

# **KEAMANAN JARINGAN KOMPUTER**

## **Scanner Web Vulnerability**



Oleh :

**NAMA : SYUKRAN RIZKI**

**NIM : 09011181520019**

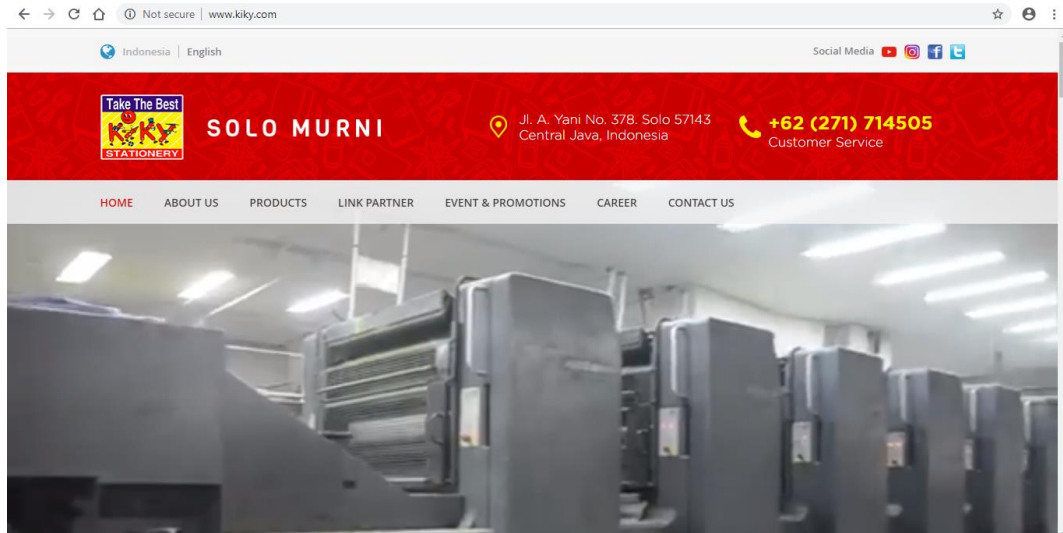
**FAKULTAS ILMU KOMPUTER**

**JURUSAN SISTEM KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

# Kiky

Website <http://www.kiky.com>



## 1. Nmap

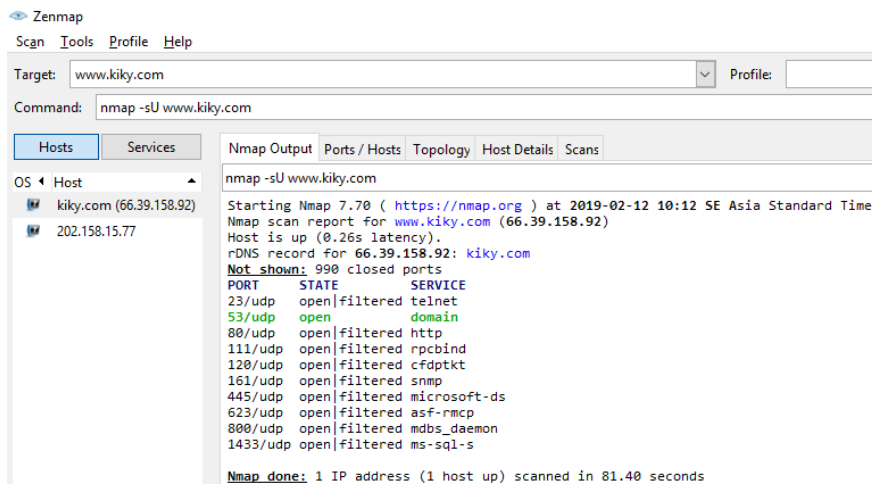
**Nmap** menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, system operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya.

```
Zenmap
Scan Tools Profile Help
Target: www.kiky.com Profile:
Command: nmap -sV www.kiky.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
kiky.com (66.39.158.92)
202.158.15.77

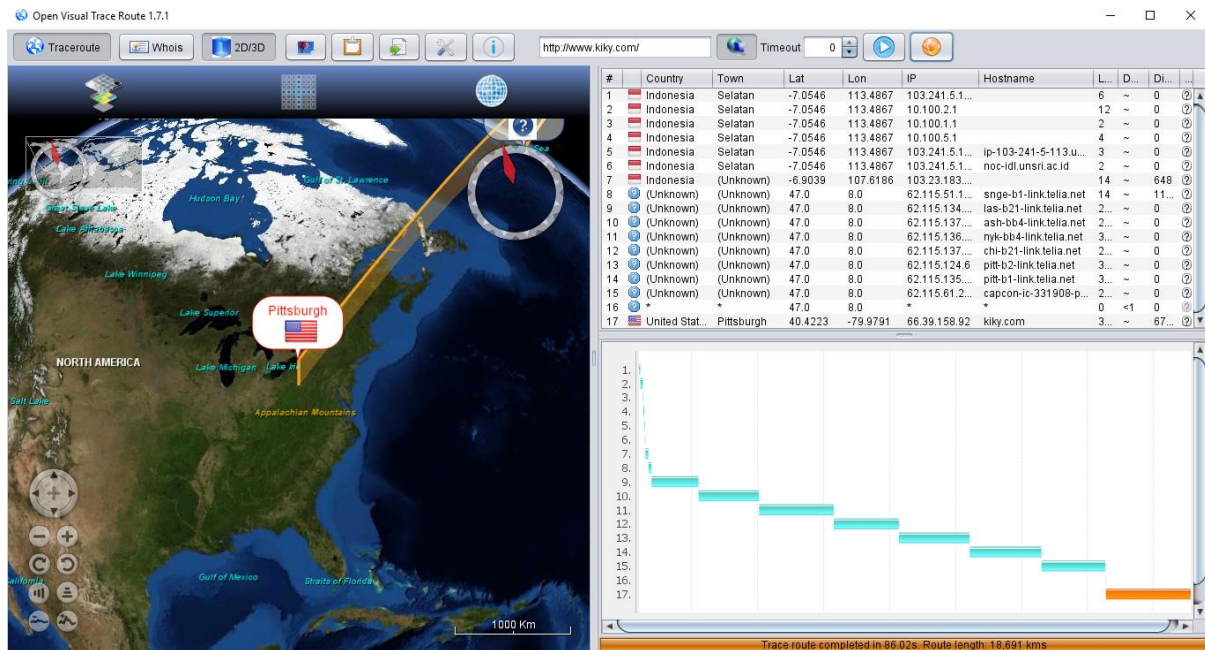
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-12 10:08 SE Asia Standard Time
Nmap scan report for www.kiky.com (66.39.158.92)
Host is up (0.26s latency).
rDNS record for 66.39.158.92: kiky.com
Not shown: 980 closed ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              ProFTPD
22/tcp    filtered ssh
23/tcp    filtered telnet
53/tcp    open  domain           ISC BIND 9.8.4-rpz2+r1005.12-P1
80/tcp    open  http             Apache httpd 2.4.38
111/tcp   filtered rpcbind
161/tcp   filtered snmp
445/tcp   filtered microsoft-ds
544/tcp   open  tcpwrapped
800/tcp   filtered mds_daemon
1433/tcp   filtered ms-sql-s
2185/tcp  open  tcpwrapped
5666/tcp  filtered nrpe
5900/tcp  filtered vnc
6667/tcp  filtered irc
7000/tcp  filtered afs3-filer
7001/tcp  filtered afs3-callback
7007/tcp  filtered afs3-bos
7777/tcp  filtered cbt
31337/tcp filtered Elite

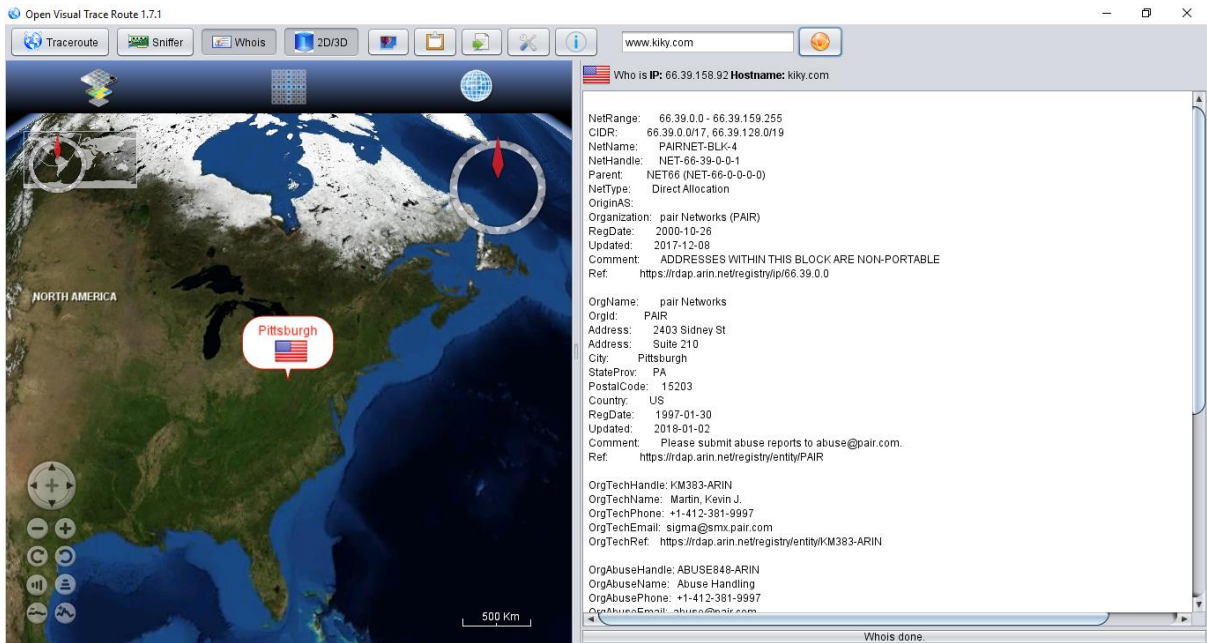
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 74.70 seconds
```



## 2. Open Visual Trace Route 1.7.1

Aplikasi Trace Route ini adalah untuk untuk menunjukkan **route** yang dilewati sebuah paket untuk mencapai tujuannya dengan mengirimkan pesan Internet Control Message Protocol (ICMP) Echo Request ke tujuan berdasarkan alamat IP tujuan dengan nilai Time to Live yang semakin meningkat, Rute yang ditampilkan adalah daftar interface router (yang paling dekat dengan host) yang terdapat pada jalur antara host dan tujuan.





Hasil dari **Who Is IP** ini adalah untuk mengetahui informasi lebih lanjut mengenai IP atau HOSTNAME yang sedang di trace di aplikasi *Open Visual Trace Route*.

### 3. Nikto (Scanning Web in Ubuntu Terminal)

*Nikto* adalah alat scanning aplikasi web yang mencari kesalahan konfigurasi, direktori web diakses secara terbuka dan sejumlah kerentanan aplikasi web. Disini saya mencetak hasil scan website dari *terminal linux* ke format **HTML** dapat dilihat dibawah ini.

kiky.com / 66.39.158.92 port 80	
<b>Target IP</b>	66.39.158.92
<b>Target hostname</b>	kiky.com
<b>Target Port</b>	80
<b>HTTP Server</b>	Apache/2.4.38
<b>Site Link (Name)</b>	<a href="http://kiky.com:80">http://kiky.com:80</a>
<b>Site Link (IP)</b>	<a href="http://66.39.158.92:80">http://66.39.158.92:80</a>
<b>URI</b>	/
<b>HTTP Method</b>	GET
<b>Description</b>	Cookie PHPSESSID created without the httponly flag
<b>Test Links</b>	<a href="http://kiky.com:80/">http://kiky.com:80/</a> <a href="http://66.39.158.92:80/">http://66.39.158.92:80/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/
<b>HTTP Method</b>	GET
<b>Description</b>	The anti-clickjacking X-Frame-Options header is not present.
<b>Test Links</b>	<a href="http://kiky.com:80/">http://kiky.com:80/</a> <a href="http://66.39.158.92:80/">http://66.39.158.92:80/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/robots.txt

<b>HTTP Method</b>	GET
<b>Description</b>	Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x167 0x5146705614100
<b>Test Links</b>	<a href="http://kiky.com:80/robots.txt">http://kiky.com:80/robots.txt</a> <a href="http://66.39.158.92:80/robots.txt">http://66.39.158.92:80/robots.txt</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	//fileupload/
<b>HTTP Method</b>	GET
<b>Description</b>	File/dir '/fileupload/' in robots.txt returned a non-forbidden or redirect HTTP code ()
<b>Test Links</b>	<a href="http://kiky.com:80/fileupload/">http://kiky.com:80/fileupload/</a> <a href="http://66.39.158.92:80/fileupload/">http://66.39.158.92:80/fileupload/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/Diss/fonts/
<b>HTTP Method</b>	GET
<b>Description</b>	File/dir 'Diss/fonts/' in robots.txt returned a non-forbidden or redirect HTTP code ()
<b>Test Links</b>	<a href="http://kiky.com:80/Diss/fonts/">http://kiky.com:80/Diss/fonts/</a> <a href="http://66.39.158.92:80/Diss/fonts/">http://66.39.158.92:80/Diss/fonts/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/Diss/images/
<b>HTTP Method</b>	GET
<b>Description</b>	File/dir 'Diss/images/' in robots.txt returned a non-forbidden or redirect HTTP code ()
<b>Test Links</b>	<a href="http://kiky.com:80/Diss/images/">http://kiky.com:80/Diss/images/</a> <a href="http://66.39.158.92:80/Diss/images/">http://66.39.158.92:80/Diss/images/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/Diss/img/
<b>HTTP Method</b>	GET
<b>Description</b>	File/dir 'Diss/img/' in robots.txt returned a non-forbidden or redirect HTTP code ()
<b>Test Links</b>	<a href="http://kiky.com:80/Diss/img/">http://kiky.com:80/Diss/img/</a> <a href="http://66.39.158.92:80/Diss/img/">http://66.39.158.92:80/Diss/img/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/Diss/inc/
<b>HTTP Method</b>	GET
<b>Description</b>	File/dir 'Diss/inc/' in robots.txt returned a non-forbidden or redirect HTTP code ()
<b>Test Links</b>	<a href="http://kiky.com:80/Diss/inc/">http://kiky.com:80/Diss/inc/</a> <a href="http://66.39.158.92:80/Diss/inc/">http://66.39.158.92:80/Diss/inc/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/Diss/js/
<b>HTTP Method</b>	GET
<b>Description</b>	File/dir 'Diss/js/' in robots.txt returned a non-forbidden or redirect HTTP code ()
<b>Test Links</b>	<a href="http://kiky.com:80/Diss/js/">http://kiky.com:80/Diss/js/</a> <a href="http://66.39.158.92:80/Diss/js/">http://66.39.158.92:80/Diss/js/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/Diss/licenses/
<b>HTTP Method</b>	GET
<b>Description</b>	File/dir 'Diss/licenses/' in robots.txt returned a non-forbidden or redirect HTTP code ()
<b>Test Links</b>	<a href="http://kiky.com:80/Diss/licenses/">http://kiky.com:80/Diss/licenses/</a> <a href="http://66.39.158.92:80/Diss/licenses/">http://66.39.158.92:80/Diss/licenses/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>

<b>URI</b>	/Diss/localexport/
<b>HTTP Method</b>	GET
<b>Description</b>	File/dir 'Diss/localexport/' in robots.txt returned a non-forbidden or redirect HTTP code ()
<b>Test Links</b>	<a href="http://kiky.com:80/Diss/localexport/">http://kiky.com:80/Diss/localexport/</a> <a href="http://66.39.158.92:80/Diss/localexport/">http://66.39.158.92:80/Diss/localexport/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/Diss/loker/
<b>HTTP Method</b>	GET
<b>Description</b>	File/dir 'Diss/loker/' in robots.txt returned a non-forbidden or redirect HTTP code ()
<b>Test Links</b>	<a href="http://kiky.com:80/Diss/loker/">http://kiky.com:80/Diss/loker/</a> <a href="http://66.39.158.92:80/Diss/loker/">http://66.39.158.92:80/Diss/loker/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/Diss/office/
<b>HTTP Method</b>	GET
<b>Description</b>	File/dir 'Diss/office/' in robots.txt returned a non-forbidden or redirect HTTP code ()
<b>Test Links</b>	<a href="http://kiky.com:80/Diss/office/">http://kiky.com:80/Diss/office/</a> <a href="http://66.39.158.92:80/Diss/office/">http://66.39.158.92:80/Diss/office/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	//produk/
<b>HTTP Method</b>	GET
<b>Description</b>	File/dir '/produk/' in robots.txt returned a non-forbidden or redirect HTTP code ()
<b>Test Links</b>	<a href="http://kiky.com:80//produk/">http://kiky.com:80//produk/</a> <a href="http://66.39.158.92:80//produk/">http://66.39.158.92:80//produk/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/Diss/user_data/
<b>HTTP Method</b>	GET
<b>Description</b>	File/dir 'Diss/user_data/' in robots.txt returned a non-forbidden or redirect HTTP code ()
<b>Test Links</b>	<a href="http://kiky.com:80/Diss/user_data/">http://kiky.com:80/Diss/user_data/</a> <a href="http://66.39.158.92:80/Diss/user_data/">http://66.39.158.92:80/Diss/user_data/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/Diss/member/
<b>HTTP Method</b>	GET
<b>Description</b>	File/dir 'Diss/member/' in robots.txt returned a non-forbidden or redirect HTTP code ()
<b>Test Links</b>	<a href="http://kiky.com:80/Diss/member/">http://kiky.com:80/Diss/member/</a> <a href="http://66.39.158.92:80/Diss/member/">http://66.39.158.92:80/Diss/member/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/robots.txt
<b>HTTP Method</b>	GET
<b>Description</b>	"robots.txt" contains 16 entries which should be manually viewed.
<b>Test Links</b>	<a href="http://kiky.com:80/robots.txt">http://kiky.com:80/robots.txt</a> <a href="http://66.39.158.92:80/robots.txt">http://66.39.158.92:80/robots.txt</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>

## Host Summary

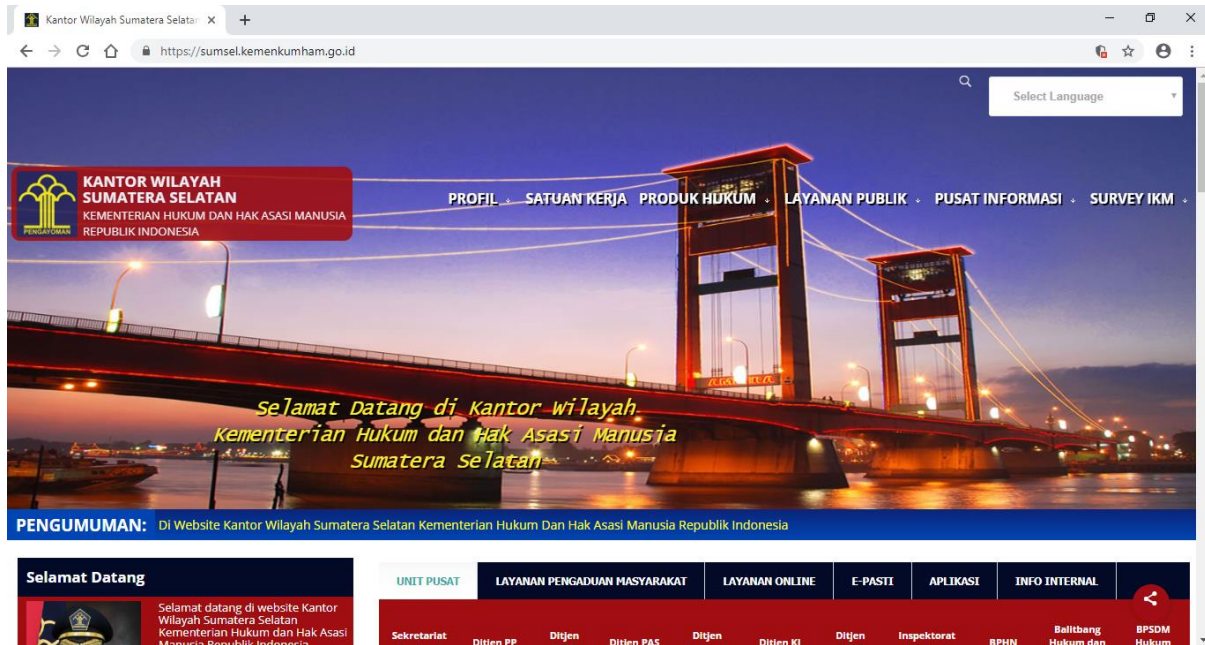
<b>Start Time</b>	1970-01-01 07:00:00
<b>End Time</b>	2019-02-14 20:34:47
<b>Elapsed Time</b>	1550151287 seconds
<b>Statistics</b>	6545 items checked, errors, findings

## Scan Summary

<b>Software Details</b>	<a href="#">Nikto 2.1.5</a>
<b>CLI Options</b>	-Display V -o nikto_scan_result_kiky.html -Format html -h 66.39.158.92
<b>Hosts Tested</b>	0
<b>Start Time</b>	Thu Feb 14 18:33:13 2019
<b>End Time</b>	Thu Jan 1 07:00:00 1970
<b>Elapsed Time</b>	seconds

# KEMENKUMHAM SUMSEL

Website <https://sumsel.kemenkumham.go.id/>

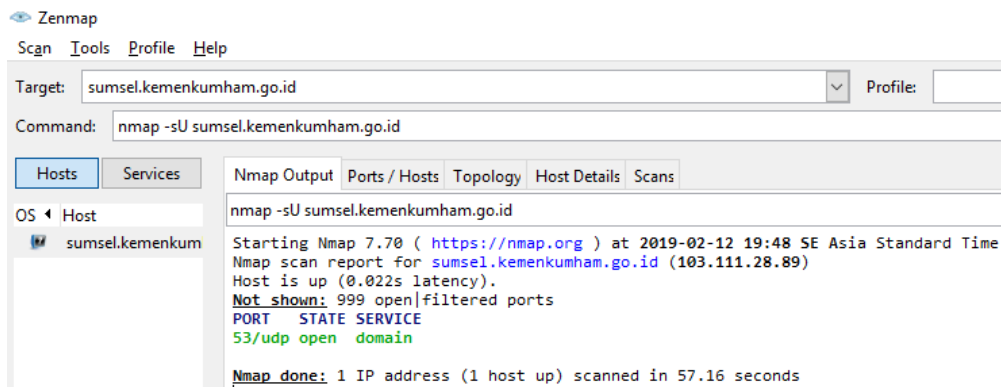


## 1. Nmap

Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, system operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya.

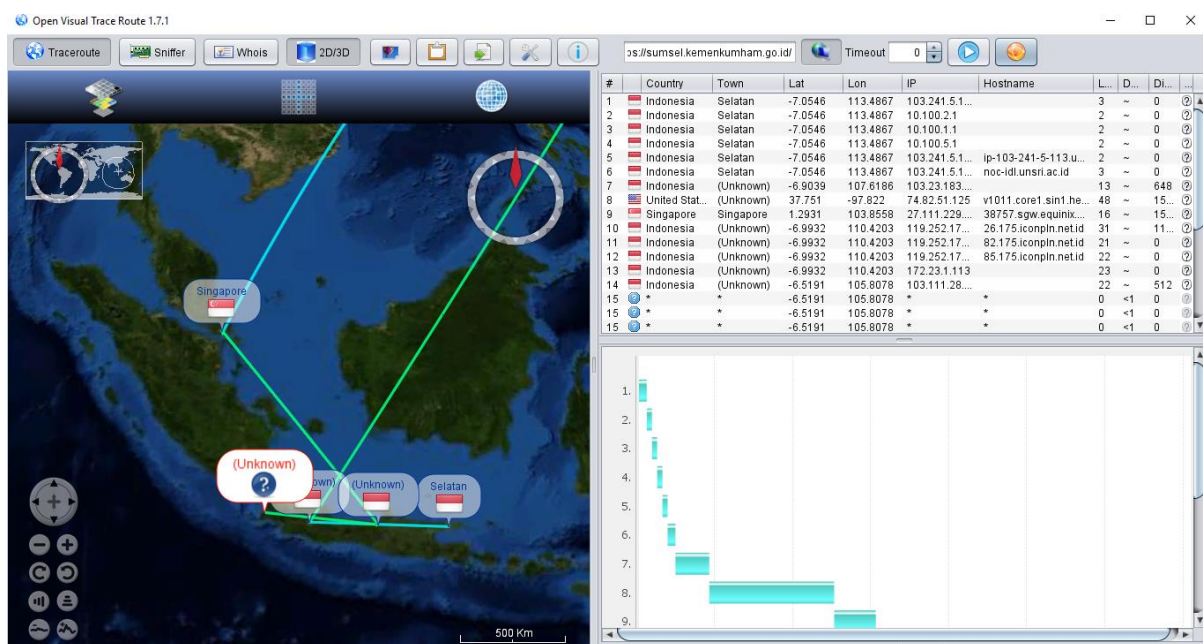
```
Zenmap
Scan Tools Profile Help
Target: sumsel.kemenkumham.go.id Profile:
Command: nmap -sV sumsel.kemenkumham.go.id
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
sumsel.kemenkumham Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-12 19:45 SE Asia Standard Time
Nmap scan report for sumsel.kemenkumham.go.id (103.111.28.89)
Host is up (0.024s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
22/tcp    filtered ssh
53/tcp    open  domain ISC BIND 9.8.4-rpz2+r1005.12-P1
80/tcp    open  http  Apache httpd 2.4.18
443/tcp   open  ssl/ssl Apache httpd (SSL-only mode)
Service Info: Host: aceh.kemenkumham.go.id
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.49 seconds
```





## 2. Open Visual Trace Route 1.7.1

Aplikasi Trace Route ini adalah untuk menunjukkan **route** yang dilewati sebuah paket untuk mencapai tujuannya dengan mengirimkan pesan Internet Control Message Protocol (ICMP) Echo Request ke tujuan berdasarkan alamat IP tujuan dengan nilai Time to Live yang semakin meningkat. Rute yang ditampilkan adalah daftar interface router (yang paling dekat dengan host) yang terdapat pada jalur antara host dan tujuan.



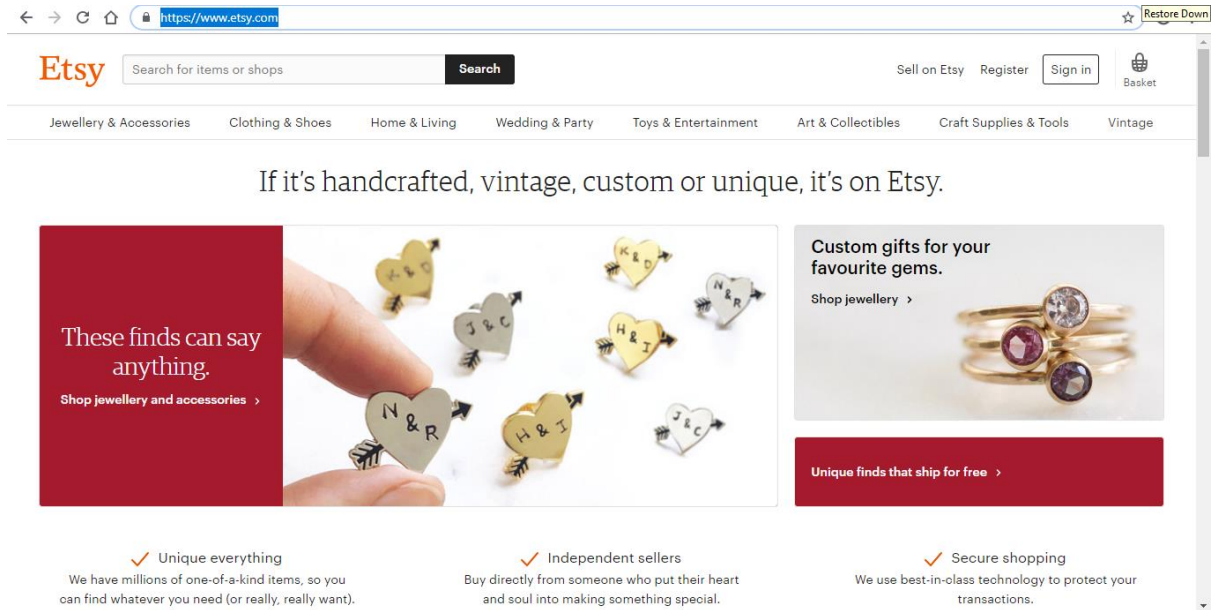
### 3. Nikto (Scanner Web in Ubuntu Terminal)

*Nikto* adalah alat scanning aplikasi web yang mencari kesalahan konfigurasi, direktori web diakses secara terbuka dan sejumlah kerentanan aplikasi web. Disini saya mencetak hasil scan website dari *terminal linux* ke format **HTML** dapat dilihat dibawah ini.

sumsel.kemenkumham.go.id / 103.111.28.89 port 443	
<b>Target IP</b>	103.111.28.89
<b>Target hostname</b>	sumsel.kemenkumham.go.id
<b>Target Port</b>	443
<b>HTTP Server</b>	Apache/2.4.18 (Ubuntu)
<b>Site Link (Name)</b>	<a href="http://sumsel.kemenkumham.go.id:443">http://sumsel.kemenkumham.go.id:443</a>
<b>Site Link (IP)</b>	<a href="http://103.111.28.89:443">http://103.111.28.89:443</a>
<b>URI</b>	/
<b>HTTP Method</b>	GET
<b>Description</b>	The anti-clickjacking X-Frame-Options header is not present.
<b>Test Links</b>	<a href="http://sumsel.kemenkumham.go.id:443/">http://sumsel.kemenkumham.go.id:443/</a> <a href="http://103.111.28.89:443/">http://103.111.28.89:443/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
Host Summary	
<b>Start Time</b>	2019-02-15 00:58:58
<b>End Time</b>	2019-02-15 01:04:09
<b>Elapsed Time</b>	311 seconds
<b>Statistics</b>	6545 items checked, 13 errors, 1 findings
Scan Summary	
<b>Software Details</b>	<a href="#">Nikto 2.1.5</a>
<b>CLI Options</b>	-Display V -o nikto_scan_result_kemenkumham.html -Format html -h https://sumsel.kemenkumham.go.id/
<b>Hosts Tested</b>	1
<b>Start Time</b>	Fri Feb 15 00:58:56 2019
<b>End Time</b>	Fri Feb 15 01:04:09 2019
<b>Elapsed Time</b>	313 seconds

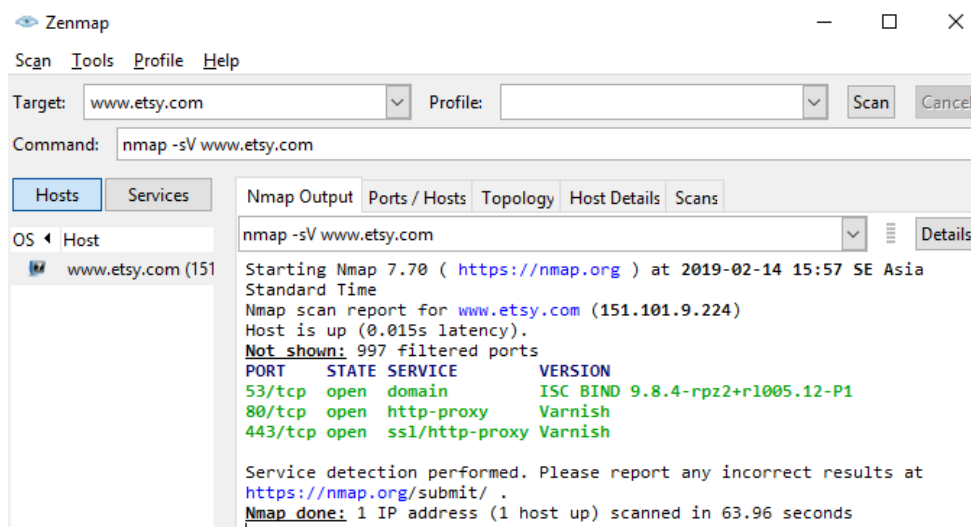
# ETSY

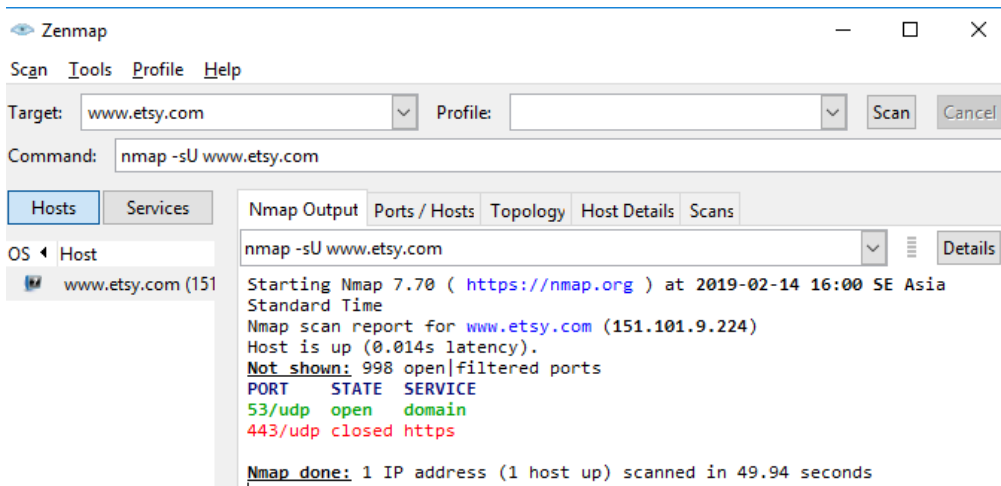
Website <https://www.etsy.com/>



## 1. Nmap

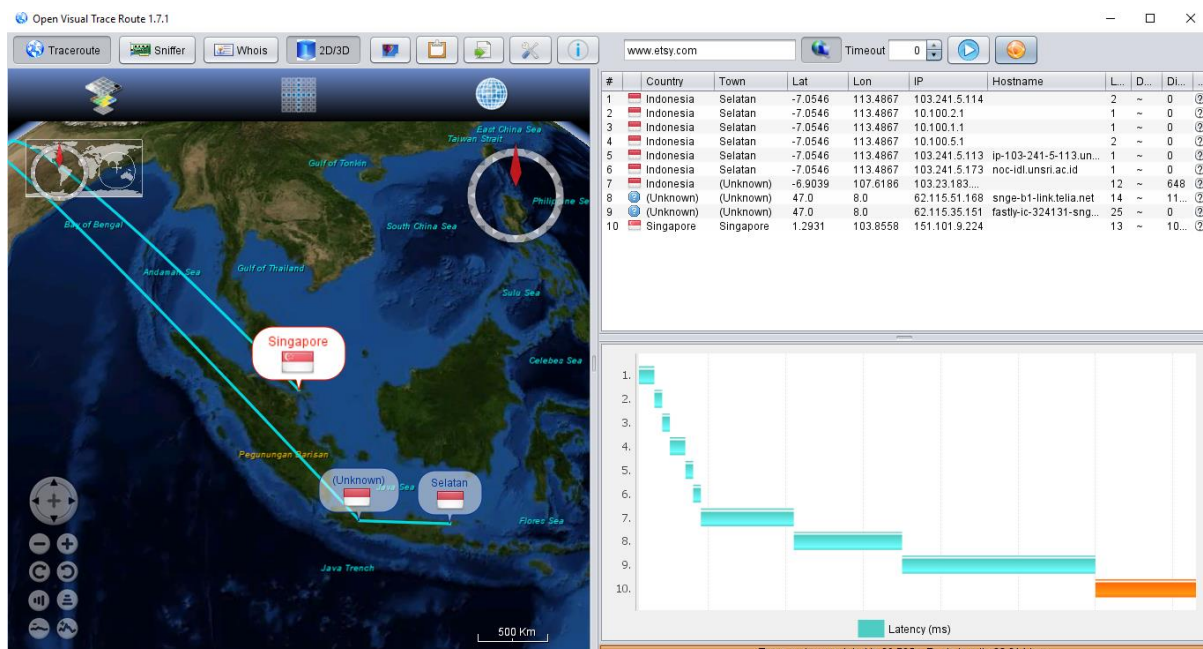
**Nmap** menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, system operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya.

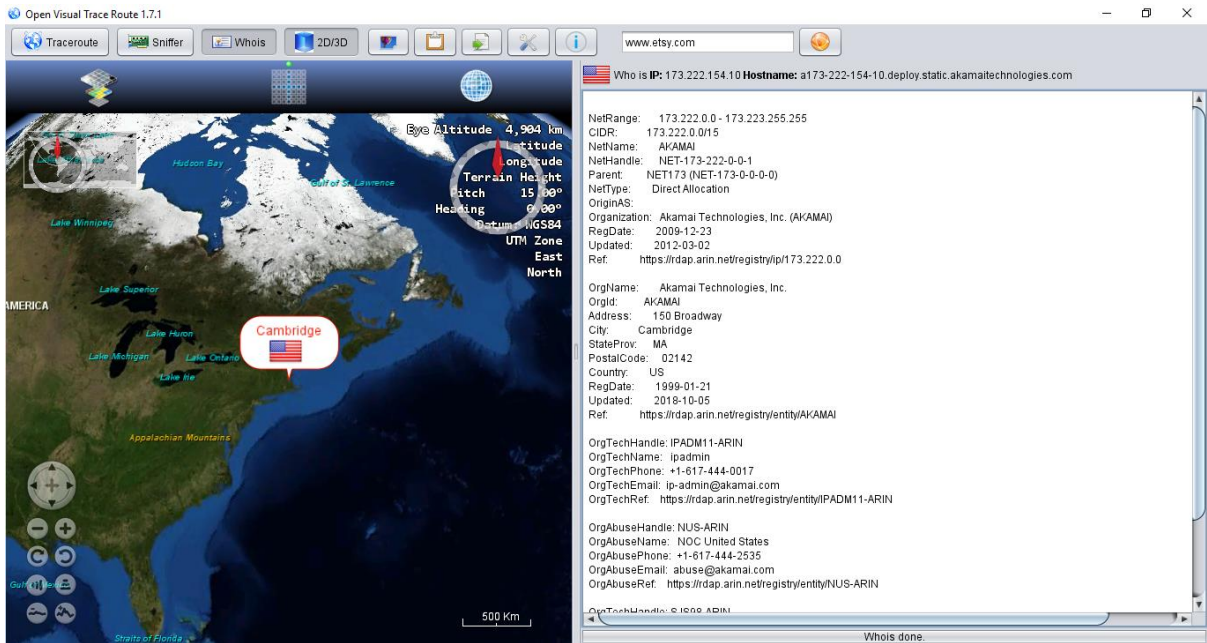




## 2. Open Visual Trace Route 1.7.1

Aplikasi Trace Route ini adalah untuk menunjukkan **route** yang dilewati sebuah paket untuk mencapai tujuannya dengan mengirimkan pesan Internet Control Message Protocol (ICMP) Echo Request ke tujuan berdasarkan alamat IP tujuan dengan nilai Time to Live yang semakin meningkat. Rute yang ditampilkan adalah daftar interface router (yang paling dekat dengan host) yang terdapat pada jalur antara host dan tujuan.





Hasil dari **Who Is IP** ini adalah untuk mengetahui informasi lebih lanjut mengenai IP atau HOSTNAME yang sedang di trace di aplikasi *Open Visual Trace Route*.

### 3. Nikto (Scanner Web in Ubuntu Terminal)

*Nikto* adalah alat scanning aplikasi web yang mencari kesalahan konfigurasi, direktori web diakses secara terbuka dan sejumlah kerentanan aplikasi web. Disini saya mencetak hasil scan website dari *terminal linux* ke format **HTML** dapat dilihat dibawah ini.

www.etsy.com / 151.101.9.224 port 80	
<b>Target IP</b>	151.101.9.224
<b>Target hostname</b>	www.etsy.com
<b>Target Port</b>	80
<b>HTTP Server</b>	Varnish
<b>Site Link (Name)</b>	<a href="http://www.etsy.com:80">http://www.etsy.com:80</a>
<b>Site Link (IP)</b>	<a href="http://151.101.9.224:80">http://151.101.9.224:80</a>
<b>URI</b>	/
<b>HTTP Method</b>	GET
<b>Description</b>	Retrieved via header: 1.1 varnish
<b>Test Links</b>	<a href="http://www.etsy.com:80/">http://www.etsy.com:80/</a> <a href="http://151.101.9.224:80/">http://151.101.9.224:80/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/
<b>HTTP Method</b>	GET
<b>Description</b>	Retrieved x-served-by header: cache-sin18023-SIN
<b>Test Links</b>	<a href="http://www.etsy.com:80/">http://www.etsy.com:80/</a> <a href="http://151.101.9.224:80/">http://151.101.9.224:80/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/

<b>HTTP Method</b>	GET
<b>Description</b>	The anti-clickjacking X-Frame-Options header is not present.
<b>Test Links</b>	<a href="http://www.etsy.com:80/">http://www.etsy.com:80/</a> <a href="http://151.101.9.224:80/">http://151.101.9.224:80/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/
<b>HTTP Method</b>	GET
<b>Description</b>	Uncommon header 'x-timer' found, with contents: S1550157315.161464.VS0,VE0
<b>Test Links</b>	<a href="http://www.etsy.com:80/">http://www.etsy.com:80/</a> <a href="http://151.101.9.224:80/">http://151.101.9.224:80/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/
<b>HTTP Method</b>	GET
<b>Description</b>	Uncommon header 'x-cache' found, with contents: MISS
<b>Test Links</b>	<a href="http://www.etsy.com:80/">http://www.etsy.com:80/</a> <a href="http://151.101.9.224:80/">http://151.101.9.224:80/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/
<b>HTTP Method</b>	GET
<b>Description</b>	Uncommon header 'x-served-by' found, with contents: cache-sin18023-SIN
<b>Test Links</b>	<a href="http://www.etsy.com:80/">http://www.etsy.com:80/</a> <a href="http://151.101.9.224:80/">http://151.101.9.224:80/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>URI</b>	/
<b>HTTP Method</b>	GET
<b>Description</b>	Uncommon header 'x-cache-hits' found, with contents: 0
<b>Test Links</b>	<a href="http://www.etsy.com:80/">http://www.etsy.com:80/</a> <a href="http://151.101.9.224:80/">http://151.101.9.224:80/</a>
<b>OSVDB Entries</b>	<a href="#">OSVDB-0</a>
<b>Host Summary</b>	
<b>Start Time</b>	2019-02-14 22:15:15
<b>End Time</b>	2019-02-14 22:18:29
<b>Elapsed Time</b>	194 seconds
<b>Statistics</b>	6545 items checked, 0 errors, 7 findings
<b>Scan Summary</b>	
<b>Software Details</b>	<a href="#">Nikto 2.1.5</a>
<b>CLI Options</b>	-Display V -o nikto_scan_result_etsy.html -Format html -h www.etsy.com
<b>Hosts Tested</b>	1
<b>Start Time</b>	Thu Feb 14 22:15:13 2019
<b>End Time</b>	Thu Feb 14 22:18:29 2019
<b>Elapsed Time</b>	196 seconds