Mengenal Social Engineering

Gani Purbosudibyo
masgani@operamail.com

Pengantar

Sampai saat ini *attacker* atau *cracker* belum menunjukkan tanda-tanda akan mengakhiri usaha-usaha membobol sistem keamanan jaringan. Dalam menangani hal itu, perusahaan-perusahaan maupun berbagai organisasi telah banyak menghabiskan baik waktu, tenaga dan biaya untuk mempertahankan dan mengamankan sistem yang dimilikinya. Antara lain dengan melakukan pembelian berbagai macam *hardware* keamanan yang mahal seperti firewall, serta melakukan *upgrading* dan *patching* pada semua sistem operasi dan aplikasi yang digunakan. Selain itu juga dilakukan *upgrading hardware* karena setiap teknologi baru yang diimplementasikan juga menuntut *hardware* baru yang lebih canggih dan mahal dari sebelumnya. Perekrutan *network administrator* yang memiliki reputasi tinggi dalam menangani sistem keamanan jaringan merupakan solusi dari sisi SDM.

Bila “sang penguasa” perusahaan terus memfokuskan diri pada usaha-usaha di atas dalam mengamankan sistem yang dimilikinya, maka segala pengeluaran dan pengorbannya akan sia-sia karena hal-hal tadi tidak akan mampu menangkal *Social Engineering* yang dilakukan oleh para *cracker* atau *attacker*.

Sebuah Kisah Nyata

Kisah berikut ini merupakan penuturan dari Kapil Raina, seorang ahli keamanan di VeriSign.

Suatu pagi di beberapa tahun yang lalu, sekelompok orang berjalan memasuki sebuah perusahaan jasa pengiriman yang tergolong besar. Beberapa saat kemudian mereka berjalan keluar dari gedung itu dan telah berhasil mendapatkan hak akses ke sistem jaringan perusahaan tadi. Bagaimana mereka melakukannya ?

Pertama, mereka telah melakukan riset mengenai perusahaan itu selama dua hari sebelumnya. Sebagai contoh, mereka telah mempelajari nama-nama pejabat berpengaruh di perusahaan itu dengan cara menghubungi pihak HRD. Selanjutnya mereka pura-pura kehilangan kunci ketika berada di pintu depan perusahaan, dan ternyata seorang pria di perusahaan tadi membukakan pintu untuk mereka tanpa curiga. Untuk saat itu mereka telah berhasil memasuki gedung sasaran. Sesampai di lantai tiga yang merupakan *secure area*, mereka pura-pura kehilangan tanda identitas. Cukup melakukan akting kehilangan dengan bagus, tersenyum ke pekerja-pekerja yang ada di situ, dan salah seorang dari mereka kemudian membukakan pintu untuk mereka dengan ramah. *Secure area* ternyata belum mampu membendung langkah mereka.

Mereka sudah tahu bahwa saat itu pemimpin perusahaan sedang bertugas keluar kota, jadi mereka bisa

dengan bebas memasuki ruang kantornya dan mendapatkan data finansial dari komputernya yang ternyata tidak terpassword sama sekali. Mereka kemudian memanggil petugas kebersihan dan meminta untuk meletakkan semua sampah perusahaan di suatu tempat di mana mereka nantinya bisa memeriksa karena beberapa karyawan ternyata suka menuliskan informasi rahasia ataupun password ke kertas lembar kerja yang tidak terpakai dan kemudian membuang begitu saja.

Selain hal-hal di atas, mereka pun telah mempelajari bagaimana cara dan gaya sang pemimpin berbicara, sehingga mereka mampu menelpon dan mengaku sebagai pemimpin perusahaan, yang sebenarnya sedang berdinas keluar kota, dan mengatakan sedang dalam keadaan terburu-buru dan lupa akan passwordnya. Sang admin pun tanpa rasa curiga dan tanpa merasa perlu melakukan proses verifikasi, segera memberikan apa yang dibutuhkan. Selanjutnya dengan berbekal berbagai informasi yang telah didapatkan, cukup dengan memakai teknik hacking standar mereka akhirnya bisa mendapatkan akses super-user di sistem jaringan perusahaan tersebut.

Dalam cerita ini, mereka sebenarnya dari pihak konsultan keamanan yang sedang melakukan audit keamanan atas permintaan pemimpin perusahaan tanpa memberitahukan sebelumnya kepada para pekerja. Mereka tidak pernah mendapat informasi sedikit pun mengenai perusahaan, para pekerja serta tidak mengenal secara dekat pemimpinnya, tapi mereka mampu mendapatkan semua akses yang diperlukan melalui *social engineering*.

Definisi Social Engineering

Ada yang mengartikan *social engineering* sebagai teknik dan seni mendapatkan informasi dari personal dengan cara mengelabui tanpa perlu melakukan hal-hal yang biasa dilakukan seorang cracker. Ada pula yang mengatakan sebagai *psychological tricks* terhadap orang yang memiliki hak akses pada suatu sistem sebagai upaya untuk mengambil informasi yang dibutuhkan. Atau bisa dianggap sebagai seni memanfaatkan kelemahan-kelemahan manusia seperti sikap tak acuh, naif atau keinginan natural manusia yang ingin disukai orang lain.

Satu hal yang perlu kita sepakati bersama adalah *social engineering* merupakan keahlian attacker dalam melakukan manipulasi yang menyebabkan orang lain percaya kepadanya. Tujuannya adalah mendapatkan informasi yang akan membantu dia dalam mendapatkan hak akses ke sistem dan mengambil informasi yang dibutuhkan dari sistem tersebut.

Metode yang Dipakai

Metode untuk melakukan *social engineering* bisa dibagi ke dalam dua cara yaitu secara fisik dan secara psikologi. Untuk metode *social engineering* secara fisik bisa dilakukan dengan mendatangi tempat kerja, melakukan hubungan telepon, memeriksa dari hasil sampah (mengambil sampah orang lain bukan merupakan pelanggaran hukum) atau dengan koneksi Internet. Bila attacker memilih mendatangi tempat kerja, dia cukup memasuki perusahaan sasaran dengan berpura-pura menjadi konsultan, pegawai operasional, atau siapa pun yang berhak memasuki perusahaan tersebut. Selanjutnya dia bisa memasuki ruang-ruang seperti pada cerita di atas, atau cukup duduk dan menunggu sampai ada pegawai yang secara ceroboh menuliskan atau membicarakan password atau informasi penting lainnya di depannya.

1. **<u>Social Engineering dengan melakukan hubungan telepon</u>**
   Yang paling sering terjadi adalah metode ini . Dengan melakukan sedikit trik seorang attacker yang berpengalaman akan mampu membuat pegawai yang menerima telepon mengucapkan username maupun passwordnya atau informasi lainnya yang dibutuhkan attacker.

   Biasanya pegawai yang bertugas di lini depan seperti bagian informasi atau *customer service* yang akan dihubungi karena selain mereka memang dilatih untuk selalu bersikap ramah dan memberikan informasi kepada penelpon. Mereka biasanya hanya mendapatkan sedikit pelatihan mengenai masalah teknik sehingga kurang mengerti bagaimana mengamankan informasi yang penting bagi keamanan perusahaan. Mereka akan selalu berusaha memberikan informasi yang diminta penelpon secepat mungkin agar bisa segera menerima penelpon berikutnya tanpa sempat memikirkan apa yang dapat dilakukan oleh penelpon dengan informasi yang telah diberikannya.

Dari mereka biasanya attacker mendapatkan informasi yang diinginkannya dengan mudah.

Bisa juga dengan langsung menelpon ke admin. Misalnya setelah seorang attacker mempelajari suatu perusahaan yang menjadi sasarannya, dia akan menelpon ke admin dengan mengaku sebagai pegawai yang ada di perusahaan tersebut. Karena dia telah mempelajari, bisa saja dia mengaku sebagai pegawai A yang menempati ruang kantor sebelah B di urutan meja ke X. Setelah merasa admin bisa diperdaya, dia akan mengatakan ,"Buku catatan kecil saya yang berisikan catatan password tertinggal di meja sehingga saya tidak bisa menyelesaikan pekerjaan saya dari rumah. Bisakah anda mengambilkan untuk saya ?" Seorang admin tentunya terlalu sibuk untuk dapat mengambilkan buku catatan seseorang, dan karena dia telah merasa yakin penelpon adalah pekerja di situ, dia cukup membuka database dan memberitahukan password ke penelpon.

2. Dumpster Diving

Dumpster diving atau juga disebut *trashing* adalah metode populer lainnya, yaitu attacker mengumpulkan informasi dengan memeriksa sampah perusahaan sasaran. Ada banyak yang bisa didapatkan seorang hacker dari sampah perusahaan selama sampah itu tidak berupa makanan busuk. Buku telepon akan memberikan petunjuk nama dan nomer orang-orang yang bisa dihubungi, kalender menunjukkan pekerja mana saja yang akan bertugas keluar kota pada saat tertentu, catatan kerja harian bisa dipelajari untuk dicari kelemahannya, dan sebagainya.

3. Koneksi Internet

Ketika seorang pekerja sedang melakukan koneksi Internet, tiba-tiba sebuah *pop-up window* keluar dan mengatakan bahwa koneksinya terputus dan untuk itu dia harus kembali menuliskan username dan passwordnya. Tanpa curiga pekerja tadi akan melakukannya dan semudah itu attacker mendapatkan informasi.

Sebuah kesalahan yang sering dilakukan adalah orang cenderung untuk menggunakan password yang sama untuk berbagai layanan yang dimilikinya, misalnya untuk e-mail, messenger, ATM, dan sebagainya. Akibatnya begitu seorang attacker berhasil mendapatkan password tadi, dia akan bisa memasuki semua layanan yang tersedia untuk orang tadi.

Pengiriman e-mail juga sering dilakukan karena e-mail bisa membawa berbagai virus dan trojan. Misalnya dengan memberitahukan bahwa *attachment file* yang disertakan di e-mail merupakan patch sistem operasi yang harus segera dijalankan. User mungkin merasa ini bukan hal yang perlu dilakukan verifikasi terlebih dahulu karena merasa e-mail itu berasal dari vendor sistem operasi yang digunakan. Selanjutnya dengan satu langkah klik user telah berhasil menanamkan trojan (meskipun tidak sengaja) yang siap membuka jalan untuk serangan.

Pada intinya dengan bekal pengetahuan dan pemahaman tentang keamanan jaringan yang kurang, manusia sebagai user bisa melakukan berbagai tindakan yang membahayakan keamanan jaringan dan secara tidak langsung membantu attacker untuk menyusup ke dalamnya.

4. Pendekatan Psikologi

Selain cara-cara di atas, seorang attacker bisa menggunakan langkah-langkah psikologis untuk mendapatkan informasi, yaitu dengan mengadakan sebuah ikatan emosional dalam tujuan mendapatkan kepercayaan. Atau seperti yang pernah Kevin Mitnick ucapkan, "*That is the whole idea: to create a sense of trust and then exploiting it*." Misalnya dengan menjalin suatu hubungan dengan orang dalam, sebagai contoh dengan memacari sekretaris dari pemimpin perusahaan. Dia lalu akan memberikan kesan sebagai orang yang bisa dipercaya dan lambat tapi pasti tidak hanya si sekretaris, tapi setiap rahasia perusahaan pun akan berada di tangannya.

Attacker bisa melakukan berbagai hal untuk sekedar menarik simpati atau menjalin hubungan dengan orang-orang yang dianggap bisa menjadi jalan untuk mencapai tujuannya dan memang pada dasarnya seni dari *social engineering* adalah bagaimana seorang attacker bisa mendapatkan kepercayaan dari pihak korban.

Penutup

Perusahaan sudah memasang router yang mahal, membeli piranti firewall kelas dunia, melakukan komunikasi dengan cabang-cabang perusahaan melalui VPN, dan di dalam jaringan diimplementasikan IDS. Tapi mengapa sistem jaringannya tetap bisa kebobolan.

Sering dikatakan bahwa dalam pemanfaatan teknologi, manusia merupakan mata rantai terlemah. Ada banyak contoh yang bisa ditunjukkan mengenai berbagai hal yang mungkin tidak sengaja dilakukan dan berakibat pada bobolnya sistem keamanan yang ada.

Tidak sabar menunggu akses internet yang lama, seorang manajer membawa modem sendiri sehingga bisa *dial-up* dari ruang kantornya dan melakukan koneksi Internet tanpa perlu berbagi *bandwidth* dengan semua pengakses di kantornya. Terbukalah jalan masuk bagi seorang attacker ke dalam jaringan.

Seorang karyawan penasaran mendapatkan kiriman e-mail dengan attachment berjudul DijaminPuas.exe dan tak sabar untuk membuka file attachment itu.

Hacker bisa saja menyamar sebagai pemulung untuk bisa memeriksa isi sampah dari organisasi sasarannya, atau menyamar sebagai pengemis, siapa tahu ada karyawan pelupa yang suka menuliskan passwordnya ke lembaran uang seribuan miliknya. Atau cukup berdandan rapi dan memakai parfum secukupnya lalu melakukan jalan sehat di depan kantor dengan harapan seorang cewek cantik yang kaya dan mempunyai jabatan yang berpengaruh di organisasi itu tertarik padanya pada pandangan pertama.

Bila semua hal di atas terjadi, sia-sialah pengeluaran dana puluhan juta rupiah yang digunakan untuk membangun sebuah sistem jaringan yang aman dan terjamin kerahasiaannya. Organisasi perlu memikirkan adanya sebuah *policy* yang mempunyai aturan yang ketat di dalam menghindari ancaman *social engineering*. Policy itu akan mengatur kapan seorang atau sebuah divisi boleh mengakses Internet. Bagaimana membuat password yang baik. Bagaimana supaya komputer tetap aman baik perangkatnya maupun informasi yang ada di dalamnya bila sewaktu-waktu ditinggal ke kamar kecil. Dan banyak hal lainnya yang bisa diatur di dalamnya.

Mungkin ini akan terasa membatasi kebebasan. Mungkin akan banyak yang merasa tidak puas. Untuk itu *policy* harus melalui proses pemikiran yang matang dalam pembuatannya dan proses sosialisasi yang baik saat akan dijalankan. Juga jangan lupa adanya program-program *security awareness* yang rutin diadakan agar semua mengerti mengapa policy itu dibuat dan apa yang ingin dicapai dari pelaksanaan policy itu.