

# MB Elettronica(Kali Tools)

## N-MAP

sudo nmap -sS

```
sudo nmap -sS 31.3.182.7
Starting Nmap 7.94SVN ( https://nmap.org )
at 2024-09-17 22:30 CEST
Nmap scan report for 7.182.3.31.in-
addr.arpa (31.3.182.7)
Host is up (0.020s latency).
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
26/tcp    filtered rsftp
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  filtered mysql
```

sudo nmap -O

Aggressive OS guesses: Linux 3.10 - 3.12 (95%), Linux 4.4 (95%), Linux 4.9 (94%), Linux 3.10 (92%), Linux 3.11 - 4.1 (91%), Linux 2.6.32 (91%), Linux 2.6.32 or 3.10 (91%), Linux 2.6.39 (91%), WatchGuard Fireware 11.8 (91%), Synology DiskStation Manager 5.1 (91%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 11 hops

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 5.17 seconds

sudo nmap -A

Traceroute

```
TRACEROUTE (using port 8080/tcp)
HOP RTT ADDRESS
1 0.26 ms H388X.homenet.telecomitalia.it (192.168.1.1)
2 ...
3 8.84 ms 172.17.107.168 (172.17.107.168)
4 13.66 ms 172.17.105.174 (172.17.105.174)
5 15.40 ms 172.19.184.66 (172.19.184.66)
6 14.49 ms 172.19.177.10 (172.19.177.10)
7 15.69 ms 172.19.0.169 (172.19.0.169)
8 14.50 ms cesenanet.mix-it.net (217.29.66.159)
9 19.23 ms 31_3_185_254.ip.cesenanet.net (31.3.185.254)
10 17.24 ms 31-3-182-254.ip.cesenanet.net (31.3.182.254)
11 19.02 ms server01.tiphys.com (31.3.182.7)
```

porta 80

```
80/tcp open  http Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
```

porta 443

```
443/tcp open  ssl/http Apache httpd
|_ssl-cert: Subject:
commonName=accademia-etrusca.org
|_Subject Alternative Name: DNS:accademia-
etrusca.org, DNS:www.accademia-
etrusca.org
|_Not valid before: 2024-08-06T19:57:21
|_Not valid after: 2024-11-04T19:57:20
|_http-server-header: Apache
|_tls-alpn:
|_ http/1.1
|_http-title: 403 Forbidden
|_ssl-date: TLS randomness does not
represent time
```