

Scanning Domain Menggunakan Tool NMap

Langkah awal :

- Install *software* atau *tools* untuk melakukan proses *scanning*. Disini saya menggunakan *tool* NMap.
- Tentukan target yang ingin di *scanning*, lalu buka *website* yang sudah dipilih.
- Jalankan aplikasi NMap lalu masukkan target yang ingin di *scanning*. Maka akan muncul hasil seperti dibawah ini.

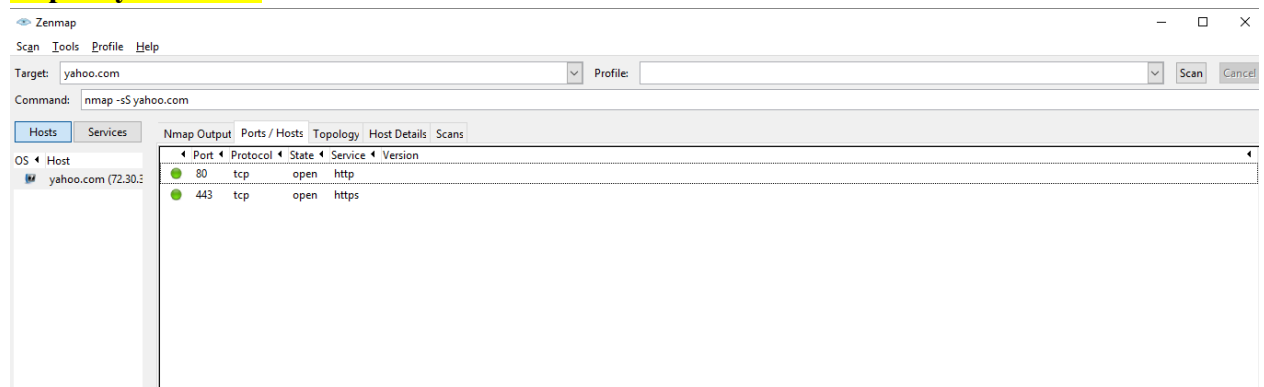
1. Domain Luar Negeri

YAHOO.COM

sS yahoo.com



sS port yahoo.com



sV yahoo.com

Target: yahoo.com
Command: nmap -sV yahoo.com

Starting Nmap 7.60 (<https://nmap.org>) at 2019-02-19 00:46 SE Asia Standard Time
Nmap scan report for yahoo.com (72.30.35.10)
Host is up (0.33s latency).
Other addresses for yahoo.com (not scanned): 98.137.246.7 72.30.35.9 98.138.219.232 98.138.219.231 98.137.246.8
rDNS record for 72.30.35.10: media-router-fp2.prod1.media.vip.bf1.yahoo.com
Not shown: 998 filtered ports

PORT	STATE	SERVICE	VERSION
80/tcp	open	http-proxy	Apache Traffic Server
443/tcp	open	ssl/http-proxy	Apache Traffic Server

Service Info: Hosts: media-router-fp1014.prod.media.bf1.yahoo.com, media-router-fp1013.prod.media.bf1.yahoo.com

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 59.76 seconds

sV port yahoo.com

Target: yahoo.com
Command: nmap -sV yahoo.com

Port	Protocol	State	Service	Version
80	tcp	open	http-proxy	Apache Traffic Server
443	tcp	open	http-proxy	Apache Traffic Server

sU yahoo.com

Target: yahoo.com
Command: nmap -sU yahoo.com

Starting Nmap 7.60 (<https://nmap.org>) at 2019-02-19 00:50 SE Asia Standard Time
Nmap scan report for yahoo.com (72.30.35.10)
Host is up (0.32s latency).
Other addresses for yahoo.com (not scanned): 98.137.246.7 72.30.35.9 98.138.219.232 98.138.219.231 98.137.246.8
rDNS record for 72.30.35.10: media-router-fp2.prod1.media.vip.bf1.yahoo.com
All 1000 scanned ports on yahoo.com (72.30.35.10) are open|filtered

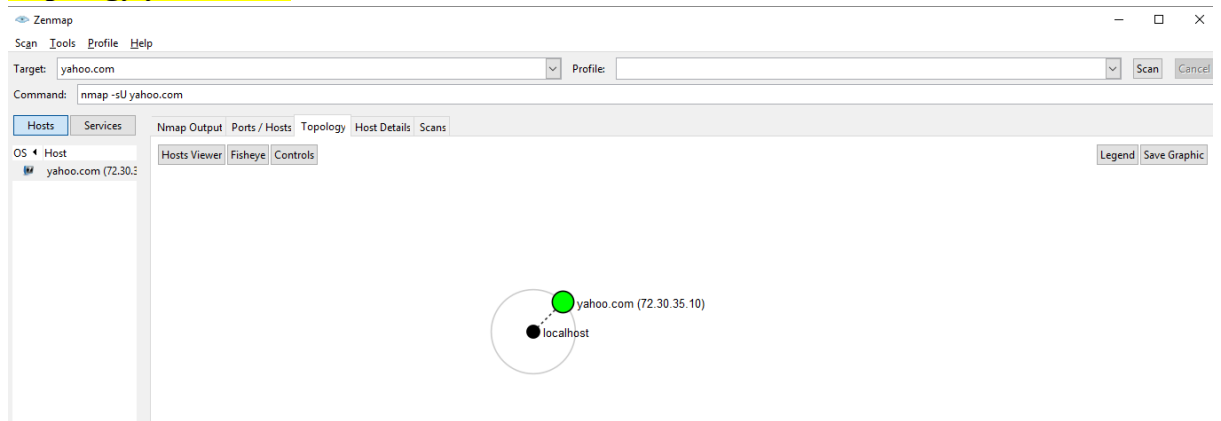
Nmap done: 1 IP address (1 host up) scanned in 351.25 seconds

sU port yahoo.com

Target: yahoo.com
Command: nmap -sU yahoo.com

Port	Protocol	State	Service	Version
80	tcp	open	http-proxy	Apache Traffic Server
443	tcp	open	http-proxy	Apache Traffic Server

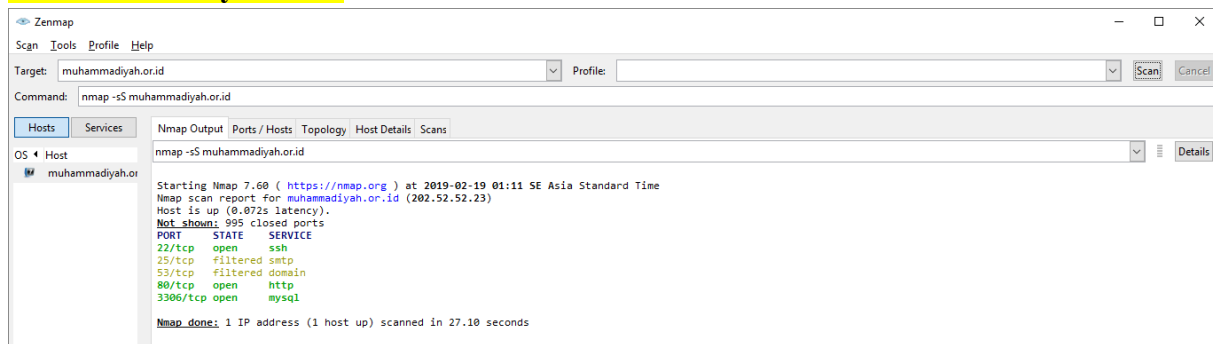
Topology yahoo.com



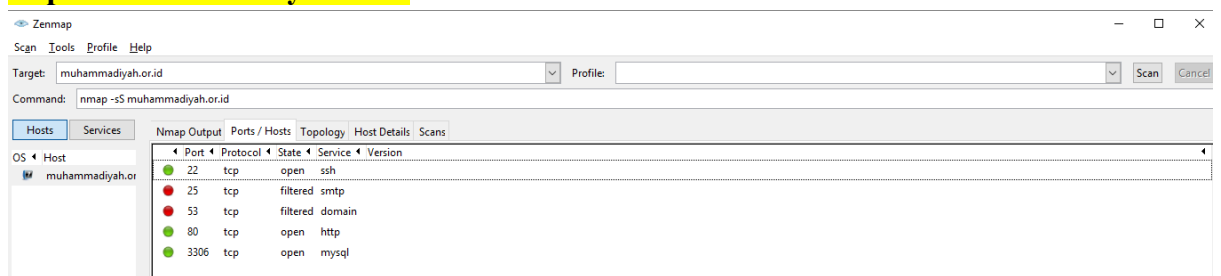
2. Domain Dalam Negeri

MUHAMMADIYAH.OR.ID

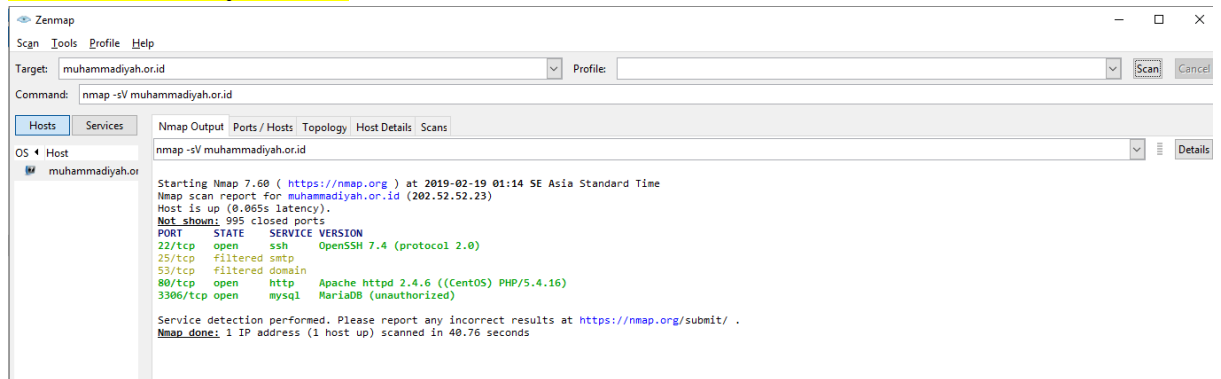
sS muhammadiyah.or.id



sS port muhammadiyah.or.id



sV muhammadiyah.or.id

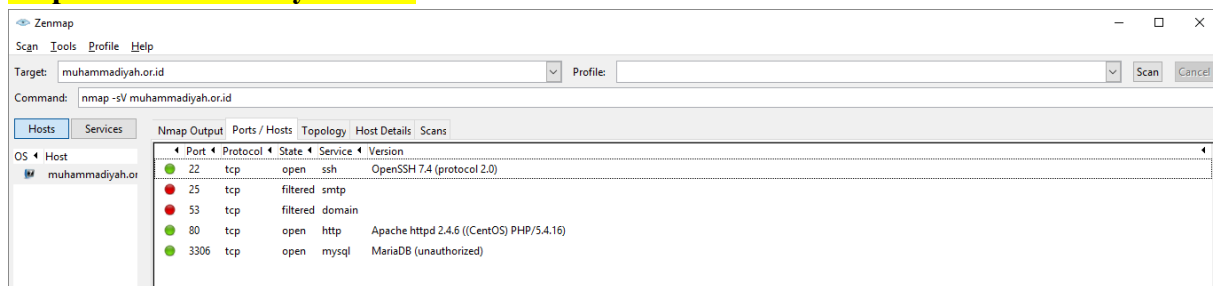


Starting Nmap 7.60 (<https://nmap.org>) at 2019-02-19 01:14 SE Asia Standard Time
Nmap scan report for muhammadiyah.or.id (202.52.52.23)
Host is up (0.065s latency).
Not shown: 995 closed ports

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.4 (protocol 2.0)
25/tcp	filtered	smtp	
53/tcp	filtered	domain	
80/tcp	open	http	Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
3306/tcp	open	mysql	MariaDB (unauthorized)

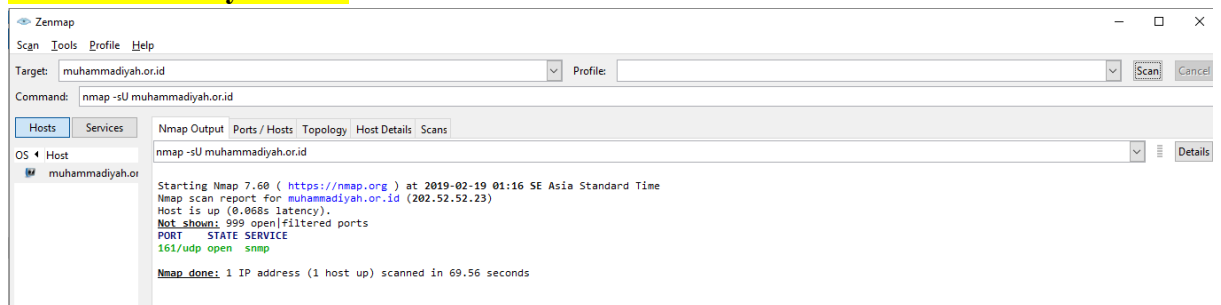
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 40.76 seconds

sV port muhammadiyah.or.id



Port	Protocol	State	Service	Version
22	tcp	open	ssh	OpenSSH 7.4 (protocol 2.0)
25	tcp	filtered	smtp	
53	tcp	filtered	domain	
80	tcp	open	http	Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
3306	tcp	open	mysql	MariaDB (unauthorized)

sU muhammadiyah.or.id

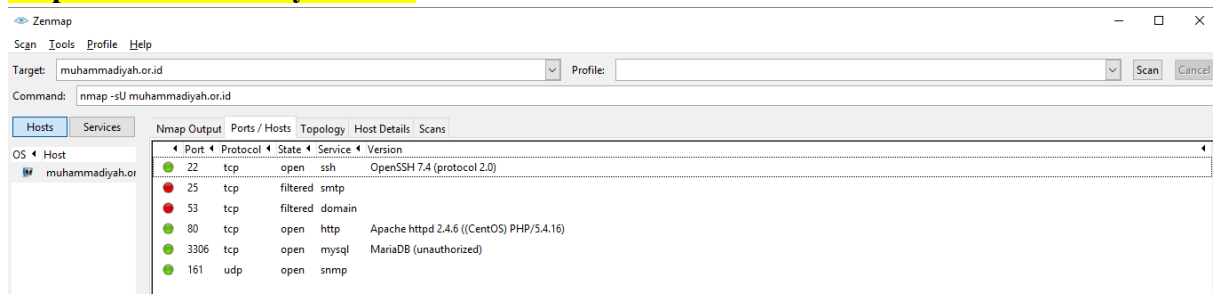


Starting Nmap 7.60 (<https://nmap.org>) at 2019-02-19 01:16 SE Asia Standard Time
Nmap scan report for muhammadiyah.or.id (202.52.52.23)
Host is up (0.065s latency).
Not shown: 999 open|filtered ports

PORT	STATE	SERVICE
161/udp	open	snmp

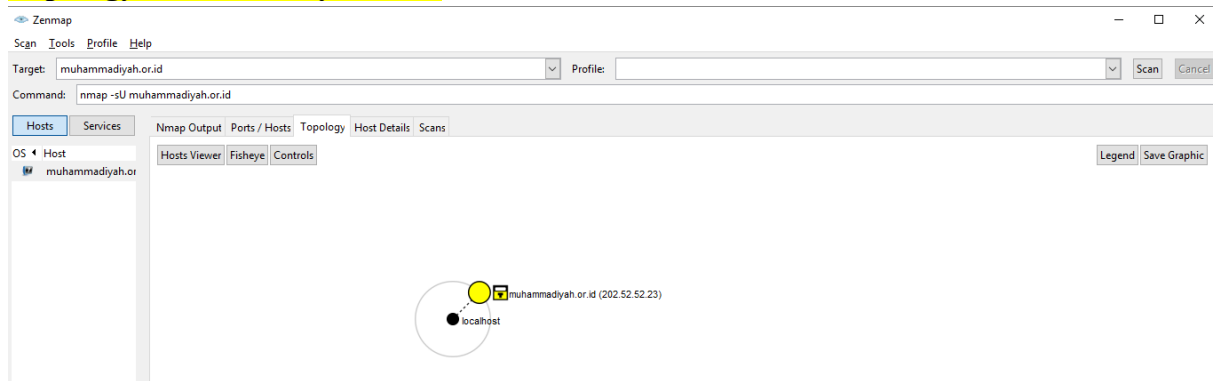
Nmap done: 1 IP address (1 host up) scanned in 69.56 seconds

sU port muhammadiyah.or.id



Port	Protocol	State	Service	Version
22	tcp	open	ssh	OpenSSH 7.4 (protocol 2.0)
25	tcp	filtered	smtp	
53	tcp	filtered	domain	
80	tcp	open	http	Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
3306	tcp	open	mysql	MariaDB (unauthorized)
161	udp	open	snmp	

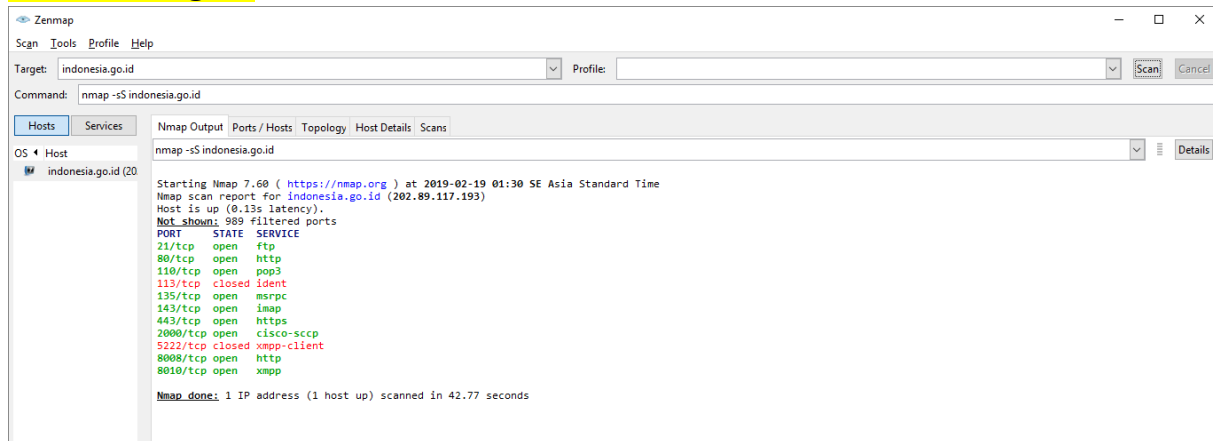
Topology muhammadiyah.or.id



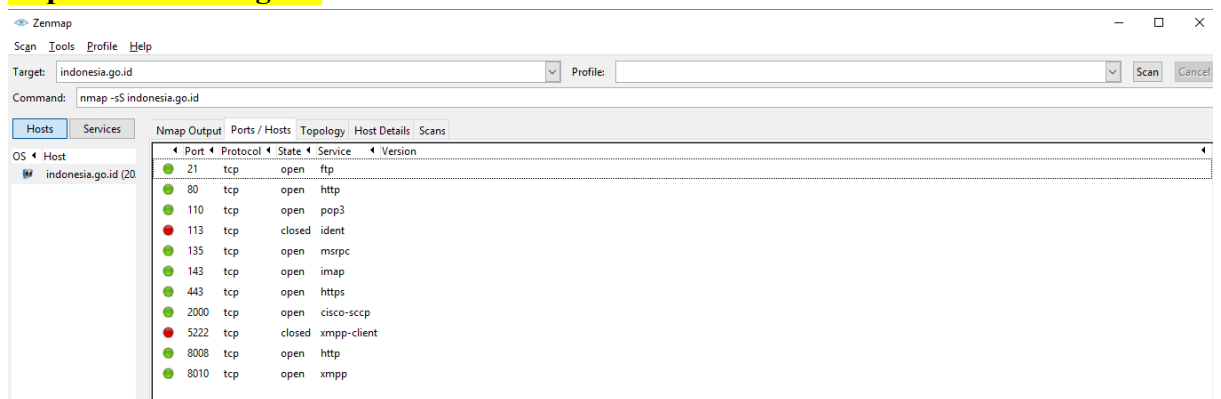
3. Domain pemerintahan

INDONESIA.GO.ID

sS Indonesia.go.id



sS port Indonesia.go.id



SV Indonesia.go.id

```
ap scan report for indonesia.go.id (202.89.117.193)
Host is up (0.13s latency).
Not shown: 989 filtered ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp?
80/tcp    open  http             Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.6.36)
110/tcp   open  pop3
113/tcp   closed ident
135/tcp   open  msrpc?
143/tcp   open  imap?
443/tcp   open  ssl/http        Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.6.36)
2000/tcp  open  cisco-scp?
5222/tcp  closed xmpp-client
8008/tcp  open  http
8010/tcp  open  ssl/http-proxy  FortiGate Web Filtering Service
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8008-TCP:V=7.60%I=7KD=2/19%Time=SCGAFAGENP=i686-pc-windows-windows%
SE:IP(GetRequest,CC,"HTTP/1.1,x20302\x20Found\r\nLocation:\x20https://:801
SE:0/\r\nConnection:\x20close\r\nX-Frame-Options:\x20SAMEORIGIN\r\nX-XSS-P
SE:Protection:\x201;\x20mode=block\r\nX-Content-Type-Options:\x20nosniff\r\n
SE:nContent-Security-Policy:\x20frame-ancestors\r\n\r\n")&#x20(FourOnFourRequ
SE:est,EF,"HTTP/1.1,x20302\x20Found\r\nLocation:\x20https://:8010/nice%20
SE:ports&C/Trajectory,tX%20bak\r\nConnection:\x20close\r\nX-Frame-Option
SE:s:\x20SAMEORIGIN\r\nX-XSS-Protection:\x201;\x20mode=block\r\nX-Content-
SE:iType-Options:\x20nosniff\r\nContent-Security-Policy:\x20frame-ancestors
SE:i\r\n\r\n")&#x20(GenericLines,CB,"HTTP/1.1,x20302\x20Found\r\nLocation:\x2
SE:0https://:8010\r\nConnection:\x20close\r\nX-Frame-Options:\x20SAMEORIGI
SE:\r\nX-XSS-Protection:\x201;\x20mode=block\r\nX-Content-Type-Options:\x
SE:i20nosniff\r\nContent-Security-Policy:\x20frame-ancestors\r\n\r\n")&#x20
SE:iTPOptions,CB,"HTTP/1.1,x20302\x20Found\r\nLocation:\x20https://:8010\r
SE:i\r\nConnection:\x20close\r\nX-Frame-Options:\x20SAMEORIGIN\r\nX-XSS-Prote
SE:ction:\x201;\x20mode=block\r\nX-Content-Type-Options:\x20nosniff\r\nCon
SE:intent-Security-Policy:\x20frame-ancestors\r\n\r\n")&#x20(RTSRequest,CB,"HT
SE:IP/1.1,x20302\x20Found\r\nLocation:\x20https://:8010\r\nConnection:\x2
SE:0close\r\nX-Frame-Options:\x20SAMEORIGIN\r\nX-XSS-Protection:\x201;\x20
SE:mode=block\r\nX-Content-Type-Options:\x20nosniff\r\nContent-Security-Po
SE:licy:\x20frame-ancestors\r\n\r\n");
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.21 seconds
```

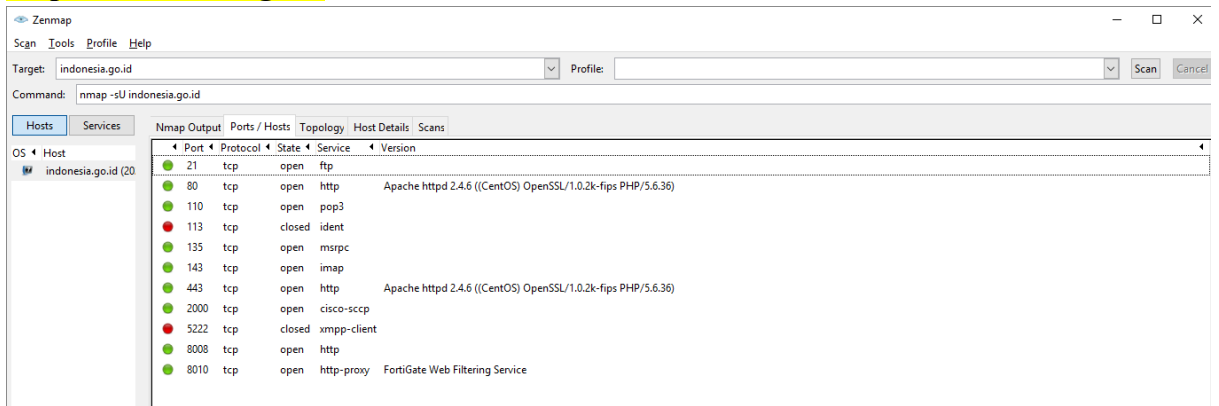
SV port Indonesia.go.id

Port	Protocol	State	Service	Version
21	tcp	open	ftp	
80	tcp	open	http	Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.6.36)
110	tcp	open	pop3	
113	tcp	closed	ident	
135	tcp	open	msrpc	
143	tcp	open	imap	
443	tcp	open	http	Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.6.36)
2000	tcp	open	cisco-scp	
5222	tcp	closed	xmpp-client	
8008	tcp	open	http	
8010	tcp	open	http-proxy	FortiGate Web Filtering Service

sU Indonesia.go.id

```
Starting Nmap 7.60 ( https://nmap.org ) at 2019-02-19 01:36 SE Asia Standard Time
Nmap scan report for indonesia.go.id (202.89.117.193)
Host is up (0.076s latency).
All 1000 scanned ports on indonesia.go.id (202.89.117.193) are open/filtered
Nmap done: 1 IP address (1 host up) scanned in 100.00 seconds
```

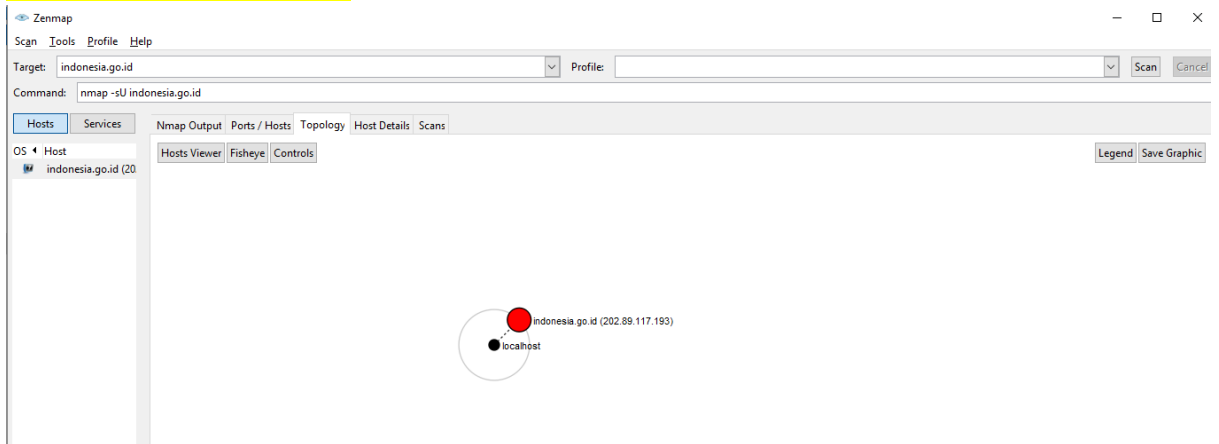
sU port Indonesia.go.id



Zenmap interface showing the results of an nmap scan for indonesia.go.id. The command used is nmap -sU indonesia.go.id. The scan results are displayed in a table with columns for Port, Protocol, State, Service, and Version.

Port	Protocol	State	Service	Version
21	tcp	open	ftp	
80	tcp	open	http	Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.6.36)
110	tcp	open	pop3	
113	tcp	closed	ident	
135	tcp	open	msrpc	
143	tcp	open	imap	
443	tcp	open	http	Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.6.36)
2000	tcp	open	cisco-scp	
5222	tcp	closed	xmpp-client	
8008	tcp	open	http	
8010	tcp	open	http-proxy	FortiGate Web Filtering Service

Topology Indonesia.go.id



Zenmap interface showing the Topology view for indonesia.go.id. The diagram illustrates the connection between the local host and the target host, indonesia.go.id (202.89.117.193).

Legend: Save Graphic