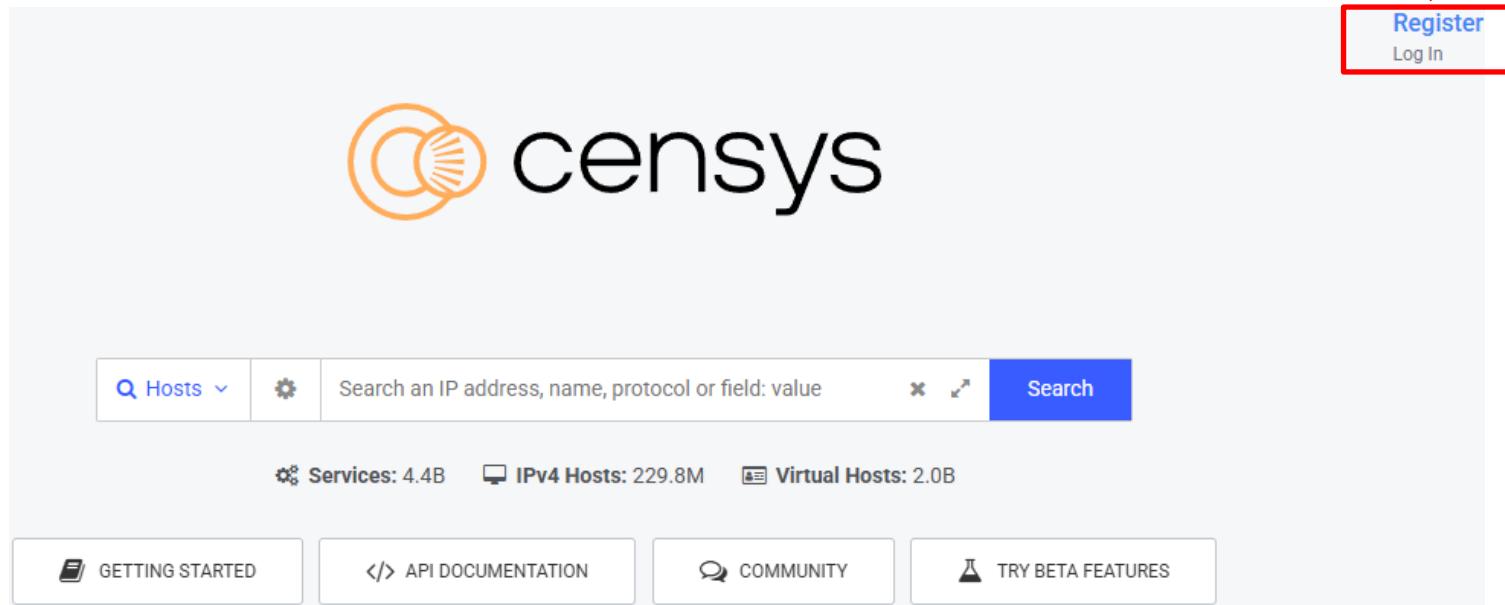


Per poter utilizzare Censys è necessaria la registrazione

# Censys

Vecchia Interfaccia Web (ancora funzionante)

➤ <https://search.censys.io/>

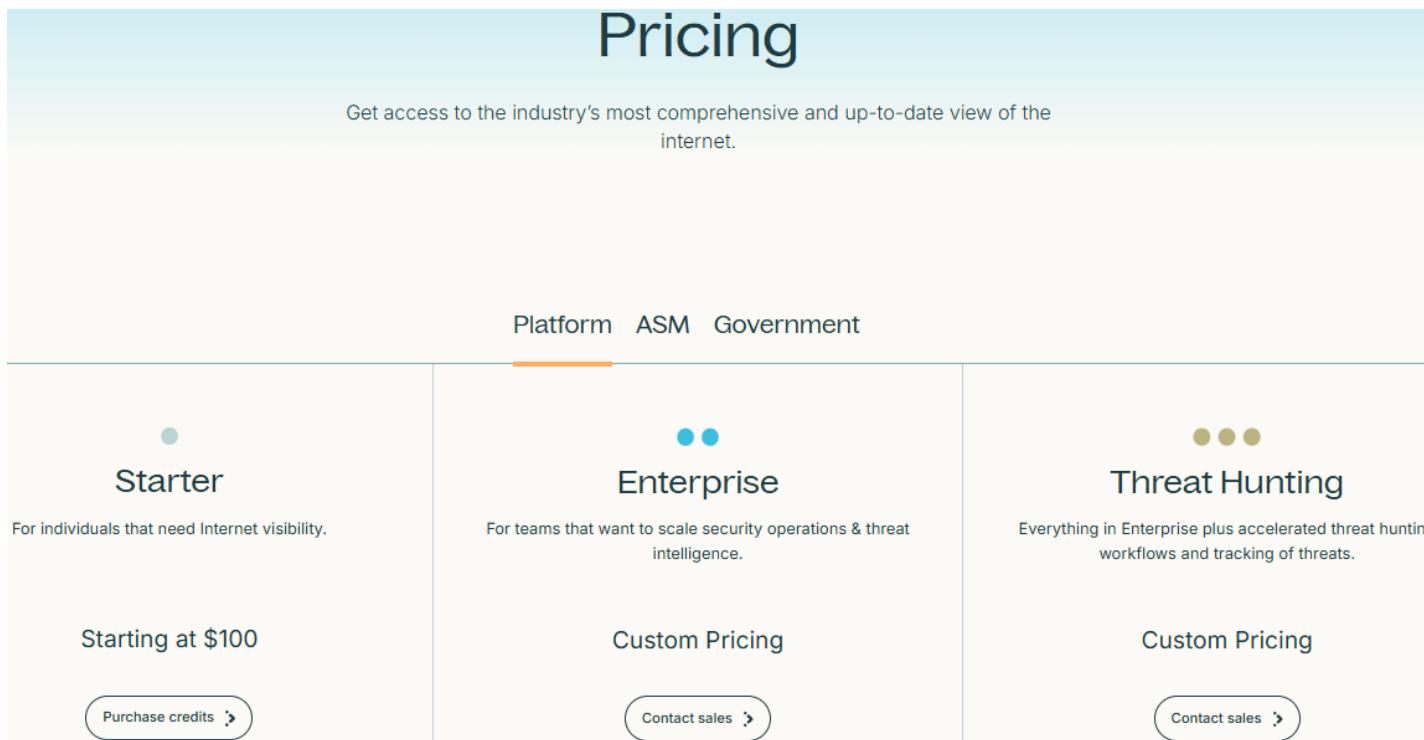


Per poter utilizzare Censys è necessaria la registrazione

# Censys

## Pricing

➤ <https://censys.com/resources/pricing>



The screenshot shows the Censys Pricing page. At the top, a teal header bar contains the word "Pricing". Below it, a sub-header reads "Get access to the industry's most comprehensive and up-to-date view of the internet." A horizontal navigation bar at the top right includes tabs for "Platform", "ASM", and "Government", with "Platform" being the active tab. The main content area displays three pricing plans: "Starter", "Enterprise", and "Threat Hunting". Each plan has a corresponding icon of colored dots above its name. The "Starter" plan is described as for individuals needing Internet visibility, starting at \$100, and includes a "Purchase credits" button. The "Enterprise" plan is described as for teams wanting to scale security operations & threat intelligence, with "Custom Pricing" available and a "Contact sales" button. The "Threat Hunting" plan is described as including everything in Enterprise plus accelerated threat hunting workflows and tracking of threats, also with "Custom Pricing" and a "Contact sales" button.

Plan	Description	Pricing	Action
Starter	For individuals that need Internet visibility.	Starting at \$100	<a href="#">Purchase credits</a>
Enterprise	For teams that want to scale security operations & threat intelligence.	Custom Pricing	<a href="#">Contact sales</a>
Threat Hunting	Everything in Enterprise plus accelerated threat hunting workflows and tracking of threats.	Custom Pricing	<a href="#">Contact sales</a>

# Censys

## Interfaccia di Ricerca

➤ <https://censys.io/>

The screenshot shows the Censys search interface. At the top, there is a navigation bar with icons for Home, Search, and Help. Below the navigation bar, a "Welcome" message is displayed. The main content area is divided into several sections:

- QUERY** (See More):
  - GEOLOCATION: Search for all hosts in Ann Arbor Michigan
  - LOGIN PAGES: Find hosts with login pages
  - HTTP BODIES: Search for web properties with default nginx bodies
  - SSH: Show hosts with SSH services running on non-standard ports
- DISCOVER**:
  - 416M Hosts
  - 16B Certificates
  - 2.8B Web Properties
- INVESTIGATE**:
  - 193 Protocols
  - 391 ASNs in Chile
  - 2K+ RDP Ports

# Censys

## Interfaccia di Ricerca – Esempio

➤ <https://censys.io/>

The screenshot shows the Censys search interface. A red box highlights the query ".\*.test.unisa.it" entered into the search bar. The interface includes sections for QUERY, DISCOVER, and INVESTIGATE, displaying various statistics such as 416M Hosts, 16B Certificates, 2.8B Web Properties, 193 Protocols, 391 ASNs in Chile, and 2K+ RDP Ports.

Home Search the Censys data for...

Welcome, Josh!

Getting Started Example Queries Data Definition

QUERY See More

QUERY See More

GEOLOCATION LOGIN PAGES HTTP BODIES SSH

DISCOVER

INVESTIGATE

193 Protocols 391 ASNs in Chile 2K+ RDP Ports

# Censys

## Interfaccia di Ricerca – Esempio

The screenshot shows the Censys search interface with the query `"*.test.unisa.it"` entered in the search bar. The results are categorized under **ASSET TYPES**, **SOFTWARE VENDORS**, and **SOFTWARE PRODUCTS**. The first result is for `ugov-pth2.test.unisa.it: 443`, which is identified as a **WEB PROPERTY**. It shows an **HTML Title** of "Open WebUI", **Browser Trust** as **Trusted**, and **Software** as **Nginx** running **Openwebui**. The second result is for `ugov-pth2.test.unisa.it: 80`, also a **WEB PROPERTY**, with an **HTML Title** of "301 Moved Permanently", **Browser Trust** as **No Data**, and **Software** as **Nginx**. The third result is for `unisa.esse3.pp.cineca.it: 443`, another **WEB PROPERTY**, with an **HTML Title** of "Homepage area pubblica, Università di Salerno", **Browser Trust** as **Trusted**, and **Software** as **Httpd**.

Search: `"*.test.unisa.it"`

**Search Results** Report Builder

**ASSET TYPES**

- Hosts: 6
- Certificates: 15
- Web Properties: 21

**SOFTWARE VENDORS**

- apache: 40
- php: 30
- f5: 10
- openwebui: 4
- apple: 2

**More ▾**

**SOFTWARE PRODUCTS**

- httpd: 40
- php: 30
- nginx: 10
- openwebui: 4
- python: 2

**More ▾**

RESULTS: 42 • DURATION: 1.61s

**ugov-pth2.test.unisa.it: 443** • WEB PROPERTY

HTML Title	Open WebUI	1 Endpoint
Browser Trust	Trusted	443 / HTTP
Software	Nginx	
	Openwebui	

**ugov-pth2.test.unisa.it: 80** • WEB PROPERTY

HTML Title	301 Moved Permanently	1 Endpoint
Browser Trust	No Data	80 / HTTP
Software	Nginx	

**unisa.esse3.pp.cineca.it: 443** • WEB PROPERTY

HTML Title	Homepage area pubblica, Università di Salerno	2 Endpoints
Browser Trust	Trusted	443 / HTTP
Software	Httpd	443 / HTTP / Root.do

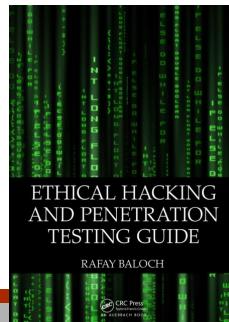
# Bibliografia

---

- **Kali Linux 2 - Assuring Security by Penetration Testing.**  
**Third Edition.** Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali. Packt Publishing. 2016
  - Capitolo 6



- **Ethical Hacking and Penetration Testing Guide.** Rafay Baloch. CRC Press. 2014
  - Capitolo 4



# Bibliografia

---

- **Guida di riferimento di Nmap (pagina del manuale)**
  - <https://nmap.org/man/it/>
  
- **Guida Rapida per Nmap**
  - <https://www.stationx.net/nmap-cheat-sheet>

# Bibliografia

---

➤ **ZoomEye**

➤ <https://www.zoomeye.org/doc>

➤ **Shodan**

➤ <https://danielmiessler.com/study/shodan/>

➤ <https://help.shodan.io/the-basics/search-query-fundamentals>

➤ <https://github.com/JavierOlmedo/shodan-filters>