Temubual dengan seorang hacker tanah air

Temubual saya dengan seorang hacker di tanah air. Namanya dirahsiakan. semoga menjadi panduan kita bersama.

Sejak bila mula hacking ni?

Saya mula hacking sejak tahun 1998/1999.

Berapa sites yang dah cuba hack?

Kalau ditanya berapa site dah cuba.. mungkin banyak.. tak ingat..

Berapa banyak yang dah berjaya kena hack, di tanah air dan di luar negara?

Bilangan server yang berjaya dihack mungkin banyak, tapi saya tak ingat... angka kasar 2000 atau lebih (tanah air dan luar negara).

Apakah server yang paling besar pernah dimasuki?

Server malaysia rahsia.. tapi adalah server yang besar.. apa yang memuaskan saya dapat memasuki satu server ns *.edu utk sebuah negara (negara tuh rahsia).. jadi macam top level domain juga... kalau kita malaysia *.edu.my.. dan beberapa server utk hosting yang mempunyai beribu domain di dalamnya ...

Platform OS mana yang mudah di hack? dan yang terpayah?

Platform OS yang mudah dihack ialah Windows NT/Windows 2000... Tetapi tengok kepada operating system itu sendiri.. tak kira apa OS... kalau default installation memang terdedah.. bergantung kepada sys admin itu sendiri .....yang terpayah kalau OS tuh dah dipatch... setakat ini Linux Slackware, Linux Debian dan Openbsd adalah antara yang susah.

Bila dah hack masuk, apa yang dibuat seterusnya?

1. Covering Trace.

Selepas mendapat root/admin privilage biasanya perkara yang utama ialah memastikan Admin tidak mengetahui yang server mereka telah dihack.. ini perlu dilakukan dengan rapi.. kerana kemungkinan root/admin mungkin ada menggunakan software tambahan cth seperti tripwire. Jadi saya harus fikirkan apa

yang mungkin root akan buat.. dan memastikan system itu adalah seperti biasa.. biasanya akan clearkan semua last dan log file.

2. Patching.

Patching adalah satu perkara yang penting.. kerana utk memastikan hackers lain tak boleh nak take over server tersebut... ini juga utk kebaikan root/admin server.. secara tak langsung server tu selamat.

3. Trojan

Trojan adalah penting untuk tujuan menyorok file... cth:... bila admin check file yang saya buat tidak dapat dikesan... begitu juga utk menyorok background proccess... dan banyak lagi.... bab trojan memang menarik...

4. Backdoor.

Backdoor adalah bertujuan utk memastikan saya boleh masuk server tersebut jika terdapat apa jua perubahan yang berlaku.. jangan terkejut... melalui backdoor biasanya orang tak nampak bila saya masuk... pintu belakang memanglah penting... keep the secret k.

5. Keep The Account.

Tugas saya adalah untuk memastikan access saya dekat server tersebut berkekalan... ada server yang hampir 3 thn masih boleh lagi diakses... tak hairanlah saya suka Solaris kerana system tersebut adalah popular (pada sekitar 90-an)... dan biasanya penggunaannya adalah lama berbanding dengan linux yang sentiasa di upgrade..

6. Protect The Server.

Yup selepas tuh saya kena protect server yang dihack utk memastikan server tu tahan lama.. sebagai root/admin kedua.. kadang2 saya akan memeriksa system file dan user... kadang2 ada user yang running backgroud proccess cth seperti bot dan bnc.. terpaksa saya kill.. kadang2 saya suspend account mereka...

Dengan meninggalkan backdoor untuk memantau capaian orang lain atau aktiviti server tersebut, apakah itu suatu cara yang beretika?

Kalau dilihat dari beberapa sudut memang perkara meninggalkan backdoor untuk

memantau akses orang lain atau aktiviti server adalah tidak beretika dan saya bersetuju. Tetapi dari sudut untuk memastikan server yang dihack berada dalam keadaan baik perkara seperti meninggalkan backdoor utk memantau akses orang lain atau aktiviti server perlu dilakukan.. contohnya, jika satu akaun user diceroboh oleh orang lain.. saya dapat mengetahui dan cuba utk memastikan penceroboh itu tidak memperolehi akses root/admin agar server tersebut terus selamat. Beretika atau tidak ini mungkin persoalan yang akan terus timbul.. tetapi yang penting.. kami mahu memastikan keadaan server berada dalam keadaan baik dan stabil..

Adakah hacking itu beretika?

Hacking boleh dibahagikan kepada beberapa kategori... ada yang menjadikan hacking sebagai tempat melepas geram atau medan utk menjadi terkenal dikalangan kawan2 kerana dapat memecah masuk sesatu server.. cthnya dengan website defacement... mungkin ini kurang beretika...

Tetapi ada juga yang memasuki server secara baik dengan menolong utk patched.. dan kadang2 email kepada admin utk... memaklumkan kehadiran mereka atau kelemahan server tersebut... tetapi malang ada administrator tidak menghiraukan email dari kami.. sehinggakan perkara yang di atas terjadi baru nak kecoh... ini di atas penerimaan masing2... jadi kita harus melihat dari beberapa aspek... biasanya saya akan menolong utk perkara yang baik..

Aplikasi/platform mana yang selalu digunakan untuk hacking? dapat dari mana?

Saya dan group ada buat research pasal exploit dan backdoor sekali dengan patches.. so utk memudahkan lagi.... kita orang ada compress semua sekali dengan script utk auto install... jadi senang... dapat root lepas tuh just run... semua script akan buat... tapi utk masa sekarang hanya utk solaris... kalau nak jual mungkin mahal... so biarlah ia menjadi rahsia..

Pasal aplikasi... biasanya kita perolehi dari laman web underground yang private.. dan ada juga diperolehi dari rakan2 dekat dalam net.. jadi ada exploit yang unreleased.. ada juga dekat securityfocus...

Platform yang digunakan utk hacking biasanya dari unix(solaris) dan attack ke server sasaran.. ini dipanggil remote exploit.. tanpa menggunakan login dan passwd (Ada juga machine di belakang firewall lepas).. jika cara biasa kita akan guna method asas iaitu finger dan try login/passwd... dan baru menggunakan local exploit...ini adalah method utk hack os... utk perkara lain boleh dibincangkan lagi...

Apa pendapat sdri tentang hacking?

Hmmm... pada pendapat saya dari kaca mata security/istilah sebenar... hacking adalah baik.. kerana dari maksud sebenar hacking ialah mereka yang tahu mengenai tcp/ip dan pandai menyelesaikan masalah yang berkaitan dengan komputer termasuklah isu security, Bahasa C dan Programming.. kerana system administrator yang sebenar adalah hackers... Ada system administrator yang mengaku mempunyai pengalaman bertahun-tahun tetapi masih lagi sama menyalahkan orang lain apabila server mereka dihack...

Dari perspektif lain pula ada yang menganggap hackers adalah penjenayah... dan ramai yang menyalahkan mereka.. tetapi kita harus melihat perkara ini secara lebih matang.. kerana dengan adanya hackers.. kita boleh menguji tahap keselamatan server kita... ini adalah untuk kebaikan..

Apa pendapat sdri tentang tahap keselamatan server di tanah air kita?

Pada asasnya tahap keselamat server di Malaysia pada masa ini adalah cukup baik.. dan memuaskan.. cuma pada sekitar tahun 1999 dan 2000 tahap keselamatan server kerajaan (*.gov.my) dan pendidikan (*.edu.my) adalah sedikit lemah... tetapi dengan adanya usaha yang dijalankan oleh MYCERT dan beberapa badan tertentu.. dengan memberi beberapa panduan.. saya rasa kita sudah cukup bersedia ke arah pembangunan IT...

Apa pendapat sdri tentang opensource.. dari segi security?

Opensource adalah utk memupuk budaya hackers.. iaitu mereka yang memahami tcp/ip dan boleh menyelesaikan masalah... jadi saya amat menyokong opensource... dan akan menolong untuk membangunkan opensource... dari segi security... ada yang menyatakan apabila source code boleh didapati maka system itu tidak selamat.. tetapi mungkin itu tanggapan bagi mereka yang tidak memahami apakah opensource sebenar... daripada kajian hampir 72%(attrition) dari defacement adalah melibatkan OS Windows.. ini kerana biasanya pathes utk Windows memerlukan masa beberapa minggu dan bulan utk dikeluarkan (kerana Microsoft saja yang boleh mengeluarkan patches.. kerana closesource)... manakala utk opensource adalah cepat mungkin dalam kadar beberapa minit/jam kerana source code available (ramai programmer)..

Saya perhatikan sebahagian dari servers yang telah kena hack, dilarikan IRC proxy. apakah ini suatu yang memakan bandwidth terhadap laluan jaringan kepada domain berkenaan?

Pada asasnya kebanyakkan aktiviti hacking bermula dari IRC.. dan ini telah menunjukkan kepada kita... memang kebarangkalian server yang dihack ada

dilarikan IRC proxy... Bagi saya, memang perkara ini memakan bandwidth malahan kadangkadang dapat menyesakkan jaringan.. tetapi ini bergantung kepada jenis IRC PROXY yang digunakan.. biasanya jika menggunakan bnc ver 2.4.6 (yang pernah saya gunakan) ini tidak banyak memakan bandwidth (Setelah dikaji).. tetapi jika menggunakan psyBNC atau bnc versi 2.6 ke atas, ada kemungkinan menggunakan banyak bandwidth. Saya mengambil satu contoh server di Malaysia (tidak disebut) ada user biasa yang melarikan IRC proxy.. dan Bot IRC... setelah memantau aktiviti mereka (sebagai root kedua)... akaun ini dimasuki oleh bukan pengguna asal.. ada kemungkinan orang lain... perkara ini hanya memakan sedikit bandwidth.. dan saya mencari penyelesaian seperti membunuh proses atau suspend act user tersebut.. Bagi saya... saya telah mengkaji bagaimana untuk tidak meningkatkan bandwidth dengan menggunakan binary yang telah dicompile semula... ini adalah bertujuan tidak memberatkan system.... dan ini telah dipraktikkan oleh kebanyakkan shell provider terkenal seperti kirenet, risingnet, dan apolloweb dengan menyediakan precompiled.. dengan mengimbangi background proccess..

Tidakkah penyalahgunaan komputer melalui hacking sama seperti mencuri?

Dari segi undang-undang hacking memang salah dan boleh di sama ertikan dengan mencuri. Contoh sebuah rumah yang dikunci/tidak dikunci dimasuki orang tanpa kebenaran dan orang itu mengambil barang di dalam rumah itu (Orang ini dipanggil pencuri).. Tetapi bagi saya, kita harus melihat hacking dari sudut yang lebih positif... setiap sistem biasanya ada kelemahan dan kelemahan ini perlu diuji supaya sistem tersebut lebih mantap.. dan ini adalah tugas seorang pentadbir sistem utk memastikan server mereka sentiasa dipantau dan dijaga supaya sistem mereka tidak diceroboh. Hacking mungkin adalah satu aktiviti yang salah jika seseorang itu menggunakan ilmunya utk merosakkan sesuatu server atau menyampaikan perkara yang tidak baik (spt web defacedment) ... tetapi jika digunakan utk kebaikan seperti memaklumkan, tolong patch dan menjaga, saya rasa hacking adalah aktiviti yang sihat dan tidak boleh disamakan dengan mencuri.

Adakah sdri pernah dibayar untuk hacking? Jika ya, berapa bayaran yg pernah diterima?

Saya tidak pernah dibayar untuk hacking, ini mungkin hobi di masa lapang... Habis duit adalah :)

Adakah terdapat firma-firma di tanah air pernah mengambil hackers untuk kerja-kerja keselamatan IT?

Hmmm... Susah nak cakap.. kebiasaan firma-firma ini melihat kelulusan kertas semata-mata.. Ada satu server contohnya (di Malaysia).. di laman web firma ini dinyatakan system admin dia berpengalaman 6 thn.. tetapi bila kena hack dah

pening.. dan mengambil masa yang lama utk mengetahui yang server firma ini telah dihack... oleh yang demikian menggunakan khidmat mereka yang tahu berkaitan security (hackers) adalah langkah yang lebih baik.

Terhadap host yang pernah di-hack, apakah katalaluan yang sering atau lazim digunakan untuk akaun admin/root?

Biasanya akaun untuk admin/root adalah katalaluan yang susah, tetapi dari pengalaman ada juga yang menggunakan katalaluan yang lemah seperti '123456' atau 'root'. Tetapi suka diingatkan di sini katalaluan utk pengguna biasa juga perlulah di set kepada kata laluan yang tidak mudah diteka. Ini bertujuan supaya akaun user biasa tidak senang diceroboh.

Apakah nasihat kepada system admin?

Administrator haruslah berfikir secara lebih matang... maksud di sini ialah belajar... dan harus menganggap hackers adalah pelengkap.. untuk menguji tahap keselamatan sesuatu server... pada pendapat saya jangan salahkan hackers.. kerana hackers adalah orang yang tidak dibayar gaji.. mereka melakukan semua ini utk beberapa tujuan.. mungkin sebagai hobi.. tetapi sebagai administrator... pastikan server mereka sentiasa dijaga.. dan dipatch... Janganlah cepat melatah menyalahkan orang lain... kerana server kita tanggungjawab kita...

Tak takutkah buat kerja hacking?

Bagi saya berani kerana benar.. takut kerana salah... jadi saya tetap menegaskan... semua orang mempunyai peluang... kalau saya tak ambil peluang tuh.. maka orang lain akan mengambilnya... jadi tugas saya ialah memastikan server yang dihack dapat dipatch dan dijaga dengan betul.. dan ini adalah tanggungjawab.. walaupun tidak dibayar.. saya gembira... jadi saya yakin saya berada di landasan yang betul... kerana utk kebaikan...

Azuddin bin Ab.Rahman, 13 Julai 2002