

**Scanning Website**  
**Tugas 2 Keamanan Jaringan Komputer**



**Oleh :**

**Siti Aisyah**

**09011181621024**

**Kelas : SK8P Indralaya**

**Dosen pengampu : Deris Stiawan, M.T., Ph.D.**

**Jurusan Sistem Komputer**  
**Fakultas Ilmu Komputer**  
**Universitas Sriwijaya**

## 1. Nmap 7.70

### a. Tokopedia.com

```
$ nmap -sS www.tokopedia.com
```

```
Address      : 47.88.140.11
```

Port	Protocol	State	Service
53	Tcp	Open	domain
80	Tcp	Open	http
443	Tcp	Open	https

```
$ nmap -sU www.tokopedia.com
```

Port	Protocol	State	Service
53	Udp	Open	domain

```
$ nmap -sV www.tokopedia.com
```

Port	Protocol	State	Service	Version
53	tcp	Open	Domain	(generic dns response:NOTIMP)
80	tcp	Open	http	
443	tcp	Open	https	

\$ nmap -A [www.tokopedia.com](http://www.tokopedia.com)

Zenmap

Scan Tools Profile Help

Target:  Profile:

Command:

Hosts Services

OS Host

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

```
nmap -A www.tokopedia.com
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-18 09:45 SE Asia Standard Time
Nmap scan report for www.tokopedia.com (47.88.232.2)
Host is up (0.015s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      (generic dns response: NOTIMP)
80/tcp    open  http
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 301 Moved Permanently
|     Date: Mon, 18 Feb 2019 02:45:37 GMT
|     Content-Type: text/html
|     Content-Length: 178
|     Connection: close
|     Location: https://accounts.tokopedia.com/
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Cache-Control: no-cache, no-store, must-revalidate
|     <html>
|     <head><title>301 Moved Permanently</title></head>
```

**Warning:** OSscan results may be unreliable because we could not find at least 1 open and 1 closed port

**Aggressive OS guesses:** Linux 3.2 - 3.16 (91%), Linux 3.4 (91%), Linux 2.6.32 - 3.10 (90%), Linux 2.6.32 - 3.13 (90%), Linux 3.10 (90%), Linux 3.2 (89%), Android 4.1 (88%), MikroTik RouterOS 6.37 (88%), Linux 2.6.38 (88%), MikroTik RouterOS 6.33 (87%)

No exact OS matches for host (test conditions non-ideal).

**Network Distance:** 1 hop

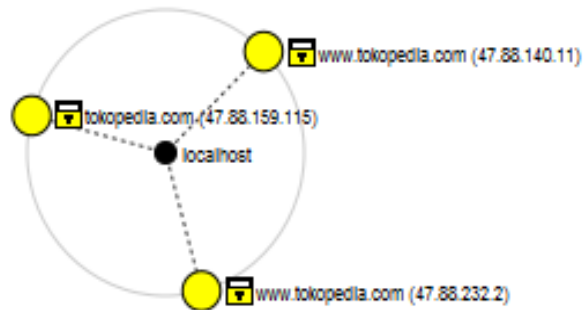
TRACEROUTE (using port 53/tcp)

HOP	RTT	ADDRESS
1	18.00 ms	47.88.232.2

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 89.18 seconds

## Topology



### b. Indonesia.go.id

\$ nmap -sS [www.indonesia.go.id](http://www.indonesia.go.id)

Address : 202.89.117.193

Port	Protocol	State	Service
21	Tcp	Open	ftp
25	Tcp	Open	smtp
53	Tcp	Open	domain
80	Tcp	Open	http
110	Tcp	Open	pop3
113	Tcp	Close	ident
135	tcp	Open	msrpc
143	Tcp	Open	imap
443	Tcp	Open	https
2000	Tcp	Open	cisco-sccp
5222	Tcp	Close	xmpp-client
8008	Tcp	Open	http
8010	Tcp	Open	xmpp

\$ nmap -sU [www.indonesia.go.id](http://www.indonesia.go.id)

Port	Protocol	State	Service
53	udp	Open	domain
1024	udp	Close	unknown

\$ nmap -sV www.indonesia.go.id

Port	Protocol	State	Service	Version
21	tcp	Open	ftp	
25	tcp	Open	smtp	
53	tcp	Open	domain	(generic dns response: NOTIMP)
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	Close	ident	
135	tcp	Open	msrpc	
143	tcp	Open	imap	
443	tcp	Open	https	Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.6.36)
2000	tcp	Open	cisco-sccp	
5222	tcp	Close	xmpp-client	
8008	tcp	Open	http	
8010	tcp	Open	http-proxy	FortiGate Web Filtering Service

\$ nmap -A [www.indonesia.go.id](http://www.indonesia.go.id)

Zenmap

Scan Tools Profile Help

Target:  Profile:

Command:

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

www.indonesia.go.

```
nmap -A www.indonesia.go.id
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-18 09:59 SE Asia Standard Time
Nmap scan report for www.indonesia.go.id (202.89.117.193)
Host is up (0.23s latency).
Not shown: 987 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp?
25/tcp    open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
53/tcp    open  domain      (generic dns response: NOTIMP)
80/tcp    open  http        Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.6.36)
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.36
|_http-title: Did not follow redirect to https://indonesia.go.id/
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)
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.36
|_http-title: 400 Bad Request
|_ssl-cert: Subject: commonName=*.indonesia.go.id
```

Filter Hosts

Target:

Command:

Hosts Services

OS Host

www.indonesia.go.

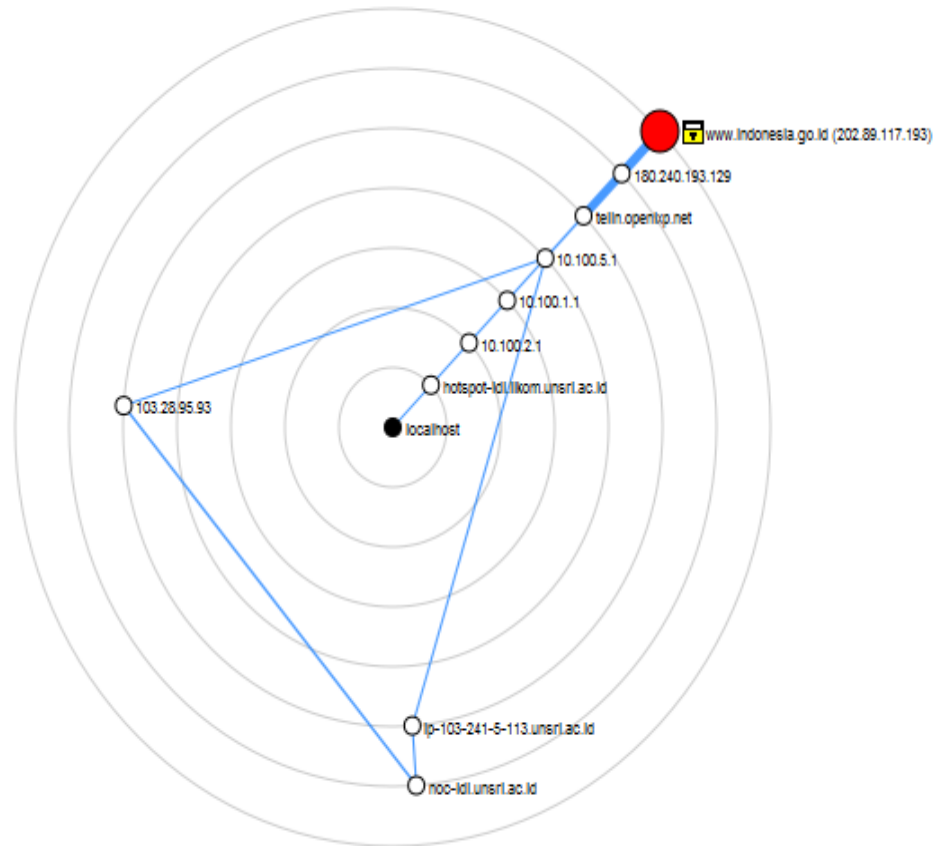
Nmap Output Ports / Hosts Topology Host Details Scans

nmap -A www.indonesia.go.id

```
|_ss1-date: 1LS randomness does not represent time
2000/tcp open  cisco-sccp?
5222/tcp closed xmpp-client
8008/tcp open  http
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 302 Found
|     Location: https://:8010/nice%20ports%2C/Tri%6Eity.txt%2ebak
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors
|   GenericLines, HTTPOptions, RTSPRequest, SIPOptions:
|     HTTP/1.1 302 Found
|     Location: https://:8010
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
```

Filter Hosts

## Topology



c. [perex.com](http://perex.com)

\$ nmap -sS [www.perex.com](http://www.perex.com)

Address : 104.236.219.51

Port	Protocol	State	Service
22	tcp	Filtered	ssh
53	tcp	Open	domain
80	tcp	Open	http
3306	tcp	Open	mysql



\$ nmap -sV [www.perex.com](http://www.perex.com)

Port	Protocol	State	Service	Version
22	tcp	filtered	ssh	
53	tcp	Open	domain	(generic dns response: NOTIMP)
80	tcp	Open	http	Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
3306	tcp	Open	mysql	MySQL 5.5.52-MariaDB

\$ nmap -A [www.perex.com](http://www.perex.com)

Zenmap

Scan Tools Profile Help

Target:  Profile:

Command:

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

www.perex.com (1)

```
nmap -A www.perex.com
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-18 10:45 SE Asia Standard Time
Nmap scan report for www.perex.com (104.236.219.51)
Host is up (0.48s latency).
rDNS record for 104.236.219.51: perex.com
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
22/tcp    filtered ssh
53/tcp    open  domain (generic dns response: NOTIMP)
80/tcp    open  http   Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
| http-title: Personality Expert: Free Professional Online Personality Test
|_Requested resource was http://www.perex.com/index.php
3306/tcp  open  mysql  MySQL 5.5.52-MariaDB
| mysql-info:
|   Protocol: 10
|   Version: 5.5.52-MariaDB
|   Thread ID: 216621
|   Capabilities flags: 63487
```

# Topology

---

