

# Extra Info Gathering

## Censys.

Lo guay de censys es que puedes hacer filtros booleanos, es decir usar and y or. De forma que si queremos buscar ip con http o https podríamos. Shodan solo permite añadir mas filtros como si fuera un and.

Aquí buscamos cámaras en madrid

The screenshot displays the Censys search results for the IP address 207.188.130.103. The interface includes a search bar at the top with the query 'location.city:madrid and camera'. Below the search bar, the 'Basic Information' section shows the network as XTRA Telecom (ES), routing as 207.188.128.0/21 via AS15704, and protocols as 23/Telnet, 8000/HTTP, 37443/HTTP, and 49152/HTTP. The '23/Telnet' service is highlighted, showing a banner message: 'Sorry, Dear! telnet service is still in lock-time, You have to wait 16 min 6 sec, If you have any problem, ask administrator for help.' The '8000/HTTP' service is also highlighted, showing a request of GET / and a status code of 200. The '37443/HTTP' service is highlighted, showing a request of GET / and a status code of 200. On the right side, a map shows the geographic location of the IP, which is Madrid, Spain. The map includes coordinates (40°24'58.7"N 3°41'36....) and a list of nearby cities: Oporto, Lisboa, Sevilla, Granada, Valencia, Alicante (Alicant), Barcelona, and Andorra. The 'Geographic Location' section lists the city as Madrid, province as Madrid, country as Spain (ES), coordinates as 40.4163, -3.6934, and timezone as Europe/Madrid.

**Basic Information**

- Network: XTRA Telecom (ES)
- Routing: 207.188.128.0/21 via AS15704
- Protocols: 23/Telnet, 8000/HTTP, 37443/HTTP, 49152/HTTP

**23/Telnet** **TCP** Observed Jan 18, 2023 at 1:47pm UTC

**Details** [VIEW ALL DATA](#)

**Banner** Sorry, Dear! telnet service is still in lock-time, You have to wait 16 min 6 sec, If you have any problem, ask administrator for help.

**8000/HTTP** **TCP** Observed Jan 17, 2023 at 4:16pm UTC

**Details** [VIEW ALL DATA](#) [GO](#)

http://207.188.130.103:8000

- Request: GET /
- Protocol: HTTP/1.1
- Status Code: 200
- Status Reason: OK
- Body Hash: sha1:b33167903eb7d80cada38511432773587981fee2

**Response Body** [EXPAND](#)

**37443/HTTP** **TCP** Observed Jan 18, 2023 at 4:57pm UTC

**Details** [VIEW ALL DATA](#) [GO](#)

https://207.188.130.103:37443

- Request: GET /
- Protocol: HTTP/1.1
- Status Code: 200

**Geographic Location**

- City: Madrid
- Province: Madrid
- Country: Spain (ES)
- Coordinates: 40.4163, -3.6934
- Timezone: Europe/Madrid



Aquí buscamos por ciudad: mosta,malta y que tenga abierto el puerto 443(https) o use HTTP

A screenshot of the Censys search results page. The search bar at the top contains the query 'location.city:mosta and services.port:443 or services.service\_name:HTTP'. The results are displayed in a table-like format. On the left, there are filters for 'Host Filters' (Autonomous System, Location) and 'Service Filters' (Service Names, Ports). The main results section shows a list of hosts with their IP addresses, ASNs, and locations. The hosts are: 213.165.174.135 (c174-135.i02-4.onvol.net), 159.20.26.85 (VFM-AS Epic Communications Limited (33874)), 77.25.196.184 (VFM-AS Epic Communications Limited (33874)), 46.11.136.202 (DATASTREAM-NET (15735)), 213.165.162.232 (c162-232.i02-1.onvol.net), 46.11.28.32 (DATASTREAM-NET (15735)), and 213.165.162.214 (c162-214.i02-1.onvol.net). Each host entry shows the services it offers, such as 443/HTTP, 80/HTTP, 81/HTTP, 86/HTTP, 17000/UNKNOWN, 21/FTP, 8050/HTTP, 137/NETBIOS, 445/SMB, and 8001/UNKNOWN.

## Alternativas a Censys.

Alternativas a Shodan y Censys hay muchas, como Zoom Eye, IVRE, FOFA.

Yo he probado Zoom Eye. No es tan completo como los demás pero supongo que si sabes que buscar cumple su función.

zoomeye.org/searchResult?q=WIFICAM

ZoomEye

WIFICAM

Result Report Maps Vulnerability

About 262,928 results (Nearly year: 12,422 results) 0.613 seconds

WIFICAM X

tomsk.ba...  
tomsk.baza333.ru  
Linux  
Nginx: 1.14.0  
Russian Federation, Moscow  
2023-01-20 01:49  
Network Management Ltd  
firstbyte.ru  
ASN: AS204997

Banner SSL

HTTP/1.1 301 Moved Permanently  
Server: nginx/1.14.0 (Ubuntu)  
Date: Thu, 19 Jan 2023 17:48:58 GMT  
Content-Type: text/html  
Content-Length: 194  
Connection: keep-alive  
Location: https://tomsk.baza333.ru/  
<!DOCTYPE html>  
<!--[if IE]><![endif]-->  
<!--[if IE 8]><html dir="ltr" lang="ru" class="ie8"><![endif]-->  
<!--[if IE 9]><html dir="ltr" lang="ru" class="ie9"><![endif]-->  
<!--[if (gt IE 9)]><![endif]-->  
<html dir="ltr" lang="ru">

34.162.15.116  
10000/http/TCP  
IDC  
United States, Unknown  
2023-01-19 21:21  
Google LLC cloud.google.com

Banner

HTTP/1.0 200 OK  
content-type: text/html; charset=utf-8  
content-length: 45134  
st: upnp:rootdevice  
usn: uuid:00082f68-0000-0000-0000-6c00009b0000::upnp:rootdevice  
ext:  
x-powered-by: ThinkPHP  
x-xsrf-token: 11512f68b7f7a231

SEARCH TYPE

Devices 262,651  
Ipv4 262,651  
Ipv6 0  
Websites 277

YEAR

2023 1023  
2022 12,476  
2021 15,998  
More

COUNTRY

China 73,393  
Viet Nam 41,522

154.58.221.42

Basic Information Component details

IP Address 154.58.221.42  
City  
Province / State Andalusia  
Country Spain  
Location 37.54427, -4.727752  
Organization codinet.es  
ISP cogentco.com  
ASN AS202766

Ports / Service 6 whois dnsAnalysis 13 Vulnerability 31 User Tags 0

Serial number	Vulnerability number	Date of discovery	Vulnerability level	Vulnerability name
1	99619	2022-12-20	high	Apache Dubbo反序列化漏洞 (CVE-2022-39198)
2	99595	2022-10-18	high	Apache Commons Text 代码执行漏洞 (CVE-2022-42889)
3	99590	2022-10-13	high	Apache Ratik 命令执行漏洞 (CVE-2022-40146)
4	99587	2022-10-09	high	Apache Common JXPath 表达式解析漏洞 (CVE-2022-41852)

## Nmap scripts.

El primer paso es clonar el repositorio donde están los scripts, hay varios y cada uno tiene sus funciones pero yo he elegido este.

```
(kali@kali)-[/usr/share/nmap/scripts]
$ sudo git clone https://github.com/vulnersCom/nmap-vulners.git
Clonando en 'nmap-vulners' ...
remote: Enumerating objects: 104, done.
remote: Counting objects: 100% (42/42), done.
remote: Compressing objects: 100% (35/35), done.
remote: Total 104 (delta 22), reused 15 (delta 7), pack-reused 62
Recibiendo objetos: 100% (104/104), 444.33 KiB | 3.34 MiB/s, listo.
Resolviendo deltas: 100% (43/43), listo.

(kali@kali)-[/usr/share/nmap/scripts]
```

Ahora vamos a ver las posibles fallas de seguridad de los puertos abiertos en la 1.0.0.0.1

```
(kali@kali)-[/usr/share/nmap/scripts]
$ sudo nmap -sV --script nmap-vulners/ 10.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-19 09:18 CET
Nmap scan report for 10.0.0.1
Host is up (0.00031s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:8.2p1:
|   CVE-2020-15778  6.8   https://vulners.com/cve/CVE-2020-15778
|   C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3  6.8   https://vulners.com/githubexploit/C94132
FD-1FA5-5342-B6EE-0DAF45EEFFE3  *EXPLOIT*
|   10213DBE-F683-58BB-B6D3-353173626207  6.8   https://vulners.com/githubexploit/10213D
BE-F683-58BB-B6D3-353173626207  *EXPLOIT*
|   CVE-2020-12062  5.0   https://vulners.com/cve/CVE-2020-12062
|   CVE-2021-28041  4.6   https://vulners.com/cve/CVE-2021-28041
|   CVE-2021-41617  4.4   https://vulners.com/cve/CVE-2021-41617
|   CVE-2020-14145  4.3   https://vulners.com/cve/CVE-2020-14145
|   CVE-2016-20012  4.3   https://vulners.com/cve/CVE-2016-20012
|   CVE-2021-36368  2.6   https://vulners.com/cve/CVE-2021-36368
53/tcp    open  domain       Unbound
80/tcp    open  http         nginx/1.19.3
|_http-server-header: nginx/1.19.3
88/tcp    open  http         nginx/1.19.3
|_http-server-header: nginx/1.19.3
89/tcp    open  http         nginx/1.19.3
|_http-server-header: nginx/1.19.3
90/tcp    open  http         nginx/1.19.3
|_http-server-header: nginx/1.19.3
3030/tcp  open  http         Node.js Express framework
3306/tcp  open  mysql        MySQL 8.0.21
3333/tcp  open  mysql        MySQL 8.0.21
8080/tcp  open  nagios-nsc   Nagios NSCA
8181/tcp  open  ssl/http     Payara Server httpd 5.2021.4 (Servlet 4.0; JSP 2.3; Azul Systems, Inc
. Java 11)
| vulners:
|   cpe:/a:payara:payara:5.2021.4:
|   PACKETSTORM:169864  4.3   https://vulners.com/packetstorm/PACKETSTORM:169864  *
EXPLOIT*
|   1337DAY-ID-38070  4.3   https://vulners.com/zdt/1337DAY-ID-38070  *EXPLOIT
*
|_   CVE-2022-45129  0.0   https://vulners.com/cve/CVE-2022-45129
```

Ahora vamos a ver las posibles fallas de seguridad de los puertos abiertos en la 1.0.0.0.12. Podemos ver que hay unas cuantas.

```
(kali@kali)-[/usr/share/nmap/scripts]
$ sudo nmap -sV --script nmap-vulners/ 10.0.0.12
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-19 09:27 CET
Nmap scan report for 10.0.0.12
Host is up (0.00049s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| vulners:
| cpe:/a:openssh:openssh:7.2p2:
| PACKETSTORM:140070 7.8 https://vulners.com/packetstorm/PACKETSTORM:140070 *EXPLOIT*
| EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 7.8 https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09 *EXPLOIT*
| EDB-ID:40888 7.8 https://vulners.com/exploitdb/EDB-ID:40888 *EXPLOIT*
| CVE-2016-8858 7.8 https://vulners.com/cve/CVE-2016-8858
| CVE-2016-6515 7.8 https://vulners.com/cve/CVE-2016-6515
| 1337DAY-ID-26494 7.8 https://vulners.com/zdt/1337DAY-ID-26494 *EXPLOIT*
| SSV:92579 7.5 https://vulners.com/seebug/SSV:92579 *EXPLOIT*
| CVE-2016-10009 7.5 https://vulners.com/cve/CVE-2016-10009
| 1337DAY-ID-26576 7.5 https://vulners.com/zdt/1337DAY-ID-26576 *EXPLOIT*
| SSV:92582 7.2 https://vulners.com/seebug/SSV:92582 *EXPLOIT*
| CVE-2016-10012 7.2 https://vulners.com/cve/CVE-2016-10012
| CVE-2015-8325 7.2 https://vulners.com/cve/CVE-2015-8325
| SSV:92580 6.9 https://vulners.com/seebug/SSV:92580 *EXPLOIT*
| CVE-2016-10010 6.9 https://vulners.com/cve/CVE-2016-10010
| 1337DAY-ID-26577 6.9 https://vulners.com/zdt/1337DAY-ID-26577 *EXPLOIT*
| EXPLOITPACK:98FE96309F95248B8C4C508837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F95248B8C4C508837551A19 *EXPLOIT*
| EXPLOITPACK:5330EA02EBDE345BFC9D60DD97F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D60DD97F9E97 *EXPLOIT*
| EDB-ID:46516 5.8 https://vulners.com/exploitdb/EDB-ID:46516 *EXPLOIT*
| EDB-ID:46193 5.8 https://vulners.com/exploitdb/EDB-ID:46193 *EXPLOIT*
| CVE-2019-6111 5.8 https://vulners.com/cve/CVE-2019-6111
| 1337DAY-ID-32328 5.8 https://vulners.com/zdt/1337DAY-ID-32328 *EXPLOIT*
| 1337DAY-ID-32009 5.8 https://vulners.com/zdt/1337DAY-ID-32009 *EXPLOIT*
| SSV:91041 5.5 https://vulners.com/seebug/SSV:91041 *EXPLOIT*
| PACKETSTORM:140019 5.5 https://vulners.com/packetstorm/PACKETSTORM:140019 *EXPLOIT*
| PACKETSTORM:136234 5.5 https://vulners.com/packetstorm/PACKETSTORM:136234 *EXPLOIT*
| EXPLOITPACK:F92411A645D85F05BDBD274FD222226F 5.5 https://vulners.com/exploitpack/EXPLOITPACK:F92411A645D85F05BDBD274FD222226F *EXPLOIT*
| EXPLOITPACK:9F2E746846C3C623A27A441281EAD138 5.5 https://vulners.com/exploitpack/EXPLOITPACK:9F2E746846C3C623A27A441281EAD138 *EXPLOIT*
| EXPLOITPACK:1902C998CBF9154396911926B4C3B330 5.5 https://vulners.com/exploitpack/EXPLOITPACK:1902C998CBF9154396911926B4C3B330 *EXPLOIT*
| EDB-ID:40858 5.5 https://vulners.com/exploitdb/EDB-ID:40858 *EXPLOIT*
| EDB-ID:40119 5.5 https://vulners.com/exploitdb/EDB-ID:40119 *EXPLOIT*
| CVE-2016-3115 5.5 https://vulners.com/cve/CVE-2016-3115
| SSH_ENUM 5.0 https://vulners.com/canvas/SSH_ENUM *EXPLOIT*

| EDB-ID:40119 5.5 https://vulners.com/exploitdb/EDB-ID:40119 *EXPLOIT*
| CVE-2016-3115 5.5 https://vulners.com/cve/CVE-2016-3115
| SSH_ENUM 5.0 https://vulners.com/canvas/SSH_ENUM *EXPLOIT*
| PACKETSTORM:150621 5.0 https://vulners.com/packetstorm/PACKETSTORM:150621 *EXPLOIT*
| EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 5.0 https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 *EXPLOIT*
| EXPLOITPACK:EBDBCS685E3276D648B4D14B75563283 5.0 https://vulners.com/exploitpack/EXPLOITPACK:EBDBCS685E3276D648B4D14B75563283 *EXPLOIT*
| EDB-ID:45939 5.0 https://vulners.com/exploitdb/EDB-ID:45939 *EXPLOIT*
| EDB-ID:45233 5.0 https://vulners.com/exploitdb/EDB-ID:45233 *EXPLOIT*
| CVE-2018-15919 5.0 https://vulners.com/cve/CVE-2018-15919
| CVE-2018-15473 5.0 https://vulners.com/cve/CVE-2018-15473
| CVE-2017-15906 5.0 https://vulners.com/cve/CVE-2017-15906
| CVE-2016-10708 5.0 https://vulners.com/cve/CVE-2016-10708
| 1337DAY-ID-31730 5.0 https://vulners.com/zdt/1337DAY-ID-31730 *EXPLOIT*
| CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617
| EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF 4.3 https://vulners.com/exploitpack/EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF *EXPLOIT*
| EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF 4.3 https://vulners.com/exploitpack/EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF *EXPLOIT*
| EDB-ID:40113 4.3 https://vulners.com/exploitdb/EDB-ID:40113 *EXPLOIT*
| CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145
| CVE-2016-6210 4.3 https://vulners.com/cve/CVE-2016-6210
| 1337DAY-ID-25440 4.3 https://vulners.com/zdt/1337DAY-ID-25440 *EXPLOIT*
| 1337DAY-ID-25438 4.3 https://vulners.com/zdt/1337DAY-ID-25438 *EXPLOIT*
| CVE-2019-6110 4.0 https://vulners.com/cve/CVE-2019-6110
| CVE-2019-6109 4.0 https://vulners.com/cve/CVE-2019-6109
| CVE-2018-20685 2.6 https://vulners.com/cve/CVE-2018-20685
| SSV:92581 2.1 https://vulners.com/seebug/SSV:92581 *EXPLOIT*
| CVE-2016-10011 2.1 https://vulners.com/cve/CVE-2016-10011
| PACKETSTORM:151227 0.0 https://vulners.com/packetstorm/PACKETSTORM:151227 *EXPLOIT*
| PACKETSTORM:140261 0.0 https://vulners.com/packetstorm/PACKETSTORM:140261 *EXPLOIT*
| PACKETSTORM:138006 0.0 https://vulners.com/packetstorm/PACKETSTORM:138006 *EXPLOIT*
| PACKETSTORM:137942 0.0 https://vulners.com/packetstorm/PACKETSTORM:137942 *EXPLOIT*
| MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS- 0.0 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS- *EXPLOIT*
| 1337DAY-ID-30937 0.0 https://vulners.com/zdt/1337DAY-ID-30937 *EXPLOIT*
25/tcp    open  smtp      Postfix smtpd
80/tcp    open  http      nginx 1.10.3 (Ubuntu)
| vulners:
| cpe:/a:nginx:nginx:1.10.3:
| OSV:CVE-2022-41742 0.0 https://vulners.com/osv/OSV:CVE-2022-41742
| OSV:CVE-2022-41741 0.0 https://vulners.com/osv/OSV:CVE-2022-41741
| OSV:CVE-2021-3618 0.0 https://vulners.com/osv/OSV:CVE-2021-3618
| OSV:CVE-2022-41742 0.0 https://vulners.com/osv/OSV:CVE-2022-41742
| OSV:CVE-2022-41741 0.0 https://vulners.com/osv/OSV:CVE-2022-41741
| OSV:CVE-2021-3618 0.0 https://vulners.com/osv/OSV:CVE-2021-3618
```



```
|_http-server-header: nginx/1.10.3 (Ubuntu)
85/tcp open http Apache httpd 2.4.18 ((Ubuntu))
vulners:
  cpe:/a:apache:http_server:2.4.18:
    CVE-2022-31813 7.5 https://vulners.com/cve/CVE-2022-31813
    CVE-2022-23943 7.5 https://vulners.com/cve/CVE-2022-23943
    CVE-2022-22720 7.5 https://vulners.com/cve/CVE-2022-22720
    CVE-2021-44790 7.5 https://vulners.com/cve/CVE-2021-44790
    CVE-2021-39275 7.5 https://vulners.com/cve/CVE-2021-39275
    CVE-2021-26691 7.5 https://vulners.com/cve/CVE-2021-26691
    CVE-2017-7679 7.5 https://vulners.com/cve/CVE-2017-7679
    CVE-2017-3169 7.5 https://vulners.com/cve/CVE-2017-3169
    CVE-2017-3167 7.5 https://vulners.com/cve/CVE-2017-3167
    CNVD-2022-73123 7.5 https://vulners.com/cnvd/CNVD-2022-73123
    CNVD-2022-03225 7.5 https://vulners.com/cnvd/CNVD-2022-03225
    CNVD-2021-102386 7.5 https://vulners.com/cnvd/CNVD-2021-102386
    EXPLOITPACK:44C5118F831D55FAF4259C41D88DA0A8 7.2 https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D88DA0A8 *EXPLOIT*
    EDB-ID:46676 7.2 https://vulners.com/exploitdb/EDB-ID:46676 *EXPLOIT*
    CVE-2019-0211 7.2 https://vulners.com/cve/CVE-2019-0211
    1337DAY-ID-32502 7.2 https://vulners.com/zdt/1337DAY-ID-32502 *EXPLOIT*
    FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 6.8 https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 *EXPLOIT*
    CVE-2021-40438 6.8 https://vulners.com/cve/CVE-2021-40438
    CVE-2020-35452 6.8 https://vulners.com/cve/CVE-2020-35452
    CVE-2018-1312 6.8 https://vulners.com/cve/CVE-2018-1312
    CVE-2017-15715 6.8 https://vulners.com/cve/CVE-2017-15715
    CVE-2016-5387 6.8 https://vulners.com/cve/CVE-2016-5387
    CNVD-2022-03224 6.8 https://vulners.com/cnvd/CNVD-2022-03224
    8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 6.8 https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 *EXPLOIT*
    4810E2D9-AC5F-5B08-BF83-DDAFA2F63332 6.8 https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BF83-DDAFA2F63332 *EXPLOIT*
    4373C92A-2755-5538-9C91-0469C995AA98 6.8 https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA98 *EXPLOIT*
    0095E929-7573-5E4A-A7FA-F6598A35E8DE 6.8 https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE *EXPLOIT*
    CVE-2022-28615 6.4 https://vulners.com/cve/CVE-2022-28615
    CVE-2021-44224 6.4 https://vulners.com/cve/CVE-2021-44224
    CVE-2019-10082 6.4 https://vulners.com/cve/CVE-2019-10082
    CVE-2017-9788 6.4 https://vulners.com/cve/CVE-2017-9788
    CVE-2019-0217 6.0 https://vulners.com/cve/CVE-2019-0217
    CVE-2022-22721 5.8 https://vulners.com/cve/CVE-2022-22721
    CVE-2020-1927 5.8 https://vulners.com/cve/CVE-2020-1927
    CVE-2019-10098 5.8 https://vulners.com/cve/CVE-2019-10098
    1337DAY-ID-33577 5.8 https://vulners.com/zdt/1337DAY-ID-33577 *EXPLOIT*
    SSV:96537 5.0 https://vulners.com/seebug/SSV:96537 *EXPLOIT*
    EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D 5.0 https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D *EXPLOIT*
    EXPLOITPACK:2666FB0676B4B582D689921651A30355 5.0 https://vulners.com/exploitpack/EXPLOITPACK:2666FB0676B4B582D689921651A30355 *EXPLOIT*

    EXPLOITPACK:2666FB0676B4B582D689921651A30355 5.0 https://vulners.com/exploitpack/EXPLOITPACK:2666FB0676B4B582D689921651A30355 *EXPLOIT*
    EDB-ID:42745 5.0 https://vulners.com/exploitdb/EDB-ID:42745 *EXPLOIT*
    EDB-ID:40909 5.0 https://vulners.com/exploitdb/EDB-ID:40909 *EXPLOIT*
    CVE-2022-30556 5.0 https://vulners.com/cve/CVE-2022-30556
    CVE-2022-29404 5.0 https://vulners.com/cve/CVE-2022-29404
    CVE-2022-28614 5.0 https://vulners.com/cve/CVE-2022-28614
    CVE-2022-26377 5.0 https://vulners.com/cve/CVE-2022-26377
    CVE-2022-22719 5.0 https://vulners.com/cve/CVE-2022-22719
    CVE-2021-34798 5.0 https://vulners.com/cve/CVE-2021-34798
    CVE-2021-33193 5.0 https://vulners.com/cve/CVE-2021-33193
    CVE-2021-26690 5.0 https://vulners.com/cve/CVE-2021-26690
    CVE-2020-1934 5.0 https://vulners.com/cve/CVE-2020-1934
    CVE-2019-17567 5.0 https://vulners.com/cve/CVE-2019-17567
    CVE-2019-0220 5.0 https://vulners.com/cve/CVE-2019-0220
    CVE-2019-0196 5.0 https://vulners.com/cve/CVE-2019-0196
    CVE-2018-17199 5.0 https://vulners.com/cve/CVE-2018-17199
    CVE-2018-17189 5.0 https://vulners.com/cve/CVE-2018-17189
    CVE-2018-1333 5.0 https://vulners.com/cve/CVE-2018-1333
    CVE-2018-1303 5.0 https://vulners.com/cve/CVE-2018-1303
    CVE-2017-9798 5.0 https://vulners.com/cve/CVE-2017-9798
    CVE-2017-15710 5.0 https://vulners.com/cve/CVE-2017-15710
    CVE-2016-8743 5.0 https://vulners.com/cve/CVE-2016-8743
    CVE-2016-8740 5.0 https://vulners.com/cve/CVE-2016-8740
    CVE-2016-4979 5.0 https://vulners.com/cve/CVE-2016-4979
    CNVD-2022-73122 5.0 https://vulners.com/cnvd/CNVD-2022-73122
    CNVD-2022-53584 5.0 https://vulners.com/cnvd/CNVD-2022-53584
    CNVD-2022-53582 5.0 https://vulners.com/cnvd/CNVD-2022-53582
    CNVD-2022-03223 5.0 https://vulners.com/cnvd/CNVD-2022-03223
    1337DAY-ID-28573 5.0 https://vulners.com/zdt/1337DAY-ID-28573 *EXPLOIT*
    CVE-2020-11985 4.3 https://vulners.com/cve/CVE-2020-11985
    CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092
    CVE-2018-1302 4.3 https://vulners.com/cve/CVE-2018-1302
    CVE-2018-1301 4.3 https://vulners.com/cve/CVE-2018-1301
    CVE-2018-11763 4.3 https://vulners.com/cve/CVE-2018-11763
    CVE-2016-4975 4.3 https://vulners.com/cve/CVE-2016-4975
    CVE-2016-1546 4.3 https://vulners.com/cve/CVE-2016-1546
    4013EC74-B3C1-5D95-938A-54197A58586D 4.3 https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D *EXPLOIT*
    1337DAY-ID-33575 4.3 https://vulners.com/zdt/1337DAY-ID-33575 *EXPLOIT*
    CVE-2018-1283 3.5 https://vulners.com/cve/CVE-2018-1283
    CVE-2016-8612 3.3 https://vulners.com/cve/CVE-2016-8612
    PACKETSTORM:152441 0.0 https://vulners.com/packetstorm/PACKETSTORM:152441 *EXPLOIT*
|_http-server-header: Apache/2.4.18 (Ubuntu)
88/tcp open ssl/http nginx 1.10.3
```

```
|_ PACKETSTORM:152441 0.0 https://vulners.com/packetstorm/PACKETSTORM:152441 *EXPLOIT*
|_http-server-header: Apache/2.4.18 (Ubuntu)
88/tcp open ssl/http nginx 1.10.3
|_ vulners:
|_ cpe:/a:nginx:nginx:1.10.3:
|_ OSV:CVE-2022-41742 0.0 https://vulners.com/osv/OSV:CVE-2022-41742
|_ OSV:CVE-2022-41741 0.0 https://vulners.com/osv/OSV:CVE-2022-41741
|_ OSV:CVE-2021-3618 0.0 https://vulners.com/osv/OSV:CVE-2021-3618
|_ OSV:CVE-2022-41742 0.0 https://vulners.com/osv/OSV:CVE-2022-41742
|_ OSV:CVE-2022-41741 0.0 https://vulners.com/osv/OSV:CVE-2022-41741
|_ OSV:CVE-2021-3618 0.0 https://vulners.com/osv/OSV:CVE-2021-3618
|_http-server-header: nginx/1.10.3 (Ubuntu)
89/tcp open http nginx 1.10.3 (Ubuntu)
|_ vulners:
|_ cpe:/a:nginx:nginx:1.10.3:
|_ OSV:CVE-2022-41742 0.0 https://vulners.com/osv/OSV:CVE-2022-41742
|_ OSV:CVE-2022-41741 0.0 https://vulners.com/osv/OSV:CVE-2022-41741
|_ OSV:CVE-2021-3618 0.0 https://vulners.com/osv/OSV:CVE-2021-3618
|_ OSV:CVE-2022-41742 0.0 https://vulners.com/osv/OSV:CVE-2022-41742
|_ OSV:CVE-2022-41741 0.0 https://vulners.com/osv/OSV:CVE-2022-41741
|_ OSV:CVE-2021-3618 0.0 https://vulners.com/osv/OSV:CVE-2021-3618
|_http-server-header: nginx/1.10.3 (Ubuntu)
389/tcp open ldap (Anonymous bind OK)
443/tcp open ssl/http nginx 1.10.3 (Ubuntu)
|_ vulners:
|_ cpe:/a:nginx:nginx:1.10.3:
|_ OSV:CVE-2022-41742 0.0 https://vulners.com/osv/OSV:CVE-2022-41742
|_ OSV:CVE-2022-41741 0.0 https://vulners.com/osv/OSV:CVE-2022-41741
|_ OSV:CVE-2021-3618 0.0 https://vulners.com/osv/OSV:CVE-2021-3618
|_ OSV:CVE-2022-41742 0.0 https://vulners.com/osv/OSV:CVE-2022-41742
|_ OSV:CVE-2022-41741 0.0 https://vulners.com/osv/OSV:CVE-2022-41741
|_ OSV:CVE-2021-3618 0.0 https://vulners.com/osv/OSV:CVE-2021-3618
|_http-server-header: nginx/1.10.3 (Ubuntu)
444/tcp open ssl/http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_ vulners:
|_ cpe:/a:apache:http_server:2.4.18:
|_ CVE-2022-31813 7.5 https://vulners.com/cve/CVE-2022-31813
|_ CVE-2022-23943 7.5 https://vulners.com/cve/CVE-2022-23943
|_ CVE-2022-22720 7.5 https://vulners.com/cve/CVE-2022-22720
|_ CVE-2021-44790 7.5 https://vulners.com/cve/CVE-2021-44790
|_ CVE-2021-39275 7.5 https://vulners.com/cve/CVE-2021-39275
|_ CVE-2021-39275 7.5 https://vulners.com/cve/CVE-2021-39275
|_ CVE-2021-26691 7.5 https://vulners.com/cve/CVE-2021-26691
|_ CVE-2017-7679 7.5 https://vulners.com/cve/CVE-2017-7679
|_ CVE-2017-3169 7.5 https://vulners.com/cve/CVE-2017-3169
|_ CVE-2017-3167 7.5 https://vulners.com/cve/CVE-2017-3167
|_ CNVD-2022-73123 7.5 https://vulners.com/cnvd/CNVD-2022-73123
|_ CNVD-2022-03225 7.5 https://vulners.com/cnvd/CNVD-2022-03225
|_ CNVD-2021-102386 7.5 https://vulners.com/cnvd/CNVD-2021-102386
|_ EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0A0B 7.2 https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0A0B *EXPLOIT*
|_ EDB-ID:46676 7.2 https://vulners.com/exploitdb/EDB-ID:46676 *EXPLOIT*
|_ CVE-2019-0211 7.2 https://vulners.com/cve/CVE-2019-0211
|_ 1337DAY-ID-32502 7.2 https://vulners.com/zdt/1337DAY-ID-32502 *EXPLOIT*
|_ FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 6.8 https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 *EXPLOIT*
|_ CVE-2021-40438 6.8 https://vulners.com/cve/CVE-2021-40438
|_ CVE-2020-35452 6.8 https://vulners.com/cve/CVE-2020-35452
|_ CVE-2018-1312 6.8 https://vulners.com/cve/CVE-2018-1312
|_ CVE-2017-15715 6.8 https://vulners.com/cve/CVE-2017-15715
|_ CVE-2016-5387 6.8 https://vulners.com/cve/CVE-2016-5387
|_ CNVD-2022-03224 6.8 https://vulners.com/cnvd/CNVD-2022-03224
|_ 8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 6.8 https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 *EXPLOIT*
|_ 4810E2D9-AC5F-5B08-BF83-DDAFA2F63332 6.8 https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BF83-DDAFA2F63332 *EXPLOIT*
|_ 4373C92A-2755-5538-9C91-0469C995AA9B 6.8 https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B *EXPLOIT*
|_ 0095E929-7573-5E4A-A7FA-F6598A35E8DE 6.8 https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE *EXPLOIT*
|_ CVE-2022-28615 6.4 https://vulners.com/cve/CVE-2022-28615
|_ CVE-2021-44224 6.4 https://vulners.com/cve/CVE-2021-44224
|_ CVE-2019-10082 6.4 https://vulners.com/cve/CVE-2019-10082
|_ CVE-2017-9788 6.4 https://vulners.com/cve/CVE-2017-9788
|_ CVE-2019-0217 6.0 https://vulners.com/cve/CVE-2019-0217
|_ CVE-2022-22721 5.8 https://vulners.com/cve/CVE-2022-22721
|_ CVE-2020-1927 5.8 https://vulners.com/cve/CVE-2020-1927
|_ CVE-2019-10098 5.8 https://vulners.com/cve/CVE-2019-10098
|_ 1337DAY-ID-33577 5.8 https://vulners.com/zdt/1337DAY-ID-33577 *EXPLOIT*
|_ SSV:96537 5.0 https://vulners.com/seebug/SSV:96537 *EXPLOIT*
|_ EXPLOITPACK:C8C256BE08FF5FE1C0405CB0AA9C075D 5.0 https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE08FF5FE1C0405CB0AA9C075D *EXPLOIT*
|_ EXPLOITPACK:2666FB0676B4B582D689921651A30355 5.0 https://vulners.com/exploitpack/EXPLOITPACK:2666FB0676B4B582D689921651A30355 *EXPLOIT*
|_ EDB-ID:42745 5.0 https://vulners.com/exploitdb/EDB-ID:42745 *EXPLOIT*
|_ EDB-ID:40909 5.0 https://vulners.com/exploitdb/EDB-ID:40909 *EXPLOIT*
|_ CVE-2022-30556 5.0 https://vulners.com/cve/CVE-2022-30556
|_ CVE-2022-29404 5.0 https://vulners.com/cve/CVE-2022-29404
|_ CVE-2022-28614 5.0 https://vulners.com/cve/CVE-2022-28614
|_ CVE-2022-26377 5.0 https://vulners.com/cve/CVE-2022-26377
|_ CVE-2022-22719 5.0 https://vulners.com/cve/CVE-2022-22719
|_ CVE-2021-34798 5.0 https://vulners.com/cve/CVE-2021-34798
```

```

| CVE-2018-17189 5.0 https://vulners.com/cve/CVE-2018-17189
| CVE-2018-1333 5.0 https://vulners.com/cve/CVE-2018-1333
| CVE-2018-1303 5.0 https://vulners.com/cve/CVE-2018-1303
| CVE-2017-9798 5.0 https://vulners.com/cve/CVE-2017-9798
| CVE-2017-15710 5.0 https://vulners.com/cve/CVE-2017-15710
| CVE-2016-8743 5.0 https://vulners.com/cve/CVE-2016-8743
| CVE-2016-8740 5.0 https://vulners.com/cve/CVE-2016-8740
| CVE-2016-4979 5.0 https://vulners.com/cve/CVE-2016-4979
| CNVD-2022-73122 5.0 https://vulners.com/cnvd/CNVD-2022-73122
| CNVD-2022-53584 5.0 https://vulners.com/cnvd/CNVD-2022-53584
| CNVD-2022-53582 5.0 https://vulners.com/cnvd/CNVD-2022-53582
| CNVD-2022-03223 5.0 https://vulners.com/cnvd/CNVD-2022-03223
| 1337DAY-ID-28573 5.0 https://vulners.com/zdt/1337DAY-ID-28573 *EXPLOIT*
| CVE-2020-11985 4.3 https://vulners.com/cve/CVE-2020-11985
| CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092
| CVE-2018-1302 4.3 https://vulners.com/cve/CVE-2018-1302
| CVE-2018-1301 4.3 https://vulners.com/cve/CVE-2018-1301
| CVE-2018-11763 4.3 https://vulners.com/cve/CVE-2018-11763
| CVE-2016-4975 4.3 https://vulners.com/cve/CVE-2016-4975
| CVE-2016-1546 4.3 https://vulners.com/cve/CVE-2016-1546
| 4013EC74-B3C1-5D95-938A-54197A58586D 4.3 https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D *EXPLOIT*
| 1337DAY-ID-33575 4.3 https://vulners.com/zdt/1337DAY-ID-33575 *EXPLOIT*
| CVE-2018-1283 3.5 https://vulners.com/cve/CVE-2018-1283
| CVE-2016-8612 3.3 https://vulners.com/cve/CVE-2016-8612
| PACKETSTORM:152441 0.0 https://vulners.com/packetstorm/PACKETSTORM:152441 *EXPLOIT*
|_
|_ 3333/tcp open http nginx 1.10.3 (Ubuntu)
|_ http-server-header: nginx/1.10.3 (Ubuntu)
|_ vulners:
|_ cpe:/a:nginx:nginx:1.10.3:
|_ OSV:CVE-2022-41742 0.0 https://vulners.com/osv/OSV:CVE-2022-41742
|_ OSV:CVE-2022-41741 0.0 https://vulners.com/osv/OSV:CVE-2022-41741
|_ OSV:CVE-2021-3618 0.0 https://vulners.com/osv/OSV:CVE-2021-3618
|_ OSV:CVE-2022-41742 0.0 https://vulners.com/osv/OSV:CVE-2022-41742
|_ OSV:CVE-2022-41741 0.0 https://vulners.com/osv/OSV:CVE-2022-41741
|_ OSV:CVE-2021-3618 0.0 https://vulners.com/osv/OSV:CVE-2021-3618
|_
|_ MAC Address: 08:00:27:58:C7:E3 (Oracle VirtualBox virtual NIC)
|_ Service Info: Host: moodle.quevedo; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.29 seconds

```

Si tuviera un mayor conocimiento estoy seguro de que seria capaz de acceder y burlar la seguridad de la 10.0.0.12, posteriormente escalar privilegios y comprometer el equipo.