

Keamanan Jaringan Komputer



Disusun Oleh

Nama : Kusuma Dwi Indriani

NIM : 09011181320017

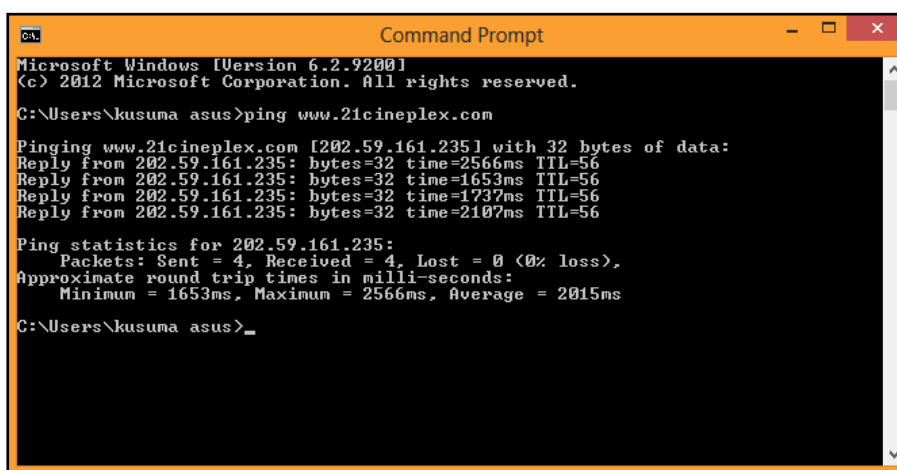
**JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA**

2017

TAHAP I. RECONNAISSANCE

Pada tahap ini yang dilakukan adalah mencari informasi dari situs target yang telah ditentukan, dalam hal ini situs yang digunakan adalah www.21cineplex.com. Adapun langkah yang dilakukan untuk mencari informasi situs target sebagai berikut:

1. **ping** 21cineplex.com pada Command Prompt untuk mendapatkan IP address dari situs target. IP address 21 cineplex.com adalah 202.59.161.235 (gambar.1)



```

Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\kusuma asus>ping www.21cineplex.com

Pinging www.21cineplex.com [202.59.161.235] with 32 bytes of data:
Reply from 202.59.161.235: bytes=32 time=2566ms TTL=56
Reply from 202.59.161.235: bytes=32 time=1653ms TTL=56
Reply from 202.59.161.235: bytes=32 time=1737ms TTL=56
Reply from 202.59.161.235: bytes=32 time=2107ms TTL=56

Ping statistics for 202.59.161.235:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1653ms, Maximum = 2566ms, Average = 2015ms

C:\Users\kusuma asus>_

```

Gambar 1. Ping 21cineplex.com

2. Cari informasi dari IP 202.59.161.235 dengan menggunakan situs **who.is**. dari sana didapat informasi berupa registrant contact information, administrative contact information, technical contact information (gambar.2)

Name	NA 21CINEPLEX
Organization	PT NUSANTARA SEJAHTERA RAYA
Address	JL. K.H WAHID HASYIM NO. 96 BLDG C
City	JAKARTA
State / Province	DKI
Postal Code	10340
Country	ID
Phone	+62.2131901188
Email	AGUSRT@GMAIL.COM

who.is Search for domains or IP addresses... Premium Domains Transfer Features

21cinema.com | 21cinema.info | 21cinema.info.tr | 21cinema.net | 21cinema.ru |

Registrar Data Make Private

Registrant Contact Information:

Name	NA 21CINEPLEX
Organization	PT NUSANTARA SEJAHTERA RAYA
Address	JL. K.H WAHID HASYIM NO. 96 BLDG C
City	JAKARTA
State / Province	DKI
Postal Code	10340
Country	ID
Phone	+62.2131901188
Email	AGUSRT@GMAIL.COM

Administrative Contact Information:

Name	NA 21CINEPLEX
Organization	PT NUSANTARA SEJAHTERA RAYA
Address	JL. K.H WAHID HASYIM NO. 96 BLDG C
City	JAKARTA
State / Province	DKI
Postal Code	10340
Country	ID
Phone	+62.2131901188
Email	AGUSRT@GMAIL.COM

Technical Contact Information:

Name	NA 21CINEPLEX
Organization	PT NUSANTARA SEJAHTERA RAYA
Address	JL. K.H WAHID HASYIM NO. 96 BLDG C
City	JAKARTA
State / Province	DKI
Postal Code	10340
Country	ID
Phone	+62.2131901188
Email	AGUSRT@GMAIL.COM

Information Updated: 2017-02-15 09:16:45

Gambar 2. Informasi Registrar Data Situs 21cineplex.com menggunakan who.is

who.is Search for domains or IP addresses... Premium Domains Transfer Features

Status clientTransferProhibited https://www.icann.org/epp/clientTransferProhibited

Important Dates

Expires On	2022-11-10
Registered On	1999-11-10
Updated On	0000-00-00

Name Servers

DNS1.NAME-SERVICES.COM	162.88.61.23
DNS2.NAME-SERVICES.COM	162.88.60.23
DNS3.NAME-SERVICES.COM	162.88.61.39
DNS4.NAME-SERVICES.COM	162.88.60.39
DNS5.NAME-SERVICES.COM	162.88.61.41

Similar Domains

21cin.com | 21cinamplex.com | 21cinaplex.com | 21cinc.com | 21cincd.com | 21cine.com | 21cine0lex.com | 21cineplex.com | 21cineex.com | 21cineflex.com | 21cineflex.com | 21cineplex.com | 21cineplex.com | 21cineplex.com | 21cinem.com | 21cinema.biz | 21cinema.com | 21cinema.info | 21cinema.info.tr | 21cinema.net | 21cinema.ru |

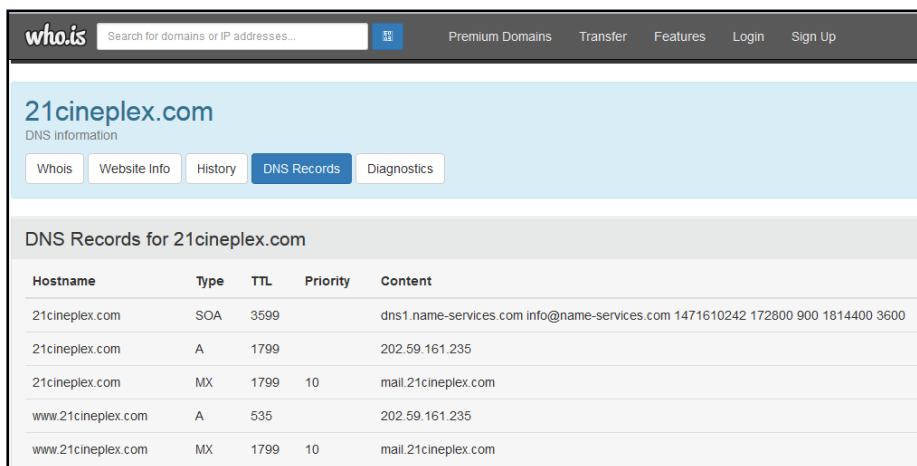
Registrar Data Make Private

Registrant Contact Information:

Name	NA 21CINEPLEX
Organization	PT NUSANTARA SEJAHTERA RAYA
Address	JL. K.H WAHID HASYIM NO. 96 BLDG C
City	JAKARTA
State / Province	DKI
Postal Code	10340
Country	ID
Phone	+62.2131901188
Email	AGUSRT@GMAIL.COM

Gambar 3. Informasi Registrar Data Situs 21cineplex.com menggunakan who.is

Situs 21cineplex.com teregistrasi pada 10 11 1999 dan akan *expire* pada 10 11 2022. Sedangkan untuk mengetahui DNS record dapat melihat info di tab DNS record web who.is (gambar.4)



The screenshot shows the 'who.is' website interface for the domain '21cineplex.com'. The 'DNS Records' tab is selected, displaying a table of DNS records. The table has columns for Hostname, Type, TTL, Priority, and Content. The records listed are:

Hostname	Type	TTL	Priority	Content
21cineplex.com	SOA	3599		dns1.name-services.com info@name-services.com 1471610242 172800 900 1814400 3600
21cineplex.com	A	1799		202.59.161.235
21cineplex.com	MX	1799	10	mail.21cineplex.com
www.21cineplex.com	A	535		202.59.161.235
www.21cineplex.com	MX	1799	10	mail.21cineplex.com

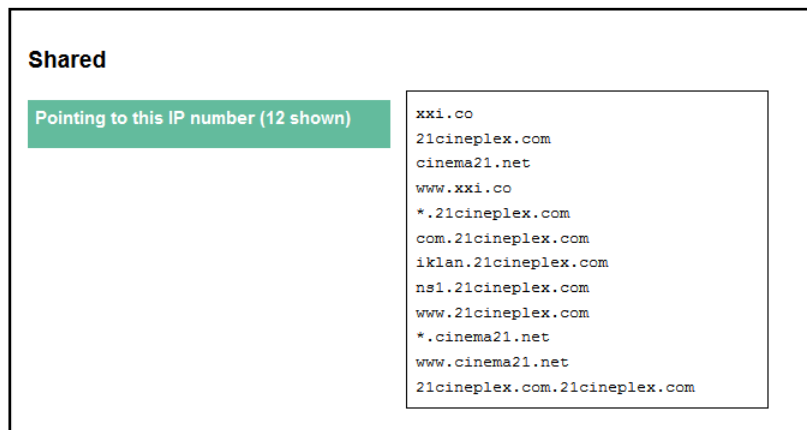
Gambar 4. Informasi DNS record Situs 21cineplex.com menggunakan who.is

Pada DNS record didapatkan informasi tentang domain name server yang digunakan oleh situs target seperti jenis DNS, waktu, priority dan konten. Dari gambar terlihat bahwa terdapat berbagai tipe DNS record yaitu SOA, A, dan MX.

- **SOA** : catatan otoritas yang menyediakan informasi server DNS tentang sebuah domain internet.
- **A** : catatan alamat memetakan sebuah nama host ke alamat IP 32-bit
- **MX** : catatan pertukaran surat memetakan sebuah nama domain ke dalam daftar mail exchange server untuk domain tersebut.

3. **Reverse IP domain Check** 202.59.161.235 melalui robtex.com untuk mengetahui user aktif atau nama domain lain yang merujuk pada web server

yang sama. Terdapat 12 nama host yang merujuk pada alamat IP 202.50.161.235 (gambar.5)



Gambar 5. Nama-nama host lain yang memiliki alamat ip 202.59.161.235 menggunakan robtex.com

Dianalisa bahwa dari 12 nama host semua hanya memiliki satu alamat IP yaitu 202.59.161.235. Tujuh dari host tersebut menggunakan mail server MAIL.21CINEPLEX.COM. Dua dari host menggunakan server NS05 dan NS06.DOMAINCONTROL.COM kemudian menjadi “nama server grup 1”. Dua menggunakan server mail ASPMX2.GOOGLEMAIL.COM, ASPMX3.GOOGLEMAIL.COM, ASPMX.L.GOOGLE.COM, ALT1.ASPMX.L.COM, dan ALT2.ASPMX.L.GOOGLE.COM kemudian menjadi “mail server group 1”. Dan satu dari host tersebut menggunakan nama server DNS1, DNS2, DNS3, DNS5.NAME-SERVICE.COM.