LAPORAN KEAMANAN JARINGAN KOMPUTER

Oleh:

NAMA	: Yoga Faturahman
NIM	: 09040581721006
Kelas	: TKJ4
Mata Kuliah	: Keamanan Jaringan Komputer

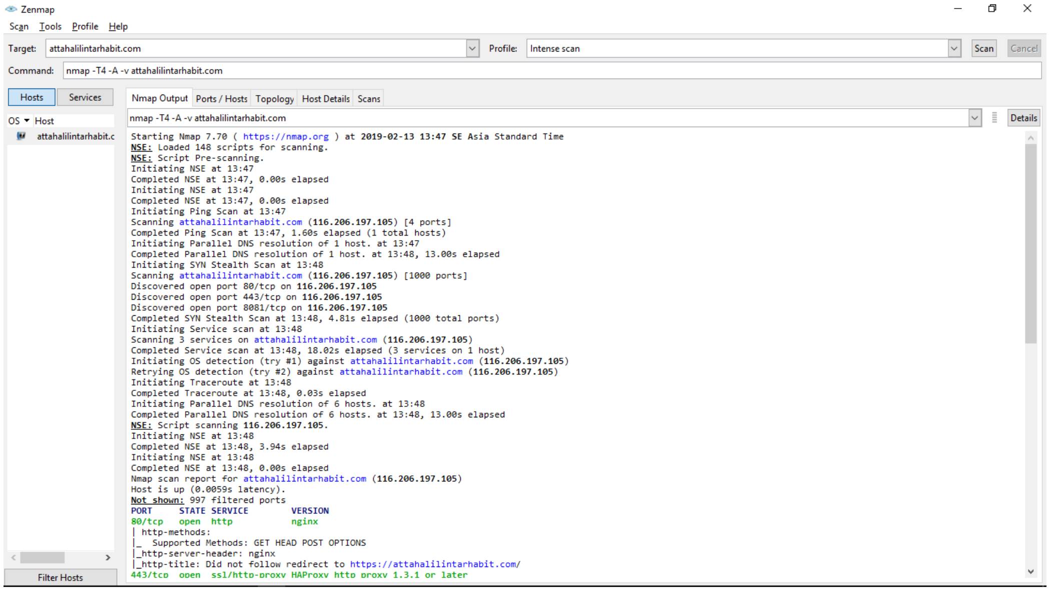
LABORATORIUM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2019

Pendahuluan

Nmap (network mapper) adalah program opensource yang biasa digunakan oleh administrator jaringan untuk memetakan, monitoring, serta troubleshoot sistem TCP/IP. Nmap (Network Mapper) adalah sebuah aplikasi atau tool yang berfungsi untuk melakukan port scanning. aplikasi ini digunakan untuk mengAudit jaringan yang ada. dengan menggunakan tool ini kita dapat melihat host yang aktif, port yang terbuka, sistem operasi yang digunakan, dan feature feature scanning lainnya.

Implementasi

menggunakan Zenmap untuk scanning network, langkah pertama buka aplikasi dan masukkan target yang akan dilakukan scanning, disini saya menggunakan https://attahalilintarhabit.com/, https://www.foxnews.com, dan http://disdukcapil.palembang.go.id

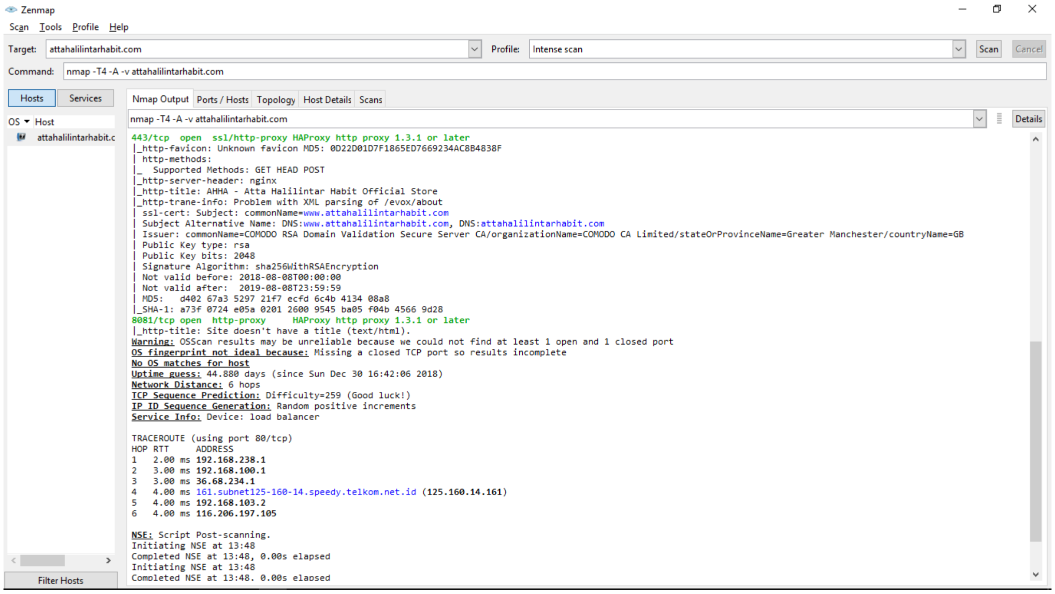


Target: attahalilintarhabit.com

Profile: Intense scan

Command: nmap -T4 -A -v attahalilintarhabit.com

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-13 13:47 SE Asia Standard Time
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:47
Completed NSE at 13:47, 0.00s elapsed
Initiating NSE at 13:47
Completed NSE at 13:47, 0.00s elapsed
Initiating Ping Scan at 13:47
Scanning attahalilintarhabit.com (116.206.197.105) [4 ports]
Completed Ping Scan at 13:47, 1.60s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:47
Completed Parallel DNS resolution of 1 host. at 13:48, 13.00s elapsed
Initiating SYN Stealth Scan at 13:48
Scanning attahalilintarhabit.com (116.206.197.105) [1000 ports]
Discovered open port 80/tcp on 116.206.197.105
Discovered open port 443/tcp on 116.206.197.105
Discovered open port 8081/tcp on 116.206.197.105
Completed SYN Stealth Scan at 13:48, 4.81s elapsed (1000 total ports)
Initiating Service scan at 13:48
Scanning 3 services on attahalilintarhabit.com (116.206.197.105)
Completed Service scan at 13:48, 18.02s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against attahalilintarhabit.com (116.206.197.105)
Retrying OS detection (try #2) against attahalilintarhabit.com (116.206.197.105)
Initiating Traceroute at 13:48
Completed Traceroute at 13:48, 0.03s elapsed
Initiating Parallel DNS resolution of 6 hosts. at 13:48
Completed Parallel DNS resolution of 6 hosts. at 13:48, 13.00s elapsed
NSE: Script scanning 116.206.197.105.
Initiating NSE at 13:48
Completed NSE at 13:48, 3.94s elapsed
Initiating NSE at 13:48
Completed NSE at 13:48, 0.00s elapsed
Nmap scan report for attahalilintarhabit.com (116.206.197.105)
Host is up (0.0059s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE         VERSION
80/tcp   open  http            nginx
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx
|_http-title: Did not follow redirect to https://attahalilintarhabit.com/
443/tcp  open  ssl/http-proxy HAProxy http proxy 1.3.1 or later
```



Target: attahalilintarhabit.com

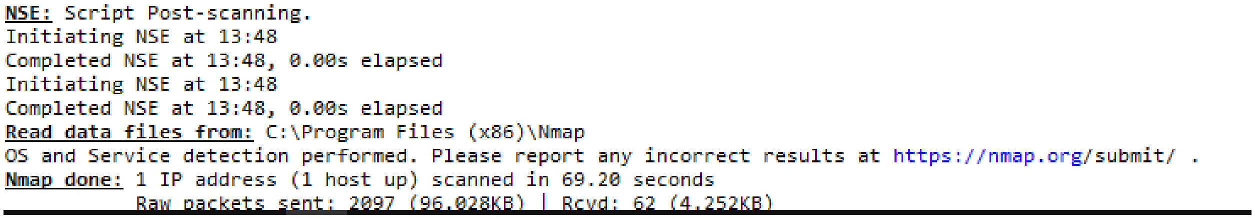
Profile: Intense scan

Command: nmap -T4 -A -v attahalilintarhabit.com

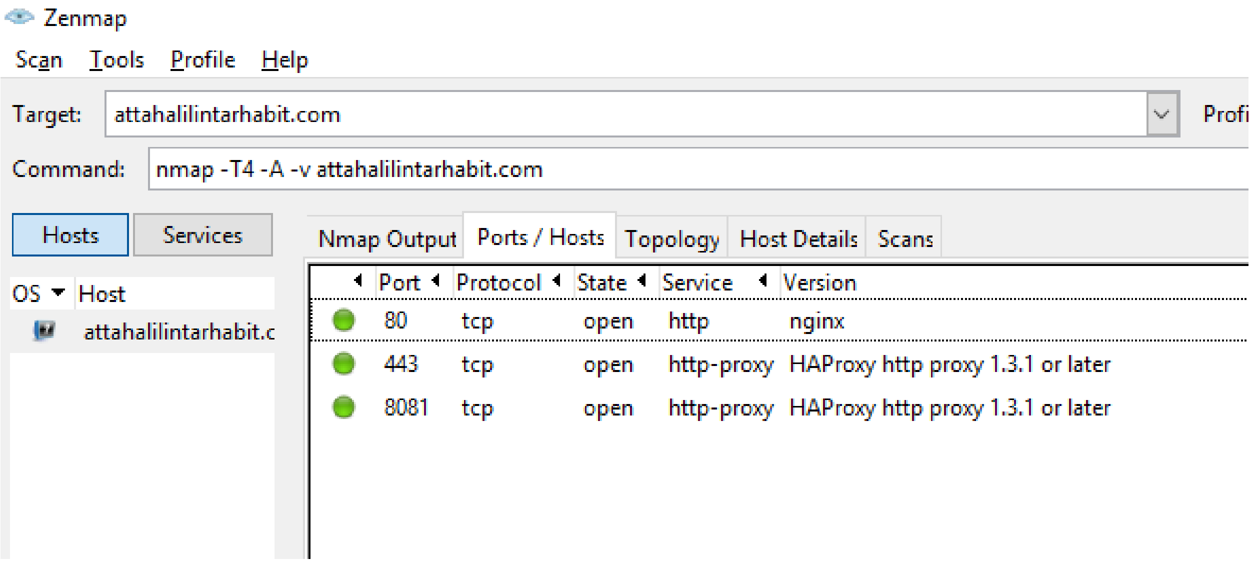
```
443/tcp  open  ssl/http-proxy HAProxy http proxy 1.3.1 or later
|_http-favicon: Unknown favicon MD5: 0D22D01D7F1865ED7669234AC8B4838F
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: nginx
|_http-title: AHHA - Atta Halilintar Habit Official Store
|_http-trane-info: Problem with XML parsing of /evox/about
| ssl-cert: Subject: commonName=www.attahalilintarhabit.com
| Subject Alternative Name: DNS:www.attahalilintarhabit.com, DNS:attahalilintarhabit.com
| Issuer: commonName=COMODO RSA Domain Validation Secure Server CA/organizationName=COMODO CA Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-08-08T00:00:00
| Not valid after:  2019-08-08T23:59:59
| MD5:   d402 67a3 5297 21f7 ecfd 6c4b 4134 08a8
|_SHA-1: a73f 0724 e05a 0201 2600 9545 ba05 f04b 4566 9d28
8081/tcp open  http-proxy     HAProxy http proxy 1.3.1 or later
|_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
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Uptime guess: 44.880 days (since Sun Dec 30 16:42:06 2018)
Network Distance: 6 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Random positive increments
Service Info: Device: load balancer

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   2.00 ms 192.168.238.1
2   3.00 ms 192.168.100.1
3   3.00 ms 36.68.234.1
4   4.00 ms 161.subnet125-160-14.speedy.telkom.net.id (125.160.14.161)
5   4.00 ms 192.168.103.2
6   4.00 ms 116.206.197.105

NSE: Script Post-scanning.
Initiating NSE at 13:48
Completed NSE at 13:48, 0.00s elapsed
Initiating NSE at 13:48
Completed NSE at 13:48, 0.00s elapsed
```



```
NSE: Script Post-scanning.
Initiating NSE at 13:48
Completed NSE at 13:48, 0.00s elapsed
Initiating NSE at 13:48
Completed NSE at 13:48, 0.00s elapsed
Read data files from: C:\Program Files (x86)\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 69.20 seconds
           Raw packets sent: 2097 (96.028KB) | Rcvd: 62 (4.252KB)
```

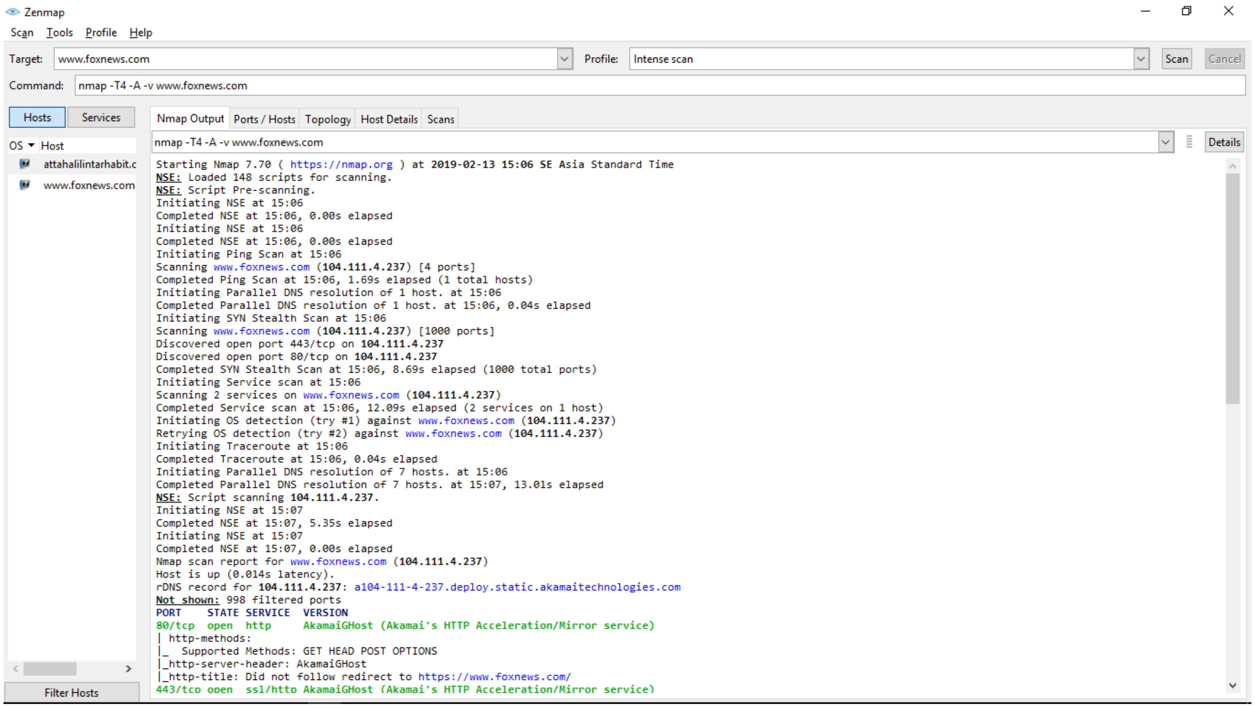


Target: attahalilintarhabit.com

Command: nmap -T4 -A -v attahalilintarhabit.com

```
OS  Host
    attahalilintarhabit.c
```

```
   Port   Protocol   State   Service      Version
●  80     tcp        open    http         nginx
●  443    tcp        open    http-proxy   HAProxy http proxy 1.3.1 or later
●  8081   tcp        open    http-proxy   HAProxy http proxy 1.3.1 or later
```



Target: www.foxnews.com

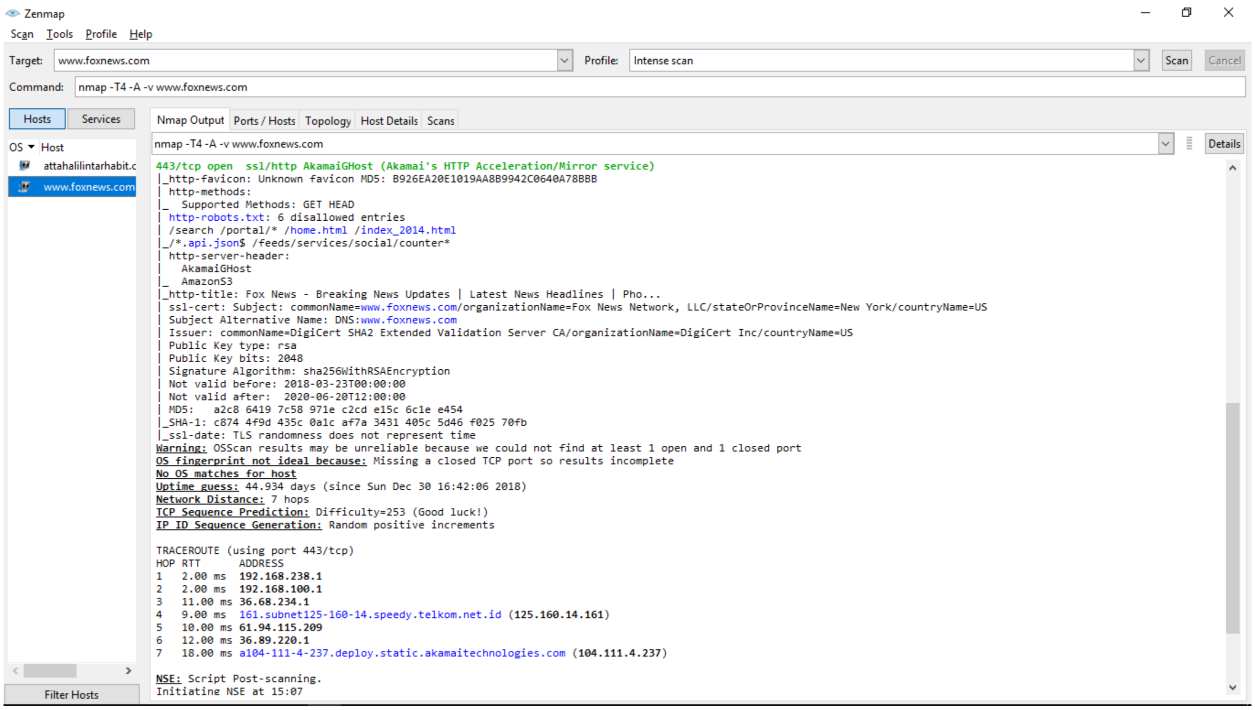
Profile: Intense scan

Command: nmap -T4 -A -v www.foxnews.com

```
OS  Host
    attahalilintarhabit.c
    www.foxnews.com
```

```
nmap -T4 -A -v www.foxnews.com
```

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-13 15:06 SE Asia Standard Time
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:06
Completed NSE at 15:06, 0.00s elapsed
Initiating NSE at 15:06
Completed NSE at 15:06, 0.00s elapsed
Initiating Ping Scan at 15:06
Scanning www.foxnews.com (104.111.4.237) [4 ports]
Completed Ping Scan at 15:06, 1.69s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:06
Completed Parallel DNS resolution of 1 host. at 15:06, 0.04s elapsed
Initiating SYN Stealth Scan at 15:06
Scanning www.foxnews.com (104.111.4.237) [1000 ports]
Discovered open port 443/tcp on 104.111.4.237
Discovered open port 80/tcp on 104.111.4.237
Completed SYN Stealth Scan at 15:06, 8.69s elapsed (1000 total ports)
Initiating Service scan at 15:06
Scanning 2 services on www.foxnews.com (104.111.4.237)
Completed Service scan at 15:06, 12.09s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against www.foxnews.com (104.111.4.237)
Retrying OS detection (try #2) against www.foxnews.com (104.111.4.237)
Initiating Traceroute at 15:06
Completed Traceroute at 15:06, 0.04s elapsed
Initiating Parallel DNS resolution of 7 hosts. at 15:06
Completed Parallel DNS resolution of 7 hosts. at 15:07, 13.01s elapsed
NSE: Script scanning 104.111.4.237.
Initiating NSE at 15:07
Completed NSE at 15:07, 5.35s elapsed
Initiating NSE at 15:07
Completed NSE at 15:07, 0.00s elapsed
Nmap scan report for www.foxnews.com (104.111.4.237)
Host is up (0.014s latency).
rDNS record for 104.111.4.237: a104-111-4-237.deploy.static.akamaitechnologies.com
Not shown: 998 filtered ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http     AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: AkamaiGHost
|_http-title: Did not follow redirect to https://www.foxnews.com/
443/tcp open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
```



Target: www.foxnews.com

Profile: Intense scan

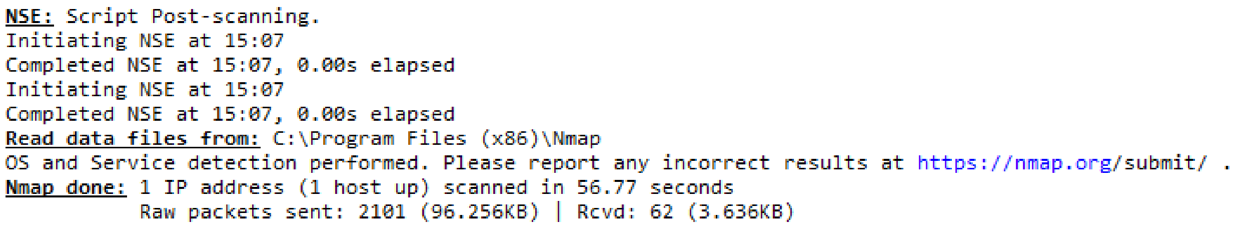
Command: nmap -T4 -A -v www.foxnews.com

nmap -T4 -A -v www.foxnews.com

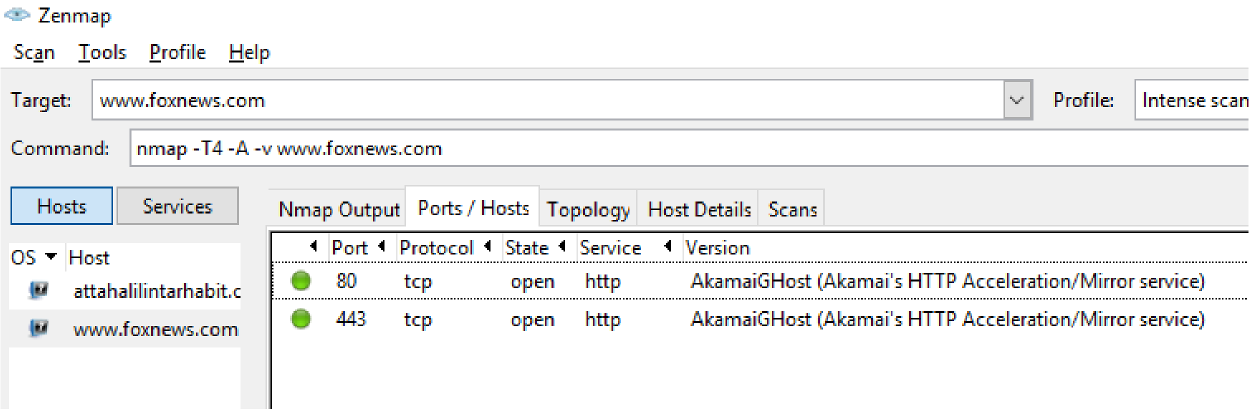
```
443/tcp open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-favicon: Unknown favicon MD5: B926EA20E1019AA8B9942C0640A78BBB
| http-methods:
|_  Supported Methods: GET HEAD
| http-robots.txt: 6 disallowed entries
| /search /portal/* /home.html /index_2014.html
|_/*.api.json$ /feeds/services/social/counter*
| http-server-header:
|   AkamaiGHost
|_  AmazonS3
|_http-title: Fox News - Breaking News Updates | Latest News Headlines | Pho...
| ssl-cert: Subject: commonName=www.foxnews.com/organizationName=Fox News Network, LLC/stateOrProvinceName=New York/countryName=US
| Subject Alternative Name: DNS:www.foxnews.com
| Issuer: commonName=DigiCert SHA2 Extended Validation Server CA/organizationName=DigiCert Inc/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-03-23T00:00:00
| Not valid after:  2020-06-20T12:00:00
| MD5:   a2c8 6419 7c58 971e c2cd e15c 6c1e e454
|_SHA-1: c874 4f9d 435c 0a1c af7a 3431 405c 5d46 f025 70fb
|_ssl-date: TLS randomness does not represent time
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Uptime guess: 44.934 days (since Sun Dec 30 16:42:06 2018)
Network Distance: 7 hops
TCP Sequence Prediction: Difficulty=253 (Good luck!)
IP ID Sequence Generation: Random positive increments

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   2.00 ms  192.168.238.1
2   2.00 ms  192.168.100.1
3   11.00 ms 36.68.234.1
4   9.00 ms  161.subnet125-160-14.speedy.telkom.net.id (125.160.14.161)
5   10.00 ms 61.94.115.209
6   12.00 ms 36.89.220.1
7   18.00 ms a104-111-4-237.deploy.static.akamaitechnologies.com (104.111.4.237)

NSE: Script Post-scanning.
Initiating NSE at 15:07
```



```
NSE: Script Post-scanning.
Initiating NSE at 15:07
Completed NSE at 15:07, 0.00s elapsed
Initiating NSE at 15:07
Completed NSE at 15:07, 0.00s elapsed
Read data files from: C:\Program Files (x86)\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 56.77 seconds
           Raw packets sent: 2101 (96.256KB) | Rcvd: 62 (3.636KB)
```

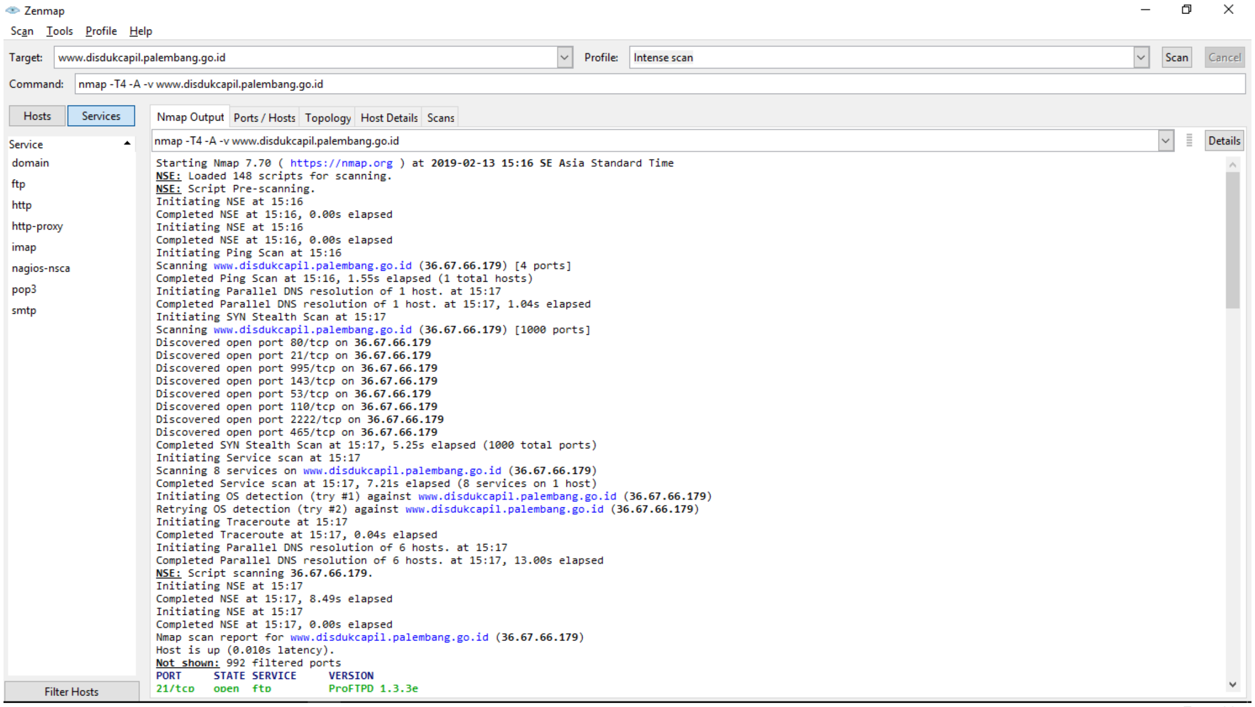


Target: www.foxnews.com

Profile: Intense scan

Command: nmap -T4 -A -v www.foxnews.com

	Port	Protocol	State	Service	Version
●	80	tcp	open	http	AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
●	443	tcp	open	http	AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)

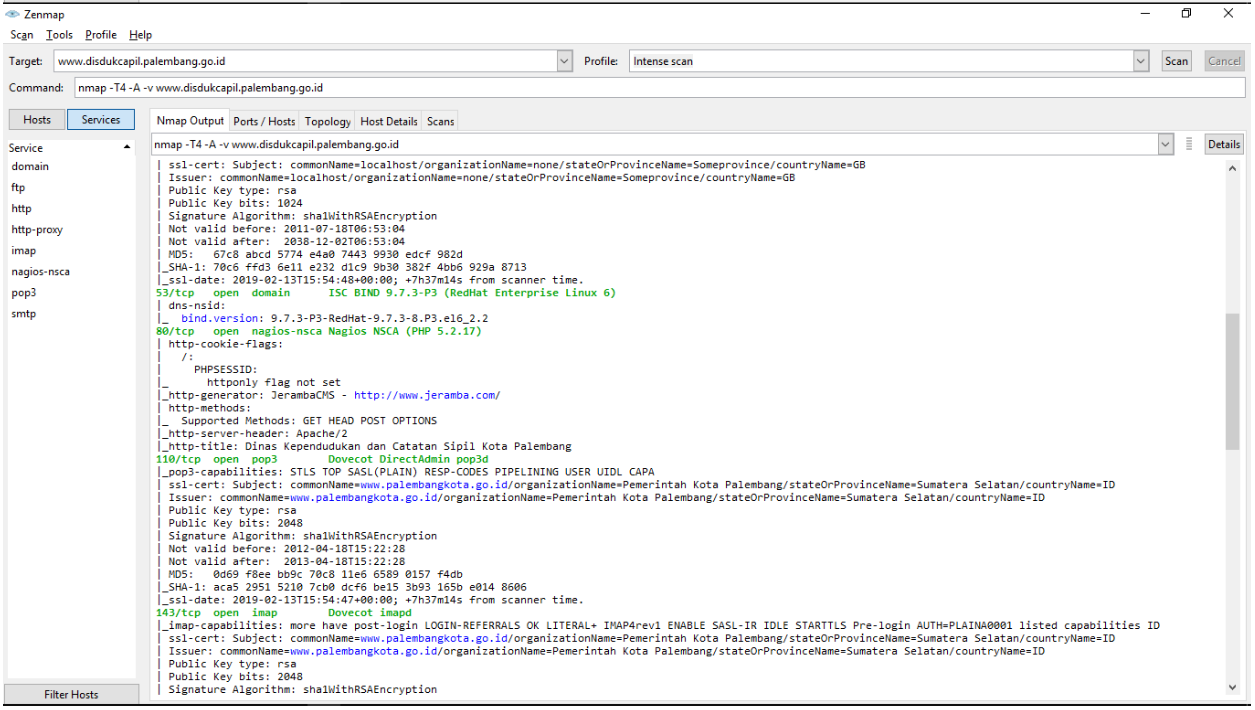


Target: www.disdukcapil.palembang.go.id

Profile: Intense scan

Command: nmap -T4 -A -v www.disdukcapil.palembang.go.id

```
nmap -T4 -A -v www.disdukcapil.palembang.go.id
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-13 15:16 SE Asia Standard Time
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:16
Completed NSE at 15:16, 0.00s elapsed
Initiating NSE at 15:16
Completed NSE at 15:16, 0.00s elapsed
Initiating Ping Scan at 15:16
Scanning www.disdukcapil.palembang.go.id (36.67.66.179) [4 ports]
Completed Ping Scan at 15:16, 1.55s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:17
Completed Parallel DNS resolution of 1 host. at 15:17, 1.04s elapsed
Initiating SYN Stealth Scan at 15:17
Scanning www.disdukcapil.palembang.go.id (36.67.66.179) [1000 ports]
Discovered open port 80/tcp on 36.67.66.179
Discovered open port 21/tcp on 36.67.66.179
Discovered open port 995/tcp on 36.67.66.179
Discovered open port 143/tcp on 36.67.66.179
Discovered open port 53/tcp on 36.67.66.179
Discovered open port 110/tcp on 36.67.66.179
Discovered open port 2222/tcp on 36.67.66.179
Discovered open port 465/tcp on 36.67.66.179
Completed SYN Stealth Scan at 15:17, 5.25s elapsed (1000 total ports)
Initiating Service scan at 15:17
Scanning 8 services on www.disdukcapil.palembang.go.id (36.67.66.179)
Completed Service scan at 15:17, 7.21s elapsed (8 services on 1 host)
Initiating OS detection (try #1) against www.disdukcapil.palembang.go.id (36.67.66.179)
Retrying OS detection (try #2) against www.disdukcapil.palembang.go.id (36.67.66.179)
Initiating Traceroute at 15:17
Completed Traceroute at 15:17, 0.04s elapsed
Initiating Parallel DNS resolution of 6 hosts. at 15:17
Completed Parallel DNS resolution of 6 hosts. at 15:17, 13.00s elapsed
NSE: Script scanning 36.67.66.179.
Initiating NSE at 15:17
Completed NSE at 15:17, 8.49s elapsed
Initiating NSE at 15:17
Completed NSE at 15:17, 0.00s elapsed
Nmap scan report for www.disdukcapil.palembang.go.id (36.67.66.179)
Host is up (0.010s latency).
Not shown: 992 filtered ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.3e
```

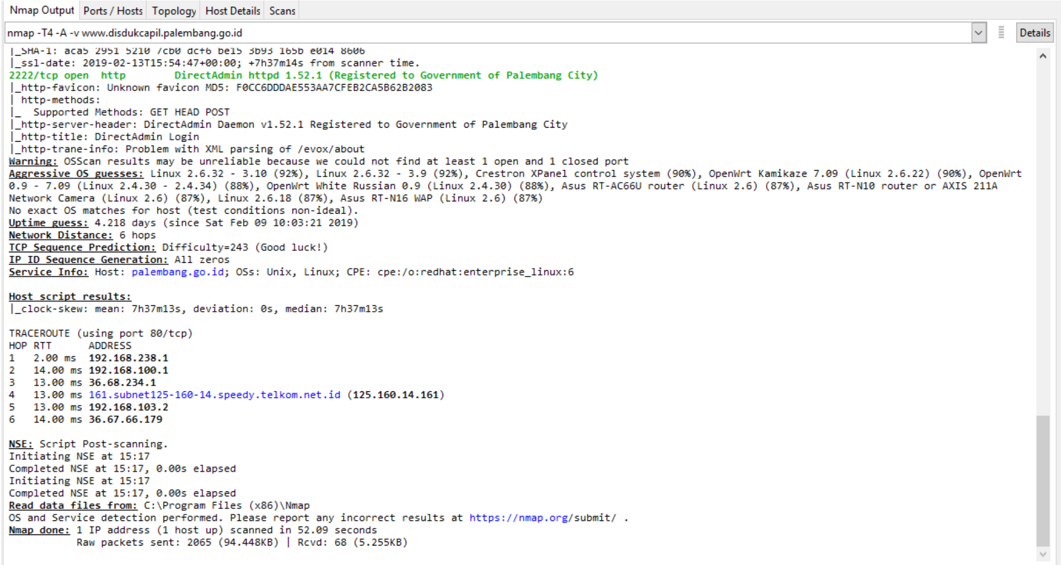


Target: www.disdukcapil.palembang.go.id

Profile: Intense scan

Command: nmap -T4 -A -v www.disdukcapil.palembang.go.id

```
nmap -T4 -A -v www.disdukcapil.palembang.go.id
| ssl-cert: Subject: commonName=localhost/organizationName=none/stateOrProvinceName=Someprovince/countryName=GB
| Issuer: commonName=localhost/organizationName=none/stateOrProvinceName=Someprovince/countryName=GB
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2011-07-18T06:53:04
| Not valid after:  2038-12-02T06:53:04
| MD5:   67c8 abcd 5774 e4a0 7443 9930 edcf 982d
|_SHA-1: 70c6 ffd3 6e11 e232 d1c9 9b30 382f 4bb6 929a 8713
|_ssl-date: 2019-02-13T15:54:48+00:00; +7h37m14s from scanner time.
53/tcp   open  domain      ISC BIND 9.7.3-P3 (RedHat Enterprise Linux 6)
| dns-nsid:
|_  bind.version: 9.7.3-P3-RedHat-9.7.3-8.P3.el6_2.2
80/tcp   open  nagios-nsca Nagios NSCA (PHP 5.2.17)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-generator: JerambaCMS - http://www.jeramba.com/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2
|_http-title: Dinas Kependudukan dan Catatan Sipil Kota Palembang
110/tcp  open  pop3        Dovecot DirectAdmin pop3d
|_pop3-capabilities: STLS TOP SASL(PLAIN) RESP-CODES PIPELINING USER UIDL CAPA
| ssl-cert: Subject: commonName=www.palembangkota.go.id/organizationName=Pemerintah Kota Palembang/stateOrProvinceName=Sumatera Selatan/countryName=ID
| Issuer: commonName=www.palembangkota.go.id/organizationName=Pemerintah Kota Palembang/stateOrProvinceName=Sumatera Selatan/countryName=ID
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2012-04-18T15:22:28
| Not valid after:  2013-04-18T15:22:28
| MD5:   0d69 f8ee bb9c 70c8 11e6 6589 0157 f4db
|_SHA-1: aca5 2951 5210 7cb0 dcf6 be15 3b93 165b e014 8606
|_ssl-date: 2019-02-13T15:54:47+00:00; +7h37m14s from scanner time.
143/tcp  open  imap        Dovecot imapd
|_imap-capabilities: more have post-login LOGIN-REFERRALS OK LITERAL+ IMAP4rev1 ENABLE SASL-IR IDLE STARTTLS Pre-login AUTH=PLAINA0001 listed capabilities ID
| ssl-cert: Subject: commonName=www.palembangkota.go.id/organizationName=Pemerintah Kota Palembang/stateOrProvinceName=Sumatera Selatan/countryName=ID
| Issuer: commonName=www.palembangkota.go.id/organizationName=Pemerintah Kota Palembang/stateOrProvinceName=Sumatera Selatan/countryName=ID
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
```



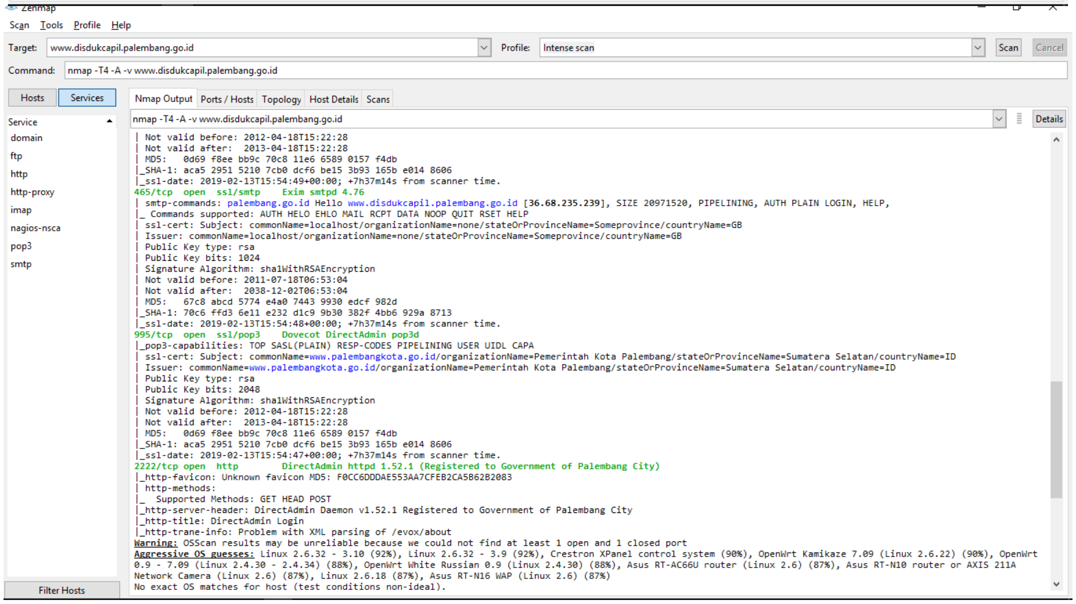
nmap -T4 -A -v www.disdukcapil.palembang.go.id

```
|_SHA-1: aca5 2951 5210 7cb0 dcf6 be15 3b93 165b e014 8606
|_ssl-date: 2019-02-13T15:54:47+00:00; +7h37m14s from scanner time.
2222/tcp open  http        DirectAdmin httpd 1.52.1 (Registered to Government of Palembang City)
|_http-favicon: Unknown favicon MD5: F0CC6DDDAE553AA7CFEB2CA5B62B2083
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: DirectAdmin Daemon v1.52.1 Registered to Government of Palembang City
|_http-title: DirectAdmin Login
|_http-trane-info: Problem with XML parsing of /evox/about
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.32 - 3.10 (92%), Linux 2.6.32 - 3.9 (92%), Crestron XPanel control system (90%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (90%), OpenWrt
0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (88%), OpenWrt White Russian 0.9 (Linux 2.4.30) (88%), Asus RT-AC66U router (Linux 2.6) (87%), Asus RT-N10 router or AXIS 211A
Network Camera (Linux 2.6) (87%), Linux 2.6.18 (87%), Asus RT-N16 WAP (Linux 2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 4.218 days (since Sat Feb 09 10:03:21 2019)
Network Distance: 6 hops
TCP Sequence Prediction: Difficulty=243 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: palembang.go.id; OSs: Unix, Linux; CPE: cpe:/o:redhat:enterprise_linux:6

Host script results:
|_clock-skew: mean: 7h37m13s, deviation: 0s, median: 7h37m13s

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   2.00 ms  192.168.238.1
2   14.00 ms 192.168.100.1
3   13.00 ms 36.68.234.1
4   13.00 ms 161.subnet125-160-14.speedy.telkom.net.id (125.160.14.161)
5   13.00 ms 192.168.103.2
6   14.00 ms 36.67.66.179

NSE: Script Post-scanning.
Initiating NSE at 15:17
Completed NSE at 15:17, 0.00s elapsed
Initiating NSE at 15:17
Completed NSE at 15:17, 0.00s elapsed
Read data files from: C:\Program Files (x86)\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 52.09 seconds
           Raw packets sent: 2065 (94.448KB) | Rcvd: 68 (5.255KB)
```



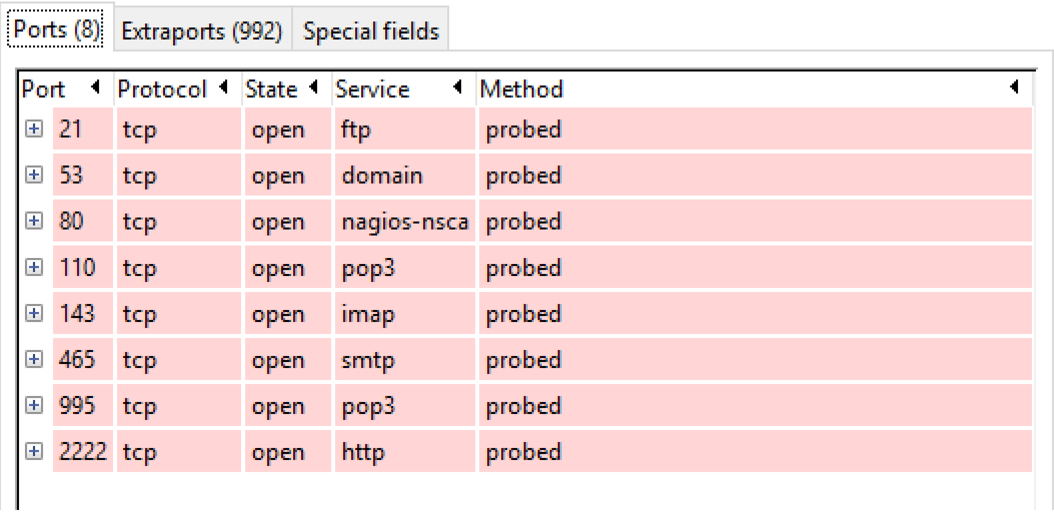
Target: www.disdukcapil.palembang.go.id

Profile: Intense scan

Command: nmap -T4 -A -v www.disdukcapil.palembang.go.id

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

```
| Not valid before: 2012-04-18T15:22:28
| Not valid after:  2013-04-18T15:22:28
| MD5:   0d69 f8ee bb9c 70c8 11e6 6589 0157 f4db
|_SHA-1: aca5 2951 5210 7cb0 dcf6 be15 3b93 165b e014 8606
|_ssl-date: 2019-02-13T15:54:49+00:00; +7h37m14s from scanner time.
465/tcp  open  ssl/smtp    Exim smtpd 4.76
| smtp-commands: palembang.go.id Hello www.disdukcapil.palembang.go.id [36.68.235.239], SIZE 20971520, PIPELINING, AUTH PLAIN LOGIN, HELP,
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA NOOP QUIT RSET HELP
| ssl-cert: Subject: commonName=localhost/organizationName=none/stateOrProvinceName=Someprovince/countryName=GB
| Issuer: commonName=localhost/organizationName=none/stateOrProvinceName=Someprovince/countryName=GB
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2011-07-18T06:53:04
| Not valid after:  2038-12-02T06:53:04
| MD5:   67c8 abcd 5774 e4a0 7443 9930 edcf 982d
|_SHA-1: 70c6 ffd3 6e11 e232 d1c9 9b30 382f 4bb6 929a 8713
|_ssl-date: 2019-02-13T15:54:48+00:00; +7h37m14s from scanner time.
995/tcp  open  ssl/pop3    Dovecot DirectAdmin pop3d
|_pop3-capabilities: TOP SASL(PLAIN) RESP-CODES PIPELINING USER UIDL CAPA
| ssl-cert: Subject: commonName=www.palembangkota.go.id/organizationName=Pemerintah Kota Palembang/stateOrProvinceName=Sumatera Selatan/countryName=ID
| Issuer: commonName=www.palembangkota.go.id/organizationName=Pemerintah Kota Palembang/stateOrProvinceName=Sumatera Selatan/countryName=ID
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2012-04-18T15:22:28
| Not valid after:  2013-04-18T15:22:28
| MD5:   0d69 f8ee bb9c 70c8 11e6 6589 0157 f4db
|_SHA-1: aca5 2951 5210 7cb0 dcf6 be15 3b93 165b e014 8606
|_ssl-date: 2019-02-13T15:54:47+00:00; +7h37m14s from scanner time.
2222/tcp open  http        DirectAdmin httpd 1.52.1 (Registered to Government of Palembang City)
|_http-favicon: Unknown favicon MD5: F0CC6DDDAE553AA7CFEB2CA5B62B2083
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: DirectAdmin Daemon v1.52.1 Registered to Government of Palembang City
|_http-title: DirectAdmin Login
|_http-trane-info: Problem with XML parsing of /evox/about
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.32 - 3.10 (92%), Linux 2.6.32 - 3.9 (92%), Crestron XPanel control system (90%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (90%), OpenWrt
0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (88%), OpenWrt White Russian 0.9 (Linux 2.4.30) (88%), Asus RT-AC66U router (Linux 2.6) (87%), Asus RT-N10 router or AXIS 211A
Network Camera (Linux 2.6) (87%), Linux 2.6.18 (87%), Asus RT-N16 WAP (Linux 2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
```

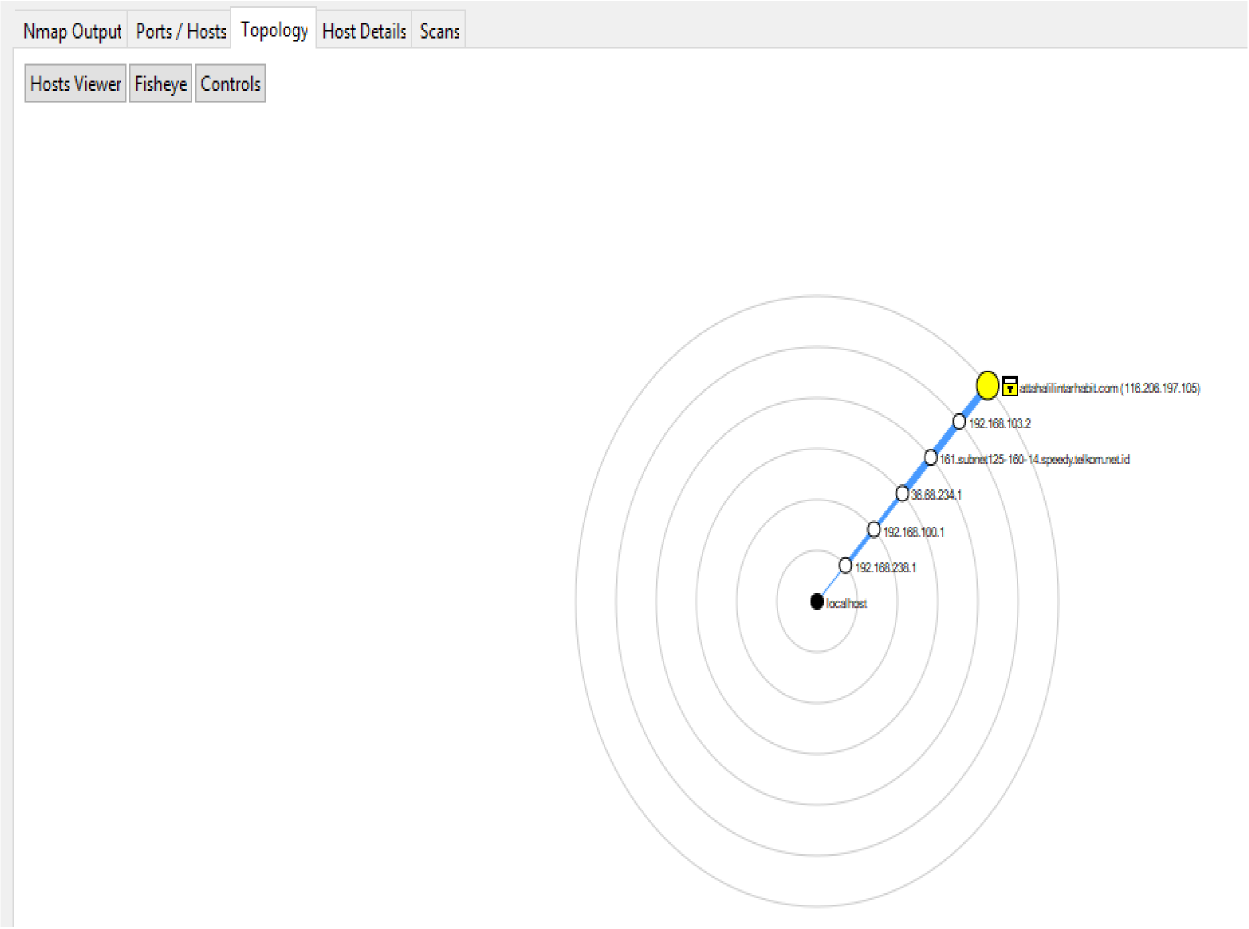


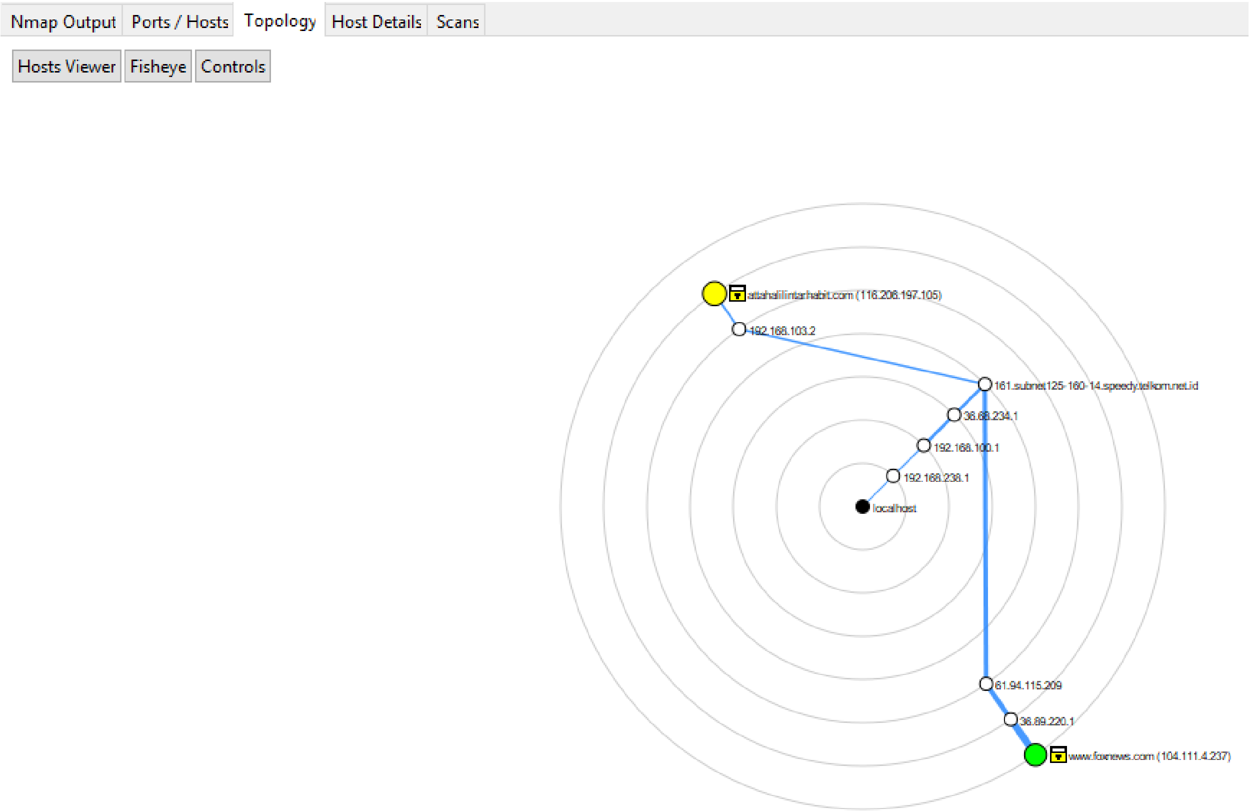
Port	Protocol	State	Service	Method
21	tcp	open	ftp	probed
53	tcp	open	domain	probed
80	tcp	open	nagios-nsca	probed
110	tcp	open	pop3	probed
143	tcp	open	imap	probed
465	tcp	open	smtp	probed
995	tcp	open	pop3	probed
2222	tcp	open	http	probed

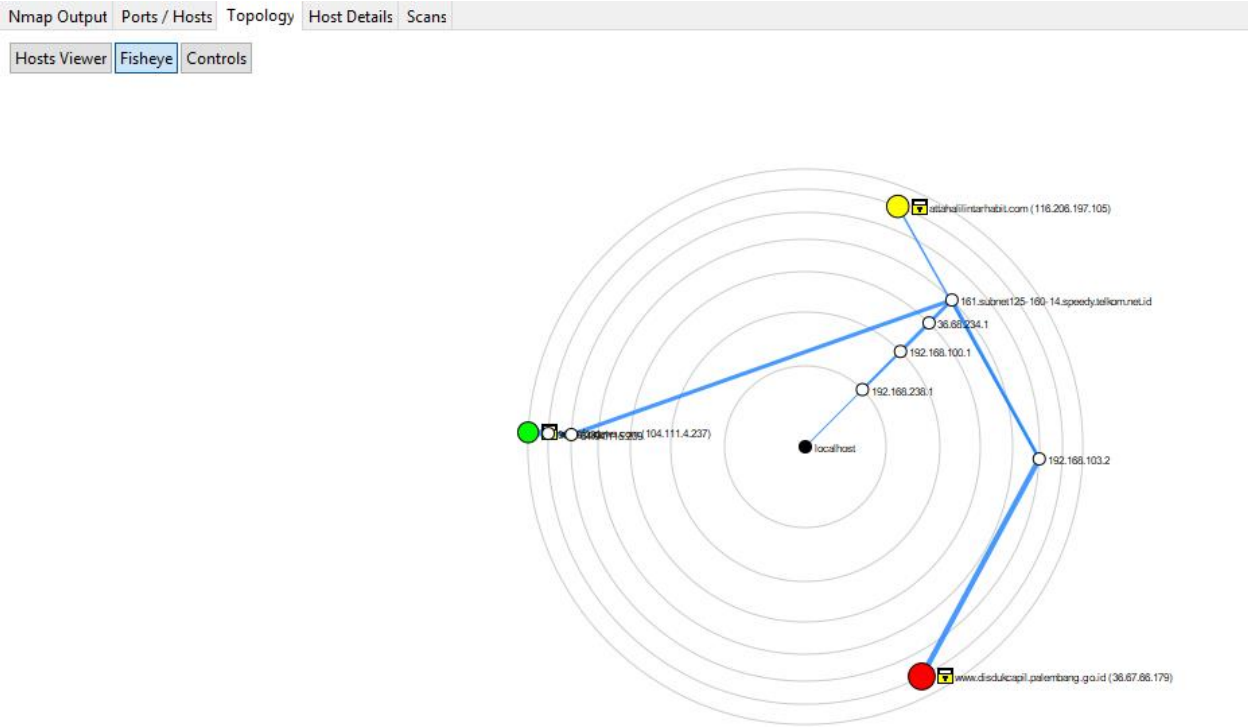
Dari hasil tersebut kita akan mengetahui beberapa hasilnya seperti pada tabel berikut:

No	Nama Situs	IP Address	Port	State	service
1	Attahalilintarhabbit.com	116.206.197.105	80/tcp	open	http
			443/tcp	open	http-proxy
			8081/tcp	open	http-proxy
2	foxnews.com	104.111.4.237	80/tcp	open	http
			443/tcp	open	http
3	disdukcapil.palembang.go.id	36.67.66.179	21/tcp	open	ftp
			53/tcp	open	domain
			80/tcp	open	nagios-nsca
			110/tcp	open	pop3
			143/tcp	open	imap
			465/tcp	open	smtp
			995/tcp	open	pop3
			2222/tcp	open	http

Untuk melihat grafiknyga klik “Topologi” maka akan muncul tampilan seperti gambar berikut




Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
attahalilintarhabit.com (116.206.197.105)
192.168.103.2
161.subnet125-160-14.speedy.telkom.net.id
36.68.234.1
192.168.100.1
192.168.238.1
localhost
61.94.115.209
36.89.220.1
www.foxnews.com (104.111.4.237)


Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
attahalilintarhabit.com (116.206.197.105)
161.subnet125-160-14.speedy.telkom.net.id
36.68.234.1
192.168.100.1
192.168.238.1
localhost
192.168.103.2
(104.111.4.237)
www.disdukcapil.palembang.go.id (36.67.66.179)