DASAR-DASAR HACKER (BAG. 3)

www.kursusgratis.bizland.com
yerianto@yahoo.com

Cari sistem yang akan dijadikan target

Cara-cara non-teknis

Jika anda telah menetapkan tujuan anda sebagai hacker yang akan menerobos sistem komputer milik orang lain, barulah anda dapat memulai mencari sistem yang akan dijadikan targetnya. Pencarian dapat dimulai dari hal-hal yang bersifat non teknis, misalnya:

- Apakah perusahaan yang sedang anda cari memiliki hompage yang berisi informasi perusahaanya di internet ?
- Jika mereka tidak memiliki homepage di internet, apakah mereka memanfaatkan fasilitas lain di internet, misalnya mereka tidak memiliki homepage tetapi memiliki address internet. Coba cari tahu addressnya dari kartu namanya.
- Jika anda memiliki kartu nama dari "sang korban", maka pertanyaan-pertanyaan di atas mungkin tidak diperlukan lagi. Karena pada umum kartu nama akan mencantumkan alamat homepage perusahaan dan atau address mail.
- Jika kartu nama pun anda tidak memiliki, cobalah telepon perusahaan tersebut dari carilah informasi dari resepsionis.

Lihatlah, masih akan banyak daftar hal-hal non teknis yang dapat anda lakukan untuk mencari informasi yang berkaitan dengan rencana anda melakukan penjebolan terhadap sistem komputer milik orang lain tersebut, bukan ?

Masih ingat cerita mengenai mahasiswi yang dapat mengelabuhi pengelola sistem komputer di laboratorium kampusnya pada bab satu ? Bisa jadi sang mahasiswi tersebut telah melakukan hal-hal non teknis sebelum melakukan hal teknis seperti menggunakan trojan horse.

Nah sebagai pengelola sistem komputer, anda harus berhati-hati terhadap pertanyaan yang mengarah ke sistem komputer anda. Bisa saja informasi yang anda sampaikan akan digunakan untuk menyerang anda di kemudian hari.

Cara-cara teknis

Masih belum juga mendapatkan informasi mengenai server yang menjadi target ? coba lah cari dari search engine yang banyak terdapat di internet. Untuk perusahaan asing, gunakan search engine asing. Sedangkan untuk perusahaan lokal sebaiknya digunakan search engine lokal.

Contoh-contoh search engine asing antara lain:

- www.yahoo.com
- www.altavista.com
- www.lycos.com
- www.hotbot.com

Contoh-contoh search engine lokal antara lain:

- www.catcha.co.id
- www.searchindonesia.com
- www.astaga.com

Sebagai latihan, coba anda mencari apakah perusahaan atau lembaga di abawah ini memiliki homepage di internet ?

- IBM
- Departemen Luar Negeri Republik Indonesia
- Ikatan Alumni Fakultas Ilmu Astronomi Universitas Merdeka

Hasil dari proses pencarian melalui searching engine mungkin akan banyak. Cobalah anda pilah-pilah mana informasi yang lebih sesuai dengan tujuan anda. Hasil dari pencarian tersebut diatas mungkin sebagai berikut:

www.ibm.net

www.deplu.go.id

Tidak ditemukan homepage Ikatan Alumni Fakultas Ilmu Astronomi Universitas Merdeka, alias mungkin lembaga tersebut tidak memiliki homepage atau sistem komputer yang terhubung ke dalam internet.

Nah jika anda telah menemukan sistem komputer atau homepage yang dimaksud, apalagi yang bisa anda perbuat ?

Kenali Sistem Yang Akan Anda Masuki

Kenali sistem anda yang akan anda masuki karena setiap sistem komputer memiliki informasi dan tata cara yang berbeda-beda. Perhatikan beberapa hal berikut ini:

1. Informasi jaringan mengenai server tersebut, misalnya:
    - Nomor Ip

- Domain
- Dns server
- Nomor port yang dipergunakan, dan lain-lain

2. Jenis sistem operasi yang dipergunakan
    - Sistem Windows NT
    - Sistem UNIX
    - Sistem Linux
3. Teknik pemrograman web yang dipergunakan
    - Php
    - Frontpage
    - ASP, dan lain-lain

Selanjutnya akan kita bahas mengenai teknik-teknik bagaimana kita mengenali server-server dari situs atau hompage yang akan kita eksplorasi lebih jauh lagi.

Berapa Nomor IP Server ?

Hal yang paling mendasar di dalam dunia hacker adalah pemahaman mengenai TCP/IP. Mengapa demikian, karena setiap komputer yang terhubung ke dalam internet memanfaatkan protokol TCP/IP. Mungkin dalam dunia sehari-hari dapat dikatakan jika anda ingin melakukan transaksi antar negara di era global, maka anda harus dapat menggunakan bahasa Inggeris. Nah bahasa inggeris ini lah yang identik dengan TCP/IP di dalam internet.

Setiap komunikasi di dalam internet dibutuhkan nomor IP unik. Nah untuk itu kita perlu tahu berapa namor IP server yang akan kita tuju tersebut. Cara yang paling mudah adalah menggunakan utilitas ping. Ping akan memberikan informasi mengenai status server tersebut berupa:

Nomor IP dari server tujuan (jika anda memasukkan nama server saja)

Status koneksi ke server tersebut, hidup atau mati

Perhatikan contoh berikut ini:

```
C:\>ping www.indosat.net.id
Pinging www.indosat.net.id [202.155.15.26] with 32 bytes of data:
Reply from 202.155.15.26: bytes=32 time=203ms TTL=118
Reply from 202.155.15.26: bytes=32 time=160ms TTL=118
Reply from 202.155.15.26: bytes=32 time=150ms TTL=118
Reply from 202.155.15.26: bytes=32 time=155ms TTL=118
C:\>
```

Aha, ternyata server www.indosat.net.id bernomor IP 202.155.15.26 !

Cara lain adalah dengan menelusuri jejak IP dari PC anda menuju server mereka. Umumnya utulitas ini dipergunakan untuk mengetahui jalur yang diergunakan oleh server tertentu.

```
C:\>tracert www.indosat.net.id
Tracing route to www.indosat.net.id [202.155.15.26]
over a maximum of 30 hops:
1 * * * Request timed out.
2 137 ms 114 ms 112 ms jatinegara-001.jatinegara.jakarta.telkom.net.id
[203.130.229.1]
3 210 ms 167 ms 140 ms 192.168.0.5
4 166 ms 161 ms 149 ms FE0-0-gw3.cibinong.telkom.net.id [202.134.3.134]
5 148 ms 157 ms 140 ms FE-1-1-0-peer.jakarta.telkom.net.id
[202.134.3.113]
6 172 ms 144 ms 171 ms s0-0-peer.jakarta.telkom.net.id [202.134.3.242]
7 164 ms 161 ms 181 ms 198.32.204.81
8 203 ms 158 ms 176 ms 202.148.63.9
9 171 ms 160 ms 169 ms 202.148.63.238
10 163 ms 156 ms 160 ms ro-isp5-gw-001.indosat.net.id [202.155.27.5]
11 179 ms 162 ms 146 ms www.indosat.net.id [202.155.15.26]
Trace complete.
C:\>
```

Ternyata server www.indosat.net memang bernomor IP 202.155.15.26

Cara lain anda dapat menggunakan software tools nslookup yang tersedia di internet seperti pada:

www.tukang.access.net.id

www.apnic.net

http://ipalloc.utah.edu/HTML_Docs/NSLookup.html

Berikut ini contoh hasil query nslookup menggunakan http://ipalloc.utah.edu/HTML_Docs/NSLookup.html terhadap situs www.astaga.com. Adapun parameter yang diisikan adalah nama domain dengan dns server di above3.net.

```
NSLookup
Select Query Type
 name_info
Lookup all information for a name
1. Enter name in 'Name/Number' field
2. Change 'Name Server' field as needed
3. Click 'Submit'
```

name_lookup

Lookup name given a number
1. Enter IP Address in 'Name/Number' field
2. Change 'Name Server' field as needed
3. Click 'Submit'

ns_lookup

Lookup the name servers for a domain
1. Enter domain name in 'Name/Number' field
2. Change 'Name Server' field as needed
3. Click 'Submit'

domain_list

List contents of a domain
1. Enter domain name in 'Name/Number' field
2. Change 'Name Server' field as needed
3. Click 'Submit'

subnet_list **List names in a subnet**
1. Enter subnet number in 'Name/Number' field
2. Change 'Name Server' field as needed
3. Click 'Submit'

Enter Query Arguments

Name/Number: astaga.com

Name Server: ns3.above.net

Lookup Clear

Hasilnya adalah sebagai berikut:

```
NSLookup Query Results
ads CNAME www2.astaga.com
adsid CNAME idlive1.astaga.com
adstream A 202.159.100.88
astaga.com. A 202.159.100.92
astaga.com. MX 0 inbound.astaga.com.criticalpath.net
astaga.com. NS ns.above.net
astaga.com. NS ns3.above.net
astaga.com. SOA dns.sitesmith.com hostmaster.sitesmith.com. (2000121900
21600 7200 864000 3600)
astaga.com. SOA dns.sitesmith.com hostmaster.sitesmith.com. (2000121900
21600 7200 864000 3600)
cari CNAME idtx1.astaga.com
chat CNAME idtx1.astaga.com
farm A 202.159.100.77
farm2 A 202.159.100.85
farm3 CNAME idlive1.astaga.com
forum CNAME astaga-com.mb.outblaze.com
games CNAME idlive1.astaga.com
iddev1 A 202.159.100.83
idlive1 A 202.159.100.84
idtx1 A 202.159.100.86
iklanbaris CNAME idlive1.astaga.com
indoap A 202.159.100.82
localhost A 127.0.0.1
mail CNAME mail.astaga.com.criticalpath.net
mailhost MX 10 inbound.astaga.com.criticalpath.net
mymail CNAME astaga-com.wr.outblaze.com
```

```
ob MX 10 astaga-com.mr.outblaze.com
ob MX 20 astaga-com-bk.mr.outblaze.com
search CNAME idtx1.astaga.com
sms A 202.159.100.74
smtp CNAME smtp.astaga.com.criticalpath.net
tell A 202.159.100.74
wap A 202.159.100.73
www NS indoap.astaga.com
www1 A 202.159.100.92
www2 A 208.184.219.10
>
> Default Server: NS3.ABOVE.NET
> [NS3.ABOVE.NET]
Address: 128.110.124.120
Address: 207.126.105.146
Default Server: ns.utah.edu
```

Ketika informasi sudah terbuka, tinggal bagaimana para "calon hacker" memanfaatkannya. Ketika informasi terbuka, tinggal bagaimana para pengelola sistem komputer dan jaringan melindungi sistemnya dengan baik dan benar.

Server apa yang dipakai dan jenis sistem operasinya

Server yang dapat dipergunakan sebagai server internet sangat beraneka ragam, mulai dari jenis PC, sampai dengan kelas server dan mereknya pun beraneka ragam. Demikian pula dengan sistem operasi dimana terdapat beraneka sistem operasi yang dapat dipergunakan sebagai server internet., namun umumnya dikelompokkan menjadi dua, yaitu berbasis windows NT dan UNIX.

Masing-masing sistem operasi memiliki karakteristik dan teknik yang berbeda. Cara masuk dan menggunakan sistem operasi windows tentu berbeda dengan sistem unix. Untuk itu sebelum mencoba masuk ke dalam sistem operasi tertentu anda harus memastikan bahwa anda sudah mengetahui sistem operasi yang anda akan tuju.

Pertanyaannya adalah sebagai orang luar bagaimana mungkin kita mengetahui apa jenis sistem operasi yang dipergunakan oleh sebuah situs di intenet. Mungkin kalau ada informasi orang dalam akan lebih mudah.

Yang dapat anda lakukan adalah mencoba mencari informasi di situs itu sendiri apakah menjelaskan sistem operasi yang dipergunakan ? atau mencari dari sistu informasi sejenis. Cara ini adalah cara-cara non teknis yang mungkin lebih cepat dan akurat dari cara teknis.

Cara lain anda bisa menggunakan aneka software tools yang ada. Tetapi sebelum kesana, cobalah beberapa situs yang mungkin bisa membantu anda mencari informasi. Salah satunya adalah www.netcraft.com. Situs ini menjelaskan sistem operasi dan aplikasi internet yang dipergunakan oleh sebuah server internet. Untuk mengetahui jenis sistem oeprasi dan aplikasi internet yang dipergunakan, anda cukup memasukan alamat dari situs internet yang diinginkan, selanjutnya www.netcraft.com yang mencari tahu dan dalam sekejap infromasi tersebut ada di depn mata anda, mudah bukan ?

Perhatikan contoh hasil penelusuran dari www.netcraft terhadap situs-stus berikut ini:

```
The site www.detik.com runs Apache/1.3.14 (Unix) (Red-Hat/Linux)
PHP/3.0.15 mod_perl/1.21 on Linux
The site www.ksei.co.id runs Microsoft-IIS/4.0 on NT4/Windows 98
```

Dengan memahami jenis sistem operasi dan aplikasi internet yang dipergunakan, anda telah memegang salah satu kunci utama untuk masuk ke dalam sistem tersebut. Selanjutnya tinggal anda pelajari kelemahan-kelemahan dari sistem operasi dan aplikasi internet tersebut. Mungkin Anda bisa memulai dengan mencari bugs yang terdapat pada masing-masing sistem operasi dan aplikasi internet tersebut. Berikut ini beberapa situs yang dapat dijadikan referensi untuk melihat bugs-bugs tersebut:

www.rootshell.com

www.ntbugtraq.com

www.securityfocus.com

Seringkali para pengelola sistem komputer dan jaringan terlalu percaya diri bahwa servernya telah dapat ditutup sedemikian rupa sehingga tidak ada yang bisa mengintip dari luar sana hanya lantara memiliki firewall. Padahal mungkin saja firewall tidak dapat berbuat banyak terhadap bugs dari sistem operasi tersebut. Berhati-hatilah bung !

Probing dan Scanning

Informasi yang diberikan oleh www.netcraft.com cukup terbatas, yaitu sekedar informasi mengenai server dan jenis aplikasi internetnya saja. Terkadang informasi tersebut dirasakan kurang. Untuk itu diperlukan software tools untuk melakukan scanning terhadap suatu server internet. Berdasarkan informasi tersebut akan terlihat lubang-lubang yang mungkin dapat dimanfaatkan oleh para hacker.

Teknik-teknik lain yang sering digunakan untuk mengintip lebih jauh mengenai sebuah server internet adalah probing dan scanning.

Probing merupakan usaha mencari informasi dengan cara mengintip langsung ke dalam sistem server internet. Scanning adalah kegiatan probing dalam jumlah yang besar dengan mengguaan tools secara otomatis. Tools tersebut secara otomatis akan mendeteksi kelemahan pada server . Dengan scanner seorang hacker di Bandung dapat mengetahui kelemahan dalam sistem komputer di Inggeris, misalnya.

Scanner sebenarnya adalah scanner untuk port TCP, yaitu sebuah program yang menyerang atau attacking port TCP/IP dan service-servicenya seperti FTP, http, telnet dan lainnya dan mencatat responsenya Dengan cara ini hacker dapat memperoleh informasi yang di dapat dari server tersebutuntuk tindakannya selanjutnya..

Banyak tools yang dapat dipergunakan sebagai scanner, baik yang bersifat komersial maupun yang non komersial. Scanner komersial sebenarnya ditujukan bagi pengelola sistem komputer atau administrator

untuk melakukan pemeriksaan terhadap sistem komputer internalnya. Hal ini untuk memastikan segala lubang telah ditutup dan tidak ada lubang baru.

Software tools scanner ini sering dimanfaatkan oleh pengelola sistem komputer dan jaringan untuk:

- Audit keamanan server dan jaringan
- Pengganti hacker sewaan (dalam beberapa hal memang cukup efektif)
- Pemeriksaan berkala untuk menghindari adanya kesalahan prosedural internal yang mengakibatkan terbukanya keamanan sistem

Namun hal ini sering disalahgunakan oleh para hacker. Umumnya para hacker akan mengambil software scanner versi beta atau versi trial. Sekalipun versi trial, terkadang sudah cukup untuk membongkar informasi dari situs tertentu.

Yang dilakukan software tools scanner terhadap server tujuan adalah menampilkan segala informasi dan kelemahan dari sistem antara lain:

- Service apa saja yang sedang dijalankan
- Siapa saja pemilik service yang sedng dijalankan
- Apakah ada account yang dapat dimanfaatkan seperti anonymous, guest dll
- Mengintip account user yang tersedia
- Apakah service yang dijalankan membutuhkan autentikasi

Beberapa scanner yang dapat dipergunakan antara lain:

- Netsonar dari cisco
- Cybercop versi windows NT
- Real secure versi windows NT
- Yap versi windows 95/NT http://www.widomaker.com/~ted/yaps/Yaps.html.
- Nessus versi Linux brbasis C Compiler
- Strobe versi UNIX
- NSS versi UNIX
- SATAN www.fish.com
- JACKAL www.giga.or.at/pub/hacker/unix
- Dan lain-lain

Salah satu yang dikategorikan sebagai software tools scanner adalah port scanner atau port mapper. Salah satu yang didemokan pada tulisan ini adalah YAPS yang dapat anda download di http://www.widomaker.com/~ted/yaps/Yaps.html. Adapun feature yang tersedia antara lain:

- Berbasis windows 95/98 atau windows NT
- Scan a single host by name.
- Scan a range of hosts by IP address.
- Scans multiple hosts simultaneously.
- Generates reports in HTML format.
- Scan TCP ports over a user defined range of ports.
- Identify Web server version and home page title.
- FTP report with anonymous logon test.
- Report on telnet response.
- Report on NNTP, SMTP, and POP servers.
- Report on Finger response.
- User defined (not system default) timeout.
- Scan Windows (SMB) Networks, even across the Internet.
- Scan the unpriviledged ports up 65535.
- Uses multiple asynchronous sockets to scan hundreds of times faster.
- Complete control over which services are scanned.
- ICMP echo (ping) test.
- Option to continue if ping fails.
- Scan up to 4096 hosts at one time.
- Define multiple ports and ranges of ports to scan.
- Enter license code to make fully functional.

Berikut ini hasil contoh proses scanner dengan menggunakan aplikasi YAP

```
YAPS Network Scan
10.10.194.1
Scan performed on system hale02
04/28/98 21:37:38
Port Scan: 7 13 19 21 23 25 37 53 69 79 80 88 109-111 113 119 137-139
143 161 162 194 220 443 512-518 529 533 540-544 744 749 995 1080 1110
```

2213 5631 5631 26000 00

Smart Scan: Resolve-Host-Name ICMP-Echo Windows-Networking Web-Servers (Show-web-source) Telnet FTP Finger SMTP-Mail POP-Mail NNTP-News Daytime
10.10.194.1 hostzz.zzzz.net

Ping Time: avg 156 min 150 max 170

Ports responding:
21 ftp
23 telnet
25 smtp
37 time
53 dns
80 http
111 sunrpc
110 pop3
113 auth
139 nbsession
143 imap
514 shell
515 printer

Total Ports: 13
Web Server at port 80: ZzzzNet - Tomorrow's Vision Today
HTTP/1.1 200 OK
Date: Wed, 29 Apr 1998 01:37:17 GMT
Server: Apache/1.2.1
Connection: close
Content-Type: text/html

```
<html>
<head>
<title>
ZzzzNet - Tomorrow's Vision Today
</title>
</head>
<body bgcolor="FFFFFF" text="000000" alink="BE0D0D" vlink="BE0D0D"
link="000DBA">
<center>
<table border="0">
<tr>
<td>
<br>
<img src="resources/images/front/logo.gif" alt="ZzzzNet Logo"
width="390" height="103"><br>
<center><a href="resources/mapfiles/logo_top.map">
<img src="resources/images/front/topbar.gif" ismap usemap="#topbar"
border="0" alt="contact | help | search" width="305"
height="27"></a><br></center>
<center><font size="-1" face="Arial">ZzzzNet Members, <a
href="http://users.Zzzz.net">click here</a>.</center>
</td>
<td>
<center>
<a href="resources/ra/welcome.ram">
<img src="resources/images/front/realaudo.gif" border=0 alt="RealAudio
Tour" width="153" height="81"></a>
</center>
</td>
</tr>
</table>
<table border="0">
<tr>
```

```
<td valign="top">
<a href="resources/mapfiles/sidebar.map">
<img src="resources/images/front/sidebar.gif" ismap usemap="#sidebar"
border="0" alt="Main Menu" width="196" height="336"></a>
</td>
<td width="300" valign="top">
<IMG SRC="resources/images/noshad2.gif" WIDTH=150 HEIGHT=106
BORDER=0><BR>
Telnet response:
FTP response:
220 hostzz FTP server (Version wu-2.4(2) Tue Oct 22 18:24:43 EDT 1996)
ready.
530 User ftp access denied..
503 Login with USER first.
215 UNIX Type: L8
SMTP (Email):
220 mail1.Zzzz.net ESMTP ZZZZNet Mail Services ready
POP (Email):
+OK Cubic Circle's v1.21 1997/08/10 POP3 ready <E73C000069844635@HOSTZZ
```

Sebuah issue yang masih terus diperdebatkan adalah apakah melakukan scanner dapat dikatakan sebagai tindakan illegal atau legal, dimana keduanya memiliki konsekuensi logis.Untuk memudahkan pemahaman terhadap legal atau illegal proses scanner adalah dapat digambarkan sebagai proses mengintip rumah orang lain. Menurut anda, apabila ada orang lain dari luar rumah yang melakukan tindakan pengintipan terhadap rumah anda, apakah legal atau ilegal. Tentu saja orang yang mengintip tersebut bisa saja menemukan bahw di rumah anda ada TV, radio, VCD dan lain sebagainya. Bahkan mungin saja orang lain tersebut menemukan bahwa ada celah di atas genteng rumah anda yang dapat dimanfaatkan untuk masuk ke dalam rumah untuk mencuri perabotan anda. Tentu saja orang yang mengintip dari luar rumah anda bisa berkilah bahwa ia hanya numpang lewat atau tidak berniat melakukan pencurian. Nah kalau sudah begini, menurut anda ini tindakan legal atau ilegal. Kalau ilegal, tentu anda akan segera "diteriakin" maling-maling-maling !