Belajar Menjadi Hacker

Onno W. Purbo
onno@indo.net.id

Hacker dengan keahliannya dapat melihat & memperbaiki kelemahan perangkat lunak di komputer; biasanya kemudian di publikasikan secara terbuka di Internet agar sistem menjadi lebih baik. Sialnya, segelintir manusia berhati jahat menggunakan informasi tersebut untuk kejahatan – mereka biasanya disebut cracker. Pada dasarnya dunia hacker & cracker tidak berbeda dengan dunia seni, disini kita berbicara seni keamanan jaringan Internet.

Saya berharap ilmu keamanan jaringan di tulisan ini digunakan untuk hal-hal yang baik – jadilah Hacker bukan Cracker. Jangan sampai anda terkena karma karena menggunakan ilmu untuk merusak milik orang lain. Apalagi, pada saat ini kebutuhan akan hacker semakin bertambah di Indonesia dengan semakin banyak dotcommers yang ingin IPO di berbagai bursa saham. Nama baik & nilai sebuah dotcom bisa jatuh bahkan menjadi tidak berharga jika dotcom di bobol. Dalam kondisi ini, para hacker di harapkan bisa menjadi konsultan keamanan bagi para dotcommers tersebut – karena SDM pihak kepolisian & aparat keamanan Indonesia amat sangat lemah & menyedihkan di bidang Teknologi Informasi & Internet. Apa boleh buat cybersquad, cyberpatrol swasta barangkali perlu di budayakan untuk survival dotcommers Indonesia di Internet.

Berbagai teknik keamanan jaringan Internet dapat di peroleh secara mudah di Internet antara lain di http://www.sans.org, http://www.rootshell.com, http://www.linuxfirewall.org/, http://www.linuxdoc.org, http://www.cerias.purdue.edu/coast/firewalls/, http://www.redhat.com/mirrors/LDP/HOWTO/. Sebagian dari teknik ini berupa buku-buku yang jumlah-nya beberapa ratus halaman yang dapat di ambil secara cuma-cuma (gratis). Beberapa Frequently Asked Questions (FAQ) tentang keamanan jaringan bisa diperoleh di http://www.iss.net/vd/mail.html, http://www.v-one.com/documents/fw-faq.htm. Dan bagi para experimenter beberapa script / program yang sudah jadi dapat diperoleh antara lain di http://bastille-linux.sourceforge.net/, http://www.redhat.com/support/docs/tips/firewall/firewallservice.html.

Bagi pembaca yang ingin memperoleh ilmu tentang jaringan dapat di download secara cuma-cuma dari http://pandu.dhs.org, http://www.bogor.net/idkf/, http://louis.idaman.com/idkf. Beberapa buku berbentuk softcopy yang dapat di ambil gratis dapat di ambil dari http://pandu.dhs.org/Buku-Online/. Kita harus berterima kasih terutama kepada team Pandu yang dimotori oleh I Made Wiryana untuk ini. Pada saat ini, saya tidak terlalu tahu adanya tempat diskusi Indonesia yang aktif membahas teknik-teknik hacking ini – tetapi mungkin bisa sebagian di diskusikan di mailing list lanjut seperti kursus-linux@yahoogroups.com & linux-admin@linux.or.id yang di operasikan oleh Kelompok Pengguna Linux Indonesia (KPLI) http://www.kpli.or.id.

Cara paling sederhana untuk melihat kelemahan sistem adalah dengan cara mencari informasi dari berbagai vendor misalnya di http://www.sans.org/newlook/publications/roadmap.htm#3b tentang kelemahan dari sistem yang mereka buat sendiri. Di samping, memonitoring berbagai mailing list di Internet yang berkaitan dengan keamanan jaringan seperti dalam daftar http://www.sans.org/newlook/publications/roadmap.htm#3e.

Dijelaskan oleh Front-line Information Security Team, “Techniques Adopted By 'System Crackers' When Attempting To Break Into Corporate or Sensitive Private Networks,” fist@ns2.co.uk

http://www.ns2.co.uk. Seorang Cracker umumnya pria usia 16-25 tahun. Berdasarkan statistik pengguna Internet di Indonesia maka sebetulnya mayoritas pengguna Internet di Indonesia adalah anak-anak muda pada usia ini juga. Memang usia ini adalah usia yang sangat ideal dalam menimba ilmu baru termasuk ilmu Internet, sangat disayangkan jika kita tidak berhasil menginternetkan ke 25000 sekolah Indonesia s/d tahun 2002 – karena tumpuan hari depan bangsa Indonesia berada di tangan anak-anak muda kita ini.

Nah, para cracker muda ini umumnya melakukan cracking untuk meningkatkan kemampuan / menggunakan sumber daya di jaringan untuk kepentingan sendiri. Umumnya para cracker adalah opportunis. Melihat kelemahan sistem dengan mejalankan program scanner. Setelah memperoleh akses root, cracker akan menginstall pintu belakang (backdoor) dan menutup semua kelemahan umum yang ada.

Seperti kita tahu, umumnya berbagai perusahaan / dotcommers akan menggunakan Internet untuk (1) hosting web server mereka, (2) komunikasi e-mail dan (3) memberikan akses web / internet kepada karyawan-nya. Pemisahan jaringan Internet dan IntraNet umumnya dilakukan dengan menggunakan teknik / software Firewall dan Proxy server. Melihat kondisi penggunaan di atas, kelemahan sistem umumnya dapat di tembus misalnya dengan menembus mailserver external / luar yang digunakan untuk memudahkan akses ke mail keluar dari perusahaan. Selain itu, dengan menggunakan agressive-SNMP scanner & program yang memaksa SNMP community string dapat mengubah sebuah router menjadi bridge (jembatan) yang kemudian dapat digunakan untuk batu loncatan untuk masuk ke dalam jaringan internal perusahaan (IntraNet).

Agar cracker terlindungi pada saat melakukan serangan, teknik cloacking (penyamaran) dilakukan dengan cara melompat dari mesin yang sebelumnya telah di compromised (ditaklukan) melalui program telnet atau rsh. Pada mesin perantara yang menggunakan Windows serangan dapat dilakukan dengan melompat dari program Wingate. Selain itu, melompat dapat dilakukan melalui perangkat proxy yang konfigurasinya kurang baik.

Setelah berhasil melompat dan memasuki sistem lain, cracker biasanya melakukan probing terhadap jaringan dan mengumpulkan informasi yang dibutuhkan. Hal ini dilakukan dengan beberapa cara, misalnya (1) menggunakan nslookup untuk menjalankan perintah 'ls <domain or network>' , (2) melihat file HTML di webserver anda untuk mengidentifikasi mesin lainnya, (3) melihat berbagai dokumen di FTP server, (4) menghubungkan diri ke mail server dan menggunakan perintah 'expn <user>', dan (5) mem-finger user di mesin-mesin eksternal lainnya.

Langkah selanjutnya, cracker akan mengidentifikasi komponen jaringan yang dipercaya oleh system apa saja. Komponen jaringan tersebut biasanya mesin administrator dan server yang biasanya di anggap paling aman di jaringan. Start dengan check akses & eksport NFS ke berbagai direktori yang kritis seperti /usr/bin, /etc dan /home. Eksploitasi mesin melalui kelemahan Common Gateway Interface (CGI), dengan akses ke file /etc/hosts.allow.

Selanjutnya cracker harus mengidentifikasi komponen jaringan yang lemah dan bisa di taklukan. Cracker bisa mengunakan program di Linux seperti ADMhack, mscan, nmap dan banyak scanner kecil lainnya. Program seperti 'ps' & 'netstat' di buat trojan (ingat cerita kuda troya? dalam cerita klasik yunani kuno) untuk menyembunyikan proses scanning. Bagi cracker yang cukup advanced dapat mengunakan aggressive-SNMP scanning untuk men-scan peralatan dengan SNMP.

Setelah cracker berhasil mengidentifikasi komponen jaringan yang lemah dan bisa di taklukan, maka cracker akan menjalan program untuk menaklukan program daemon yang lemah di server. Program daemon adalah program di server yang biasanya berjalan di belakang layar (sebagai daemon / setan).

Keberhasilan menaklukan program daemon ini akan memungkinkan seorang Cracker untuk memperoleh akses sebagai ‘root’ (administrator tertinggi di server).

Untuk menghilangkan jejak, seorang cracker biasanya melakukan operasi pembersihan 'clean-up‘ operation dengan cara membersihkan berbagai log file. Dan menambahkan program untuk masuk dari pintu belakang 'backdooring'. Mengganti file .rhosts di /usr/bin untuk memudahkan akses ke mesin yang di taklukan melalui rsh & csh.

Selanjutnya seorang cracker dapat menggunakan mesin yang sudah ditaklukan untuk kepentingannya sendiri, misalnya mengambil informasi sensitif yang seharusnya tidak dibacanya; mengcracking mesin lain dengan melompat dari mesin yang di taklukan; memasang sniffer untuk melihat / mencatat berbagai trafik / komunikasi yang lewat; bahkan bisa mematikan sistem / jaringan dengan cara menjalankan perintah ‘rm –rf / &’. Yang terakhir akan sangat fatal akibatnya karena sistem akan hancur sama sekali, terutama jika semua software di letakan di harddisk. Proses re-install seluruh sistem harus di lakukan, akan memusingkan jika hal ini dilakukan di mesin-mesin yang menjalankan misi kritis.

Oleh karena itu semua mesin & router yang menjalankan misi kritis sebaiknya selalu di periksa keamanannya & di patch oleh software yang lebih baru. Backup menjadi penting sekali terutama pada mesin-mesin yang menjalankan misi kritis supaya terselamatkan dari ulah cracker yang men-disable sistem dengan ‘rm –rf / &’.

Bagi kita yang sehari-hari bergelut di Internet biasanya justru akan sangat menghargai keberadaan para hacker (bukan Cracker). Karena berkat para hacker-lah Internet ada dan dapat kita nikmati seperti sekarang ini, bahkan terus di perbaiki untuk menjadi sistem yang lebih baik lagi. Berbagai kelemahan sistem di perbaiki karena kepandaian rekan-rekan hacker yang sering kali mengerjakan perbaikan tsb. secara sukarela karena hobby-nya. Apalagi seringkali hasil hacking-nya di sebarkan secara cuma-cuma di Internet untuk keperluan masyarakat Internet. Sebuah nilai & budaya gotong royong yang mulia justru tumbuh di dunia maya Internet yang biasanya terkesan futuristik dan jauh dari rasa sosial.

Pengembangan para hobbiest hacker ini menjadi penting sekali untuk keberlangsungan / survival dotcommers di wahana Internet Indonesia. Sebagai salah satu bentuk nyatanya, dalam waktu dekat Insya Allah sekitar pertengahan April 2001 akan di adakan hacking competition di Internet untuk membobol sebuah server yang telah di tentukan terlebih dahulu. Hacking competition tersebut di motori oleh anak-anak muda di Kelompok Pengguna Linux Indonesia (KPLI) Semarang yang digerakan oleh anak muda seperti Kresno Aji (masaji@telkom.net), Agus Hartanto (hartx@writeme.com) & Lekso Budi Handoko (handoko@riset.dinus.ac.id). Seperti umumnya anak-anak muda lainnya, mereka umumnya bermodal cekak – bantuan & sponsor tentunya akan sangat bermanfaat dan dinantikan oleh rekan-rekan muda ini.

Mudah-mudahan semua ini akan menambah semangat pembaca, khususnya pembaca muda, untuk bergerak di dunia hacker yang mengasyikan dan menantang. Kalau kata Captain Jean Luc Picard di Film Startrek Next Generation, “To boldly go where no one has gone before”.