

About Nmap

**[http://
nmap.org/](http://nmap.org/)**

Created by
Gordon Lyon in
1997

Already
installed on Kali
Linux

GUI version
called Zenmap
(also on Kali
Linux)

```
Starting Nmap 7.12 ( https://nmap.org ) at 2017-07-01 07:05 EDT
Nmap scan report for 192.168.101.10
Host is up (0.032s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE VERSION
25/tcp    open  smtp    Postfix smtpd
|_smtp-commands: mail.ptest.lab, PIPELINING, SIZE, ETRN, STARTTLS, AUTH PLAIN LOGIN, AUTH=PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-cert: Subject: commonName=mail.test.lab/organizationName=mail.test.lab/stateOrProvinceName=GuangDong/countryName=CN
|_Not valid before: 2017-04-22T19:19:57
|_Not valid after: 2027-04-20T19:19:57
|_ssl-date: TLS randomness does not represent time
80/tcp    open  http    nginx 1.12.0
|_http-title: 403 Forbidden
88/tcp    open  http    nginx 1.6.2
|_http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: nginx/1.6.2
|_http-title: Users
8080/tcp  open  http    nginx
|_http-open-proxy: Proxy might be redirecting requests
|_http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: nginx
|_http-title: Site doesn't have a title (text/html).
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2
Network Distance: 2 hops
Service Info: Host: mail.ptest.lab

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   0.43 ms  192.168.93.2
2   0.30 ms  192.168.101.10

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.94 seconds
```

Using NMAP

- **Host discovery (ping based)**

```
$ nmap -sP 10.0.1.0-255
```

- **OS detection**

```
$ nmap -O 10.0.1.101
```

- **Full TCP port scanning**

```
$ nmap -p0-65535 10.0.1.101
```

- **Version detection**

```
$ nmap -sV 10.0.1.101
```

- **Export a full scan to a file**

```
$ nmap -O -sV -p0-65535 10.0.1.101 -oN target.nmap
```