TUGAS

KEAMANAN JARINGAN KOMPUTER

Nama : Dede Triseptiawan

Nim : 09011181320001

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

Yang dimaksud dengan “reconnaissance” adalah suatu tahap persiapan dimana hacker atau pihak yang akan melakukan “serangan” berusaha mencari informasi sebanyak-banyaknya mengenai target atau sasaran sistem yang ingin diserang sebelum rangkaian proses penyerangan dilaksanakan.


## Background

| | | | |
|---|---|---|---|
| **Site title** | SUMEKS - Harian Pagi Sumatera Ekspres Palembang \| Koran Palembang \| Terbesar Di Sumatera Selatan \| Koran Sumsel \| Sumex \| Sumek | **Date first seen** | July 1997 |
| **Site rank** | | **Primary language** | Indonesian |
| **Description** | SUMEKS - Harian pagi Sumatera Ekspres Palembang menyajikan berita seputar Nasional, Internasional, Olahraga, Hiburan, ekonomi dan seluruh berita tentang palembang dan sumatera selatan. Sumatera Ekspres koran terbesar di sumatera selatan. metropolis, sumsel, xpresi, dor, weekend, society biz, berita utama, update news, headnews, berita terkini di palembang, berita terhangat di palembang, koran pagi palermbang, koran pagi sumsel, koran wong palembang, koran terbaik di palembang, koran sumeks, Sumex, Sumek | | |
| **Keywords** | *Not Present* | | |

Percobaan ini menggunakan web sumeks.co.id, yang merupakan web berita koran harian sumatera ekspres palembang

## Network

| | | | |
|---|---|---|---|
| **Site** | http://www.sumeks.co.id | **Netblock Owner** | PT Apik Media Inovasi |
| **Domain** | sumeks.co.id | **Nameserver** | ns1.sumeksgrup.com |
| **IP address** | 103.241.24.101 | **DNS admin** | managed@jetdino.com |
| **IPv6 address** | *Not Present* | **Reverse DNS** | *unknown* |
| **Domain registrar** | pandi.or.id | **Nameserver organisation** | *unknown* |
| **Organisation** | Pt. Citra Bumi Sumatera, Gedung Graha Pena Jl. Kol H Burlian No.773 KM.6,5, Palembang, 30152, Indonesia | **Hosting company** | apik.co.id |
| **Top Level Domain** | Indonesia (.co.id) | **DNS Security Extensions** | *unknown* |
| **Hosting country** | ID | | |

Pada gambar diatas didapat dari hasil capture web netcraft.com untuk melihat detail web sumeks, dimana pada hasil diatas ip dari sumeks.co.id adalah 103.241.24.101, dan web tersebut teregistrasi di pandi.or.id dan dibuat oleh pt.apik media inovasi(apik.co.id). Nama server pada web tersebut ns1.sumeksgrup.com dan admin DNS di kelola oleh managed@jetindo.com. Berikut hasil ping dan traceroute pc ke web sumeks.co.id

- Pada saat ping sumeks.co.id

PING sumeks.co.id (103.241.24.101) 56(84) bytes of data.
64 bytes from 103.241.24.101: icmp_seq=1 ttl=46 time=257 ms
64 bytes from 103.241.24.101: icmp_seq=2 ttl=46 time=253 ms
64 bytes from 103.241.24.101: icmp_seq=3 ttl=46 time=253 ms
64 bytes from 103.241.24.101: icmp_seq=4 ttl=46 time=257 ms
64 bytes from 103.241.24.101: icmp_seq=5 ttl=46 time=257 ms

--- sumeks.co.id ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 253.489/255.859/257.415/1.760 ms

- Pada saat traceroute

traceroute to sumeks.co.id (103.241.24.101), 30 hops max, 60 byte packets
1 ip-10-0-0-14.ec2.internal (10.0.0.14) 0.721 ms 0.719 ms 0.725 ms
2 216.182.224.140 (216.182.224.140) 20.556 ms 20.556 ms 20.586 ms
3 100.66.8.220 (100.66.8.220) 18.473 ms 100.66.8.212 (100.66.8.212) 12.553 ms 100.66.8.214 (100.66.8.214) 22.625 ms
4 100.66.10.98 (100.66.10.98) 22.456 ms 100.66.10.196 (100.66.10.196) 16.185 ms 100.66.10.46 (100.66.10.46) 19.634 ms
5 100.66.6.53 (100.66.6.53) 21.962 ms 100.66.6.227 (100.66.6.227) 46.931 ms 100.66.6.213 (100.66.6.213) 10.379 ms
6 100.66.4.177 (100.66.4.177) 17.520 ms 100.66.4.49 (100.66.4.49) 15.850 ms 100.66.4.109 (100.66.4.109) 16.968 ms
7 100.65.9.33 (100.65.9.33) 0.654 ms 100.65.9.225 (100.65.9.225) 0.632 ms 100.65.8.225 (100.65.8.225) 0.614 ms
8 205.251.245.54 (205.251.245.54) 1.452 ms 205.251.244.198 (205.251.244.198) 1.466 ms 205.251.245.235 (205.251.245.235) 1.466 ms
9 54.239.111.30 (54.239.111.30) 80.798 ms 54.239.111.18 (54.239.111.18) 9.896 ms 54.239.111.26 (54.239.111.26) 26.952 ms
10 54.239.108.177 (54.239.108.177) 1.621 ms 54.239.108.173 (54.239.108.173) 1.599 ms 54.239.111.227 (54.239.111.227) 3.983 ms
11 10gigabitethernet2-2.core1.ash1.he.net (206.126.236.37) 11.371 ms 11.000 ms v416.core1.ash1.he.net (209.51.168.65) 275.007 ms
12 100ge12-1.core1.par2.he.net (184.105.213.174) 85.884 ms 85.411 ms 84.702 ms
13 10ge3-1.core1.sin1.he.net (184.105.222.114) 268.430 ms 268.428 ms 261.202 ms
14 pt-multidata-rancana-prima.10gigabitethernet1-9.core1.sin1.he.net (27.50.36.154) 275.160 ms 275.128 ms 275.130 ms
15 202.72.204.14 (202.72.204.14) 273.714 ms 273.681 ms 273.690 ms
16 202.72.198.10 (202.72.198.10) 283.126 ms 281.547 ms 282.000 ms
17 103.241.24.101 (103.241.24.101) 251.434 ms 251.344 ms 251.393 ms

```
Domain ID:PANDI-DO274714
Domain Name:SUMEKS.CO.ID
Created On:17-Dec-1996 13:34:44 UTC
Last Updated On:20-Sep-2016 02:27:05 UTC
Expiration Date:01-Oct-2018 23:59:59 UTC
Status:clientTransferProhibited
Status:serverTransferProhibited
Registrant ID:04yudha5
Registrant Name:Yudha Pranata
Registrant Organization:PT. CITRA BUMI SUMATERA
Registrant Street1:Gedung Graha Pena Jl. Kol H Burlian No.773 KM.6,5
Registrant City:Palembang
Registrant State/Province:Sumatera Selatan
Registrant Postal Code:30152
Registrant Country:ID
Registrant Phone:+62.711411768x1234
Registrant FAX:+62.711420066
Registrant Email:yoedhas@gmail.com
```

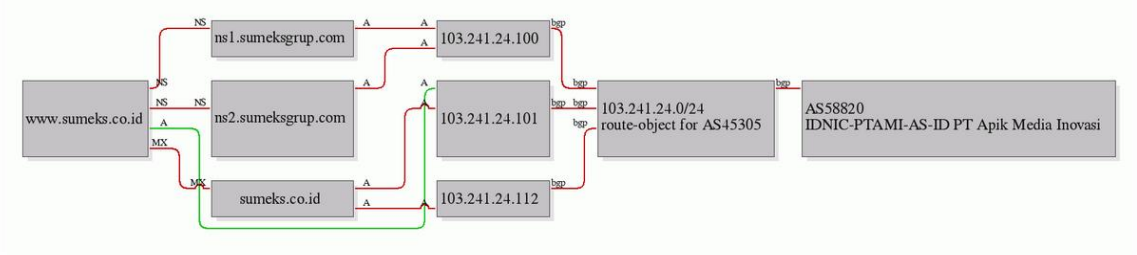
```
Sponsoring Registrar ID:indoreg
Sponsoring Registrar Organization:INDOREG
Sponsoring Registrar City:Jakarta
Sponsoring Registrar Postal Code:11520
Sponsoring Registrar Country:ID
Sponsoring Registrar Phone:0215821567
Name Server:ns1.sumeksgrup.com
Name Server:ns2.sumeksgrup.com
DNSSEC:Unsigned
```

Pada gambar diatas hasil whois dari web sumeks.co.id yang didapat dari http://allwhois.org berisi tentang nama domain, dibuat tahun berapa, kapan di update terakhir, kapan expired, dan data admin yang bertanggung jawab terhadap web tersebut lain-lain.

DNS Records for sumeks.co.id

| Hostname | Type | TTL | Priority | Content |
|---|---|---|---|---|
| sumeks.co.id | SOA | 86399 | | ns1.sumeksgrup.com managed@jetdino.com 2016123105 3600 7200 1209600 86400 |
| sumeks.co.id | NS | 86285 | | ns1.sumeksgrup.com |
| sumeks.co.id | NS | 86285 | | ns2.sumeksgrup.com |
| sumeks.co.id | A | 14399 | | 103.241.24.101 |
| sumeks.co.id | MX | 14399 | 0 | sumeks.co.id |
| www.sumeks.co.id | A | 7039 | | 103.241.24.101 |
| www.sumeks.co.id | CNAME | 7038 | | sumeks.co.id |
| www.sumeks.co.id | MX | 14399 | 0 | sumeks.co.id |

Ada beberapa jenis DNS yang terekam dari sumeks.co.id diantaranya, SOA record atau catatan otoritas awal (Start of Authority) mengacu server DNS yang mengediakan otorisasi informasi tentang sebuah domain Internet. NS record atau catatan server nama memetakan sebuah nama domain ke dalam satu daftar dari server DNS untuk domain tersebut. Pewakilan bergantung kepada record NS. A record atau catatan alamat memetakan sebuah nama host ke alamat IP 32-bit (untuk IPv4). A Record adalah DNS record yang paling sering dgunakan untuk memetakan hostname, yaitu untuk mengarahkan domain ke alamat IP tertentu. MX record atau catatan pertukaran surat memetakan sebuah nama domain ke dalam daftar mail exchange server untuk domain tersebut. CNAME record atau catatan nama kanonik membuat alias untuk nama domain. Domain yang di-alias-kan memiliki seluruh subdomain dan record DNS seperti aslinya. CNAME sering digunakan untuk mengarahkan beberapa domain atau subdomain ke webhosting yang sama. Berikut diagram sebuah domain web sumeks.co.id menuju BGP (Border Gateway Protocol) yang merupakan salah satu jenis routing protocol yang ada di dunia komunikasi data. Sebagai sebuah routing protocol, BGP memiliki kemampuan melakukan pengumpulan rute, pertukaran rute dan menentukan rute terbaik menuju ke sebuah lokasi dalam jaringan. Routing protocol juga pasti dilengkapi dengan algoritma yang pintar dalam mencari jalan terbaik.



## Hosting History

| Netblock owner | IP address | OS | Web server | Last seen Refresh |
|---|---|---|---|---|
| PT. Beon Intermedia Corporate / Direct member IDNIC Jalan Jemur Andayani 50 Komplek Ruko Surya Inti Permata Blok C 17 Surabaya | 103.27.207.138 | Linux | Apache/2.2.29 Unix mod_ssl/2.2.29 OpenSSL/1.0.1e-fips mod_bwlimited/1.4 | 21-May-2015 |
| PT. ARDH GLOBAL INDONESIA Corporate / Direct member IDNIC Komplek Ruko Golden Madrid II Blok B-23 BSD-City, Tangerang, Banten 15321. | 180.235.148.169 | Linux | Apache/2.2.15 Unix mod_ssl/2.2.15 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.13 mod_perl/2.0.4 Perl/v5.8.8 | 21-May-2014 |
| INDOSAT Internet Corporate Customer Palembang INDOSATs Internet Corporate Customer Palembang | 124.195.9.138 | Linux | - | 13-Sep-2013 |
| INDOSAT Internet Corporate Customer Palembang INDOSATs Internet Corporate Customer Palembang | 124.195.9.138 | Linux | Apache/2.2.8 FreeBSD mod_ssl/2.2.8 OpenSSL/0.9.8h DAV/2 PHP/5.2.6 with Suhosin-Patch | 14-Aug-2008 |
| kosong_256 Timur | 202.152.32.211 | Linux | Apache/2.0.40 | 20-Apr-2007 |

Pada gambar diatas sumeks.co.id pada tahun 2007 menggunakan kosong_256 timur sebagai netblock owner dengan os linux dan ip address 202.152.32.211 dengan web server apache versi 2.0.40. dan pada tahun yang terbaru 2015, sumeks.co.id menggunakan jasa netblock owner pt.beon intermedia corporate/direct member IDNIC dengan ip address 103.27.207.138 dan ,menggunakan os linux dengan webserver apache versi 2.2.29