LAPORAN TUGAS

KEAMANAN JARINGAN KOMPUTER

(Disusun untuk memenuhi tugas mata kuliah keamanan jaringan komputer)

DisusunOleh :

Nama   : Deri Andany

NIM   : 09011181621001

Kelas   : SK7A

DosenPengampuh: Deris Stiawan, Ph. D

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2019

Pada laporan ini, saya akan menggunakan tool Zenmap untuk melakukan scanning pada dua website, yaitu www.palembang.go.id dan www.terengganu.gov.my .

Berikut adalah hasil yang saya dapatkan untuk website www.palembang.go.id :

```
PORT      STATE   SERVICE          VERSION
23/tcp    closed  telnet
25/tcp    open    tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
53/tcp    open    domain           ISC BIND 9.8.4-rpz2+rl005.12-P1
| dns-nsid:
|_  bind.version: 9.8.4-rpz2+rl005.12-P1
80/tcp    open    tcpwrapped
83/tcp    closed  mit-ml-dev
110/tcp   open    tcpwrapped
111/tcp   open    tcpwrapped
113/tcp   closed  ident
125/tcp   closed  locus-map
135/tcp   closed  msrpc
139/tcp   closed  netbios-ssn
143/tcp   open    tcpwrapped
144/tcp   closed  news
199/tcp   closed  smux
256/tcp   closed  fw1-secureremote
443/tcp   open    tcpwrapped
445/tcp   closed  microsoft-ds
554/tcp   closed  rtsp
587/tcp   open    tcpwrapped
|_smtp-commands: Couldn't establish connection on port 587
700/tcp   closed  epp
900/tcp   closed  omginitialrefs
993/tcp   open    tcpwrapped
```

```
900/tcp    closed  omginitialrefs
993/tcp    open    tcpwrapped
995/tcp    open    tcpwrapped
999/tcp    closed  garcon
1000/tcp   closed  cadlock
1025/tcp   closed  NFS-or-IIS
1028/tcp   closed  unknown
1030/tcp   closed  iad1
1036/tcp   closed  nsstp
1088/tcp   closed  cplscrambler-al
1095/tcp   closed  nicelink
1187/tcp   closed  alias
1233/tcp   closed  univ-appserver
1720/tcp   closed  h323q931
1862/tcp   closed  mysql-cm-agent
2046/tcp   closed  sdfunc
3306/tcp   open    tcpwrapped
3389/tcp   closed  ms-wbt-server
4006/tcp   closed  pxc-spvr
4125/tcp   closed  rww
4126/tcp   closed  ddrepl
5000/tcp   closed  upnp
5225/tcp   closed  hp-server
5550/tcp   closed  sdadmind
5900/tcp   closed  vnc
6389/tcp   closed  clariion-evr01
7070/tcp   closed  realserver
8007/tcp   closed  ajp12
```

nmap -T4 -A -v palembang.go.id

```
 6    3.03 ms   ip-103-241-5-113.unsri.ac.id (103.241.5.113)
 7   10.98 ms   noc-idl.unsri.ac.id (103.241.5.173)
 8   12.15 ms   114-5-176-225.resources.indosat.com (114.5.176.225)
 9   28.47 ms   114-0-2-69.resources.indosat.com (114.0.2.69)
10   27.95 ms   114-0-78-194.resources.indosat.com (114.0.78.194)
11   27.85 ms   114-0-78-205.resources.indosat.com (114.0.78.205)
12   35.55 ms   119.110.116.122
13   35.75 ms   119.110.112.217
14   44.56 ms   119.110.114.54
15   25.25 ms   192.168.120.6
16   29.84 ms   IP-93-110.nap.net.id (103.80.93.110)
17   28.62 ms   wifiku.openixp.net (218.100.27.23)
18   43.09 ms   103.253.1.22
19   ... 30

NSE: Script Post-scanning.
Initiating NSE at 14:33
Completed NSE at 14:33, 0.00s elapsed
Initiating NSE at 14:33
Completed NSE at 14:33, 0.00s elapsed
Initiating NSE at 14:33
Completed NSE at 14:33, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 416.12 seconds
           Raw packets sent: 2217 (102.564KB) | Rcvd: 91 (4.550KB)
```

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Hosts Viewer | Fisheye | Controls
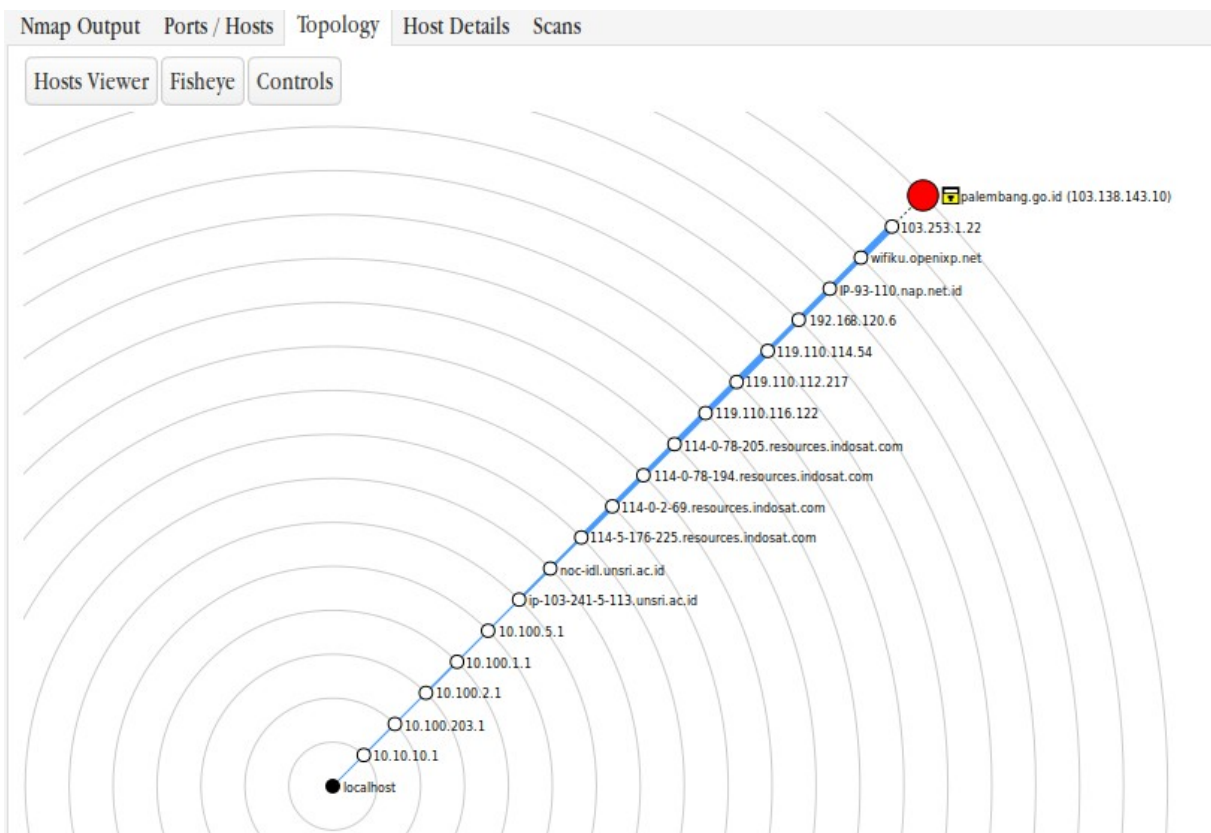
Nmap Output | Ports / Hosts | Topology | **Host Details** | Scans

⊟ palembang.go.id (103.138.143.10)

    ⊟ Host Status

State:	up
Open ports:	11
Filtered ports:	944
Closed ports:	45
Scanned ports:	1000
Up time:	3281692
Last boot:	Sat Sep 28 14:58:17 2019

    ⊟ Addresses

IPv4:	103.138.143.10
IPv6:	Not available
MAC:	Not available

    ⊟ Hostnames

Name - Type:	palembang.go.id - user
Name - Type:	mail.palembang.go.id - PTR

    ⊟ Operating System

Name:	Linux 3.2
Accuracy:	94%

        ⊞ Ports used

        ⊞ OS Classes

Nmap Output | **Ports / Hosts** | Topology | Host Details | Scans

	Port	Protocol	State	Service	Version
●	23	tcp	closed	telnet	
●	25	tcp	open	tcpwrapped	
●	53	tcp	open	domain	ISC BIND 9.8.4-rpz2+rl005.12-P1
●	80	tcp	open	tcpwrapped	
●	83	tcp	closed	mit-ml-dev	
●	110	tcp	open	tcpwrapped	
●	111	tcp	open	tcpwrapped	
●	113	tcp	closed	ident	
●	125	tcp	closed	locus-map	
●	135	tcp	closed	msrpc	
●	139	tcp	closed	netbios-ssn	
●	143	tcp	open	tcpwrapped	
●	144	tcp	closed	news	
●	199	tcp	closed	smux	
●	256	tcp	closed	fw1-secureremote	
●	443	tcp	open	tcpwrapped	
●	445	tcp	closed	microsoft-ds	
●	554	tcp	closed	rtsp	

	Port	Protocol	State	Service	Version
🟢	587	tcp	open	tcpwrapped	
🔴	700	tcp	closed	epp	
🔴	900	tcp	closed	omginitialrefs	
🟢	993	tcp	open	tcpwrapped	
🟢	995	tcp	open	tcpwrapped	
🔴	999	tcp	closed	garcon	
🔴	1000	tcp	closed	cadlock	
🔴	1025	tcp	closed	NFS-or-IIS	
🔴	1028	tcp	closed	unknown	
🔴	1030	tcp	closed	iad1	
🔴	1036	tcp	closed	nsstp	
🔴	1088	tcp	closed	cplscrambler-al	
🔴	1095	tcp	closed	nicelink	
🔴	1187	tcp	closed	alias	
🔴	1233	tcp	closed	univ-appserver	
🔴	1720	tcp	closed	h323q931	
🔴	1862	tcp	closed	mysql-cm-agent	
🔴	2046	tcp	closed	sdfunc	
🟢	3306	tcp	open	tcpwrapped	

Port	Protocol	State	Service	Version
3389	tcp	closed	ms-wbt-server	
4006	tcp	closed	pxc-spvr	
4125	tcp	closed	rww	
4126	tcp	closed	ddrepl	
5000	tcp	closed	upnp	
5225	tcp	closed	hp-server	
5550	tcp	closed	sdadmind	
5900	tcp	closed	vnc	
6389	tcp	closed	clariion-evr01	
7070	tcp	closed	realserver	
8007	tcp	closed	ajp12	
8011	tcp	closed	unknown	
8080	tcp	closed	http-proxy	
8081	tcp	closed	blackice-icecap	
8888	tcp	closed	sun-answerbook	
9290	tcp	closed	unknown	
9575	tcp	closed	unknown	
12345	tcp	closed	netbus	
27356	tcp	closed	unknown	

```
(base) hades@hades-pc:~$ traceroute www.palembang.go.id
traceroute to www.palembang.go.id (103.138.143.10), 30 hops max, 60 byte packets
 1  10.10.10.1 (10.10.10.1)  0.291 ms  4.486 ms  4.482 ms
 2  10.100.203.1 (10.100.203.1)  1.407 ms  1.371 ms  1.405 ms
 3  10.100.2.1 (10.100.2.1)  1.568 ms  1.517 ms  1.564 ms
 4  10.100.1.1 (10.100.1.1)  1.593 ms  1.653 ms  1.667 ms
 5  10.100.5.1 (10.100.5.1)  1.763 ms  1.715 ms  1.666 ms
 6  ip-103-241-5-113.unsri.ac.id (103.241.5.113)  1.761 ms  0.771 ms  1.207 ms
 7  noc-idl.unsri.ac.id (103.241.5.173)  1.222 ms  1.236 ms  1.247 ms
 8  114-5-176-225.resources.indosat.com (114.5.176.225)  10.548 ms  10.569 ms  10.553 ms
 9  114-0-2-69.resources.indosat.com (114.0.2.69)  24.310 ms  24.357 ms  24.369 ms
10  114-0-78-194.resources.indosat.com (114.0.78.194)  23.360 ms  23.419 ms  23.437 ms
11  114-0-78-205.resources.indosat.com (114.0.78.205)  24.100 ms  24.208 ms  24.232 ms
12  119.110.116.166 (119.110.116.166)  34.483 ms  34.416 ms 119.110.116.122 (119.110.116.122)  34.307 ms
13  119.110.112.217 (119.110.112.217)  34.463 ms  34.324 ms  34.342 ms
14  119.110.114.54 (119.110.114.54)  34.552 ms  34.529 ms  34.490 ms
15  192.168.120.6 (192.168.120.6)  23.322 ms  23.129 ms  23.172 ms
16  IP-93-110.nap.net.id (103.80.93.110)  23.288 ms  23.240 ms  23.222 ms
17  wifiku.openixp.net (218.100.27.23)  23.508 ms  23.255 ms  23.238 ms
18  103.253.1.22 (103.253.1.22)  32.840 ms  32.747 ms  32.544 ms
19  mail.palembang.go.id (103.138.143.10)  32.870 ms  33.022 ms  33.016 ms
```

Berikut ini adalah informasi yang saya dapatkan dari website www.terengganu.gov.my :

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

`nmap -T4 -A -v www.terengganu.gov.my`

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-05 14:43 WIB
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:43
Completed NSE at 14:43, 0.00s elapsed
Initiating NSE at 14:43
Completed NSE at 14:43, 0.00s elapsed
Initiating NSE at 14:43
Completed NSE at 14:43, 0.00s elapsed
Initiating Ping Scan at 14:43
Scanning www.terengganu.gov.my (202.188.29.142) [4 ports]
Completed Ping Scan at 14:43, 0.34s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:43
Completed Parallel DNS resolution of 1 host. at 14:43, 1.85s elapsed
Initiating SYN Stealth Scan at 14:43
Scanning www.terengganu.gov.my (202.188.29.142) [1000 ports]
Discovered open port 53/tcp on 202.188.29.142
Discovered open port 80/tcp on 202.188.29.142
Discovered open port 1720/tcp on 202.188.29.142
Completed SYN Stealth Scan at 14:43, 15.22s elapsed (1000 total ports)
Initiating Service scan at 14:43
Scanning 3 services on www.terengganu.gov.my (202.188.29.142)
Completed Service scan at 14:43, 33.59s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against www.terengganu.gov.my (202.188.29.142)
Retrying OS detection (try #2) against www.terengganu.gov.my (202.188.29.142)
Initiating Traceroute at 14:44
Completed Traceroute at 14:44, 3.01s elapsed
```

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

`nmap -T4 -A -v www.terengganu.gov.my`

```
Initiating Parallel DNS resolution of 17 hosts. at 14:44
Completed Parallel DNS resolution of 17 hosts. at 14:44, 1.84s elapsed
NSE: Script scanning 202.188.29.142.
Initiating NSE at 14:44
Completed NSE at 14:44, 8.40s elapsed
Initiating NSE at 14:44
Completed NSE at 14:44, 1.27s elapsed
Initiating NSE at 14:44
Completed NSE at 14:44, 0.00s elapsed
Nmap scan report for www.terengganu.gov.my (202.188.29.142)
Host is up (0.19s latency).
Not shown: 980 closed ports
PORT      STATE     SERVICE        VERSION
22/tcp    filtered  ssh
53/tcp    open      domain         ISC BIND 9.8.4-rpz2+rl005.12-P1
| dns-nsid:
|_  bind.version: 9.8.4-rpz2+rl005.12-P1
80/tcp    open      http           Apache httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
|_http-title: Portal Rasmi Kerajaan Negeri Terengganu
1720/tcp  open      h323q931?
1723/tcp  filtered  pptp
3001/tcp  filtered  nessus
3389/tcp  filtered  ms-wbt-server
5900/tcp  filtered  vnc
6000/tcp  filtered  X11
```

```
Nmap Output    Ports / Hosts    Topology    Host Details    Scans

nmap -T4 -A -v www.terengganu.gov.my                                              ⌄  ☰  Det

6006/tcp filtered X11
6001/tcp filtered X11:1
6002/tcp filtered X11:2
6003/tcp filtered X11:3
6004/tcp filtered X11:4
6005/tcp filtered X11:5
6006/tcp filtered X11:6
6007/tcp filtered X11:7
6009/tcp filtered X11:9
6025/tcp filtered x11
6059/tcp filtered X11:59
8291/tcp filtered unknown
Device type: general purpose|broadband router|firewall|storage-misc|printer
Running (JUST GUESSING): Linux 3.X|2.6.X|4.X (95%), WatchGuard Fireware 11.X (86%), Drobo embedded (86%),
Olivetti embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:4 cpe:/
o:linux:linux_kernel:3 cpe:/o:watchguard:fireware:11.8 cpe:/h:drobo:5n cpe:/o:linux:linux_kernel cpe:/
h:olivetti:65c-9
Aggressive OS guesses: Linux 3.2 (95%), Linux 3.2 - 3.8 (91%), Linux 2.6.32 - 3.13 (91%), Linux 3.8 (91%),
Linux 3.2 - 3.16 (89%), Linux 2.6.32 - 3.10 (88%), Linux 3.10 - 4.11 (88%), Linux 2.6.32 (88%), Linux 3.11 -
4.1 (87%), Linux 2.6.26 - 2.6.35 (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 37.990 days (since Sat Sep 28 14:58:14 2019)
Network Distance: 18 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 554/tcp)
```

```
Nmap Output    Ports / Hosts    Topology    Host Details    Scans

nmap -T4 -A -v www.terengganu.gov.my

TRACEROUTE (using port 554/tcp)
HOP RTT        ADDRESS
1    11.95 ms  10.10.10.1
2    4.60 ms   10.100.203.1
3    2.78 ms   10.100.2.1
4    5.05 ms   10.100.1.1
5    6.98 ms   10.100.5.1
6    4.70 ms   ip-103-241-5-113.unsri.ac.id (103.241.5.113)
7    3.46 ms   noc-idl.unsri.ac.id (103.241.5.173)
8    18.40 ms  114-5-176-225.resources.indosat.com (114.5.176.225)
9    33.55 ms  114-0-2-69.resources.indosat.com (114.0.2.69)
10   31.01 ms  114-0-15-43.resources.indosat.com (114.0.15.43)
11   287.92 ms 100ge16-1.core1.lon2.he.net (72.52.92.213)
12   306.14 ms 100ge13-2.core1.nyc4.he.net (72.52.92.166)
13   286.71 ms 100ge8-1.core1.sjc2.he.net (184.105.81.218)
14   299.91 ms telekom-malaysia-inc.100gigabitethernet16-2.core1.sjc2.he.net (64.71.148.166)
15   304.58 ms 10.55.131.58
16   307.68 ms 1.9.190.54
17   ...
18   313.15 ms 202.188.29.142

NSE: Script Post-scanning.
Initiating NSE at 14:44
Completed NSE at 14:44, 0.00s elapsed
Initiating NSE at 14:44
Completed NSE at 14:44, 0.00s elapsed
Initiating NSE at 14:44
Completed NSE at 14:44, 0.00s elapsed
```

	Port	Protocol	State	Service	Version
🔴	22	tcp	filtered	ssh	
🟢	53	tcp	open	domain	ISC BIND 9.8.4-rpz2+rl005.12-P1
🟢	80	tcp	open	http	Apache httpd
🟢	1720	tcp	open	h323q931	
🔴	1723	tcp	filtered	pptp	
🔴	3001	tcp	filtered	nessus	
🔴	3389	tcp	filtered	ms-wbt-server	
🔴	5900	tcp	filtered	vnc	
🔴	6000	tcp	filtered	X11	
🔴	6001	tcp	filtered	X11:1	
🔴	6002	tcp	filtered	X11:2	
🔴	6003	tcp	filtered	X11:3	
🔴	6004	tcp	filtered	X11:4	
🔴	6005	tcp	filtered	X11:5	
🔴	6006	tcp	filtered	X11:6	
🔴	6007	tcp	filtered	X11:7	
🔴	6009	tcp	filtered	X11:9	
🔴	6025	tcp	filtered	x11	

Hosts Viewer | Fisheye | Controls

www.terengganu.gov.my (202.188.29.142)
1.9.190.54
10.55.131.58
telekom-malaysia-inc.100gigabitethernet16-2.core1.sjc2.he.net
100ge8-1.core1.sjc2.he.net
100ge13-2.core1.nyc4.he.net
100ge16-1.core1.lon2.he.net
114-0-15-43.resources.indosat.com
114-0-2-69.resources.indosat.com
114-5-176-225.resources.indosat.com
noc-idl.unsri.ac.id
ip-103-241-5-113.unsri.ac.id
10.100.5.1
10.100.1.1
10.100.2.1
10.100.203.1
10.10.10.1
localhost

```
Nmap Output   Ports / Hosts   Topology   Host Details   Scans

⊟ www.terengganu.gov.my (202.188.29.142)
    ⊟ Host Status
        State:              up
        Open ports:         3
        Filtered ports:     17
        Closed ports:       980
        Scanned ports:      1000
        Up time:            3282367
        Last boot:          Sat Sep 28 14:58:14 2019

    ⊟ Addresses
        IPv4:   202.188.29.142
        IPv6:   Not available
        MAC:    Not available

    ⊟ Hostnames
        Name - Type:   www.terengganu.gov.my - user

    ⊟ Operating System
        Name:      Linux 3.2
        Accuracy:              95%

        ⊞ Ports used
        ⊞ OS Classes
```

```
(base) hades@hades-pc:~$ traceroute www.terengganu.gov.my
traceroute to www.terengganu.gov.my (202.188.29.142), 30 hops max, 60 byte packets
 1  10.10.10.1 (10.10.10.1)  0.181 ms  0.259 ms  0.296 ms
 2  10.100.203.1 (10.100.203.1)  1.277 ms  1.208 ms  1.262 ms
 3  10.100.2.1 (10.100.2.1)  1.271 ms  1.280 ms  1.396 ms
 4  10.100.1.1 (10.100.1.1)  1.676 ms  1.696 ms  1.703 ms
 5  10.100.5.1 (10.100.5.1)  1.714 ms  1.725 ms  1.735 ms
 6  ip-103-241-5-113.unsri.ac.id (103.241.5.113)  1.747 ms  0.615 ms  0.625 ms
 7  noc-idl.unsri.ac.id (103.241.5.173)  0.815 ms  1.035 ms  1.010 ms
 8  114-5-176-225.resources.indosat.com (114.5.176.225)  19.873 ms  19.884 ms  19.888 ms
 9  114-0-2-69.resources.indosat.com (114.0.2.69)  33.216 ms  33.226 ms  33.212 ms
10  114-0-15-43.resources.indosat.com (114.0.15.43)  33.359 ms  33.276 ms  33.341 ms
11  100ge16-1.core1.lon2.he.net (72.52.92.213)  278.905 ms  296.518 ms  279.129 ms
12  100ge13-2.core1.nyc4.he.net (72.52.92.166)  307.571 ms  308.883 ms  317.743 ms
13  100ge8-1.core1.sjc2.he.net (184.105.81.218)  278.448 ms  277.797 ms  291.744 ms
14  telekom-malaysia-inc.100gigabitethernet16-2.core1.sjc2.he.net (64.71.148.166)  292.526 ms  289.295 ms  290.273 ms
15  * * *
16  1.9.190.54 (1.9.190.54)  299.439 ms  303.217 ms  304.550 ms
17  * * *
18  202.188.29.142 (202.188.29.142)  306.963 ms  306.782 ms  306.167 ms
(base) hades@hades-pc:~$
```

Dari hasil scan di atas di dapatkan banyak informasi mengenai website tersebut, seperti port yang di aktifkan, di closed, dan di filter, system operasi, IP yang digunakan, dan lebih banyak lagi informasi yang di dapatkan yang bias digunakan untuk proses scanning pada tahap berikutnya.

Catatan :

Segala task yang dikerjakan di atas hanya untuk tujuan riset dan tugas semata, bukan untuk kegiatan kejahatan cyber dan lainnya.