DASAR-DASAR HACKER (BAG. 2)

www.kursusgratis.bizland.com
yerianto@yahoo.com

Mencari sistem komputer yang akan dimasuki

Pada tahapan ini yang perlu menjadi forkus utama adalah:

- Tetapkan alasan mengapa Anda harus melakukan penjebolan terhadap sebuah server
- Cari sistem yang akan dijadikan target
- Kenali sistem yang akan Anda masuki

Tetapkan alasan mengapa anda harus menjebol sebuah server

Sebelum anda melakukan sesuatu anda harus menetapkan tujuannya. Demikian halnya ketika seorang hacker akan menjebol sebuah server, mereka harus menetapkan tujuan dan targetnya secara jelas. Tujuan yang jelas akan sangat memotivasi anda sebagai hacker sejati.

Banyak alasan mengapa hacker harus menjebol server atau situs tertentu, baik yang sifatnya individualistis atau kelompok bahkan negara. Antara lain:

1. Membantu administrator pengelola situs yang akan dijebol agar tidak dijebol oleh hacker jahat yang bermaksud mencuri data
2. Mengungkapkan pendapat kelompoknya.
3. Melakukan tindakan kriminal
4. Menjadikannya sebagai profesi
5. Iseng-iseng saja

Masih banyak alasan yang dapat Anda gunakan sebagai alasan. Apapun alasannya, anda harus pahami bahwa semua tindakan anda akan menimbulkan resiko. Dan itu semua harus anda pertanggungjawabkan sendiri akibatnya, baik akibat positif maupun negatif.

Perhatikan kutipan berita mengenai tingkah laku hacker yang dapat dikategorikan sebagai membantu pengelola situs yang akan dijebol agar tidak dijebol oleh hacker jahat yang bermaksud negatif. Langkah seperti dilakukan oleh hacker Stolen seperti diberitakan oleh www.detik.com sebagai berikut:

Wawancara dengan Penjarah Domain
Stolen:Pemilik Domain Juga Salah
Reporter: Donny B.U.

detikcom - Jakarta, Masih ingat Stolen yang menggunakan e-mail stolen8910@yahoo.com? Para pemilik domain yang sempat dijarah domainnya oleh Stolen pasti sangat penasaran, siapa dan apa tujuan dia melakukan hal yang notabene.
Yang jelas, Stolen yang mengaku bukan warga negara Indonesia ini tidak ingin disebutkan siapa jati diri yang sesungguhnya. Berikut ini intisari dari bincang-bincang **detikcom** dengan Stolen, Selasa (7/3/2000). Beberapa bagian telah mengalami pengeditan tanpa mengurangi arti dan makna.

detikcom : Stolen, sebelumnya bisakah menceritakan sedikit tentang siapa anda?
Stolen : Saya pria, seorang konsultan spesialis pembuatan e-commerce dan teknologi Internet. Usia saya berkisar antara 20 - 30 tahun. Saya tidak tinggal di Indonesia.

Apakah anda memiliki alasan tertentu ketika membajak beberapa domain name?
Well, saya tidak memiliki kepentingan tertentu dalam hal ini. Saya hanya ingin menunjukkan beberapa hole di dalam prosedur NetSol, terutama pendaftaran domain. Saya menemukan beberapa admin domain tidak memiliki cukup pengetahuan untuk melindungi domain-domain mereka.
Tahukah anda bahwa pemilik Integrasi.com tidak pernah menghubungi saya atau bahkan juga tidak mencoba mengambil kembali domain mereka hingga melewati 1 minggu (sejak dijarah)? Inikah jenis reaksi yang anda inginkan dari seorang administrator domain?

Apakah domain yang telah anda bajak hanya dimiliki oleh orang Indonesia saja?
Tidak juga. Ada juga domain dari negara-negara lain di penjuru dunia. Tetapi kebanyakan memang berbasis di Indonesia. Saya ingin menegaskan satu hal, saya tidak peduli lokasi pemilik sebuah domain ketika saya mengambil (domain tersebut). Setelah saya mengambilnya, baru saya mengerti (dimana basisnya).

Berapa domain yang telah berhasil anda bajak?
Di Indonesia total 15 buah. Rata-rata saya hanya memiliki 5 domain dalam satu saat. Sekarang ini, seluruh domain telah diambil kembali oleh pemiliknya. Kemungkinan administrator (domain tersebut) dapat mempelajari sesuatu dari kejadian (penjarahan) tersebut.

Apa saja domain Indonesia tersebut?
agisstore.com, bursamobil.com, citadel-hobby.com, i-mall2000.com, indoexchange.com, indosat.com, integrasi.com, internetinstan.com, parklanejakarta.com, plasa.com, pyridam.com, swanet.com, baliwww.com, eastjava.com, dan binus-tph.com

Menurut anda, mudahnya sebuah domain name dibajak disebabkan karena apa?
Sudah jelas, karena kelemahan dari prosedur pendaftaran domain di NetSol. Bukan dari InterNIC. Tetapi, saya juga menyalahkan pemilik (domain). Jika seseorang mengambil domain milik saya, saya akan mencota mengambil kembali sesegera mungkin.
Dan taukah anda? Dari seluruh 15 domain tersebut, tidak satupun pemiliknya mencoba segera mengambil kembali domain tersebut. Response tercepat yang saya dapatkan adalah setelah 2 hari. Bayangkan, 2 hari sesudah pembajakan!

Omong-omong, apa yang akan anda lakukan dengan domain yang telah berhasil anda bajak tersebut?
Saya membiarkan pemiliknya mengambil kembali. Seperti yang telah saya katakan sebelumnya, saya tidak memiliki kepentingan tersembunyi apapun. Jika mereka dapat mengambil kembali, silakan saja.
Jika mereka mampu. By the way, salah satu pemilik domain, kalau tidak salah plasa.com yang pemiliknya menggunakan e-mail dns@commerce.net.id, sebenarnya "meminta dengan amat sangat" kepada saya untuk mengembalikan domain mereka.

Terimakasih atas kesempatan melakukan bincang-bincang kali ini
Terimakasih kembali.

Aksi hacker Stolen masih berlanjut, tetapi tetap dengan nuansa membantu mengingatkan para pengelola sistem komputer agar memelihara dan menjaga situsnya dengan lebih baik lagi. Berikut ini berita mengenai aksi hacker Stolen dengan melakukan checkup server-server dari situs Indonesia seperti diberitakan oleh www.detik.com sebagai berikut:

Hacker Stolen: 61 Situs Indonesia Sudah Saya Check-up
Reporter: Donny B.U.

detikcom - Jakarta, Masih ingat hacker Stolen dalam beberapa kasus pembobolan situs Indonesia menggunakan *MS00-078 security hole*? Setelah beberapa kasus tersebut, Stolen lalu lebih memfokuskan 'security check terhadap situs-situs Indonesia. Berikut adalah hasilnya yang disampaikan kepada detikcom, Senin (27/11/2000).

"Beberapa bulan yang lalu, saya menemukan banyak sekali situs dengan domain .ID yang rapuh terhadap MS00-078 security hole. Saya menemukan sekitar 61 situs yang belum memasang patchnya," ujar Stolen. Kemudian Stolen mengupload file temporary.html ke webserver situs-situs tersebut, tepatnya ke root directory C:\ atau D:\. "Saya cukup senang karena dari beberapa situs tersebut telah mensetting permissionnya dengan bagus, sehingga saya tidak dapat mengupload file ke webservernya meskipun tetap memiliki hole. Server tersebut adalah asiavictory.co.id, aetna.co.id, deacons.co.id, mjk-ajinomoto.co.id, pramindo.co.id, dan tms.co.id.

"Seminggu kemudian, saya kembali memeriksa ke-61 situs-situs tersebut dan mendapatkan sebagian dari mereka telah memasang patchnya. Situs tersebut adalah warnet.web.id, metra.net.id, indofood.co.id, marklin.co.id, pelangi-cimandiri.co.id, dan philips.co.id. Tetapi berhubung mereka memasang patch sesudah saya mengupload file temporary.html sebelumnya, mereka tetap akan menemukan file tersebut di root directory mereka," papar Stolen.

Berhubung sedang banyak kerjaan, Stolen terpaksa menghentikan sementara kegiatan security check tersebut untuk sementara waktu. Dalam masa reses tersebut, Stolen mendapat pemberitahuan dari situs hacker attrition.org yang mengabarkan bahwa beberapa situs Indonesia telah dihacked.

"Saya membandingkan situs-situs yang dihacked tersebut dengan daftar 61 situs yang saya punya, dan ada sebagian yang memang masuk dalam daftar tersebut. Situs-situs tersebut tampaknya dihacked oleh AntiHackerlink," ujar Stolen

"Nah, baru-baru ini saya bisa melanjutkan memeriksa situs-situs Indonesia kembali. Saya mendapatkan sebagian besar dari mereka kini telah memasang patch di webserver mereka. Situs-situs tersebut adalah transone.net.id, mdp.ac.id, tarumanagara.ac.id, ums.ac.id, bapepam.go.id, deptranspph.go.id, jakarta.go.id, pustekkom.go.id, transkep.go.id, argo.co.id, car.co.id, codistrib.co.id, daein.co.id, dbms.co.id, indoexpress.co.id, intellisys.co.id, iverson.co.id, kit.co.id, korindo.co.id, kpw.co.id, latinusa.co.id, limma.co.id, lyman.co.id, mcdonalds.co.id, mmi-pt.co.id, mobisel.co.id, nhm.co.id, pdc.co.id, plnjaya.co.id, primus.co.id, ptwbi.co.id, quadras.co.id, sampet.co.id, scomptec.co.id, sei.co.id, spij.co.id, sucofindo.co.id, summit.co.id, teijin.co.id, trisula.co.id, unipro.co.id, usg.co.id dan yongma.co.id. Tetapi sama seperti pada kategori kedua, situs-situs tersebut juga telah terdapat file temporary.html di root directory yang pernah saya upload sebelumnya," ujar Stolen.

"Tinggal enam situs lagi yang belum mempatched webserver mereka. Situs tersebut adalah idln.or.id, postel.go.id, asmaraindo.co.id, inaport1.co.id, perhutani.co.id, dan pln.co.id. Dengan menggunakan MS00-078 security hole, siapa pun dapat melihat isi dari webserver mereka," ujar Stolen.
Dari keenam situs terakhir tersebut, empat diantaranya mensetting permissionnya dengan bagus sehingga Stolen tidak dapat mengoverwrite halaman depan situs tersebut. "Tetapi dua diantaranya, yaitu asmaraindo.co.id dan pln.co.id sangat-sangat buruk, karena saya dapat saja mengganti default page mereka," tandas Stolen.

"Itulah keseluruhan informasi yang bisa saya sampaikan hingga hari ini," ujar Stolen. "Saya akan tetap memonitor situs-situs Indonesia. Setelah saya selesai memeriksa semua situs yang berdomain .ID, saya akan mencoba beralih ke situs-situs berdomain .COM/NET/ORG," ujar Stolen mengakhiri kisahnya.

Ada juga hacker yang melakukan tindakan negatif dengan maksud mencari perhatian. Berikut ini kelompok hacker yang bermaksud mengungkapkan pendapat kelompoknya seperti pada kelompok pendukung kasus hacker wenas berikut ini:

Tuntut Wenas Dibebaskan
Antihackerlink Bobol Situs S'pore
Reporter: Sigit Widodo

detikcom - Jakarta, Apa jadinya bila hacker Indonesia ditangkap dan diadili di Singapura? Kelompok Antihackerlink Selasa (15/8/2000) menyikapinya dengan melakukan cyber war dan membobol situs-situs Singapura.

Situs Singapura yang pertama kali terkena getahnya adalah situs *www.geiser.com.sg*.
Kelompok Antihackerlink mengubah tampilan halaman index situs tersebut dengan sebuah halaman penuh animasi berlatar belakang warna hitam.
Kata-kata "Happy Birthday Singapore", "Do not mess with Indonesian Hackers", "Free Wenas" dan "Or We Will F*!k Singapore Server" silih berganti tampil di halaman index. Di bagian atas halaman tersebut tercantum nama Antihackerlink dan di bagian bawah terdapat pesan sebagai berikut:

This is not a GAME, this is REAL what you see now is our ultimatum for unsecured computer system, nothing destroyed... we just came with peace and leave this page as our sign.
What we want is just let our brother _wenas aka hC-_ free, because he did all things for knowledge.

"Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for." - The Conscience of a Hacker - The Mentor.
Freedom of knowledge. Freedom of speech. Freedom to Decide.
Greets to:
all ppl at #antihackerlink - irc.dal.net

Pembobolan situs Singapura ini dilakukan untuk menuntut pembebasan Wenas alias HC- (15 tahun), salah seorang hacker dedengkot kelompok Antihackerlink, yang saat ini tengah menjadi terdakwa di pengadilan Singapura.
Wenas ditangkap setelah membobol situs Data Storage Institute (DSI) di Singapura dan dikenakan 16 tuntutan. Keputusan pengadilan ini akan digelar di Singapura pada 22 Agustus 2000 mendatang. Saat ini Wenas dikenakan tahanan negeri (tahanan kota - Red) dan tidak boleh keluar dari Singapura.

Yang lebih membahayakan adalah mereka yang memiliki maksud-maksud kriminal seperti pencurian data kartu kredit, pencurian informasi perusahaan dan lain sebagainya. Coba perhatikan berita di bawah ini.

2000 Data dan Kartu Kredit Digasak
Situs E-commerce Dibobol Hacker
Reporter: Donny B.U.

detikcom - Jakarta, Hacker komputer menyerang kembali, memaksa sebuah situs e-commerce NewYork untuk memberitahu kepada pelanggannya bahwa nomor kartu kredit mereka telah dicuri dan dipasang di suatu situs di Internet.
Situs yang apes tersebut ialah www.SalesGate.com, merupakan contoh terakhir bagaimana sebuah situs bisnis online ditampar oleh pembobolan sistem sekuriti. Serangan tersebut meningkatkan kepedulian antar pelanggan, eksekutif industri dan otoritas penegak hukum.

Sekitar 2000 data telah digasak dari database SalesGate, termasuk nomor kartu kredit dan informasi pribadi lainnya. Sialnya lagi, data-data kartu kredit tersebut lagi-lagi dipajang di sebuah situs di Internet.
Menurut situs CNET News, hingga Jumat (3/2/2000) pihak SalesGate telah melakukan koordinasi secara intensif dengan Secret Service di Amerika untuk menangkap hacker yang bertanggung jawab atas pembobolan sistem sekuriti mereka.

SalesGate adalah sebuah situs jual-beli dimana bisnis kecil datang untuk menawarkan produk dan jasa mereka pada lokasi yang terpusat. SalesGate menjamin sekuriti dari transaksi tersebut dan telah memasang pesan di situs mereka yang menjanjikan akan mengembalikan semua dana yang terpotong dari kartu kredit yang digasak tersebut.

Sebelumnya pada pertengahan Januari 2000 seorang hacker bernama Maxus telah membobol toko CD online, CD Universe, dan membawa lari sekitar 350 ribu nomor kartu kredit. Maxus lalu memasang beberapa ribu nomor tersebut di Internet dan meminta tebusan sebesar US $ 100 ribu dari perusahaan tersebut.
Pihak CD Universe tidak bersedia mengikuti permintaan Maxus dan segera menghubungi pihak FBI untuk melakukan pelacakan. Hingga kini Maxus tersebut belum terungkap jati diri yang sebenarnya.

Kembali ke SalesGate, pihak perusahaan telah memberitahu pelanggan mereka bahwa sistem sekuriti mereka kebobolan dan telah membatalkan semua kartu kredit mereka langsung dengan perusahaan yang mengeluarkan kartu kredit tersebut.

```
Bukan itu saja, pelanggan juga diwanti-wanti untuk mewaspadai apabila ada
tagihan pembelian yang tidak dikenal yang mengacu kepada "SalesGate" atau
"Internet Management Service".
Sistem sekuriti yang lemah atau hacker yang jago?
```

Selanjutnya yang termasuk kategori iseng-iseng adalah mereka yang baru belajar menjadi hacker. Biasanya yang baru saja mendapatkan trik-trik menjebol situs alias hacker script kiddies. Hacker model seperti ini sangat banyak terjadi di Indonesia. Mereka tidak punya agenda apa-apa dan hanya sekedar mengetes dan mencoba trik. Biasanya mereka hanya mencoret-coret situs milik orang lain dengan tidak meninggalkan pesan berarti bagi pemiliknya.

Nah, jika Anda seorang pengelola sistem komputer alias administrator, coba pikirkan dan pahami, apakah situs anda memiliki potensi diserbu oleh hacker. Jika ya, apa kira-kira motifnya. Dari sana anda bisa menyusun strategi pembendungan terhadap serbuan hacker. Jika perlu anda menyiapkan perangkat yang dapat menjebak para hacker tersebut.

Misalnya saja anda pengelola situs bisnis, apakah ada untungnya seorang hacker menjebol situs anda ? Bagaimana jika perusahaan saingan anda berniat mempermalukan perusahaan anda ? Atau anda secara tidak sengaja mengundang para hacker iseng untuk "menguliti" anda habis-habis ?

Sekali lagi yang paling mudah bagi pengelola sistem komputer dan jaringan adalah pahami alasan para hacker dan susun strategi perlindungan atau sering disebut setup policy atau kebijakan perusahaan anda.

Untuk soal keamanan, biaya menjadi sangat tidak tak terbatas. Jika perusahaan Anda bergerak di bidang finansial berbasis internet, maka setiap kebobolan situs anda akan sangat berdampak terhadap kepercayaan perusahaan anda. Jika demikian, maka masalah keamanan tidak bisa ditawar-tawar lagi. Namun jika situs anda di internet hanya sekedar informasi product dan tidak memanfaatkan e-commerce, mungkin keamanannya tidak perlu menggunakan kecanggihan tingkat tinggi, mungkin tidak perlu firewall melainkan cukup menggunakan router yang setupnya terpasang dengan baik dan benar.

Bersambung ke Bagian 3