NAMA : IRSAL HAMDI
KELAS : SIBIL 7B
NIM : 09031381924098
MATA KULIAH : KOMPUTER DAN MASYARAKAT

KEJAHATAN HACKING MELALUI JARINGAN INTERNET DI INDONESIA

LATAR BELAKANG MASALAH

Internet merupakan suatu teknologi digital yang dengan berbagai kecanggihannya mampu menghubungkan antara satu individu dengan individu yang lainnya melalui jaringan virtual sehingga keduannya dapat berinteraksi secara langsung walaupun tidak secara face to face. Dalam bidang teknologi, internet adalah sebuah mahakarya yang sangat luar biasa karena dapat mempertemukan antara individu dengan komponen mesin dalam sebuah jaringan vitual sehingga menghasilkan suatu dunia baru yang disebut sengan dunia maya (cyberspace), dimana manusia dapat memerintahkan kepada komponen mesin untuk melakukan sesuatu yang kemudian komponen mesin menginformasikan apa yang telah diinformasikan ke dalam bentuk audio-visual.

Seiring dengan perkembangan internet yang begitu pesatnya, disisi lain juga diikuti dengan timbulnya permasalahan baru yang sukar untuk dipecahkan. Selain itu juga internet telah membawa perubahan besar terhadap perilaku dan pola hidup daripada individu yang cenderung untuk memilih melakukan segala sesuatu serba cepat dan serta sapat berinteraksi dengan individu yang lainnya tanpa harus bertatap muka secara langsung. Salah satu hal yang meresahkan para pengguna internet (netter) adalah semakin maraknya aktivitas hacking yang dilakukan oleh seorang atau sekelompok orang dengan maksud dan tujuan tertentu. Proses Hacking ini sendirisangat bervariasi tergantung teknik, keahlian serta perangkat lunak (software) dan perangkat keras (hardware) yang digunakan .

TUJUAN

1.Untuk mengetahui apakah yang menjadi cakupan kejahatan hacking melalui jaringan internet?
2.Bagaimanakah penanggulangan kejahatan hacking melalui jaringan internet

MANFAAT

1.Untuk Memperolah informasi terhadap sistem hacking.
2.Untuk menganggulani dan menambah keamanan aplikasi terhadap sitstem hacking.

CAKUPAN KEJAHATAN HACKING MELALUI JARINGAN INTERNET DI INDONESIA

Penggunaan internet di Indonesia baru sebatas hiburan dan percobaan, memang setiap harinya begitu banyak orang yang log-in ke internet. Internet pada dasarnya digunakan untuk meningkatkan dan mempercepat proses serta memperlebar jaringan bisnis, sebagai wahana ilmiah untuk mencapai referensi berbagai perpustakaan di seluruh dunia. Namun orang Indonesia secara moral belum siap menghadapi teknologi baru ini.

Teknologi selain membawa keuntungan berupa semakin dipermudahnya hidup manusia, juga membawa kerugian-kerugian berupa semakin dipermudahnya penjahat melakukan kejahatannya. Tekonlogi juga memberi pengaruh yang signifikan dalam pemahaman mengenai kejahatan terutama terhadap aliran-aliran kriminilogi yang menitik beratkan pada faktor manusia, baik secara lahir maupun psikologis.

Meluasnya jaringan global internet mengisyaratkan adanya harapan akan terjadinya perubahan ruang dan jarak. Perkembangan tersebut jga akan menuju pada terbentuknya sistem tingkah laku tertentu melalui unsur-unsur dominan berupa pengalaman dan budaya dalam penggunaan informasi.

Hacking merupakan permasalahan yang penting dalam jaringan internet global. Memang khususnya di Indonesia aktifitas hacking belum menjadi sorotan masyarakat namun semenjak situs Partai Golkar diserang pada 9 Juli 2006 oleh Iqra Syafaat yang menyebabkan tampilan halaman berubah merupakan peringatan yang keras terutama bagi para aparat pemerintah.

Dalam proses hacking terdapat kode etik yang menjadi patokan bagi para calon hacker maupun hacker professional. Kode etik itu adalah sebagai berikut:

a.Akses ke komputer atau apapun yang dapat mengajari anda bagaimana dunia bekerja haruslah tidak terbatas.
b.Semua informasi haruslah gratis (bebas)
c.Jangan pernah percaya kepada otoritas
d.Hackers atau siapapun ahruslah dihargai dengan kemampuan hackingnya, bukan dikarenakan bagus criteria sepeti tingaktan, umur dan posisi
e.Kita dapat membuat keindahan dengan komputer
f.Komputer dapat membuat hidup kita lebih baik
g.Seperti lampu ‘Aladdin’, kita dapat membuat apapun dalam genggaman.3

Khusus mengenai proses hacking memang tidak harus selalu sama karena tergantung pada keahlian yang dimiliki. Namun pada umumnya langkah-langkah yang digunakan sebelum memulai sebuah proses hacking yaitu:

a.Foot printing : Proses mencari informasi tentang korban sebanyak- banyaknya.
b.Scanning : Proses lanjutan dengan menganalisa service yang dijalankan di internet
c.Enumeration : Proses lajutan dengan mencoba koneksi ke mesin targ
d.Gaining Access : Pengambil alihan ke target berdasarkan informasi yang dapatkan.
e.Escalating Privilege: Meningkatkan hak akses jika telah berhasil masuk ke dalam sistem.
f.Covering Tracks : Menutupi jejak dengan menghapus segala macam log agar tidak terlacak.
g.Denial of Service : Membanjiri target dengan data sehingga mesian tidak dapat berfungsi.

Selain itu hal terpenting yang perlu diperhatikan yaitu metode-metode hacking untuk mendapatkan hak akses ke dalam sistem komputer yang dimiliki oleh targetnya sehingga menyebabkan kehilangan data-data bahkan sampai kerusakan perangkat lunak (software) dan perangkat keras (harware) yang trdapat dalam computer. Metode-metode hacking tersebut adalah sebagai berikut:

a.DOS (Denial of Service) attack : adalah serangan yang dilakukan dengan mengirimkan paket sampah. Hasil dari serangan ini adalah terhentinya layanan server (server down), dikarenakan bandwith penuh. Serangan ini juga mengakibatkan backbone dimana server menginduk menjadi macet, bahkan pelayanan menjadi terhenti sama sekali.

b.Defacing : jenis serangan ini, adalah dengan mengganti halaman depan suatu situs, atau dengan mengganti isi, baik sebagian atau keseluruhan dengan halaman buatan si penyusup.

c.Spoofing : Serangan ini dilakukan dengan cara pengalihan alamat IP dari suatu situs ke alamat yang di kehendaki oleh si penyusup. Biasanya dialihkan ke situs porno. Model serangan ini biasanya dilakukan pada situs-situs pemerintah atau institusi lainnya sebagai bentuk protes.

d.Carding : Serangan ini biasanya dilakukan oleh para ‘pencuri’ kartu kredit, dengan tujuan biasa mendapatkan nomor kartu kredit dengan tidak sah.

e.Database Exploit : Pencurian database suatu situs e-commerce, sehingga mendapatkan banyak nomor kartu kredit dengan ‘Cuma-Cuma’.

f.Pembuatan situs palsu : Modus ini dilakukan dengan menbuat situs e-commerce palsu. Sehingga pada saat terjadi transaksi ‘fiktif’, nomor krtu dan validasi dari pemilik asli bisa di dapatkan dengan mudah.

g.Menggunakan keylogger : Cara ini biasa terjadi di warnet atau pada layanan internet umum lainnya. Bisa dilakukan oleh orang dalam atau sesama pengunjung sendiri. Dengan cara menanamkan program logger pada PC sasaran. Sehingga, bilamana terjadi transaksi online, nomor krtu dan kta sandi (password)akan tercatat secara otomatis paa masing-masing PC

h.Root Compromise : Metode ini merupakan metode teknis penyusupan tertinggi dibandingkan metode lainnya. Karena menuntut pengetahuan (skill), kesabaran dan profesionalisme yang tinggi.5

TEKNIK_TEKNIK HACKING

a.Pemanfaatan local cache

Pada saat kita melihat suatu alamat situs, sebenarnya browser kita meminta halaman tersebut kepada web server. Web server kemudian mengirimkan kode HTML ke komputer client. Browser akan menyimpan halaman ini di komputer local sebagai cache agar pada saat membutuhkan halaman yang sama tidak perlu memintanaya ke web server lagi yang lebih lambat. Setelah itu halaman yang sudah di download ke komputer client akan dieksekusi dan ditampilkan ke computer kita

Halaman cache tersebut dicopy ke hard disk kemudian dibuka dengan notepad. Local cache juga dimanfaatkan oleh hacker untuk melihat situs mana saja yang dikunjungi oleh seseorang. Selain itu, local cache juga menyimpan banyak sekali informasi karena tanpa disadari password juga tersimpan disitu.

b.Menggunakan SQL (Structured Query Language) Injection

SQL adalah suatu bahasa yang digunakan untuk mendapatkan atau merubah data didalam relational database. Statement SQL yang banyak digunakan pada setiap database sangat beragam dan unik. SQL juga merupakan bahasa query yang paling banyak digunakan serta powerfull. Biasanya SQL Injection digunakan bersama-sama dengan bahasa pemrograman lainnya seperti Python, ASP, C, C++, Java dan Visual Basic.

c.Menyerang dengan Target XSS (Cross-Site Scripting)

XSS atau sering disebut dengan Cross-Side Scripting semenjak ditemukan dan dipublukasikan ke mailing list Bugtrq (securityfocus.com) pada pertengahan tahun 2002, ratusan situs telah menjadi korban seperti hotmail, yahoo, e-bay serta software seperti ISS, apache, dan lain-lain.7

Cross-Side Scripting disingkat XSS karena jika disingkat CSS maka akan sama dengan CSS yang sudah sangat dikenal yaitu Cascading Style Sheets sebagai pemformat HTML (HiperText Markup Language). XSS merupakan kelemahan software atau aplikasi yang memenfaatkan input form seperti SQL Injection, namun bedanya kalau SQL Injection target penyerangannya adalah database server maka target XSS adalah browser client.

USAHA PENANGGULANGAN KEJAHATAN HACKING

beberapa alternatif yang dapat digunakan untuk mangamankan sistem jaringan internet dari para penysup (hacker) serta menaggulangi terjadinya kejahatan hacking. beberapa alternatif tersebut adalah sebagai berikut:

a.Memasang Proteksi

Dalam menjaga privasi informasi, memasang proteksi merupakan hal utama. Proteksi ini dapat berupa antivirus maupun firewall. Antivirus digunakan untuk mendeteksi program-program yang dapat merusak sistem-sistem dan data yang ada di dalam komputer, seperti:

1).Virus; suatu program atau code yang mengandakan/mereplikasikan dirinya, yaitu menginfeksi program lain, boot sector, sektor partisi, atau document yang mendukung macro, dengan cara memasukkan dirinya atau melampirkan (attaching) dirinya ke medium tersebut.

2).Worm; suatu progaram yang membuat copy dari dirinya sendiri, contohnya darisatu drive ke drive yang lain, atau mengcopy dirinya menggunakan e-mail.

3).Trojan Horse; suatu program yang tidak mereplikasikan atau mengcopy dirinya, tetapi mengakibatkan kerusakan atau melemahkan keamanan komputer karena pengirim trojan horse dapat mengendalikan komputer korban.

4).Backdoor; suatu program semacam trojan horse dengan kemampuan mencuri data atau password.20

Lain halnya dengan firewall, program ini digunakan untuk memfilter koneksi, akses, informasi bahkan e-mail. Memang firewall ini melakukan filter secara umum maupun data-data yang diprogramkan terlebih dahulu serta tingkatan kemanan yang diinginkan.

b.Memantau serangan

Seringkali serangan dari penyusup (hacker) dilakukan tanpa sepengetahuan dari administrator (network security), maka perlu digunakan sistem pemantau terhadap serangan tersebut. Sistem ini dinamakan Intruder Detection System (IDS) . secara langsung sistem ini memberikan tanda peringatan kepada administrator berupaalaram, sinyal bahkan pesan e-mail jika adanya serangan. Salah satu contoh IDS yaitu tcpdump untuk menganalisis paket apa saja yang lewat 21

c.Mengatur keamanan program

Saat membuat sistem keamanan jaringan komputer seringkali administrator (network security) tidak memperhatikan hal-hal kecil yang dapat dimanfaatkan oleh penyusup (hacker), nantinya akan menjadi masalah besar. Oleh karena itu, diperlukan keteliltian dalam membuat

suatu program, misalnya pemilihan karakter-karakter khusus yang digunakan untuk pemrograman serta ketelitian perhitungan alogaritma dalam pembuatam program.

d.Menutup service yang tidak diperlukan

Pada umumnya suatu Operation System (OS) terdapat layanan (service) yang diikutsertakan dan dijalankan secara umum (default). Contohnya seperti Telnet, memlaui Telnet ini seseorang dapat berhubungan dengan sedemikian banyak komputer di tempat lain di internet dan secara interaktif dapat mencari berbagai data, file, software dan informasi lainnya.22 Namun dibalik kegunaannya tersebut tanpa disadari layanan ini dapat dimanfaaatkan oleh penyusup (hacker) untuk melakukan hacking terhadap suatu web, misalnya merubah tampilan halaman situs. Oleh karena itu, jika tidak diperlukan sebaiknya layanan tersebut ditutup.

e.Menggunakan Publick-Key Cryptogrphy (Kunci Umum Pengacakan)

Selain sistem, data-data penting yang ada di dalam komputer perlu dijamin keamanannya dengan menggunakan Publick-Key Cryptogrphy (Kunci Umum Pengacakan). Dengan bantuan program ini otomstis informasi yang di kirimkan maupun diterima akan diacak (encrypt)dan jika ingin membukannya (decrypt) diperlukan kata sandi (password) yang sebelumnya telah disepakati bersama. kunci umum pengackan ini dilakukan dengan menggunakan Publick Key Insfrastructures
yang dimiliki oleh lembaga penyelenggaranyauntuk mendukung Digital Signature (tanda tangan elektronik).

f.Melakukan Backup

Mengingat perkembangan kejahatan hacking yang semakin kompleks dan informasi sebagai sasaran utamanya maka dengan melakukan backup secara berkala merupakan suatu alternatif yang sangat diperlukan karena jika penyusup (hacker) telah menaklukkan sistem pengamanannya maka selanjutnya yang menjadi sasaran adalah data-data di dalam komputer korban, jika sudah disalin maka ada kemungkinan data-data asli yang ada di dalam komputer korban tersebut akan dirusak atau dimanipulasi sehingga tidak dapat digunakan hal itu dimaksudkan untuk meghilangkan jejak.

Semua usaha yang dilakukan dalam penanggulangan kejahatan hacking melalui jaringan internet di Indonesia baik memamui jalur hukum maupun di luar jalur hukum masing-masing pihak harus memiliki sikap optimis, artinya bagaimanapun dan apapun kejahatan yang telah dilakukan pasti selalu ada jalan keluarnya. Sikap optimis seperti ini harus ditanamkan pada semua pengguna internet baik masyarakat maupun aparat pemerintah. Khusus bagi POLRI sebagai penegak hukum, sikap optimis ini akan mempertajam semangat bahwa semua kejahatan akan diberantas. Di dalam kehidupan ini selalu saja ada kemenangan bagi penegakkan hukum dan keadilan serta tetap ada kekalahan untuk setiap tindak kejahatan.

LINK

https://youtu.be/Bq44KaknRTA