



KEAMANAN JARINGAN

HIMPUNAN SISWA TI

SMKN 5 Malang

Foreword :

Tujuan dari penulisan artikel ini adalah untuk menyediakan landasan umum yang bagus akan pemahaman keamanan jaringan komputer. Pemahaman dasar pada keamanan jaringan komputer sangat perlu untuk merawat jaringan komputer tanpa harus terjadi insiden keamanan didalam jaringan itu. Artikel ini juga sebagai bahan ilustrasi beberapa insiden keamanan yang terjadi dan mencoba menjelaskan bagaimana cara melindungi dengan mengambil keuntungan dari celah keamanan itu sendiri.

Artikel ini tidak akan menjelaskan secara detil akan tetapi para pembaca setidaknya telah mendapat suatu gambaran yang bagus dan mungkin mendapat ide untuk dimana mencari jawaban apabila ingin mencari beberapa informasi tambahan.

Penulis....

Keamanan Jaringan Komputer

Keamanan jaringan komputer sendiri sering dipandang sebagai hasil dari beberapa faktor. Faktor ini bervariasi tergantung pada bahan dasar, tetapi secara normal setidaknya beberapa hal dibawah ini diikutsertakan :

- Confidentiality (kerahasiaan).
- Integrity (integritas).
- Availability (ketersediaan).

Keamanan klasik penting ini tidak cukup untuk mencakup semua aspek dari keamanan jaringan komputer pada masa sekarang [1]. Hal-hal tersebut dapat dikombinasikan lagi oleh beberapa hal penting lainnya yang dapat membuat keamanan jaringan komputer dapat ditingkatkan lagi dengan mengikut sertakan hal dibawah ini:

- Nonrepudiation.
- Authenticity.
- Possession.
- Utility.

Availability (ketersediaan).

Ketersediaan data atau layanan dapat dengan mudah dipantau oleh pengguna dari sebuah layanan. Yang dimana ketidaktersediaan dari sebuah layanan (service) dapat menjadi sebuah halangan untuk maju bagi sebuah perusahaan dan bahkan dapat berdampak lebih buruk lagi, yaitu penghentian proses produksi [1]. Sehingga untuk semua aktifitas jaringan, ketersediaan data sangat penting untuk sebuah system agar dapat terus berjalan dengan benar.

Confidentiality (kerahasiaan).

Ada beberapa jenis informasi yang tersedia didalam sebuah jaringan komputer. Setiap data yang berbeda pasti mempunyai grup pengguna yang berbeda pula dan data dapat dikelompokkan sehingga beberapa pembatasan kepada penggunaan data harus ditentukan. Pada umumnya data yang terdapat didalam suatu perusahaan bersifat rahasia dan tidak boleh diketahui oleh pihak ketiga yang bertujuan untuk menjaga rahasia perusahaan dan strategi perusahaan [2]. Backdoor, sebagai contoh, melanggar kebijakan perusahaan dikarenakan menyediakan akses yang tidak diinginkan kedalam jaringan komputer perusahaan.

Kerahasiaan dapat ditingkatkan dan didalam beberapa kasus pengenkripsian data atau menggunakan VPN [22][2]. Topik ini tidak akan, tetapi bagaimanapun juga, akan disertakan dalam tulisan ini. Kontrol akses adalah cara yang lazim digunakan untuk membatasi akses kedalam sebuah jaringan komputer. Sebuah cara yang mudah tetapi mampu untuk membatasi akses adalah dengan

menggunakan kombinasi dari username-dan-password untuk proses otentifikasi pengguna dan memberikan akses kepada pengguna (user) yang telah dikenali [2]. Didalam beberapa lingkungan kerja keamanan jaringan komputer, ini dibahas dan dipisahkan dalam konteks otentifikasi [3].

Integrity (integritas).

Jaringan komputer yang dapat diandalkan juga berdasar pada fakta bahwa data yang tersedia apa yang sudah seharusnya. Jaringan komputer mau tidak mau harus terlindungi dari serangan (attacks) yang dapat merubah data selama dalam proses persinggahan (transmit) [4]. Man-in-the-Middle merupakan jenis serangan yang dapat merubah integritas dari sebuah data yang mana penyerang (attacker) dapat membajak "session" atau memanipulasi data yang terkirim [5].

Didalam jaringan komputer yang aman, partisipan dari sebuah "transaksi" data harus yakin bahwa orang yang terlibat dalam komunikasi data dapat diandalkan dan dapat dipercaya. Keamanan dari sebuah komunikasi data sangat diperlukan pada sebuah tingkatan yang dipastikan data tidak berubah selama proses pengiriman dan penerimaan pada saat komunikasi data. Ini tidak harus selalu berarti bahwa "traffic" perlu di enkripsi, tapi juga tidak tertutup kemungkinan serangan "Man-in-the-Middle" dapat terjadi.

Nonrepudiation.

Setiap tindakan yang dilakukan dalam sebuah system yang aman telah diawasi (logged), ini dapat berarti penggunaan alat (tool) untuk melakukan pengecekan system berfungsi sebagaimana seharusnya. "Log" juga tidak dapat dipisahkan dari bagian keamanan "system" yang dimana bila terjadi sebuah penyusupan atau serangan lain akan sangat membantu proses investigasi [17]. "Log" dan catatan waktu, sebagai contoh, bagian penting dari bukti di pengadilan jika cracker tertangkap dan diadili. Untuk alasan ini maka "nonrepudiation" dianggap sebagai sebuah faktor penting didalam keamanan

jaringan komputer yang berkompeten.

ITU-T telah mendefinisikan "nonrepudition" sebagai berikut :

1. Kemampuan untuk mencegah seorang pengirim untuk menyangkal kemudian bahwa dia telah mengirim pesan atau melakukan sebuah tindakan.
2. Proteksi dari penyangkalan oleh satu satu dari entitas yang terlibat didalam sebuah komunikasi yang turut serta secara keseluruhan atau sebagian dari komunikasi yang terjadi [7].

Jaringan komputer dan system data yang lain dibangun dari beberapa komponen yang berbeda yang dimana masing-masing mempunyai karakteristik spesial untuk keamanan. Sebuah jaringan komputer yang aman perlu masalah keamanan yang harus diperhatikan disemua sektor, yang mana rantai keamanan yang komplit sangat lemah, selemah titik terlemahnya [8]. Pengguna (user) merupakan bagian penting dari sebuah rantai. "Social engineering" merupakan cara yang efisien untuk

mencari celah (vulnerabilities) pada suatu system [21] dan kebanyakan orang menggunakan "password" yang mudah ditebak. Ini juga berarti meninggalkan "workstation" tidak dalam keadaan terkunci pada saat makan siang atau yang lainnya.

Sistem operasi (operating system : Windows, Unix, Linux, MacOS) terdapat dimana-mana, komputer mempunyai sistem operasi yang berbeda-beda antara satu dengan yang lainnya (tergantung selera), dan bahkan router juga dijalankan oleh sistem operasi. Setiap sistem operasi mempunyai gaya dan karakteristik sendiri yang membedakannya dengan sistem operasi yang lainnya, dan beberapa bahkan digunakan untuk kepentingan "server". Beberapa sistem operasi juga mempunyai masalah yang dapat digunakan sehingga menyebabkan sistem operasi tersebut berhenti merespon pengguna.

Layanan pada "server" memainkan peranan penting dalam keamanan. Developer perangkat lunak mengumumkan celah keamanan pada perangkat lunak dengan cepat. Alasan yang digunakan adalah celah ini kemungkinan akan digunakan oleh pihak yang tidak bertanggung jawab untuk menyusupi sebuah system ataupun setiap pengguna komputer. Pengelola atau pengguna server dan workstation harus melakukan pengecekan untuk "update" masalah keamanan secara reguler.

Perangkat keras mungkin sedikit susah dipahami sebagai sesuatu yang mempunyai potensi untuk mempunyai masalah keamanan. Yang sesungguhnya adalah sangat berbeda dengan apa yang kita pikirkan, apabila perangkat keras terletak di sebuah lokasi yang tidak aman maka terdapat resiko untuk pemasangan perangkat keras yang tidak diinginkan kedalam jaringan komputer dan ini dapat membuat penyusupan menjadi mudah. Juga, bila sebuah perangkat keras jaringan computer dirubah setting-nya ke konfigurasi default oleh orang luar.

Pemilihan jenis metode transmisi juga mempunyai peranan penting didalam masalah keamanan. Setiap informasi rahasia tidak boleh di transmisikan secara wireless, setidaknya tidak tanpa menggunakan enkripsi yang bagus, sehingga setiap orang dapat menyadap komunikasi "wireless" yang terkirim. Sangat dianjurkan untuk menggunakan firewall untuk membatasi akses kedalam jaringan komputer ke tingkat yang dibutuhkan. Firewall juga dapat menjadi titik terlemah[9], yang mana dapat membuat perasaan aman [10]. Firewall harus mengizinkan arus data kedalam sebuah jaringan komputer jika terdapat juga arus data keluar dari jaringan komputer tersebut melalui firewall dan ini dapat menjadi titik terlemah. Fakta penting lainnya bahwa tidak semua serangan dilancarkan melalui firewall [10].

Mengamankan Jaringan Komputer

Mengamankan jaringan komputer membutuhkan tiga tingkatan proses. Untuk mengamankan jaringan komputer kita harus dapat melakukan pemetaan terhadap ancaman yang mungkin terjadi.

Prevention (pencegahan).

Kebanyakan dari ancaman akan dapat ditepis dengan mudah, walaupun keadaan yang benar-benar 100% aman belum tentu dapat dicapai. Akses yang tidak diinginkan kedalam jaringan komputer dapat dicegah dengan memilih dan melakukan konfigurasi layanan (services) yang berjalan dengan hati-hati.

Observation (observasi).

Ketika sebuah jaringan komputer sedang berjalan, dan sebuah akses yang tidak diinginkan dicegah, maka proses perawatan dilakukan. Perawatan jaringan komputer harus termasuk melihat isi log yang tidak normal yang dapat merujuk ke masalah keamanan yang tidak terpantau. System IDS dapat digunakan sebagai bagian dari proses observasi tetapi menggunakan IDS seharusnya tidak merujuk kepada ketidak-pedulian pada informasi log yang disediakan.

Response (respon).

Bila sesuatu yang tidak diinginkan terjadi dan keamanan suatu system telah berhasil disusupi, maka personil perawatan harus segera mengambil tindakan. Tergantung pada proses produktifitas dan masalah yang menyangkut dengan keamanan maka tindakan yang tepat harus segera dilaksanakan. Bila sebuah proses sangat vital pengaruhnya kepada fungsi system dan apabila di-shutdown akan menyebabkan lebih banyak kerugian daripada membiarkan system yang telah berhasil disusupi tetap dibiarkan berjalan, maka harus dipertimbangkan untuk direncanakan perawatan pada saat yang tepat [1]. Ini merupakan masalah yang sulit dikarenakan tidak seorangpun akan segera tahu apa yang menjadi celah begitu system telah berhasil disusupi dari luar.

Victims/statistic (korban/statistik).

Keamanan jaringan komputer meliputi beberapa hal yang berbeda yang mempengaruhi keamanan secara keseluruhan. Serangan keamanan jaringan komputer dan penggunaan yang salah dan sebagai contoh adalah virus, serangan dari dalam jaringan komputer itu sendiri, pencurian perangkat keras (hardware), penetrasi kedalam system, serangan "Denial of Service" (DoS), sabotase, serangan "wireless" terhadap jaringan komputer, penggantian halaman depan situs (website defacement), dan penggunaan yang salah terhadap aplikasi web. Statistik menunjukkan jumlah penyusupan didalam area ini sudah cukup banyak berkurang dari tahun 2003 [24], tipe variasi dari serangan, bagaimanapun juga, menyebabkan hampir setiap orang adalah sasaran yang menarik.

Masalah keamanan

Jaringan komputer moderen adalah entitas dari banyak komponen kecil. Disini akan dijelaskan beberapa titik lemah dari komponen yang berbeda.

Weak protocols (protokol yang lemah).

Komunikasi jaringan komputer menggunakan protokol antara client dan server. Kebanyakan dari protokol yang digunakan saat ini merupakan protocol yang telah digunakan beberapa dasawarsa belakangan. Protokol lama ini, seperti File Transmission Protocol (FTP), TFTP ataupun telnet [11], tidak didesain untuk menjadi benar-benar aman. Malahan faktanya kebanyakan dari protocol ini sudah seharusnya digantikan dengan protokol yang jauh lebih aman, dikarenakan banyak titik rawan yang dapat menyebabkan pengguna (user) yang tidak bertanggung jawab dapat melakukan eksploitasi. Sebagai contoh, seseorang dengan mudah dapat mengawasi "traffic" dari telnet dan dapat mencari tahu nama user dan password.

Software issue (masalah perangkat lunak).

Menjadi sesuatu yang mudah untuk melakukan eksploitasi celah pada perangkat lunak. Celah ini biasanya tidak secara sengaja dibuat tapi kebanyakan semua orang mengalami kerugian dari kelemahan seperti ini. Celah ini biasanya dibakukan bahwa apapun yang dijalankan oleh "root" pasti mempunyai akses "root", yaitu kemampuan untuk melakukan segalanya didalam system tersebut. Eksploitasi yang sebenarnya mengambil keuntungan dari lemahnya penanganan data yang tidak diduga oleh pengguna, sebagai contoh, buffer overflow dari celah keamanan "format string" merupakan hal yang biasa saat ini.

Eksploitasi terhadap celah tersebut akan menuju kepada situasi dimana hak akses pengguna akan dapat dinaikkan ke tingkat akses yang lebih tinggi. Ini disebut juga dengan "rooting" sebuah "host" dikarenakan penyerang biasanya membidik untuk mendapatkan hak akses "root" [2].

Buffer overflow.

"Buffer overflow" mempunyai arti sama dengan istilahnya. Programmer telah mengalokasikan sekian besar memory untuk beberapa variabel spesifik. Bagaimanapun juga, dengan celah keamanan ini, maka variabel ini dapat dipaksa menuliskan kedalam "stack" tanpa harus melakukan pengecekan kembali bila panjang variabel tersebut diizinkan. Jika data yang berada didalam buffer ternyata lebih panjang daripada yang diharapkan, maka kemungkinan akan melakukan penulisan kembali stack frame dari "return address" sehingga alamat dari proses eksekusi program dapat dirubah.

Penulis "malicious code" biasanya akan melakukan eksploitasi terhadap penulisan kembali "return address" dengan merubah "return address" kepada "shellcode" pilihan mereka sendiri untuk melakukan pembatalan akses "shell" dengan menggunakan hak akses dari "user-id" dari program yang

tereksploitasi tersebut [12]. "Shellcode" ini tidak harus disertakan dalam program yang tereksploitasi, tetapi biasanya dituliskan ke dalam bagian celah dari "buffer". Ini merupakan trik yang biasa digunakan pada variabel

"environment" seperti ini.

"Buffer overflow" adalah masalah fundamental berdasarkan dari arsitektur komputasi modern. Ruang untuk variabel dan kode itu sendiri tidak dapat dipisahkan kedalam blok yang berbeda didalam "memory". Sebuah perubahan didalam arsitektur dapat dengan mudah menyelesaikan masalah ini, tapi perubahan bukan sesuatu yang mudah untuk dilakukan dikarenakan arsitektur yang digunakan saat ini sudah sangat banyak digunakan.

Format string.

Metode penyerangan "format string" merupakan sebuah metode penyerangan baru, ini diumumkan kepada publik diakhir tahun 2000. Metode ini ditemukan oleh hacker 6 bulan sebelum diumumkan kepada masyarakat luas. Secara fundamental celah ini mengingatkan kita akan miripnya dengan celah "buffer overflow" [13].

Kecuali celah tersebut tercipta dikarenakan kemalasan (laziness), ketidakpedulian (ignorance), atau programmer yang mempunyai skill pas-pasan. Celah "format string" biasanya disebabkan oleh kurangnya "format string" seperti "%s" di beberapa bagian dari program yang menciptakan output, sebagai contoh fungsi printf() di C/C++. Bila input diberikan dengan melewati "format string" seperti "%d" dan "%s" kepada program maka dengan mudah melihat "stack dump" atau penggunaan teknik seperti pada "buffer overflow".

Celah ini berdasarkan pada "truncated format string" dari "input". Ini merujuk kepada situasi dimana secara external, data yang disuplai yang diinterpretasikan sebagai bagian dari "format string argument" [13]. Dengan secara spesial membuat suatu input dapat menyebabkan program yang bermasalah menunjukkan isi memory dan juga kontrol kepada eksekusi program dengan menuliskan apa saja kepada lokasi pilihan sama seperti pada eksploitasi "overflow".

Hardware issue (masalah perangkat keras).

Biasanya perangkat keras tidak mempunyai masalah pada penyerangan yang terjadi. Perangkat lunak yang dijalankan oleh perangkat keras dan kemungkinan kurangnya dokumentasi spesifikasi teknis merupakan suatu titik lemah. Berikut ini merupakan contoh bagaimana perangkat keras mempunyai masalah dengan keamanan.

contoh 1: Cisco

Sudah lazim router cisco dianggap mempunyai masalah sistematis didalam perangkat lunak IOS (Interwork operating system) yang digunakan oleh mereka sebagai sistem operasi pada tahun 2003. Celah dalam perangkat lunak dapat menuju kepada "denial of service" (Dos) dari semua perangkat

router. Masalah keamanan ini terdapat dalam cara IOS menangani protokol 53(SWIPE), 55(IP Mobility) dan 77(Sun ND) dengan nilai TTL (Time to live) 0 atau 1 [23].

Biasanya, Protocol Independent Multicast (PIM) dengan semua nilai untuk hidup, dapat menyebabkan router menandai input permintaan yang penuh terhadap "interface" yang dikirimkan. Sebagai permintaan bila penuh, maka router tidak akan melakukan proses "traffic" apapun terhadap "interface" yang dipertanyakan [3]. Cisco juga mempunyai beberapa celah keamanan yang terdokumentasi dan "patch" yang diperlukan telah tersedia untuk waktu yang cukup lama.

contoh 2: Linksys

Perangkat linksys mempunyai harga yang cukup murah sehingga banyak digunakan oleh orang. Beberapa perangkat linksys mempunyai masalah dengan celah keamanan yang dapat menuju kepada serangan "denial of service" (DoS). Celah keamanan yang memprihatinkan terdapat pada penanganan parameter "URL Embedded" yang dikirimkan kepada perangkat.

Misconfiguration (konfigurasi yang salah).

Kesalahan konfigurasi pada server dan perangkat keras (hardware) sangat sering membuat para penyusup dapat masuk kedalam suatu system dengan mudah. Sebagai contoh, penggantian halaman depan suatu situs dikarenakan kesalahan konfigurasi pada perangkat lunak "www-server" ataupun modulnya. Konfigurasi yang tidak hati-hati dapat menyebabkan usaha penyusupan menjadi jauh lebih mudah terlebih jika ada pilihan lain yang dapat diambil oleh para penyusup.

Sebagai contoh, sebuah server yang menjalankan beberapa layanan SSH dapat dengan mudah disusupi apabila mengizinkan penggunaan protokol versi 1 atau "remote root login" (RLOGIN) diizinkan. Kesalahan konfigurasi yang jelas ini menyebabkan terbukanya celah keamanan dengan penggunaan protokol versi 1, seperti "buffer overflow" yang dapat menyebabkan penyusup dapat mengambil hak akses "root" ataupun juga dengan menggunakan metode "brute-force password" untuk dapat menebak password "root".

DoS, DDoS.

Serangan Denial of Service adalah serangan yang mengakibatkan setiap korbannya akan berhenti merespon [5] atau "bertingkah" tidak lazim. Contoh serangan klasik "DoS" adalah "Ping of Death" dan "Syn Flood" yang untungnya sudah hampir tidak dapat dijumpai pada saat sekarang. Biasanya serangan DoS menyerang celah yang terdapat pada layanan system atau pada protokol jaringan kerja untuk menyebabkan layanan tidak dapat digunakan. Teknik yang lainnya adalah menyebabkan system korban "tersedak" dikarenakan banyaknya paket yang diterima yang harus diproses melebihi kemampuan dari system itu sendiri atau menyebabkan terjadinya "bottleneck" pada bandwidth yang dipakai oleh system.

Serangan "Distributed Denial of Service" (DDoS) merupakan tipe serangan yang lebih terorganisasi. Jenis serangan ini biasanya membutuhkan persiapan dan juga taktik untuk dapat menjatuhkan korbannya dengan cepat dan sebelumnya biasanya para penyerang akan mencari system kecil yang dapat dikuasai dan setelah mendapat banyak system kecil maka penyerang akan menyerang system yang besar dengan menjalankan ribuan bahkan puluhan ribu system kecil secara bersamaan untuk menjatuhkan sebuah system yang besar [5].

Worm "MyDoom" yang terkenal itu dibuat untuk melancarkan serangan besar-besaran dari puluhan ribu system yang terinfeksi untuk menyerang situs www.sco.com. Serangan itu sukses besar yang menyebabkan www.sco.com harus dipindahkan dari DNS untuk dapat menjalankan kembali layanan [20].

Viruses (virus).

Salah satu definisi dari program virus adalah menyisipkan dirinya kepada objek lain seperti file executable dan beberapa jenis dokumen yang banyak dipakai orang. Selain kemampuan untuk mereplikasi dirinya sendiri, virus dapat menyimpan dan menjalankan sebuah tugas spesifik. Tugas tersebut bisa bersifat menghancurkan atau sekedar menampilkan sesuatu ke layar monitor korban dan bisa saja bertugas untuk mencari suatu jenis file untuk dikirimkan secara acak ke internet bahkan dapat melakukan format pada hard disk korban [18].

Virus yang tersebar di internet yang belum dikenali tidak akan dapat ditangkap oleh program antivirus ataupun semacamnya yang meskipun korban telah terjangkiti tetapi tidak mengetahuinya. Perangkat lunak antivirus biasanya mengenali virus atau calon virus melalui tanda yang spesifik yang terdapat pada bagian inti virus itu sendiri. Beberapa virus menggunakan tehnik polymorphic agar luput terdeteksi oleh antivirus.

Kebiasaan virus polymorphic adalah merubah dirinya pada setiap infeksi yang terjadi yang menyebabkan pendeteksian menjadi jauh lebih sulit [18]. Praktisnya setiap platform komputer mempunyai virus masing-masing dan ada beberapa virus yang mempunyai kemampuan menjangkiti beberapa platform yang berbeda (multi-platform). Virus multi-platform biasanya menyerang executable ataupun dokumen pada Windows dikarenakan kepopuleran oleh system operasi Microsoft Windows dan Microsoft Office sehingga banyak ditemukan virus yang bertujuan untuk menghancurkan "kerajaan" Microsoft Corp [4].

Worms.

Sebuah "worm" komputer merupakan program yang menyebar sendiri dengan cara mengirimkan dirinya sendiri ke system yang lainnya. Worm tidak akan menyisipkan dirinya kepada objek lain [18]. Pada saat sekarang banyak terjadi penyebaran worm dikarenakan para pengguna komputer tidak melakukan update pada perangkat lunak yang mereka gunakan, yang dimana ini berarti, sebagai

contoh, Outlook Express mempunyai fungsi yang dapat mengizinkan eksekusi pada file sisipan (attachment) e-mail tanpa campur tangan dari pengguna komputer itu sendiri.

Trojan horse.

Trojan horse adalah program yang berpura-pura tidak berbahaya tetapi sebenarnya mereka sesuatu yang lain [18]. Salah fungsi yang biasa terdapat pada "trojan horse" adalah melakukan instalasi "backdoor" sehingga si pembuat program dapat menyusup kedalam komputer atau system korban.

junk mail (surat sampah).

"junk mail" sesungguhnya bukan suatu ancaman keamanan yang serius, tetapi dengan penyebaran virus dan worm melalui e-mail, maka jumlah junk mail juga ikut bertambah. Ancaman keamanan sesungguhnya bukan dari e-mail sampah itu sendiri melainkan file sisipannya (attachment) yang patut diwaspadai dikarenakan penyebaran virus dan worm menggunakan metode ini.

Time bomb (bom waktu).

"Time bomb" adalah program yang mempunyai tugas tetapi dengan waktu tertentu baru akan menjalankan tugasnya. Beberapa jenis virus dan worm juga mempunyai kesamaan fungsi dengan aplikasi ini. Time bomb berbeda dengan virus ataupun worm dikarenakan dia tidak melakukan replikasi terhadap dirinya tetapi melakukan instalasi sendiri kedalam system.

Hacking: Hackers and Victims (hacking: pelaku dan korban)

Hacker dikategorikan kedalam beberapa kategori yang berbeda tergantung pada jenis kegiatan mereka. Kebanyakan hacker adalah para "script-kiddies" yang biasa menggunakan exploit atau program yang tersedia di internet untuk melancarkan aksi mereka [19]. Jika tujuan mereka adalah untuk kepentingan komersial atau kepentingan militer maka taruhannya menjadi lebih tinggi dan biasanya mereka akan memilih korban mereka dengan hati-hati.

Alasan dibalik hacking sendiri bermacam-macam. Script kiddies biasanya akan melakukan "scanning" beberapa blok IP untuk mencari kemungkinan host yang "vulnerable" (bisa diserang) dan mencoba melakukan eksploitasi kepada beberapa daemon yang ditemukan. Satu grup hacker biasanya mencoba program atau script yang mereka kembangkan untuk melihat apakah hasil kerja mereka sukses. Tapi bagaimanapun juga, seseorang dapat menjadi "black-hat" ataupun "white-hat" tergantung pada filosofi, nilai etis dan motivasi mereka sendiri.

"White-hat" berarti jika seorang "hacker" berhasil dalam usahanya dan sebagai contoh berhasil masuk kedalam sebuah system yang bukan tanggung jawab dia, maka dia akan memberitahukan kepada system administrator mengenai celah keamanan yang terdapat di dalam system tersebut dan bagaimana cara menutup celah keamanan itu serta cara memperkuat host tersebut (host hardening). Tujuan dasarnya adalah untuk penelitian. "White-hat" biasanya adalah para "security professional" dan disewa untuk melakukan "system penetration" atau memberikan konsultasi keamanan jaringan.

"Black-hat" adalah orang yang dipanggil "white-hat" sebagai "cracker" (pembongkar). Tujuan para "cracker" tidak selalu baik, mereka biasanya masuk kedalam suatu system untuk mencuri informasi atau mempersiapkan system itu untuk melakukan serangan terhadap system yang lain, "DDoS" sebagai contoh. "Black-hat" biasanya meninggalkan backdoor di system yang berhasil disusupi.

Terdapat juga jenis **"grey-hat"** atau orang yang tidak merusak tapi sering menyusup kedalam system lain tanpa memberitahu kepada System administrator system tersebut apabila terdapat celah keamanan, mereka tidak terlalu merusak tapi juga tipe yang tidak terlalu diinginkan.

Different Types of Attacking (jenis-jenis serangan)

Scanning.

"Scanning" adalah metode bagaimana caranya mendapatkan informasi sebanyak-banyaknya dari IP/Network korban. Biasanya "scanning" dijalankan secara otomatis mengingat "scanning" pada "multiple-host" sangat menyita waktu. "Hackers" biasanya mengumpulkan informasi dari hasil "scanning" ini. Dengan mengumpulkan informasi yang dibutuhkan maka "hackers" dapat menyiapkan serangan yang akan dilancarkan.

Nmap merupakan sebuah network scanner yang banyak digunakan oleh para professional di bidang network security, walaupun ada tool yang khusus dibuat untuk tujuan hacking, tapi belum dapat mengalahkan kepopuleran nmap.

Nessus juga merupakan network scanner tapi juga akan melaporkan apabila terdapat celah keamanan pada target yang diperiksanya. Hacker biasanya menggunakan Nessus untuk pengumpulan informasi sebelum benar-benar melancarkan serangan.

Untungnya beberapa scanner meninggalkan "jejak" yang unik yang memungkinkan para System administrator untuk mengetahui bahwa system mereka telah di-scanning sehingga mereka bisa segera membaca artikel terbaru yang berhubungan dengan informasi log.

Password cracking.

"Brute-force" adalah sebuah tehnik dimana akan dicobakan semua kemungkinan kata kunci (password) untuk bisa ditebak untuk bisa mengakses kedalam sebuah system. Membongkar kata kunci dengan tehnik ini sangat lambat tapi efisien, semua kata kunci dapat ditebak asalkan waktu tersedia.

Untuk membalikkan "hash" pada kata kunci merupakan suatu yang hal yang mustahil, tapi ada beberapa cara untuk membongkar kata kunci tersebut walaupun tingkat keberhasilannya tergantung dari kuat lemahnya pemilihan kata kunci oleh pengguna. Bila seseorang dapat mengambil data "hash" yang menyimpan kata kunci maka cara yang lumayan efisien untuk dipakai adalah dengan menggunakan metode "dictionary attack" yang dapat dilakukan oleh utility John The Ripper [27].

Masih terdapat beberapa cara lainnya seperti "hash look-up table" tapi sangat menyita "resources" dan waktu.

Rootkit.

"Rootkit" adalah alat untuk menghilangkan jejak apabila telah dilakukan penyusupan. Rootkit biasanya mengikutkan beberapa tool yang dipakai oleh system dengan sudah dimodifikasi sehingga dapat menutupi jejak. Sebagai contoh, memodifikasi "PS" di linux atau unix sehingga tidak dapat melihat background process yang berjalan.

Defending (bertahan)

Firewall.

Komputer dan jaringan kerja yang terhubung dengan internet perlu untuk dilindungi dari serangan. Firewall adalah cara yang lumayan efektif untuk melakukannya. Secara umum firewall akan memisahkan public network dan private network.

Tipe firewall dapat dibagi menjadi beberapa kategori, contohnya: Packet Filtering Firewall, "Proxy Firewall".

Logs.

Seorang system administrator wajib untuk melihat log dari system dari waktu ke waktu. Dengan melihat log maka system administrator dapat melihat aktifitas yang terjadi dan kemungkinan besar dapat melakukan antisipasi apabila terlihat beberapa aktifitas yang mencurigakan terjadi.

IDS. (Intrusion Detection System)

Satu cara umum melakukan otomatisasi pada pengawasan penyusupan adalah dengan menggunakan IDS. IDS akan mendeteksi jenis serangan dari "signature" atau "pattern" pada aktifitas jaringan. Bahkan dapat melakukan blokade terhadap traffic yang mencurigakan.

Honeypot.

"HoneyPot" adalah server "umpan" yang merupakan pengalih perhatian. Tujuan dari honeypot adalah mereka tidak menjalankan layanan sebagaimana umumnya server tetapi berpura-pura menjalankannya sehingga membiarkan para penyusup untuk berpikir bahwa mereka benar-benar adalah "server" yang sesungguhnya. Honeypot juga bermanfaat untuk melihat tehnik yang digunakan oleh para penyusup untuk dapat masuk kedalam system juga sebagai alat untuk mengumpulkan bukti sehingga para penyusup dapat diproses secara hukum.

Configuration.

Seperti yang telah dibahas sebelumnya, konfigurasi yang hati-hati akan membantu anda untuk bertahan terhadap kemungkinan serangan yang terjadi. Kebanyakan dari kasus penggantian halaman muka situs (web defacement) terjadi dikarenakan kesalahan konfigurasi sehingga menyebabkan pihak ketiga dapat mengambil keuntungan dari kesalahan ini.

Conclusion

Knowing the Laws of Security (Russel, Ryan):

Client-Side Security doesn't work.

1. You cannot securely exchange encryption keys without a shared piece of information.
2. Malicious code cannot be 100 percent protected against.
3. Any malicious code can be completely morphed to bypass signature detection.
4. Any intrusion detection system (IDS) can be evaded.
5. Secret cryptographic algorithm are not secure.
6. If a key isn't required, you do not have encryption - you have encoding.
7. Password cannot be securely stored on the client unless there is another password to protect them.
8. In order for a system to begin to be considered secure, it must undergo an independent security audit.
9. Security through obscurity does not work.

The Ten Immutable Laws of Security

www.microsoft.com/technet/columns/security/10imlaws.asp

1. if a bad guy can persuade you to run his program on your computer, it's not your computer anymore.
2. if a bad guy can alter the operating system on your computer, it's not your computer anymore.
3. if a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
4. if you allow a bad guy to upload program to your website, it's not your website anymore.
5. weak password trump strong security.
6. a machine is only as secure as the administrator is trust-worthy.
7. encrypted data is only as secure as the decryption key.
8. an out-dated virus scanner is only marginally better than no virus scanner at all.
9. absolute anonymity isn't practical, in real life or on the web.
10. technology is not a panacea.

Reference:

1. Bosworth Seymor, Kebay M. E: Computer Security Handbook 4ed, John Wiley & Sons 2002
2. Check Point Software Technologies: Principles of Network Security, Check Point Software Technologies 2003
3. Kaye Doug, Loosely Coupled: Missing Pieces of Web Services, RDS Press 2003
4. Skillsoft Press: Cryptography Protocols and Algorithms, Skillsoft press 2003
5. Menga Justin, Timm Carl: CCSP: Secure Intrusion Detection and SAFE Implementation Study Guide, Sybex 2004
6. Howard Michael: Designing Secure Web-Bases Applications for Microsoft Windows 2000, Microsoft Press 2000
7. ITU-T: Compendium of Approved ITU-T Security Definitions, edition 2003 February, ITU 2003
8. Peuhkuri Markus: Lecture Material: Securing the Network and Information, 2004
9. Nguyen Hung Q., Johnson Bob, Hackett Michael: Testing Applications on the Web: Test Planning for Mobile and Internet-Based System 2nd Edition, John Wiley & Sons 2003
10. Russell Ryan et al., Stealing the Network: How to Own the Box, Syngress Publishing 2003
11. Koconis David, Murray Jim, Purvis Jos, Wassom Darrin: Securing Linux: A Survival Guide for Linux Security, SANS Institute 2003
12. Erickson Jon: Hacking: The Art of Exploitation, No Starch Press 2003
13. Mirza Ahmad David R. Et al.: Hack Proofing Your Network, 2nd Edition, Syngress Publishing 2002
14. Wang Wallace: Steal This Computer Book 3: What They Won't Tell You About the Internet, No Starch Press 2003
15. Preethan V. V.:Internet Security and Firewalls, Premier Press 2002
16. Brenton Chris, Hunt Cameron: Mastering Network Security, 2nd Edition, Sybex 2003
17. Litlejohn Shinder, Debra : Scene of The Cybercrime - Computer Forensic handbook, Syngress Publishing 2003
18. Crayton Christopher A.: The SecurityExam Guide: TestTakers Guide Series. Charles River Media 2003
19. Schmied Will et al.:MCSE/MCSA Implementing & Administering Security in a Windows 2000 Network Study Guide, Syngress Publisig 2003
20. Netcraft: Site Outages for The SCO Group, http://news.netcraft.com/archives/2004/05/27/site_outages_for_the_sco_group.html
21. Kevin Mitnick: The Art of Deception, John Wiley & Sons 2003
22. Shimonski Robert J. Et al.: The Best Damn Firewall Book Period, Syngress Publishing 2003

23. Andres Steven, Kenyon Brian: Security Sage's Guide to Hardening the Network Infrastructure, Syngress Publishing 2004
24. CSI/FBI: Computer Crime and Security Survey 2004
25. Address Mandy, Cox Phil, Tittel Ed (ed): CIW Security Professional Certification Bible, John Wiley & Sons 2001

From : echo zine

<http://histi.wordpress.com>
histismkn5@yahoo.com