

## *Casing The Establishment*

Mencari Informasi Awal  
Sebelum Menyerang Target



## Cari Informasi Tentang Target

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

## Contoh tabel target

Nama	No IP	Alive	OS	Services
www.bank.com	10.10...	ya	Windows NT SP 6	http
xyz.	10.10.10.1	Ya	Windows 2000, SP3	NetBIOS, ftp, http (IIS)
mail.bank.com				SMTP

## FOOTPRINTING

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

## Data-data dari domain name

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

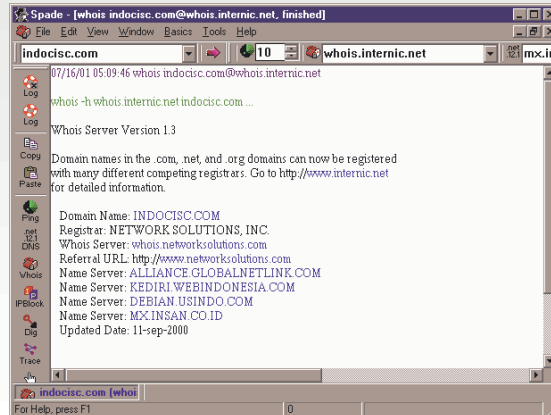
## whois

- Unix% whois "acme."@whois.crsnic.net
- Unix% whois "acme.net"@whois.crsnic.net
- Unix% whois acme.net@whois.networksolutions.com



# Whois dengan Sam Spade

<http://www.samspade.org>



versi 3, 2003

Casing the joint

-7-



## 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
```

versi 3, 2003

Casing the joint

-8-



## Program "host"

- Mencari informasi mengenai name server (ns), mail record (mx), dll.
- Unix% **host** [www.indocisc.com](http://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

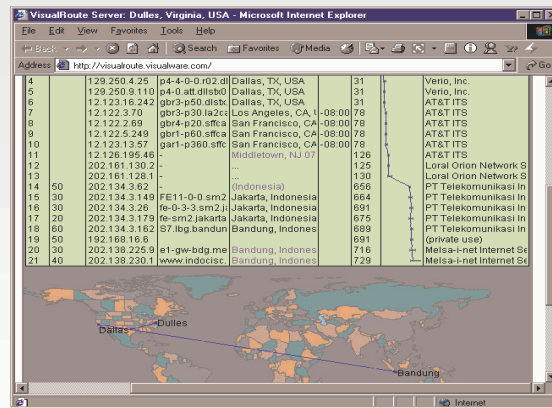
- Zone transfer harusnya dibatasi
- Zone transfer via web  
<http://us.mirror.menandmice/cgi-bin/DoDig>  
Name server:  
Domain name:  
Query type: **Zone Transfer (AXFR)**



# Routing

- Traceroute untuk mengetahui routing
- Unix  
tracert 167.205.21.82
- Windows  
DOS> tracert 167.205.21.82
- Web  
- <http://visualroute.visualware.com>

<http://visualroute.visualware.com>



## Server hidup?

- Ping, gping, hping  
mencari host yang hidup (alive)
- Unix% `gping 192 168 1 1 254 | fping -a`  
192.168.1.254 is alive  
192.168.1.227 is alive  
192.168.1.1 is alive  
192.168.1.190 is alive
- Unix% `fping -g 192.168.1.0/24`
- Membutuhkan ICMP traffic
- Unix% `hping 192.168.1.2 -S -p 80 -f`

## Masih tentang ping

- 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
- Windows: pinger dari Rhino9  
<http://www.nmrc.org/files/snt>

## 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      : 0xFFFFFFFFE0
```

## 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

- Servis 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

- Melihat servis di sebuah host

- UNIX

- Strobe

- `strobe 192.168.1.10`

- Nmap

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

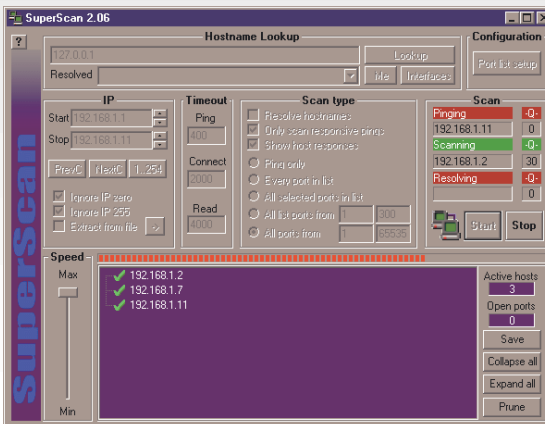
- Netcat:

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

- `udp_scan`

## Scanning Tools: Windows

- NetScan Tools Pro 2000
- SuperScan



versi 3, 2003

Casing the joint

-19-



## 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

versi 3, 2003

Casing the joint

-20-



## 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

- Program penangkal langsung melakukan pemblokiran

- access control list (/etc/hosts.deny)
- mengubah routing table (drop)
- mengubah rule dari firewall
- Contoh software: portsentry

## OS Fingerprinting

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



## Application fingerprinting

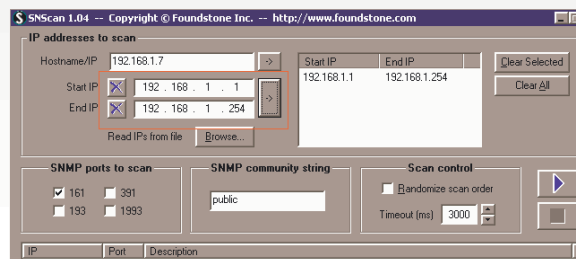
- Banner grabbing: dari aplikasi (misal SMTP)  
telnet server.name 25
- ```
echo -e "GET /index.html HTTP/1.0\n\n" | nc  
192.168.1.3 80 | less
```

```
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`



versi 3, 2003

Casing the joint

-25-



## 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`

versi 3, 2003

Casing the joint

-26-



## Langkah Selanjutnya?

- Memenuhi “tabel” target data-data

| Nama          | No IP      | Alive | OS            | Services                 |
|---------------|------------|-------|---------------|--------------------------|
| www.bank.com  | 10.10...   | ya    | Win NT SP 6   | http                     |
| xyz.          | 10.10.10.1 | Ya    | Win 2000, SP3 | NetBIOS, ftp, http (IIS) |
| mail.bank.com |            |       |               | SMTP                     |

- Melakukan searching untuk membandingkan target dengan daftar eksploitasi
- Selanjutnya: initial access (mulai masuk)
- Issues
  - Security policy. Apakah scanning termasuk hal yang illegal? Di beberapa tempat: ya