Masyarakat Underground Dunia Maya

Onno W Purbo
onno@indo.net.id

Masyarakat Underground? Bawah tanah? … Betul, masyarakat yang tidak terlihat, tidak terdeteksi, seperti siluman, mereka hidup & berjaya di dunia maya – tanpa terdeteksi oleh pengguna Internet biasa, tak terdeteksi oleh sistem administrator WARNET & ISP.

Siapakah mereka? – mereka adalah para hacker. Media & stereotype masyarakat membentuk karakter hacker sebagai orang jahat dan suka merusak. Stereotype ABG 15-20 tahun-an, yang duduk di belakang komputer berjam-jam, masuk ke sistem dan men-delete, berbelanja menggunakan kartu kredit curian atau menghancurkan apa saja yang bisa mereka hancurkan – "anak" ini dikenal sebagai cracker bukan sebagai hacker. Cracker ini yang sering anda dengar di berita / media, mematikan situs web, menghapus data dan membuat kekacauan kemanapun mereka pergi. Hacker yang betul sebenarnya tidak seperti yang ada dalam stereotype banyak orang di atas.

Di dunia elektronik underground nama jelas & nama lengkap tidak digunakan. Orang biasanya menggunakan nama alias, callsign atau nama samaran. Hal ini memungkinkan kita bisa menyamarkan identitas, dan hanya di kenali sesama underground. Beberapa nama diantara hacker Indonesia bisa dikenali seperti hC, cbug, litherr, fwerd, d_ajax, r3dshadow, cwarrior, ladybug, chiko, gelo, BigDaddy dsb..

Apakah perbedaan mendasar antara seorang cracker & hacker? Di http://www.whatis.com, cracker di definisikan sebagai "seseorang yang masuk ke sistem orang lain, biasanya di jaringan komputer, membypass password atau lisensi program komputer, atau secara sengaja melawan keamanan komputer. Cracker dapat mengerjakan hal ini untuk keuntungan, maksud jahat, atau karena sebab lainnya karena ada tantangan. Beberapa proses pembobolan dilakukan untuk menunjukan kelemahan keamanan sistem"

Berbeda dengan Cracker, Hacker menurut Eric Raymond di definisikan sebagai programmer yang pandai. Sebuah hack yang baik adalah solusi yang cantik kepada masalah programming dan "hacking" adalah proses pembuatan-nya. Ada beberapa karakteristik yang menandakan seseorang adalah hacker, seperti (1) dia suka belajar detail dari bahasa pemrograman atau system, (2) dia melakukan pemrograman tidak cuma berteori saja, (3) dia bisa menghargai, menikmati hasil hacking orang lain, (4) dia dapat secara cepat belajar pemrogramman, dan (5) dia ahli dalam bahasa pemrograman tertentu atau sistem tertentu, seperti "UNIX hacker".

Yang menarik, ternyata dalam dunia hacker terjadi strata / tingkatan / level yang diberikan oleh komunitas hacker kepada seseorang karena kepiawaiannya, bukan karena umur atau senioritasnya. Proses yang paling berat adalah untuk memperoleh pengakuan / derajat / acknowledgement diantara masyarakat underground, seorang hacker harus mampu membuat program untuk meng-eksploit kelemahan sistem, menulis tutorial (artikel) biasanya dalam format ASCII text biasa, aktif diskusi di mailing list / IRC channel para hacker, membuat situs web dsb. Entah kenapa warna background situs web para hacker seringkali berwarna hitam gelap, mungkin untuk memberikan kesan misterius. Proses

memperoleh acknowledgement / pengakuan, akan memakan waktu lama bulanan bahkan tahun, tergantung ke piawaian hacker tersebut.

Proses memperoleh pengakuan di antara sesama hacker tidak lepas dari etika & aturan main dunia underground. Etika ini yang akhirnya akan membedakan antara hacker & cracker, maupun hacker kelas rendahan seperti Lamer & Script Kiddies. Salah satu etika yang berhasil di formulasikan dengan baik ada di buku Hackers: Heroes of the Computer Revolution, yang ditulis oleh Steven Levy 1984, ada enam (6) etika yang perlu di resapi seorang hacker:

1. Akses ke komputer – dan apapun yang akan mengajarkan kepada anda bagaimana dunia ini berjalan / bekerja – harus dilakukan tanpa batas & totalitas. Selalu mengutamakan pengalaman lapangan!
2. Semua informasi harus bebas, terbuka, transparan, tidak di sembunyikan.
3. Tidak pernah percaya pada otoritas, penguasa – percaya pada desentralisasi.
4. Seorang hacker hanya di nilai dari kemampuan hackingnya, bukan kriteria buatan seperti gelar, umur, posisi atau suku bangsa.
5. Seorang hacker membuat seni & keindahan di komputer.
6. Komputer dapat mengubah hidup anda menuju yang lebih baik.

Gambaran umum aturan main yang perlu di ikuti seorang hacker seperti di jelaskan oleh Scorpio http://packetstorm.securify.com/docs/hack/ethics/my.code.of.ethics.html, yaitu:

- Di atas segalanya, hormati pengetahuan & kebebasan informasi.
- Memberitahukan sistem administrator akan adanya pelanggaran keamanan / lubang di keamanan yang anda lihat.
- Jangan mengambil keuntungan yang tidak fair dari hack.
- Tidak mendistribusikan & mengumpulkan software bajakan.
- Tidak pernah mengambil resiko yang bodoh – selalu mengetahui kemampuan sendiri.
- Selalu bersedia untuk secara terbuka / bebas / gratis memberitahukan & mengajarkan berbagai informasi & metoda yang diperoleh.
- Tidak pernah meng-hack sebuah sistem untuk mencuri uang.
- Tidak pernah memberikan akses ke seseorang yang akan membuat kerusakan.
- Tidak pernah secara sengaja menghapus & merusak file di komputer yang dihack.
- Hormati mesin yang di hack, dan memperlakukan dia seperti mesin sendiri.

Jelas dari Etika & Aturan main Hacker di atas, sangat tidak mungkin seorang hacker betulan akan membuat kerusakan di komputer.
Tentunya ada berbagai tingkatan / strata di dunia underground. Saya yakin tidak semua orang setuju dengan derajat yang akan dijelaskan disini, karena ada kesan arogan terutama pada level yang tinggi. Secara umum yang paling tinggi (suhu) hacker sering di sebut ‘Elite’; di Indonesia mungkin lebih sering di sebut ‘suhu’. Sedangkan, di ujung lain derajat hacker dikenal ‘wanna-be’ hacker atau dikenal sebagai ‘Lamers’. Yang pasti para pencuri kartu kredit bukanlah seorang hacker tingkat tinggi, mereka hanyalah termasuk kategori hacker kelas paling rendah / kacangan yang sering kali di sebut sebagai Lamer. Mereka adalah orang tanpa pengalaman & pengetahuan biasanya ingin menjadi hacker (wanna-be hacker). Lamer biasanya membaca atau mendengar tentang hacker & ingin seperti itu. Penggunaan komputer Lamer terutama untuk main game, IRC, tukar menukar software prirate, mencuri kartu kredit. Biasanya melakukan hacking menggunakan software trojan, nuke & DoS (Denial of Service). Biasanya menyombongkan diri melalui IRC channel dsb. Karena banyak kekurangannya untuk mencapai elite, dalam perkembangannya Lamer hanya akan sampai level developed kiddie atau script kiddie saja.

Developed Kiddie, dua tingkat di atas Lamer – di sebut Kiddie karena kelompok ini masih muda (ABG) & masih sekolah (SMU atau sederajat). Mereka membaca tentang metoda hacking & caranya di berbagai kesempatan. Mereka mencoba berbagai sistem sampai akhirnya berhasil & memproklamirkan kemenangan ke lainnya. Umumnya mereka masih menggunakan Grafik User Interface (GUI) & baru belajar basic dari UNIX, tanpa mampu menemukan lubang kelemahan baru di sistem operasi.

Script Kiddie, seperti tingkat di atasnya, yaitu developed kiddie, biasanya melakukan aktifitas hacking berbasis pada Grafical User Interface (GUI). Seperti juga Lamers, mereka hanya mempunyai pengetahuan teknis networking yang sangat minimal. Hacking dilakukan menggunakan trojan untuk menakuti & menyusahkan hidup sebagian pengguna Internet.

Dua tingkat tertinggi para hacker & yang membuat legenda di underground dunia maya, adalah tingkat Elite & Semi Elite. Barangkali kalau di terjemahkan ke bahasa Indonesia, tingkat ini merupakan suhu dunia underground. Elite juga dikenal sebagai 3l33t, 3l337, 31337 atau kombinasi dari itu; merupakan ujung tombak industri keamanan jaringan. Mereka mengerti sistem operasi luar dalam, sanggup mengkonfigurasi & menyambungkan jaringan secara global. Sanggup melakukan pemrogramman setiap harinya. Sebuah anugrah yang sangat alami, mereka biasanya effisien & trampil, menggunakan pengetahuannya dengan tepat. Mereka seperti siluman dapat memasuki sistem tanpa di ketahui, walaupun mereka tidak akan menghancurkan data-data. Karena mereka selalu mengikuti peraturan yang ada.

Semi Elite - hacker ini biasanya lebih muda daripada Elite. Mereka juga mempunyai kemampuan & pengetahuan luas tentang komputer. Mereka mengerti tentang sistem operasi (termasuk lubangnya). Biasanya dilengkapi dengan sejumlah kecil program cukup untuk mengubah program eksploit. Banyak serangan yang dipublikasi dilakukan oleh hacker kaliber ini, sialnya oleh para Elite mereka sering kali di kategorikan Lamer.

Sombong merupakan salah satu sebab utama seorang hacker tertangkap. Mereka menyombongkan diri & memproklamirkan apa yang mereka capai untuk memperoleh pengakuan dari yang lain. Hacker lain, karena pengetahuan-nya masih kurang, biasanya akan memilih target secara hati-hati, tanpa terlihat, diam-diam seperti siluman di kegelapan malam. Setelah melalui banyak semedi & membaca banyak buku-buku tentang kerja jaringan komputer, Request For Comment (RFC) di Internet & mempraktekan socket programming. Semua ini tidak pernah di ajarkan di bangku sekolah maupun kuliah manapun. Secara perlahan mereka akan naik hirarki mereka sesuai dengan kemampuannya, tanpa menyombongkan dirinya – itulah para suhu dunia underground. Salah satu suhu hacker di Indonesia yang saya hormati & kagumi kebetulan bekas murid saya sendiri di Teknik Elektro ITB, beliau relatif masih muda + sekarang telah menjadi seorang penting di Research & Development Telkomsel.

Umumnya pembuatan software akan sangat berterima kasih akan masukan dari para hacker, karena dengan adanya masukan ini software yang mereka buat menjadi semakin baik. Memang kadang eksploit yang dihasilkan para hacker tidak langsung di peroleh si perusahaan software, tapi di tahan oleh komunitas underground ini – sampai digunakan oleh lamers & membuat kekacauan.

Bagaimana proses hacking dilakukan? Ah ini bagian paling menarik dalam dunia underground. Ada bermacam-macam teknik hacking, yang paling menyebalkan adalah jika terjadi Denial of Service (DoS) yang menyebabkan server / komputer yang kita gunakan menjadi macet / mati. Terlepas dari masalah menyebalkan, secara umum ada empat (4) langkah sederhana yang biasanya dilakukan, yaitu:

1. Membuka akses ke situs.
2. Hacking root (superuser)
3. Menghilangkan jejak.

4. Membuat backdoor (jalan belakang), untuk masuk di kemudian hari.

Hmmm bagaimana secara singkat lebih jauh proses hacking ini dilakukan? Untuk dapat mengakses ke dalam sebuah situs biasanya melalui beberapa proses terlebih dulu, seperti hal-nya dinas intelejen, kita harus tahu persis segala sesuatu tentang perusahaan & situs yang akan kita masuki, rencana melarikan diri kalau ada apa-apa dsb. Proses intelejen ini dilakukan dalam tiga (3) tahapan besar, yaitu footprinting, scanning & enumeration. Footprinting untuk mengetahui seberapa besar scope / wilayah serangan bisa dilihat dari berbagai file HTML perusahaan tsb, perintah whois, host, dig, nslookup pada Linux untuk melihat scope host yang perlu di serang / di amankan. Scanning untuk melihat servis apa saja yang ada di mesin-mesin tersebut, topologi jaringan dsb. bisa dilakukan mengunakan perintah ping, traceroute, nmap, strobe, udp_scan, netcat di Linux & terakhir Cheops untuk melakukan network mapping. Enumeration sistem operasi yang jalan di server target apakah Windows NT/2000 / Linux / Netware. Program seperti snmputil, enum, dumpsec, showmount, rcpinfo, finger menjadi sangat “handy”.

Setelah proses intelejen di lakukan dengan baik proses serangan dapat mulai dikerjakan. 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. Detail sepuluh (10) besar serangan di Internet bisa dibaca di http://www.sans.org/topten.html. 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 hacker 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 / proxy server; dapat melalui unauthenticated SOCKproxy port 1080 atau open Web proxy port 80, 81, 8000, 8080. Daftar WinGate server di maintain oleh CyberArmy di http://www.cyberarmy.com/wingate/.

Langkah selanjutnya, hacker 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 hacker harus mengidentifikasi komponen jaringan yang lemah dan bisa di taklukan. Hacker 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 hacker yang cukup advanced dapat mengunakan aggressive-SNMP scanning untuk men-scan peralatan dengan SNMP.

Setelah hacker berhasil mengidentifikasi komponen jaringan yang lemah dan bisa di taklukan, maka hacker akan menjalan program untuk menaklukan program daemon yang lemah di server. Cara paling sederhana menggunakan script kiddies yang tersedia di Internet di http://www.technotronics.com / http://www.hackingexposed.com seperti cgiscan.c, phfscan.c dsb. Program daemon adalah program di server yang biasanya berjalan di belakang layar (sebagai daemon / setan). Keberhasilan menaklukan

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

Untuk menghilangkan jejak, seorang hacker biasanya melakukan operasi pembersihan 'clean-up‘ operation dengan cara membersihkan berbagai log file. Program seperti zap, wzap, wted, remove akan membantu. Walaupun simpel text editor seperti vi dapat juga melakukan pekerjaan itu. Jangan lupa menambahkan program 'backdooring' dengan cara Mengganti file .rhosts di /usr/bin untuk memudahkan akses ke mesin yang di taklukan melalui rsh & csh. Selanjutnya seorang hacker dapat menggunakan mesin yang sudah ditaklukan untuk kepentingannya sendiri, tapi seorang hacker yang baik akan memberitahukan sistem administrator tentang kelemahan sistemnya & tidak akan pernah menjalankan perintah ‘rm –rf / &’.

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 / &’.

Cukup banyak situs di Internet yang bisa menjadi basis pengetahuan underground, beberapa diantara-nya berbahasa Indonesia seperti Kecoa Elektronik http://www.k-elektronik.org, Hackerlink http://www.hackerlink.or.id, maupun Anti-hackerlink (entah dimana lokasinya). Referensi terbaik mungkin bisa dibaca di berbagai situs di luar negeri seperti http://packetstorm.securify.com, http://www.hackingexposed.com, http://neworder.box.sk, http://www.sans.org, http://www.rootshell.com.