



Karena ragam serangan begitu banyak, istilah keamanan komputer pun begitu variatif namanya.

Namun, jangan bingung. Artikel ini akan menuntun Anda memahami sejumlah istilah keamanan yang populer. Bukan sekadar definisi, kami pun mengulas permasalahan yang umum diakibatkan serta cara penanggulangannya.

Jadi, pastikan Anda menandai atau menyimpan artikel ini dalam *bookmark*. Kapan saja Anda menemukan problem keamanan di komputer, siapa tahu artikel ini bisa membantu.

(Brama Setyadi)

(Artikel ini pernah dimuat di dalam majalah InfoKomputer edisi Agustus 2010)□



Adware

Definisi:

Adware atau kepanjangan dari Advertising Ware, adalah jenis program komputer yang berfungsi untuk menampilkan iklan di layar monitor.

Masalah yang ditimbulkan:

Pada dasarnya Adware dibuat untuk kebutuhan pemasaran sebuah produk atau jasa. Selama digunakan dalam kondisi normal Adware sama sekali tidak bermasalah atau berbahaya, misal adware yang disematkan pada program gratisan untuk mendukung pengembangan aplikasi yang bersangkutan.

Tapi, Adware bisa menjadi masalah jika:

- Memaksa untuk memasang/menginstalasi dirinya di sebuah komputer
- Menetap dalam komputer dan tidak bisa / sulit untuk dihilangkan
- Mengambil data dari kegiatan berkomputer dan mengirimkannya ke sumber

tertentu tanpa konfirmasi dari si pemilik komputer

- Melakukan instalasi aplikasi lain yang tidak terkait dengan iklan yang ditampilkan

Semua Adware sangat mungkin untuk menjadikan sebuah komputer atau sistem menjadi lambat karena penggunaan sumber daya multimedia. Selain sistem, koneksi internet bisa berpotensi melambat karena Adware selalu mengunduh materi iklan yang baru.

Beberapa jenis Adware seperti “pop up ads” mungkin bisa mengganggu pengguna komputer karena muncul sewaktu-waktu saat komputer sedang digunakan untuk hal lain yang tidak terkait dengan adware.

Pencegahan/Penetralisir:

1. Hati hati menggunakan aplikasi/program gratisan
2. Gunakan program anti Adware seperti ad-aware buatan Lavasoft (www.lavasoft.com)



Malware Bootsector

Definisi:

Sesuai namanya, Malware Bootsector menetap bootsector harddisk untuk selanjutnya melakukan penyebaran diri dengan cara memodifikasi program yang pertama kali jalan di sebuah sistem, misal sistem operasi (OS)

Masalah yang ditimbulkan:

Jenis malware ini paling banyak digunakan untuk menyebarkan virus karena bekerja dengan cara mengubah informasi boot sector asli di harddisk. Sistem operasi yang telah terinfeksi akan menjadi zombie (sistem suruhan) untuk menyebarkan malware ke semua media simpan yang ditemukannya, termasuk CD ROM, USB Flash disk.

Selain di harddisk, malware yang satu ini juga bisa menginfeksi beragam media simpan, termasuk CD ROM, DVD ROM, floppy disk, dan USB Flash Disk.

Pencegahan/Penetralsir:

1. Gunakan program antivirus
2. Install ulang Windows



Brute Force

Definisi:

Brute Force adalah salah satu cara yang digunakan cracker untuk menebak kata kunci (*password*) tertentu.

Prosesnya dilakukan dengan cara menebak secara urutan sebuah kombinasi password mulai dari kombinasi angka 0 sampai , A sampai Z, dan seterusnya pada setiap digit kata kunci.

Masalah yang ditimbulkan:

Sebuah kata kunci yang berhasil ditebak dengan teknik Brute Force mengakibatkan akses ilegal terhadap sebuah akun. Jika yang berhasil ditebak adalah akun administrator (petinggi dalam sebuah sistem), maka bukan tidak mungkin sistem tersebut akan berpindah tangan (*take over*).

Brute Force adalah teknik menembus sistem yang paling populer dan bisa digunakan di hampir semua sistem yang menggunakan sistem otentikasi berbasis kata kunci.

Pencegahan/Penetralsir:

1. Buat kata kunci yang tidak mudah ditebak. Misal, gabungan angka, huruf dan kombinasi karakter khusus seperti “ &^%\$#@*”
2. Buat kata kunci dengan jumlah karakter tidak kurang dari 8. Makin panjang jumlah karakter yang digunakan makin sulit dan butuh waktu untuk Brute Force bisa menebak sebuah kombinasi.



Serangan Distributed Denial of Service (DDoS)

Definisi:

Distributed Denial of Service (DDoS) adalah serangan terhadap sebuah komputer atau server yang dilakukan oleh banyak komputer lain yang saling terhubung melalui internet.

Masalah yang ditimbulkan:

Karena serangan DDoS dilakukan oleh banyak komputer terhadap satu target (komputer/server) maka masalah teringan yang mungkin terjadi adalah sulitnya sebuah komputer atau server yang menjadi korban untuk diakses.

Kasus terburuk dalam serangan DDoS adalah kelumpuhan total sebuah mesin akibat kerusakan perangkat keras karena “dihujani” paket data yang sangat besar. Beberapa sistem yang sangat menarik bagi penyerang DDoS antara lain: Web server, FTP Server, Email Server, dan sebagainya.

DDoS juga sering kali melibatkan malware yang disebut dengan botnet. Ia bekerja mirip trojan yang menembuh ke sistem tertentu dan menjadikannya komputer suruhan (zombie). Itulah sebabnya pengguna komputer yang dipakai untuk menyerang komputer lain kadang tidak menyadarinya.

Pencegahan/Penetralsir:

Meskipun tidak ada cara terbaik untuk menghindari DDoS namun identifikasi mana titik terlemah dalam jaringan serta penggunaan Firewall yang mampu menghilangkan paket DDoS secara otomatis adalah 2 cara yang dapat dilakukan untuk melindungi sistem dari serangan ini.

Penggunaan perangkat siap pakai macam Cisco Self Defending Network Appliance juga bisa dijadikan pilihan lain untuk mengelak dari serangan DDoS.



Email Malware

Definisi:

Email Malware adalah jenis-jenis Malware (virus, trojan, rootkit, dan lain-lain) yang disebar dalam bentuk lampiran (attachment) email.

Masalah yang ditimbulkan:

Malware yang disebar lewat email dalam bentuk lampiran memiliki sifat perusak yang sama dengan malware yang menyebarkan dirinya lewat media lain. Malware email ini juga selalu menggandakan dirinya lewat media email yang dikirim tanpa sepengetahuan korbannya.

Beberapa malware terbaru yang dilaporkan tidak cuma membawa file berbahaya dalam rupa lampiran, tapi ada yang hanya menyisipkan alamat ke sebuah situs tertentu yang jika dibuka akan mengunduh malware lain untuk menginfeksi sistem.

Pencegahan/Penetralsir:

Serangan jenis ini bisa dengan mudah dihindari dengan penggunaan aplikasi Anti-Spam atau sejenisnya yang terdapat dalam paket aplikasi keamanan atau yang berdisi sendiri macam yang dibuat oleh Comodo (www.comodoantispam.com).

Cara murah lainnya adalah dengan tidak membuka file lampiran berformat executable (.bat, .exe, .vbs, .com) tanpa diperiksa oleh aplikasi Antivirus.



Exploit

Definisi:

Exploit adalah sejenis software atau aplikasi yang dibuat untuk menyerang kelemahan dalam sebuah sistem secara spesifik untuk mendapatkan akses atau menginfeksi.

Masalah yang ditimbulkan:

Jika sebuah Exploit berhasil menemukan sebuah titik lemah dalam sistem, maka dia bisa dengan mudah memasukkan malware lain atau melumpuhkan sebuah sistem. Exploit juga bisa dimanfaatkan cracker untuk menyusup ke dalam sistem sebelum disadari oleh vendor aplikasi yang terkena dampaknya, hal ini biasa dikenal dengan sebuta Zero-Day Exploit.

Pencegahan/Penetralsir:

1. Menggunakan aplikasi antivirus dengan update terbaru
2. Memastikan sebuah sistem mendapatkan patch atau update terbaru.
3. Menggunakan teknologi proteksi Buffer Overflow
4. Menggunakan program personal firewall



Fake Antivirus (Antivirus Palsu)

Definisi:

Fake Antivirus merupakan program antivirus palsu yang beroperasi dengan cara menakut-nakuti pengguna komputer dan memberikan informasi palsu bahwa sebuah komputer telah terinfeksi virus. Kemudian antivirus gadungan ini

menyarankan untuk membeli lisensinya sekaligus memberikan jasa palsu pembersihan virus. Program seperti ini dikenal juga dengan sebutan Scareware

Masalah yang ditimbulkan:

Meskipun masuk dalam kategori malware sekaligus Adware, program Antivirus ini tidak terlalu berbahaya bagi sistem. Tugasnya hanyalah menipu pengguna komputer agar membeli sesuatu yang sebenarnya tidak dibutuhkan.

Proses penyebaran antivirus palsu ini juga tidak semasih malware lain yang memanfaatkan kelemahan sistem. Sebab senjata andalan Antivirus palsu adalah dengan melakukan penipuan dengan cara mengubah hasil (misalkan) mesin pencari di internet sehingga seakan-akan antivirus ini terlihat seperti penyedia layanan keamanan asli.

Pencegahan/Penetralsir:

1. Pastikan Anda memilih antivirus dengan merek terkenal dan dibuat oleh perusahaan yang kredibel, misal: Symantec, Sophos, McAfee, TrendMicro, F-Secure, dan lain sebagainya.
2. Gunakan program antivirus seperti pada point 1 dengan kondisi update terbaru.



Hoax □

Definisi:

Hoax adalah berita bohong/palsu tentang sebuah tren yang beredar atau diedarkan di internet, baik melalui email, website, blog, atau sejenisnya sehingga menimbulkan kekuatiran tertentu.

Masalah yang ditimbulkan:

Masalah paling serius yang ditimbulkan dari sebuah Hoax yang beredar adalah kepanikan dan penipuan. Pada tingkat tertentu Hoax juga bisa digunakan untuk kampanye hitam atas sebuah produk atau pribadi. Karena bersifat berantai, Hoax bukan tidak mungkin mampu membebani jaringan internet dan server email sehingga terjadi kelambanan akses atau tidak berfungsinya penyedia layanan email.

Pencegahan/Penetralsir:

Hoax tidak dapat dicegah oleh program antivirus atau antimalware manapun, sebab ia menyerang psikologis pengguna komputer dan bukan komputer itu sendiri. Oleh karena itu, perilaku bijak dalam meneruskan sebuah berita ke teman atau kerabat diperlukan untuk menghindari penyebaran Hoax. Cara efektif lain adalah dengan mencari sumber kedua (second opinion) terhadap berita yang diterima melalui internet.



Keylogger

Definisi:

Keylogger merupakan kegiatan merekam semua input yang dimasukkan oleh keyboard yang kemudian disimpan untuk dianalisa.

Masalah yang ditimbulkan:

Karena sifatnya yang bisa merekam semua informasi yang datang dari keyboard, maka Keylogger yang berupa aplikasi sering kali digunakan untuk mencuri informasi sensitif macam username, password, nomor kartu kredit, nomor PIN, dan lain-lain.

Informasi yang berhasil didapat ini akan sangat berbahaya jika kemudian dikirim ke pihak yang tidak bertanggung jawab secara otomatis dengan bantuan virus atau trojan tanpa diketahui korbannya.

Pencegahan/Penetralsir:

Beberapa jenis aplikasi Keylogger sangat sulit untuk dideteksi. Oleh karena itu ada baiknya jika menggunakan fasilitas keyboard di layar (OnScreen Keyboard) milik Windows saat menggunakan komputer umum (misal di warung internet). Aplikasi seperti ini juga bisa diunduh dengan cuma-cuma di www.march-of-faces.org/resources/vkt.html



Malware Ponsel

Definisi:

Malware ponsel dibuat khusus untuk menyerang ponsel dengan sistem operasi tertentu, termasuk jenis ponsel pintar seperti Personal Digital Assistant (PDA), Blackberry, dan sejenisnya.

Masalah yang ditimbulkan:

Selain bisa merusak sistem operasi ponsel, malware jenis ini juga memiliki penyebaran yang unik dan umumnya menggunakan konektivitas yang dimiliki ponsel tersebut. Salah satu yang paling populer adalah Bluetooth.

Karena ia bisa mengaktifkan Bluetooth dengan otomatis dan tanpa terdeteksi, maka ponsel yang tertular malware ini akan lebih cepat kehabisan baterai dibanding ponsel yang berjalan dalam kondisi normal. Koneksi Bluetooth yang senantiasa aktif ini bukan tidak mungkin bisa merusak perangkat pemancar radio Bluetooth atau merusak komponen lain karena kepanasan (overheat).

Pencegahan/Penetralisir:

Beberapa malware ponsel seperti Cabir-A atau Skull bisa dideteksi dengan mudah oleh antivirus ponsel seperti yang dimiliki F-Secure atau Norton (symantec). Namun, varian terbaru seperti file PDF yang berpotensi menyerang lubang pada Blackberry belum diantisipasi oleh produsen Antivirus. Hal termudah adalah dengan tidak memasang sembarang aplikasi pada ponsel-ponsel yang rentan (punya sistem operasi pasaran seperti Symbian).



Phishing

Definisi:

Phishing adalah sebuah bentuk penipuan elektronik.

Umumnya phishing dilakukan agar seseorang/korban mau membagi informasi sensitif kepada pihak tertentu dengan memanfaatkan kredibilitas dari perusahaan besar/ternama (misal: bank, asuransi, kartu kredit, penyedia layanan internet, dan lain-lain). Phishing terbanyak disebarkan lewat email dan situs web.

Masalah yang ditimbulkan:

Seorang korban phishing tidak akan menyadari bahwa dirinya adalah korban penipuan. Sehingga bukan tidak mungkin data-data sensitif yang didapat dari korban disalah gunakan untuk menipu pihak lain, atau mengambil keuntungan

dari korban. Kalau sudah begini, harta bisa jadi taruhan utama korban yang terkena phishing.

Target utama yang disasar oleh Phishers (orang yang melakukan phishing) adalah orang yang memiliki akun di bank atau kartu kredit. Phishing juga tidak jarang dikirimkan dalam rupa kejutan berhadiah dimana korban harus menyetorkan uang dalam jumlah tertentu.

Pencegahan/penetralsir:

1. Jangan pernah mengirimkan data pribadi seperti nomor kartu kredit, PIN ATM atau apapun melalui email sekalipun diminta oleh bank, perusahaan kartu kredit atau apapun dimana Anda terdaftar didalamnya. Karena perusahaan tadi tidak pernah dan tidak akan pernah meminta data pribadi melalui email.
 2. Jangan mudah percaya jika Anda diminta membayar sesuatu atas hadiah yang telah Anda menangkan tanpa melakukan pemeriksaan kepada pihak yang terkait.
-



Rootkit

Definisi:

Rootkit adalah sebuah program yang bisa menyembunyikan program lain atau proses yang berjalan pada sebuah komputer. Rootkit ini sering kali

digunakan untuk menyembunyikan aktivitas malware atau mencuri data.

Masalah yang ditimbulkan:

Rootkit yang digunakan untuk menyembunyikan aplikasi keylogger berpotensi menyulitkan deteksi terhadap pencurian data sensitif yang dimasukkan lewat keyboard. Karena sifatnya yang bisa menyembunyikan proses, Rootkit seringkali digunakan untuk menyembunyikan malware yang sudah tertanam dalam sistem untuk kepentingan menyerang sistem lain (DDoS) tanpa sepengetahuan pengguna komputer.

Pencegahan/Penetralsir:

1. Gunakan aplikasi antivirus atau antimalware yang memiliki fitur antirootkit didalamnya.
2. Beberapa rootkit memerlukan aplikasi tersendiri (seperti Sophos Antirootkit - <http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html>) agar bisa dihapus sempurna.



Social Engineering

Definisi:

Social Engineering adalah trik yang dilakukan oleh seorang hacker/cracker

untuk membodohi korbannya agar mau melakukan sesuatu.

Biasanya hal-hal yang dilakukan terkait social engineering adalah menghasut agar seorang korban mau mengunjungi situs web tertentu atau menjalankan file berbahaya yang diselipkan dalam lampiran email.

Masalah yang ditimbulkan:

Banyak akibat merugikan yang disebabkan oleh social engineering karena seorang korban tidak menyadari bahwa dirinya sudah tertipu. Kasus terbanyak dari teknik ini adalah kehilangan password, akun, atau berpindahnya data-data rahasia ke pihak tertentu.

Masalah lain yang ditimbulkan adalah menyebarnya virus atau malware komputer karena seorang korban menganggap sebuah berita hasil social engineering adalah benar sekaligus ikut menyebarkannya.

Pencegahan/Penetralsir:

Karena tidak terlalu melibatkan hal teknis di bidang teknologi komputer, satu-satunya cara menghindari social engineering adalah mewaspadaai semua hasutan, berita, atau informasi dari berbagai pihak. Termasuk teman atau kerabat yang sudah dikenal sekalipun. Cek ulang ke sumber lain bisa jadi langkah efektif untuk menghindari social engineering.



Spam

Definisi:

Spam adalah email yang tidak diinginkan yang masuk ke dalam kotak email seseorang dan dikirim secara massal. Email seperti ini umumnya berisi iklan komersil yang mengajak seseorang untuk membeli atau melihat produk atau jasa.

Masalah yang ditimbulkan:

Banyak laporan yang menyebutkan bahwa masalah utama dari Spam adalah hilangnya waktu dengan sia-sia. Ada benarnya memang, karena email spam kebanyakan tidak diinginkan oleh penerimanya dan butuh waktu untuk menghapus pesan-pesan tersebut. Ini akan jadi masalah tambahan jika jumlah spam sudah mencapai ratusan dalam sehari.

Spam juga tidak jarang ikut andil dalam penyebaran malware, karena ini cara paling mudah dan murah untuk mempublikasikan social engineering, malware, dan phishing sekaligus.

Pencegahan/Penetralsir:

Saat ini produsen aplikasi keamanan sudah menyediakan program Anti-Spam yang handal. Beberapa diantaranya dipaket dalam aplikasi antivirus. Situs <http://www.freeantispam.org/> bahkan menyediakan program seperti ini dalam

lisensi gratis.



Spyware

Definisi:

Spyware adalah perangkat lunak yang memungkinkan pengiklan atau hacker memperoleh informasi sensitif tanpa diketahui oleh korbannya.

Masalah yang ditimbulkan:

Karena sifatnya yang tidak mudah diketahui, spyware seringkali digunakan untuk mencuri data berharga dari pengguna komputer. Kalau sudah begini, jangan heran jika tiba-tiba password, nomor pin atm, nomor kartu kredit dan lain sebagainya tiba-tiba berpindah tangan.

Pencegahan/Penetralsir:

Sebuah sistem bisa tertular spyware hanya dengan mengunjungi situs web tertentu (yang berbahaya). Beberapa situs yang mengandung spyware akan meminta instalasi aplikasi melalui jendela pop up. Tapi ada juga yang langsung memasang dirinya tanpa permisi.

Untuk menghindari hal ini pastikan browser yang digunakan untuk berselancar di internet sudah memiliki sistem pelaporan terhadap situs berbahaya. Browser seperti Internet Explorer 8, Firefox (dengan plugin NoScript), Google Chrome, dan Opera sudah menyediakan fasilitas ini.



Trojan

Definisi:

Trojan adalah sebuah program yang seakan-seakan bekerja seperti program baik-baik.

Padahal ia menyembunyikan fungsi rahasia yang membahayakan sistem. Trojan juga kadang dijadikan sebutan pengganti untuk malware lain seperti bot, backdoor trojan dan downloader trojan.

Masalah yang ditimbulkan:

Trojan sering kali terlihat seperti program biasa yang bisa digunakan untuk produktivitas. Ia juga sering mengklaim dirinya hanya memiliki fungsi tunggal untuk keperluan tertentu. Namun, tanpa sepengetahuan korban, ia menjalankan fungsi lain seperti pencurian data atau mencari kelemahan sistem. Informasi ini kemudian dikirim ke hacker tanpa sepengetahuan korban.

Trojan banyak disebar di aplikasi bajakan, termasuk keygenerator (untuk membuat nomor lisensi palsu) dan sejenisnya. Jumlah trojan saat ini juga tumbuh pesat dibanding virus karena kemampuannya menyebar dengan mandiri.

Pencegahan/Penetralisir:

Trojan bisa dikenali dengan mudah oleh aplikasi antivirus atau antimalware dengan update terbaru. Disarankan untuk selalu memeriksa aplikasi hasil download dari internet menggunakan program / aplikasi antivirus.