Dasar-Dasar Social Engineering
Bagian I: Taktik para Hacker

Betha Aris S <betha@obscure.org>

Judul Asli:
Social Engineering Fundamentals, Part I: Hacker Tactics
by Sarah Granger
last updated December 18, 2001

Diterjemahkan Oleh:
Betha Aris S <betha@obscure.org>

Suatu pagi beberapa tahun yang lalu, sekelompok orang asing berjalan memasuki perusahaan pengapalan dan keluar dengan keluar dengan membawa akses jaringan keseluruhan korporat perusahaan. Bagaimana mereka melakukannya. Dengan mendapatkan sedikit akses, perlahan-lahan, dari sejumlah pekerja yang berbeda dalam perusahaan itu. Pertama, mereka melakukan riset tentang oerusahaan selama dua hari sebelum berusaha menjejakkan kaki pada premis-premisnya. Misalnya, mereka mempelajari nama-nama para pekerja dengan memanggil HR. Kemudian mereka berandai-andai kehilangan kunci pintu depan, dan seorang lelaki membiarkan mereka masuk. Kemudian mereka 'kehilangan' kartu identitas mereka ketika memasuki wilayah aman lantai tiga, tersenyum, dan kemudian sseorang pekerja yang baik hati membuka pintu untuk mereka.

Orang-orang asing tahu kalau CFO berada di luar kota, sehingga mereka masuk ke kantornya dan mendapatkan data finansial dari komputer yang tak tak terkunci(unlocked). Mereka membongkar-bongkar seluruh trash, menemukan semua jenis dokumen yang berguna. Mereka meminta sebuah tong penyimpanan pada seorang pesuruh untuk untuk menampung semua isi bawaan mereka dan membawa semua data keluar dari bangunan. Orang-orang asing itu telah mempelajari suara CFO, sehingga mereka bisa menelpon, berpura-pura menjadi CFO, dengan tergesa-gesa, karena memerlukan password jaringannya. Dari sana mereka menggunakan alat kerja hacking teknis reguler untuk mendapatkan akses super-user ke dalam sistem.

Dalam kasus ini, orang-orang asing tersebut adalah konsultan-konsultan jaringan yang menampilkan suatu audit keamanan bagi CFO tanpa sepengetahuan pekerja lainnya. Mereka tidak pernah diberi informasi istimewa apapun dari CFO namun mampu mendapatkan semua akses yang mereka ingin kan melalui social engineering.(Kisah ini dibahas ulang oleh Kapil Raina, sekarang ini ia adalah seorang ahli sekuriti pada Verisiign dan seorang co-author dari mCommerce Security: A Beginner's Guide, yang didasarkan pada suatu pengalaman kerja aktual dengan seorang pekerja sebelumnya)

Definisi

Sebagian besar artikel yang telah saya baca tentang topik social engineering mulai dengan beberapa bentuk definisi seperti “seni dan ilmu memaksa orang untuk memenuhi harapan anda”(Bernz 2), “suatu pemanfaatan trik-trik psikologis hacker luar pada seorang user legitimate dari sebuah sistem komputer” (Palumbo), atau “mendapatkan informasi yang diperlukan (misalnya sebuah password) dari seseorang daripada merusak sebuah sistem” (Berg). Dalam kenyataannya, social engineering bisa menjadi

berbagai dan semua hal-hal yang disebutkan di atas, tergantung dimana anda duduk atau mengambil posisi. Satu hal yang kelihatan disetujui semuma orang adalah bahwa social engineering umumnya suatu manipulasi cerdas tentang tendensi kemanusiaan natural yang dipercaya dari seorang. Tujuan hacker adalah untuk mendapatkan informasi yang akan mengizinkan dia untuk mendapatkan akses yang tak terotorisasi(tak legal) pada sistem yang diinginkan dan informasi yang berlokasi pada sistem itu.

Security adalah segala hal yang berkaitan dengan kepercayaan. Kepercayaan adalah perlindungan dan otentisitas. Umumnya disetujui sebagai jalinan paling lemah dalam alur keamanan, kemauan manusia yang natural untuk menerima kata-kata seseorang meninggalkan hal-hal yang rentan diserang. Banyak ahli security yang berpengalaman menekankan fakta ini. Tak jadi soal banyaknya artikel yang telah diterbitkan tentang firewall, belang(patches), dan lubang-lubang jaringan, kita hanya bisa mengurangi ancaman sebanyak mungkin... da kemudian terserah pada Maggie dalam menilai temannya , Will, menelponnya dari suatu tempat terpencil untuk mempertahankan agar jaringan keseluruhan benar-benar aman.

Target dan Serangan

Tujuan dasar social engineering sama seperti umumnya hacking: mendapatkan akses tidak resmi pada sistem atau informasi untuk melakukan penipuan, intrusi jaringan, mata-mata industrial, pencurian identitas, atau secara sederhana untuk mengganggu sistem atau jaringan. Target-target tipikal termasuk perusahaan telepon ddan jasa-jasa pemberian jawaban, perusahaan dan lembaga keuangan dengan nama besar, badan-badan militer dan pemerintah dan rumah sakit. Boom internet memiliki andil dalam serangan-serangan rekayasa industri sejak awal, namun umumnya serangan terfokus pada entitas-entitas yang lebih besar.

Menemukan teladan yang baikdan nyata dari serangan-serangan social engineering adalah sulit. Organisasi-organisasi yang dijadikan sasaran tidak mau mengijinkan bahwa mereka dikorbankan(lebih-lebih, mengijinkan suatu terobosan security fundamental tidak hanya memalukan, ia mungkin merusak reputasi organisasi) dan/atau serangan-serangan tidak terdokumentasi dengan baik sehingga tak seorangpun yang benar-benar yakin apakah ada suatu serangan social engineering atau tidak. Kkatakan sja mengapa organisasi dijadikan sasaran melalui social engineering – baiklah, ini seringkalil merupakan suatu cara yang lebih mudah untuk mendapatkan akses melanggar hukum daripada berbagai macam bentuk hacking teknis. Bahkan untuk orang-orang teknis, hal ini seringkali jauh lebih sederhana untuk sekedar mengangkat telepon dan meminta password seseorang. Dan yang paling sering, persis seperti itulah yang akan dilakukan oleh seorang hacker. Serangan-serangan social engineering berlangsung pada dua level: fisik dan psikologis. Pertama, kita memfokuskan pada setting fisik untuk serangan ini: tempat kerja, telepon, tempat sampah, dan bahkan on-line. Di tempat kerja, hacker bisa dengan mudah melewati pintu, seperti di dalam bioskop, dan berpura-pura menjadi seorang pekerja pemeliharaan atau konsultan yang memiliki akses pada organisasi. Kemudian seorang penyusup menyelundup melalui kantor sampai dia menemukan suatu password baru yang tergeletak dan keluar dari bangunan dengan informasi di tangan lebih dari cukup untuk mengeksploitasi jaringan dari rumah setelah malam itu. Teknik lain untuk mendapatkan informasi adalah dengan berdiri di sana dan mengamati pekerja yang lalai mengetikkan password.

Social Engineering dengan telepon

Jenis yang paling lazim dari serangan-serangan social engineering dilakukan dengan telepon. Seorang hacker akan menelpon dan meniru seseorang dalam suatu kedudukan berwenang atau yang relevan dan secara

gradual menarik informasi dari user. Kursi bantun secara partikuler condong pada tipe serangan ini. Hacker mampu berpura-pura mereka sedang menelpon dari dalam perusahaan dengan memainkan tipuan atau trik pada PBX atau operator perusahaan, sehingga pemanggil ID tidak selalu menjadi pertahanan terbaik. Ini merupakan trik PBX klasik, memelihara the Computer Security Institute: "'Hai, saya AT&T rep, Saya sedaang macet. Saya prlu anda untuk menekan sebuah bunch tombol untuk saya.'"

Dan di ini adalah bentuk yang lebih baik: "Mereka akan menelpon anda ppada tengah maalam: 'Apakah anda sedang ditelpon dari Mesir beberapa jam yang lalu? 'Tidak.' Dan mereka aan berkata, 'baiklah, kami sedang menerima telepon yang benar-benar aktif sekrang ini, yaitu dari kartu telepon anda dan ini menuju ke Mesir dan sebagaimana kenyataannya, anda mendapatkan sekitar 2.000 dollar kembalian dari sesorang yang menggunakan kartu anda. Anda bertanggungjawab atas 2.000 dollar itu, anda harus membayarnya.....' Mereka akan berkata, 'saya melakukan pekerjaan saya sesuai jalurnya dengan membebaskan biaya 2.000 dollar uuntuk anda. Namun anda perlu memberitahukan nomor kartu AT&T anda dan PIN-nya dan kemuudian saya akan membebskan biaya anda. Orang-orang jatuh karena hal ini." (Computer Security Institute).

Bagian bantuan secra partikuler rentan karena mereka dalam posisi yang secara spesifik untuk membantu, suatu fakta yang mungkin dieksploitasi oleh orang-orang yang berusaha mendapatkan informasi yang melanggar hukum. Pekerja Bagian bantuan dilatih untuk ramah dan memberikan informasi, sehingga ia menjadi tambang emas bagi social engineering. sebagian besar pekerja bagian bantuan umumnya dididik dalam wilayah aman dan mendapatkan kenyamanan, sehingga mereka cenderung hanya menjawab pertanyaan dan terus melayani telepon berikutnya. Hal ini bisa menciptakan lubang keamanan yang besar.

Fasilitator dari suatu lembaga keamanan komputer sekarang ini, diilustrasikan rentan dari Bagian bantuan ketika dia menelpon sebuah perusahaan, menerima transfer, dan mencapai bagian bantuan. 'Siapa pengawas yang menjalankan kewajibannya nanti malam? 'Oh, pengawas nanti malam adalah Betty.' 'Izinkan saya berbicara pada Betty.' [Dia dihubungkan pada Betty.] 'Hai Betty, ada berita buruk?' 'Tidak, Mengapa?' '...Sistem-mu sedang down.' Dia berkata, 'Sistem saya tidak down, kami sedang berjalan baik-baik saja.' Dia berkata, 'Lebih baik kamu keluar dari sistem.' Betty keluar dari sistem. Dia berkata, 'Sekarang sign in kembali.' Betty sing in kembali. Dia berkata, "Kita bahkan tidak melihat sebuah blip, kami melihat tidaak ada perubahan.' Dia berkata, 'Sign off kembali. 'Betty melakukannya. 'Betty, sekarang aku harus masuk sign on sebagai kamu di sini untuk memperkirakan apa yang terjadi dengan ID kamu. Izinkan aku mengetahui ID user dan password-mu.' Maka Pengawas senior ini memberitahukan dari Bagian bantuan ID user dan password-nya." Sangat cerdas.

Suatu variasi tentang tema telepon adalah pembayaran telepon atau ATM. Hacker benar-benar bekerjakeras dalam surfing dan mendapatkan nomor kartu kredit dan PIN dengan cara ini. (Itu terjadi pada salah satu teman saya di sebagian besar bandar udara di Amerika Serikat.). orang-orang selalu berdiri di sekitar anjungan telepon di sekitar bandara, sehingga ia menjadi tempat yang paling beresiko.

Diving Dumpster

Dumpster diving, juga dikenal sebagai sampah, adalah metode populer lain dari social engineering. Sejumlah informasi yang sangat besar bisa dikumpulkan melalui company Dumpster. The LAN Times mendaftar daftar-daftar berikut sebagai potensi kebocoran keamanan dalam trash kita: "Buku telepon perusahaan, grafik organisasi, memo, panduan kerja kebijakan

perusahaan, kalender pertemuan, peristiwa-peristiwa dan peletakan jabatan, panduan kerja sistem, printout data yang sensitif atau nama login dan password, printout kode, disket dan tape sumber, kepala surat perusahaan dan formulir memo, dan pperangkat keras lama."

Sumber-sumber data ini menyediakan suatu jalur informasi yang kaya untuk para hacker. Buku telepon memberikan nama-nama pada para hacker dan jumlah orang untuk dijadikan target dan diimpersonasikan. Grafik-grafik organisasional berisi informasi tentang orang yang berada dalam posisis kewenangan organisasi. Memo menyediakan tidbit kecil dari informas yang bermanfaat guna menciptakan otentisitas. Panduan kebijakan memperlihatkan pada para hacker bagaimana aman atau tidak amannya sebuah perusahaan. Kalender sangat hebat –mereka mungkin memberitahu penyerang tentang pekerja mana yang keluar kota pada waktu-waktu ttertentu. Panduan kerja sistem, data sensitif, dan sumber informasi teknis lainnya mungkin memberikan kunci-kunci pasti yang mereka perlukan untuk membuka jaringan. Akhirnya, perangkat keras yang lama, khususnya drive-drive keras, bisa direstorasi untuk menyediakan bentuk-bentuk informasi yang bermanfaat. (kita akan mendiskusikan bagaimana merapikan semua ini dalam penginstallan kedua dalam rangkaian ini, cukuplah dikatakan, pemotong adalah suatu tempat yang baik untuk memulainya.

Social engineering on-line

Internet adalah lahan subur bagi para teknisi sosiaal yang ingin mendapatkan password. Kelemahan utamanya adalah banyaknya user yang sering mengulangi pemanfaatan sebuah password sederhana pada setiap tranksaksi: Yahoo, Travelocity, Gap.com, dan sebagainya. Maka sekali seorang hacker memiliki stu password, dia mungkin bisa masuk ke dalam berbagai transaksi. Satu cara dimana seorang hacker diketahui mendapatkan jenis password ini adalah melalui uatu formulir on-line: mereka bisa

mengirimkan beberapa bentuk informasi perjudian kuda dan meminta user untuk menempatkan namanya(termasuk alamat e-mail –cara itu, dia bahkan mungkin mendapatkan password transaksi keseluruhan seseorang) dan passwordnya. Formulir ini bisa dikirimkan lewat e-mail atau melalui US-Mail. US-Mail menyediakan suatu bentuk yang lebih baik sehingga perjudian kuda bisa menjadi usaha yang sah.

Cara lain mendapatkan informasi on-line yang dilakukan seorang hacker adalah dengan berpura-pura menjadi administrator jaringan, mengirimkan e-mail melalui jaringan dan meminta password seorang user. Jenis serangan social engineering ini umumnya tidak bekerja dengan baik, karena user umumnya lebih sadar hacker ketika sedang online, namun ini menjadi sesuatu yang perlu diperhitungkan. Lebih jauh lagi, pop-up windows bisa diinstal oleh hacker untuk berpura-pura sebagai bagian suatu jaringan dan eminta user untuk memasukkan kembali username dan password untuk mengatasi beberapa bentuk masalah. Sampai pada titik ini, sebagian besar user seharusnya tahu untuk tidak mengirimkan password dalam teks yang jelas, namun ia tidak pernah menyakitkan untuk memiliki suatu reminder ukuran keamanan sederhana dari administrator sistem. Bahkan lebih baik administrator sistem mungkin ingin mengingatkan user mereka untuk menunjukkan pasword dalam bentuk apapun kecuali percakapan langsung tatap-muka dengan anggota staf yang diberi wewenang dan dipercayai.

E-mail juga bisa digunakan sebagai sarana untuk mendapatkan akses lebih langsung pada suatu sistem. Misalnya, attachment surat yang dikirmkan dari seseorang yang otentik bisa membawa virus, worm dan trojan horses. Contoh yang baik dari hal ini adalah sebuah hack AOL yang didokumentasikan oleh VIGILANTe: “Dalam kasus itu, hacker memintaa dukungan teknologi AOL dan berbicara dengan person pendukung selama stu jam. Selama percakapan, hacker menyebutkan bahwa mobilnya dijual murah. Pendukung teknologi tertaarik sehingga hacker mengirimkan sebuah

attachment e-mail ‘dengan sebuah gambar mobil.’ Sekalipun sebuah gambar mobil, surat tersebut mengeksekusikan suatu penyelundupan lewat jalan belakang yang membuka koneksi dari AOL melalui firewall.”

Persuasi

Hacker itu sendiri mengajarkan social engineering dari suatu sudut pandang psikologis dengan menekankan bagaimana menciptakan suatu lingkungan psikologis sempurna bagi serangan. Metode mendasar persuasi meliputi: impersonasi, ingrasiasi, konformitas, penyebaran tanggungjawab, dan persahabatan lama yang jelas. Dengan mengabaikan metode yang digunakan, ssaran utamanya adalah untuk meyakinkan orang yang memperlihatkan informasi bahwa social engineer pada kenyataanya adalah suatu person yang bisa mereka percayai dengan informasi yang sensitif tersebut. Kunci penting lainnya adalah jangan pernah meminta terlalu banyak informasi pada suatu waktu, namun mintalah sedikit dari tiap-tip orang untuk memelihara suatu bentuk hubungan yang nyaman.

Impersonation umumnya berarti menciptakan beberapa bentuk karakter dan memerankan perannya. Semakin lebih sederhana perannya, akan lebih baik. Kadang-kadang ini hanya bisa berarti menelpon, dan berkata: “Hai, Saya Joe di MIS dan saya memerlukan password anda,” namun hal itu tidak elalu berhasil. Lain kali, hacker akan mempelajari seorang individu nyata dalam sebuah organisasi dan menunggu sampai orang itu keluar kota untuk mengimpersonasikannya lewat telepon. Menurut Bernz, seorang hacker yang telah menuliskan secara ekstensif tentang subyek ini, mereka menggunakan kotak kecil untuk menyamarkan suara mereka dan mempelajari pola-pola bicara dan grafik-grafik org. Saya katakan ini merupakan tipe serangan impersonasi yang sedikitnya paling memungkinkan karena ia melakukan persiapan dengan baik, dan itu benar-benaar terjadi.

Beberapa pperan umum yang mungkin dimainkan dalam serangan impersonasi termasuk: seorang montir, pendukung TI, manajer, suatu pihak ektigaa yang dipercaya(misalnya seorang asisten eksekutif presiden yang menelpon dan mengatakan bahwa presiden membolehkan dia meminta informas tertentu), atau seorang pekerja tamu. Dalam sebuah perusahaan raksasa, tidak sulit melakukan hal ini. Tiidak ada cara untuk mengetahui setiap orang –kartu identittas bisa dipalsu. Sebagian besar peran ini jatuh ke kategori seseorang dengan suatu kewenangan, yang mengarahkan kita pada ingrasiasi. Sebagian besar pekerja ingin mengesankan bos-nya, sehinggga merekaa akan membungkukkan punggungnya untuk menyediakan informasi yang dipersyaratkan bagi siapapun yang sedang berkuasa.

Konformitas adalah suatu tingkah-laku yang didasarkan pada kelompok, namun kadangkala bisa digunakan dalam setting individual dengan meyakinkan user bahwa setiap orang lain telah memberikan informasi yang sama pada hacker sekaran diminta misalnya apakah hacker itu mengimpersonasikan seorrang manajer TI. Ketika hacker menyerang dengan cara-cara semacam itu untuk menyebarkan tanggungjawab pada pekerja yang memberikan passwordnya, hal itu membebankan tekanan pada para pekerja.

Ketika ragu-ragu, cara terbaik untuk mendapatkan informasi dalam suatu serangan social engineering adalah dengan berteman. Idenya di sini adalah karena rata-rata uuser ingin mempercayai koleganya di telepon dan ingin membantu, sehingga hacker benar-benar hanya butuh untuk bisa dipercaya secara mendasar. Di luar itu, sebagian besar pekerja merespon dengan baik, khususnya pada perempuan. Snjungan ringan dan permainan mata mungkin akan membantu melembutkan pekerja yang dijadikan sasaran untuk bekerjasama lebih jauh, namun hacker yang cerdas tahu kapan ia harus berhenti mengorek informasi, tepat sebelum pekerja menduga adanya hal—hal yang aneh. Suatu senyuman, jika pada seseorang, atau suatu ucapan

terima kasih akan melancarkan deal. Dan jika itu tidak cukup, pertanyaan rutin user baru seringkali pula bisa digunakanan: “saya bingung, (sembari menaikkan alis) bisakah anda membantu saya?”

Reverse social engineering

Suatu metode yang maju dan final dalam mendapatkan informasi yang melanggar hukum ini dikenal sebagai “reverse social engineering”. Hal ini terjadi ketika seorang hacker menciptakan suatu persona yang muncul dan berada dalam suatu posisis kewenangan sehingga pekerja akan memintanya informasi dibandingkan dengan cara lainnya. Jika diteliti, direncanakan dan dilakukan dengan baik, serangan reverse social engineering mungkin menawarkan suatu kesempatan yang lebih baik bagi hacker untuk mendapatkan data yang berharga dari pekerja; namun, hal ini mensyaratkan suatu bentuk persiapan, penelitian, dan pra-hacking yang besar agar berhasil.

Berdasarkan pada Methods of Hacking: Social Engineering, suatu makalah yang ditulis oleh Rick Nelson, tig bagian serangan-serangan reverse social engineering adalah sabotase, iklan, dan assisting. Gacker men-sabotase suatu jaringan, menyebabkan suatu masalah muncul. Hacker itu kemudian mengiklankan bahwa dia adalah orang yang tepat untuk mengatasi permasalahan, dan kemumdian, ketika dia datang untuk mengatasi masalah, dia mensyaratkan jumlah tertentu informasi dari para pekerja dan mendapatkan apa yang benarr-benar ia inginkan. Mereka tidak pernah tahu bahwa tu adalah hacker, karena permasalahan jaringan mereka telah selesai diperbaiki dan setiap orang menjadi bahagia.

Kesimpulan

Tentu saja tidak ada artikel social engineering yang lengkap tanpa menyebutkan Kevin Mitnick, sehingga saya menyimpulkan dengan suatu kutipan darinya lewat artikel tentang Fokus Keamanan(Security Fokus):

“Anda bisa saja membeli suatu teknologi dan jasa yang menguntungkan dan infrastruktur jaringan anda masih tetap rentan pada manipulasi gaya lama.” Tetap perhatikan bagian II: Strategi Pertempuran, yang akan melihat cara-cara melawan serangan-serangan dengan mengidentifikasikan serangan-serangan, dan dengan menggunakan teknologi, pelatihan dan kebijakan preventif.