Ir. Budi Rahardjo, M.Sc., Ph.D

Teknik Komputer – STEI ITB

Casing The Joint

Mencari Informasi Awal Sebelum Menyerang Target

II3230 - Keamanan Informasi

Casing The Joint

Mencari Informasi Awal

Sebelum menyerang/mengevaluasi dari Target

1. slang. To **observe a place** in order to **familiarize** oneself with its workings in preparation for some criminal activity (often robbery). Judging from the security footage, those men **cased the joint** hours before robbing it.
2. slang. By extension, to thoroughly examine a place.

Reconnaissance

re·con·nais·sance

rəˈkänəsəns/

noun

noun: **reconnaissance**; plural noun: **reconnaissances**

- military observation of a region to locate an enemy or ascertain strategic features.
- preliminary surveying or research.

Cari Informasi Tentang Target

- Footprinting:
  - mencari *company profile* (dari sisi securitynya):
    apakah perusahaan sedang membuka kantor cabang baru?
- Scanning:
  - mencari “pintu” dan “jendela” yang terbuka
- Membuat tabel tentang target
  - Nomor IP, nama, alive?, services, jenis OS

Contoh tabel target (bank.co.id)

Inilah tabel yang ingin kita penuhi
Catatan: awalnya tabel kosong

Nama	No IP	Alive	OS	Services
www.bank.co.id	10.10.1.80	ya	Windows server	http, https
file.bank.co.id	10.10.1.143	ya	Windows 2000, SP3	NetBIOS, samba, ftp, http, https
mail.bank.co.id	10.10.1.25	ya	Linux	SMTP
…				…

FOOTPRINTING

- Internet/Intranet
  - **Domain Name System** (DNS)
  - TCP / UDP services pada setiap sistem
  - Arsitektur / OS
  - SNMP, routing table
- Remote access
  - Nomor telepon akses & authentication

Domain Name System (DNS)

[dilanjutkan ke slides khusus DNS]

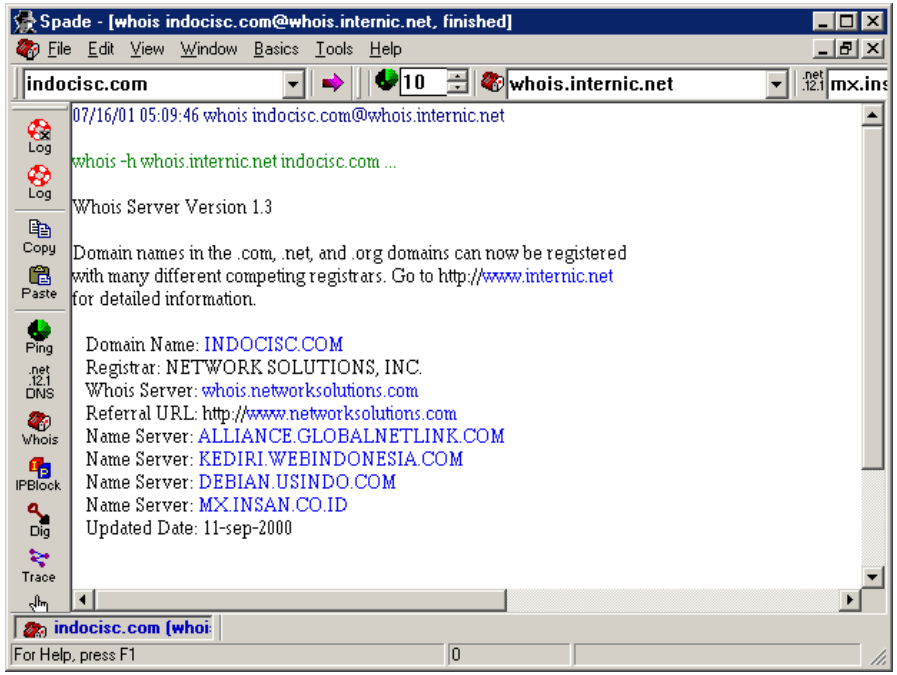
Data dari nama domain

- Menggunakan tools: whois, dig, nslookup, host, bahkan search engine
  - Data server dari target (Name Server), alamat kantor, nomor IP, MX record
  - Komputer-komputer dan nomor IP-nya
  - Sebagian besar dari data ini tersedia untuk publik
    (analogi: sama dengan alamat dari sebuah perusahaan)

whois

- `Unix% whois “acme.”@whois.crsnic.net`
- `Unix% whois “acme.net”@whois.crsnic.net`
- `Unix% whois acme.net@whois.networksolutions.com`

Whois dengan Sam Spade



Program “nslookup”

- Nslookup untuk mencari informasi domain
- `Unix% **nslookup ns @dns.server domain.name**`
- Zone transfer dengan nslookup

```
Unix% nslookup
> server 167.205.21.82
> set type=any
> ls -d Acme.net >> /tmp/zone_out
> ctrl-D

more /tmp/zone_out
```

Program “host”

- Mencari informasi mengenai name server (ns), mail record (mx), dll.
- `Unix% **host www.indocisc.com**`
  `www.indocisc.com has address 202.138.225.178`
- `Unix% **host -t ns indocisc.com**`
  `indocisc.com name server home.globalnetlink.com.`
  `Indocisc.com name server mx.insan.co.id.`
- `Unix% **host -t mx indocisc.com**`
  `indocisc.com mail is handled by 5`
  `mx.insan.co.id.`
- `Unix% **host -l indocisc.com mx.insan.co.id**`

Masih Tentang DNS

- Zone transfer harusnya dibatasi
- Zone transfer via web
  - ada beberapa situs web yang menyediakan layanan ini

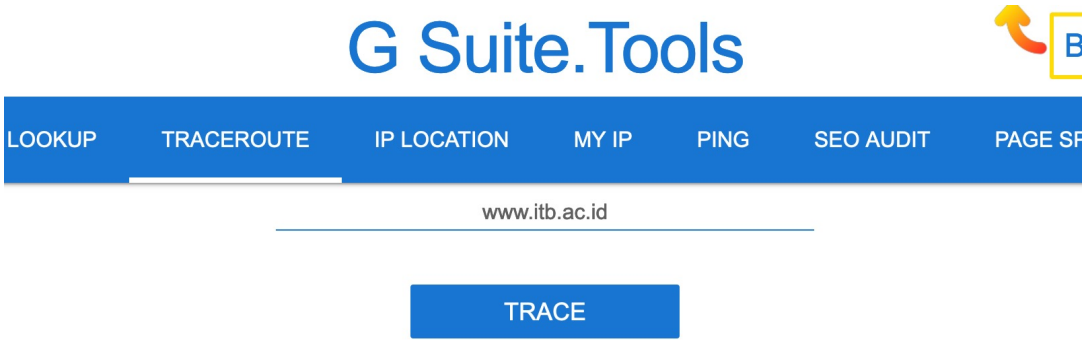
Routing

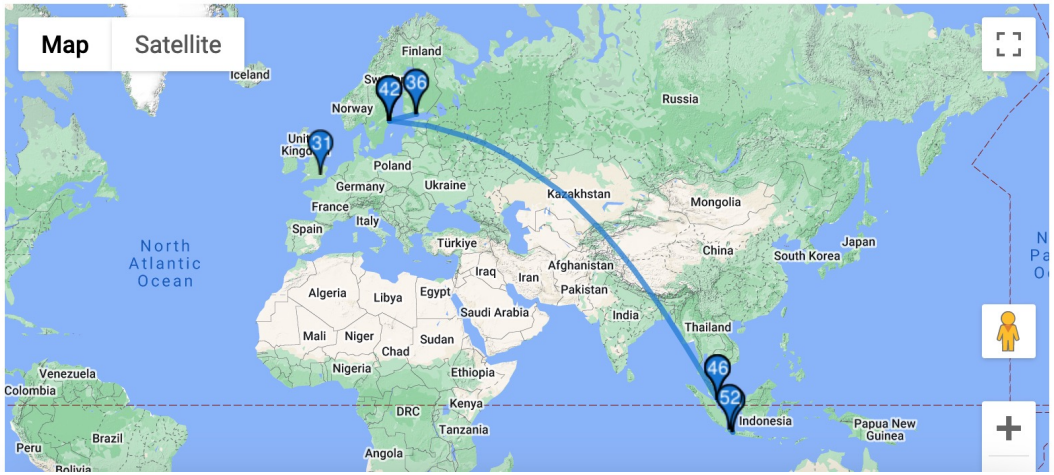
- Traceroute untuk mengetahui routing
- Unix

  `traceroute 167.205.21.82`
- Windows

  `DOS> tracert 167.205.21.82`
- Web
  - `GSuite`

https://gsuite.tools/traceroute





Tabel target

- Tabel mulai terisi

Nama	No IP	Alive	OS	Services
www.bank.co.id	10.10.1.80	…	…	…
file.bank.co.id	10.10.1.143	…	…	…
mail.bank.co.id	10.10.1.25	…	…	…
…				…

Host (komputer) hidup?

- Ping, fping, gping, hping
  mencari host yang hidup (*alive*)
- `Unix% fping -g 192.168.1.0/24`
- `Unix% gping 192.168.1.1`
- Membutuhkan ICMP traffic
- `Unix% hping 192.168.1.2 -S -p 80 -f`

Ping dengan NMAP

- `Unix% nmap -sP 192.168.1.0/24`
- Kalau ICMP diblokir
  `nmap -sP -PT80 192.168.1.0/24`
  mengirimkan paket ACK dan menunggu paket RST untuk menandakan host alive

ICMP Query

- Mencari informasi dengan mengirimkan paket ICMP
  - `Unix% icmpquery -t 192.168.1.1`
    `192.168.1.1 : 11:36:19`
  - `Unix% icmpquery -m 192.168.1.1`
    `192.168.1.1 : 0xFFFFFFE0`

Tabel target

- Tabel mulai terisi

Nama	No IP	Alive	OS	Services
www.bank.co.id	10.10.1.80	ya	…	…
Fileserver.bank.co.id	10.10.1.143	?	…	…
mail.bank.co.id	10.10.1.25	ya	…	…
…				…

Servis di Internet

- /etc/services

```
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
ftp             21/tcp
ssh             22/tcp
telnet          23/tcp
```

- Dijalankan melalui *inetd* atau sebagai *daemon* (di belakang layar)

Servis via inetd

- Serivis dicatat dalam berkas `/etc/inetd.conf` :

```
# contoh
# <service_name> <sock_type> <proto> <flags> <user> <server_path>
<args>

ftp             stream  tcp     nowait  root    /usr/sbin/tcpd
/usr/local/sbin/proftpd

pop-3           stream  tcp     nowait  root    /usr/sbin/tcpd
/usr/sbin/ipop3d
```


Scanning / Probing

- UNIX
  - Nmap

    ```
    nmap -sS 192.168.1.1
    nmap -sF 192.168.1.0/24 -oN outfile
    ```

  - Netcat:

    ```
    nc -v -z -w2 192.168.1.1 1-140
    nc -u -v -z -w2 192.168.1.1 1-140
    ```

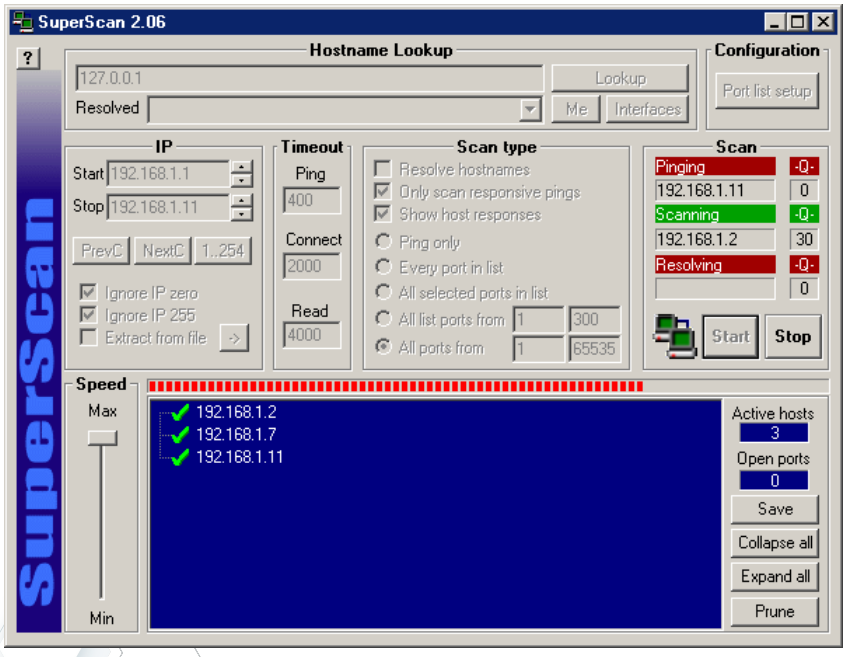
  - udp_scan

$ nmap localhost

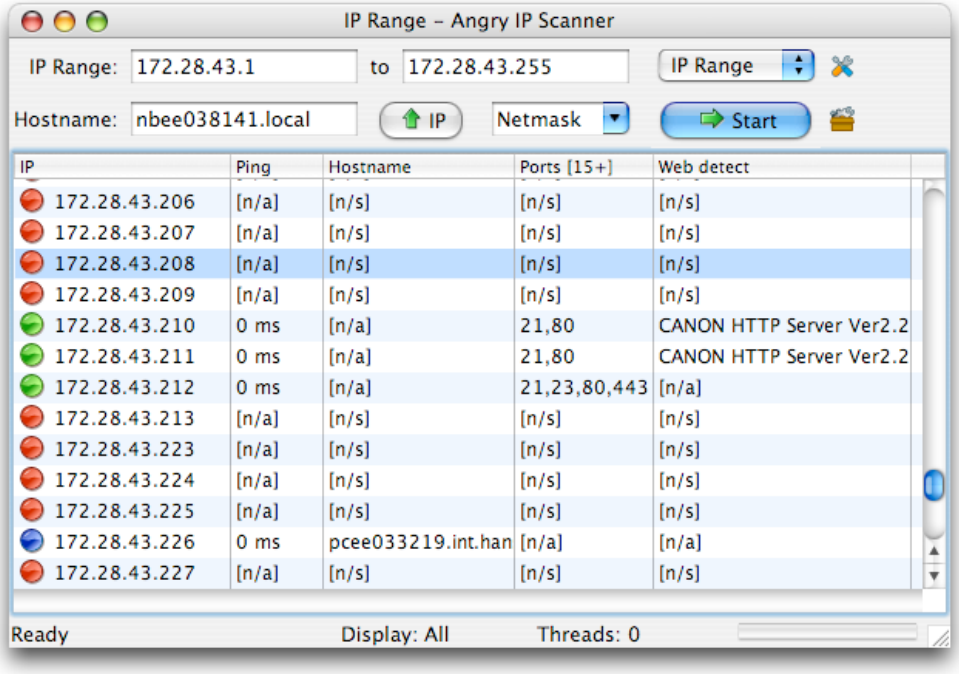
```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-20 11:20 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00015s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT    STATE SERVICE
7/tcp   open  echo
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds
```

Scanning Tools: Windows | MacOS

- SuperScan



- Angry Scanner



Jenis Scan

- TCP connect scan
- TCP SYN scan
- TCP FIN scan
- TCP Xmas Tree scan
- TCP Null scan
- TCP ACK scan
- TCP Window scan
- TCP RPC scan
- UDP scan

Deteksi Scanning

- Syslog, icmplog
- **root# tail /var/log/syslog**

```
May 16 15:40:42 epson tcplogd: "Syn probe"
notebook[192.168.1.4]:[8422]>epson[192.168.1.2]:[635]
May 16 15:40:42 epson tcplogd: "Syn probe"
notebook[192.168.1.4]:[8423]>epson[192.168.1.2]:ssl-ldap
May 16 15:40:42 epson tcplogd: "Syn probe"
notebook[192.168.1.4]:[8426]>epson[192.168.1.2]:[637]
May 16 15:40:42 epson tcplogd: "Syn probe"
notebook[192.168.1.4]:[8429]>epson[192.168.1.2
```


Penangkal Scanning

- Langsung melakukan pemblokiran
  - access control list (/etc/hosts.deny)
  - mengubah routing table (drop packet)
  - mengubah rule dari firewall
  - Contoh software: portsentry, IPS

Tabel target

- Mulai terisi

Nama	No IP	Alive	OS	Services
www.bank.co.id	10.10.1.80	ya	…	web
Fileserver.bank.co.id	10.10.1.143	?	…	File sharing, web, ftp
mail.bank.co.id	10.10.1.25	ya	…	SMTP
…				…

OS Fingerprinting

- Menentukan jenis OS dengan melihat ciri implementasi TCP/IP stack
  - Queso
  - Nmap
    ```
    nmap -O 192.168.1.1
    ```
  - X (passive OS detection)

Initial TTL & TCP Window Size

(SYN or SYN+ACK packet)

https://www.netresec.com/?page=Blog&month=2011-11&post=Passive-OS-Fingerprinting

Operating System (OS)	IP Initial TTL	TCP window size
Linux (kernel 2.4 and 2.6)	64	5840
Google's customized Linux	64	5720
FreeBSD	64	65535
Windows XP	128	65535
Windows 7, Vista and Server 2008	128	8192
Cisco Router (IOS 12.4)	255	4128

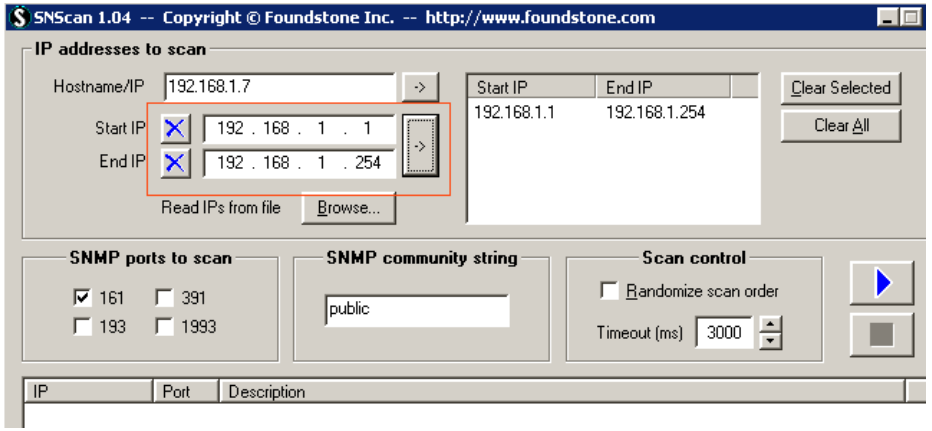
Application fingerprinting

- Banner grabbing: dari aplikasi (misal SMTP)
  telnet server.name 25
- `echo -e "GET /index.html HTTP/1.0\n\n" | nc 192.168.1.3 80 | less`

```
Date: Sat, 27 Apr 2002 02:34:10 GMT
Server: Apache/1.3.24 (Unix) Debian GNU/Linux PHP/4.1.2
Last-Modified: Thu, 19 Jul 2001 13:21:07 GMT
ETag: "fa59-ffe-3b56dec3"
Accept-Ranges: bytes
Content-Length: 4094
Connection: close
Content-Type: text/html; charset=iso-8859-1
```


Deteksi melalui SNMP

- `indocisc% snmpget 192.168.0.1 public system.sysDescr.0`
  `system.sysDescr.0 = Linux agumon 2.4.18 #1 SMP Web Apr 24 04:33:13 WIT 2002 i686`
- *Syntax: snmpwalk target community oid*
- `indocisc% snmpwalk 192.168.0.1 public system`
  `indocisc% snmpwalk 192.168.0.1 public interfaces.ifTable.ifEntry.ifDescr`
  `interfaces.ifTable.ifEntry.ifDescr.1 = lo`
  `interfaces.ifTable.ifEntry.ifDescr.2 = eth0`



Enumerasi di sistem Windows

- C:\WINDOWS> **net view**
  \\KOMPUTERKU   Pentium III
  C:\WINDOWS> net view \\komputerku
  Sharename Type Comment

  C   Disk
- C:\WINDOWS> **nbtstat –a 192.168.1.1**
- C:\WINDOWS> **nbtscan 192.168.1.0/24**

Langkah Selanjutnya?

- Memenuhi "tabel" target data-data

Nama	No IP	Alive	OS	Services
www.bank.co.id	10.10…	ya	Windows server	http, https
xyz.	10.10.10.1	Ya	Win 2000, SP3	NetBIOS, ftp, http (IIS)
mail.bank.co.id				SMTP

- Melakukan searching untuk membandingkan target dengan daftar eksploitasi. Atau melakukan vulnerabiliy mapping terhadap data di tabel
- Selanjutnya: initial access (mulai masuk)
- Issues
  - ***Security policy***. Apakah scanning termasuk hal yang illegal? Di beberapa tempat: ya. Dianggap tidak bersahabat (unfriendly)
  - Melakukan otomatisasi