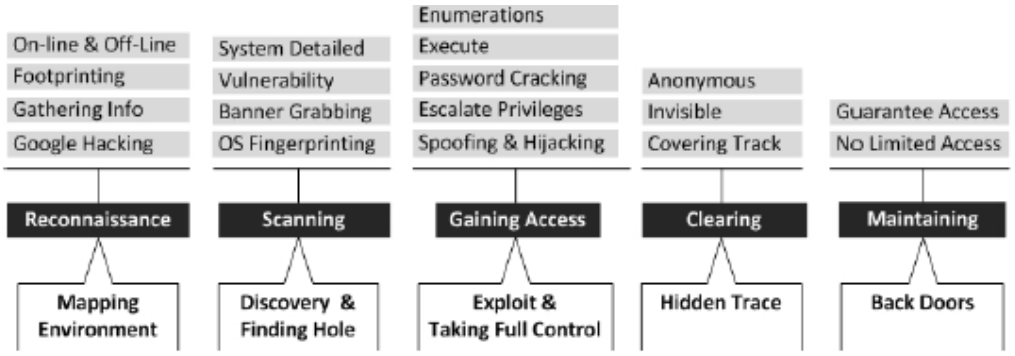
Dimas Wahyudi / 09011281320004
Fakultas Ilmu Komputer, Sistem Komputer, Universitas Sriwijaya
mail.dimaswahyudi@gmail.com

Reconnaissance

Dasar Teori : *Reconnaissance*

Reconnaissance adalah tahap kegiatan dimana penyerang mengumpulkan informasi sebanyak mungkin mengenai target. Informasi yang diperoleh dari hasil kegiatan ini berupa informasi dasar yang berguna, seperti : *IP Address, topology network, network resources* dan informasi personal tentang *user* yang diperlukan untuk tahap selanjutnya. Pada tahapnya, s*earch engine* umumnya digunakan untuk memperoleh informasi dari sumber *online*, saat *offline* pengumpulan informasi dicapai dengan membawa bagian dari informasi yang tersebar ditambah dengan rekayasa sosial (*social engineering*) sebagai data digunakan untuk melakukan pengintaian terhadap lingkungan target. *Reconnaissance* terdiri dari : (1) *active reconnaissance* berupa aktivitas pengumpulan data dengan bertatap muka langsung dengan target, hal ini berkaitan dengan pengumpulan informasi secara *offline* dengan informasi awal yang diperoleh dari informasi *online*. (2) *passive reconnaissance* adalah aktivitas pengumpulan data melalui media perantara, seperti berita media masa televisi, radio, koran, maupun internet, dimana berita tersebut disajikan oleh pihak di luar target. *Reconnaissance* merupakan tahapan pertama dalam melakukan percobaan untuk menembus atau menyerang (*attack*) sebuah sistem. Ada beberapa langkah dan teknik yang umumnya digunakan ketika mencoba menembus atau menyerang (*attack*) sebuah sistem, seperti terlihat pada gambar 1.



Gambar 1. Langkah dan teknik penyerangan (*attack*)

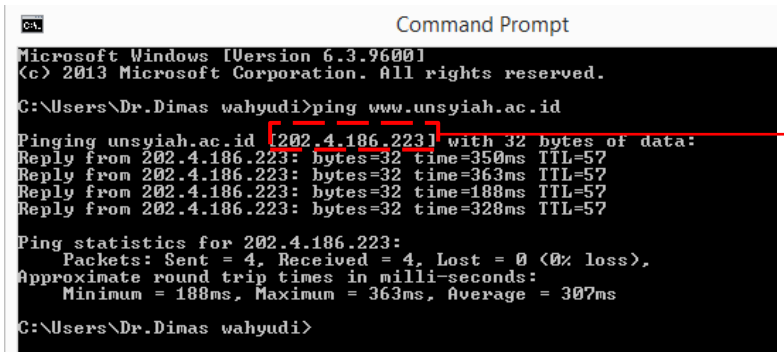
Percobaan : *Reconnaissance*

Target : www.unsyiah.ac.id

Sebelum melakukan tahap *penetration tester*, kita perlu untuk memeriksa *reachability* dari komputer di jaringan. Ping adalah salah satu utilitas yang akan memungkinkan untuk mengumpulkan informasi penting seperti *IP Address*, *maximum packet frame size*, jumlah *hop* dan informasi lainnya.

Dimas Wahyudi / 09011281320004
Fakultas Ilmu Komputer, Sistem Komputer, Universitas Sriwijaya
mail.dimaswahyudi@gmail.com

Tahap : Mencari *IP Address*

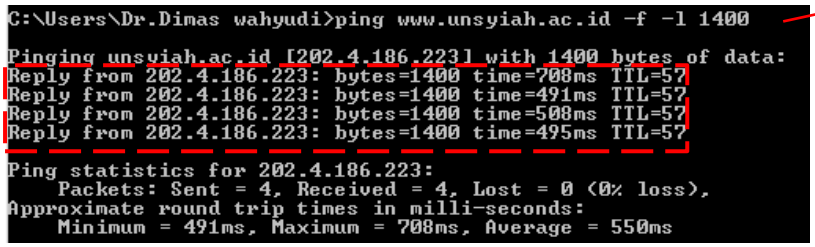


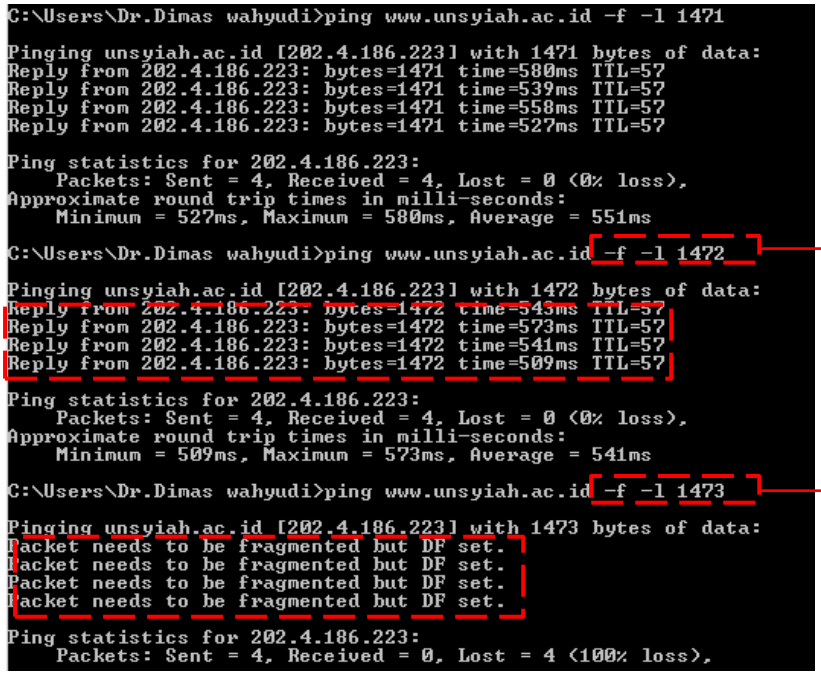
***IP Address* : 202.4.186.223**

Tahap : *Maximum frame size*

DF : *Frame size* terlalu besar

1500 < *Frame size* > 1400





Maximum frame size* = 1472 *bytes

DF : *Frame size* terlalu besar

Dari percobaan diatas diketahui bahwa ukuran *frame size* target adalah kurang dari 1500 *bytes* dan besar dari 1400 *bytes* (1500 *bytes* < *frame size* > 1400 *bytes*). Maka dari informasi awal ini kita dapat mengukur dengan melakukan tes mulai dari nilai > 1400 *bytes*, hingga kita menemukan *maximum frame size* adalah 1472 *bytes*.

Tahap : Mengukur jumlah hop

```
C:\Users\Dr.Dimas wahyudi>ping www.unsyiah.ac.id -i 1 -n 1

Pinging unsyiah.ac.id [202.4.186.223] with 32 bytes of data:
Reply from 192.168.43.1: TTL expired in transit.

Ping statistics for 202.4.186.223:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

C:\Users\Dr.Dimas wahyudi>ping www.unsyiah.ac.id -i 2 -n 1

Pinging unsyiah.ac.id [202.4.186.223] with 32 bytes of data:
Request timed out.

Ping statistics for 202.4.186.223:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

C:\Users\Dr.Dimas wahyudi>ping www.unsyiah.ac.id -i 3 -n 1

Pinging unsyiah.ac.id [202.4.186.223] with 32 bytes of data:
Request timed out.

Ping statistics for 202.4.186.223:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

C:\Users\Dr.Dimas wahyudi>ping www.unsyiah.ac.id -i 4 -n 1

Pinging unsyiah.ac.id [202.4.186.223] with 32 bytes of data:
Request timed out.

Ping statistics for 202.4.186.223:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

C:\Users\Dr.Dimas wahyudi>ping www.unsyiah.ac.id -i 5 -n 1

Pinging unsyiah.ac.id [202.4.186.223] with 32 bytes of data:
Reply from 114.120.194.85: TTL expired in transit.
```

```
C:\Users\Dr.Dimas wahyudi>ping www.unsyiah.ac.id -i 9 -n 1

Pinging unsyiah.ac.id [202.4.186.223] with 32 bytes of data:
Reply from 36.66.26.22: TTL expired in transit.

Ping statistics for 202.4.186.223:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

C:\Users\Dr.Dimas wahyudi>ping www.unsyiah.ac.id -i 10 -n 1

Pinging unsyiah.ac.id [202.4.186.223] with 32 bytes of data:
Reply from 202.4.186.223: bytes=32 time=166ms TTL=57

Ping statistics for 202.4.186.223:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 166ms, Maximum = 166ms, Average = 166ms
```

TTL Response = 10 hops

Dari percobaan diatas diketahui bahwa ping yang berhasil mencapai www.unsyih.ac.id adalah 15 hops, dimana output akan sama dengan hasil trace route.

Tahap : *nslookup*

Nslookup digunakan untuk melihat informasi seputar Domain Name Systems (DNS) pada sebuah domain. Dengan menggunakan web tools seperti www.who.is kita dapat memproleh informasi terkait domain target, seperti NS (Name Server), CNAME (Canonical of an alias), MX (Mail Exchager), dan informasi lainnya.

Dimas Wahyudi / 09011281320004
Fakultas Ilmu Komputer, Sistem Komputer, Universitas Sriwijaya
mail.dimaswahyudi@gmail.com

https://who.is/whois/unsyiah.ac.id

Name Servers

NS.UNSYIAH.AC.ID	180.250.115.21
NS3.UNSYIAH.AC.ID	202.4.186.5

Non-Authoritative Answer

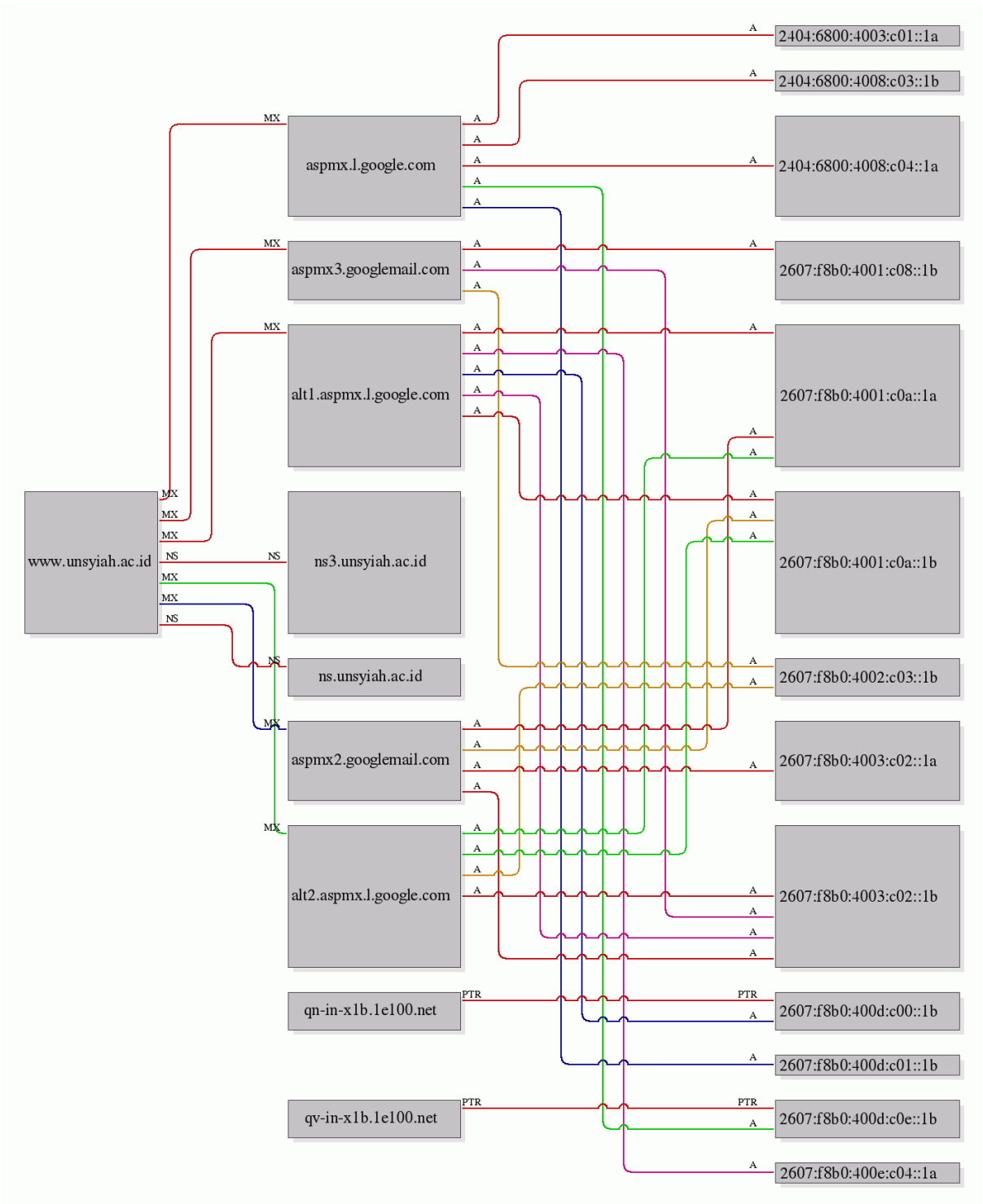
DNS Records for unsyiah.ac.id

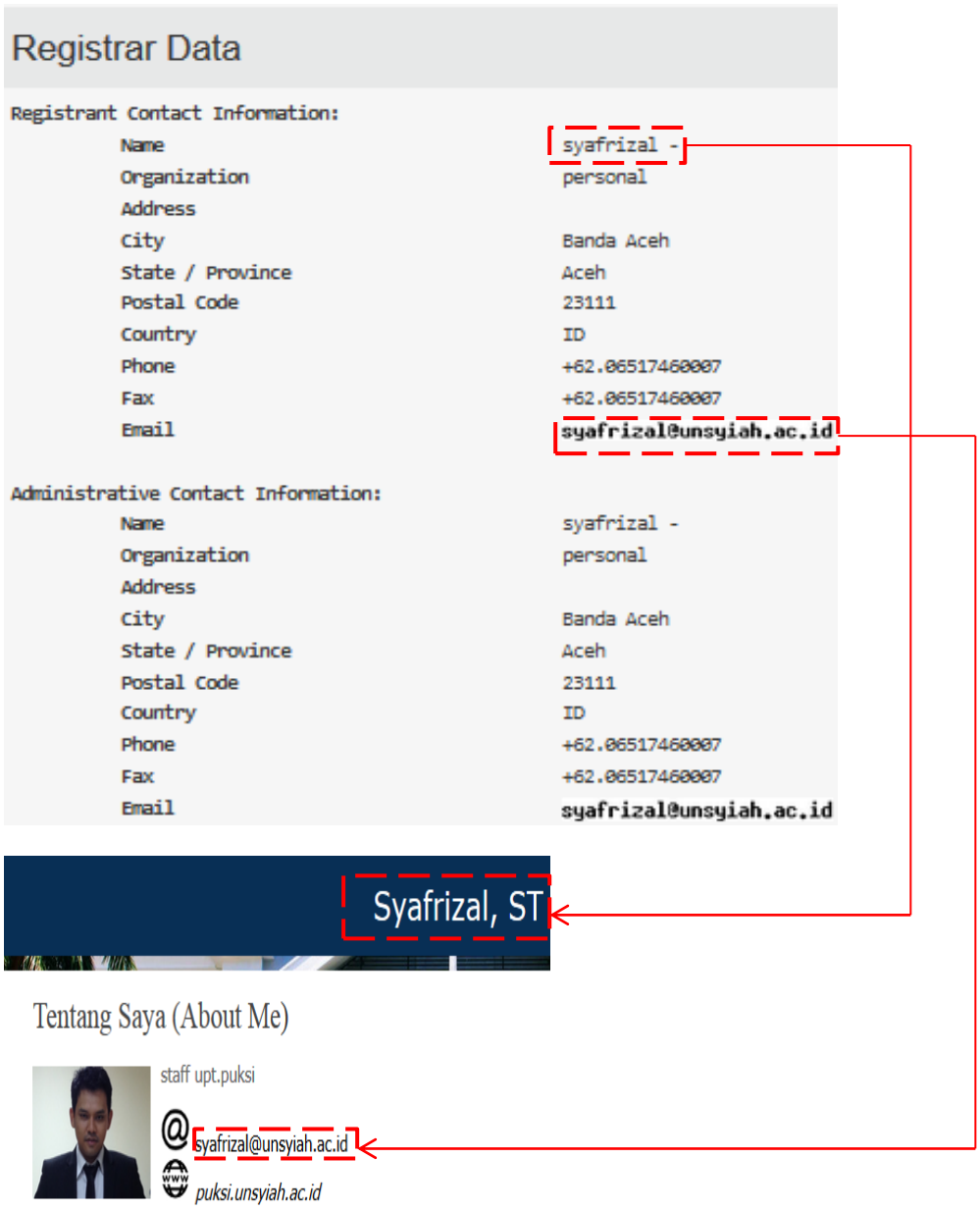
Hostname	Type	TTL	Priority	Content
unsyiah.ac.id	SOA	38399		ns.unsyiah.ac.id info@unsyiah.ac.id 2015012101 10800 3600 1209600 38400
unsyiah.ac.id	NS	14399		ns3.unsyiah.ac.id
unsyiah.ac.id	NS	14399		ns.unsyiah.ac.id
unsyiah.ac.id	A	5518		202.4.186.223
unsyiah.ac.id	MX	2762	5	alt1.aspmx.l.google.com
unsyiah.ac.id	MX	2762	5	alt2.aspmx.l.google.com
unsyiah.ac.id	MX	2762	10	aspmx2.googlemail.com
unsyiah.ac.id	MX	2762	10	aspmx3.googlemail.com
unsyiah.ac.id	MX	2762	1	aspmx.l.google.com
www.unsyiah.ac.id	A	14399		202.4.186.223
www.unsyiah.ac.id	CNAME	14399		unsyiah.ac.id
www.unsyiah.ac.id	MX	3599	5	alt1.aspmx.l.google.com
www.unsyiah.ac.id	MX	3599	5	alt2.aspmx.l.google.com
www.unsyiah.ac.id	MX	3599	10	aspmx3.googlemail.com
www.unsyiah.ac.id	MX	3599	1	aspmx.l.google.com

DNS record types

	Type	Name	Function
Zone	SOA	Start Of Authority	Defines a DNS zone
	NS	Name Server	Identifies servers, delegates subdomains
Basic	A	IPv4 Address	Name-to-address translation
	AAAA	IPv6 Address	Name-to-IPv6-address translation
	PTR	Pointer	Address-to-name translation
	MX	Mail Exchanger	Controls email routing
Security and DNSSEC	DS	Delegation Signer	Hash of signed child zone's key-signing key
	DNSKEY	Public Key	Public key for a DNS name
	NSEC	Next Secure	Used with DNSSEC for negative answers
	NSEC3[a]	Next Secure v3	Used with DNSSEC for negative answers
	RRSIG	Signature	Signed, authenticated resource record set
	DLV	Lookaside	Nonroot trust anchor for DNSSEC
	SSHFP	SSH Fingerprint	SSH host key, allows verification via DNS
	SPF	Sender Policy	Identifies mail servers, inhibits forging
	DKIM	Domain Keys	Verify email sender and message integrity
Optional	CNAME	Canonical Name	Nicknames or aliases for a host
	SRV	Services	Gives locations of well-known services
	TXT	Text	Comments or untyped information[b]

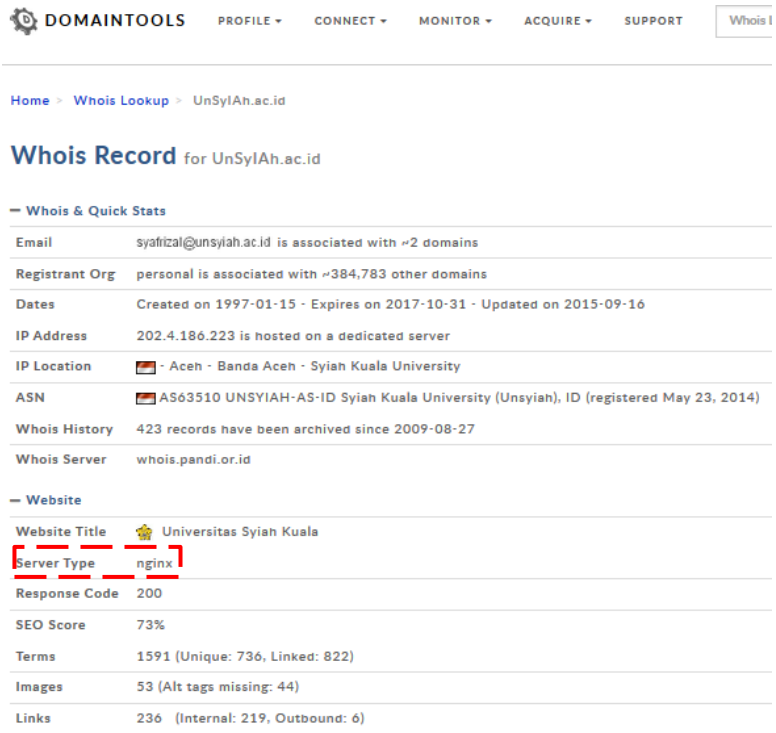
Dimas Wahyudi / 09011281320004
Fakultas Ilmu Komputer, Sistem Komputer, Universitas Sriwijaya
mail.dimaswahyudi@gmail.com





Dari informasi yang diperoleh diketahui bahwa yang bersangkutan melakukan register dengan nama asli. Dari informasi ini kita dapat menelusuri informasi personal yang bersangkutan, diketahui bahwa yang bersangkutan adalah seorang staff UPT PUKSI dari universitas syiah kuala.

Dimas Wahyudi / 09011281320004
Fakultas Ilmu Komputer, Sistem Komputer, Universitas Sriwijaya
mail.dimaswahyudi@gmail.com



Dari informasi diatas diketahui bahwa tipe server yang digunakan adalah *nginx*. *Nginx* adalah server HTTP dan *Proxy* dengan kode sumber terbuka yang bisa juga berfungsi sebagai *proxy* IMAP/POP3. Dengan adanya informasi ini memungkinkan kita untuk mencari celah pada server yang menggunakan nginx, informasi ini dapat kita peroleh melalui situs seperti www.cve.mitre.org.

Daftar Pustaka

[1] A. H. Abdullah, "Cyber-Attack Penetration Test and Vulnerability Analysis," vol. 13, no. 1, pp. 125–132.

[2] I. C. of E.-C. C. (EC-Council), "Footprinting and Reconnaissance," *Certif. Ethical Hacker V8.00*.