HACKER INSIDE

TOP SECRET

FILE 2

HACKER INSIDE

TOP SECRET

EDITORA AFILIADA

HACKER INSIDE

TOP SECRET

SUMÁRIO

Capítulo 1 - Instalação do Linux

1. Conectiva Linux 11

1.1. Instalação 11

1.2. Particionamento de disco 12

1.3. Instalação 13

1.4. Configuração da rede 14

1.5. Vídeo 14

1.6. Criação de usuários 15

1.7. Finalizando a instalação 15

2. Slackware 8 15

2.1. Preparando o disco 16

2.2. Dimensionando a partição..... 16

2.3. Boot a partir do CD-ROM 16

2.4. A Instalação..... 17

2.5. Kernels para dispositivos IDE (.i): 17

2.6. Kernels para dispositivos SCSI (.s): 18

2.7. Criando as partições Linux..... 19

Capítulo 2 - Esteganografia

1. Esteganografia.....25

1.1. Jpegx 26

1.2. Limpando uma mensagem de uma imagem.....31

2. Conceitos de Criptografia 31

2.1. Introdução 31

2.2. Operações..... 32

2.3. Certificado Digital..... 32

2.4. Sistema de chave pública (Pretty Good Privacy/PGP) 33

3. Criptoanálise..... 36

3.1. Introdução 36

3.2. Tipos de Ataque 37

3.2.1. Ataque por texto ilegível 37

3.2.2. Ataque por combinação 37

3.2.3. Ataque por encriptação 37

3.2.4. Conclusão 37

Capítulo 3 - Pesquisa de Informação

Descobrindo IP de Website 43

Descobrindo IPs em chats 44

Salas de bate-papo 44

Pegando IP em salas que aceitam imagens 45

IRC 45

Descobrir IP por engenharia social 46

Descobrindo um IP no icq 2000/2002 47

O IP de uma máquina na mesma rede 48

Capítulo 4 - Proteção

1. Firewalls 51

2. Tipos de Firewall 51

2.1. Firewalls baseados em filtragem de pacotes 51

2.2. Firewalls baseados em aplicações 52

3. Roteamento Dinâmico 53

TABELAS 55

Capítulo 5 - Senhas

PGP 75

Keylogger 83

Espionagem - Keylogger 83

Como utilizar o programa 83

Capítulo 6 - Desafio Hacker

Prova 1 88

Prova 2 91

Capítulo 1

INSTALAÇÃO DO LINUX

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

Apesar de haver diversas distribuições Linux, seu funcionamento e sua instalação são parecidos, com este capítulo, você aprende a instalar o Conectiva Linux 8 e o Slackware 8, suas distribuições mais utilizadas em empresas e hackers. Os dois podem ser baixados na Internet, verifique no site: *www.linux.org* ou *www.isolinux.org*

1. Conectiva Linux

1.1. Instalação

Antes de tudo, verifique se o seu computador tem suporte a reinicio por CD-ROM, se sim, habilite-o na Bios. Caso haja dúvida, consulte o manual da placa mãe.

Na maioria dos micros, a BIOS é acessada pressionando o botão *DEL* ou *F2* enquanto o micro está sendo ligado, para isso, basta pressionar o botão correto até que apareça a tela da BIOS, em seguida, marque a opção para que o micro seja iniciado a partir do CD-ROM, salve as configurações, insira o primeiro CD-ROM do Linux, reinicie o micro e siga os passos:

1. Ao iniciar o micro pelo CD-Rom do Conectiva Linux, surge uma tela com sete opções, utilize a seta direcional do teclado para escolher uma das opções, marque *Conectiva Linux 8+* e pressione a tecla *Enter*.

2. O Linux fará uma varredura em toda sua máquina à procura dos drivers corretos para os dispositivos que estão instalados. Esse procedimento pode demorar alguns minutos, dependendo das configurações do seu PC.

3. Caso haja algum problema relacionado a sua placa de vídeo, reinicie a instalação e, ao invés de selecionar o item *Conectiva Linux 8+*, escolha *Conectiva Linux 8+ Vesa* e pressione a tecla *Enter*.

4. No quadro seguinte, marque com o mouse o idioma desejado e, então, pressione o botão *Próximo*. Ao selecionar um idioma, não só as telas de instalação serão no idioma escolhido, também todo o sistema que será instalado.

5. A próxima etapa é a seleção do mouse, geralmente, o Linux encontra o dispositivo automaticamente, caso contrário, basta marcar a opção correta na lista e pressionar o botão *Próximo*.

6. Na tela *Seleção de teclado*, basta escolher o modelo do teclado e layout correspondente, na maioria dos casos, os teclados seguem o modelo *Brazilian ABNT2* e layout *Brazilian*, se houver dúvidas, consulte o manual do seu PC ou mesmo do teclado. Para prosseguir, clique em *Próximo*.

7. Aguarde enquanto os módulos do Kernel são carregados e, na tela que surgir, deve-se selecionar o tipo de instalação, ou seja, para o que será utilizada essa máquina, se houver espaço em disco disponível, escolha *Todos os pacotes*, pois, se no futuro você necessitar utilizar alguma ferramenta, não será necessária a instalação de novos pacotes ou problemas de dependência, que nada mais são do que programas que necessitam de outros arquivos.

8. Marque o item *Forçar seleção de pacotes* e *Forçar particionamento manual*, a seguir, pressione o botão *Próximo*.

1.2. Particionamento de disco

O particionamento de disco nada mais é do que a divisão de disco. No Linux, são necessárias duas partições, uma para o sistema e os arquivos e a outra será utilizada em conjunto como área de troca, que funcionará em conjunto com a memória RAM, ajudando o processamento em algumas aplicações. O quadro que aparece na seqüência da instalação corresponde ao particionamento do disco, veja como proceder:

1. Verifique se existe alguma partição que esteja em uso, é aconselhável deixar somente o Linux nessa máquina, já que ela será o servidor de arquivos de sua rede, se houver dados que não possam ser apagados, saia da instalação e faça uma cópia desses arquivos e volte a esta etapa.

2. Para criar as partições, deve existir espaço não alocado no disco, é só verificar se aparece uma linha com a denominação *free* no campo *tipo*. Verifique o tamanho do espaço livre e se atende às suas necessidades.

3. O próprio instalador pode fazer o particionamento automático basta clicar em *Particionamento automático*. Se preferir criar as partições automaticamente, clique com o mouse sobre o espaço livre (*free*) e pressione o botão *Adicionar*.

4. Na tela que surge, marque a opção "*/*" no ponto de montagem (significa que o sistema será instalado na raiz). No campo *Sist. De Arq* (sistema de arquivos), escolha *Ext3* e o tipo de partição *Primary*. Vá ao campo *Tamanho* e digite o tamanho dessa partição em *MB* (Megabytes), marque o item *Formatar* e dê *OK*.

5. Agora é hora de criar a partição de troca, proceda da mesma maneira, clicando na linha que mostra a área livre do disco, vá a *Adicionar* e a *Sist. De Arq*. Escolha *Linux Swap*, no tamanho da partição, digite pelo menos o dobro da sua memória RAM em MB, marque a opção *Formatar* e dê *OK*.

6. Para criar mais partições para alocar arquivos, basta proceder como no passo 4, mas, ao invés de escolher o ponto de montagem como "*/*", digite outro diretório, como por exemplo, /disco2 ou /temp e dê *OK*, crie quantas partições forem necessárias.

7. Ao finalizar o particionamento, clique em *Próximo*, a seguir, será feita uma pergunta e, se tudo estiver correto, pressione *Sim*, caso contrário, clique em *Não* e acerte o particionamento.

8. Espere a formatação das partições, dependendo da configuração da máquina e do tamanho das partições, esse processo pode demorar alguns minutos.

1.3. Instalação

No quadro seguinte, selecione os pacotes que precisará, como dito anteriormente, instale todos os pacotes ou, então, somente os que

desejar, como por exemplo, *servidor de rede*, marque também o *KDE*, que é um módulo gráfico e também o *Linuxconf*, um aplicativo que reúne algumas configurações do sistema, eles podem ser úteis para configurar algumas aplicações. Dê *Próximo*.

A instalação será iniciada, aguarde até a finalização do procedimento. Não se esqueça de que o tempo de instalação depende da configuração da máquina e dos pacotes que serão instalados.

1.4. Configuração da rede

A próxima etapa é a configuração do dispositivo de rede (placa de rede), o procedimento é feito todo nessa tela. Verifique como configurar:

1. No primeiro campo, digite o nome da máquina, por exemplo, *server*. Nos itens abaixo, você deve escolher como configurar a rede, no nosso caso, escolha *Configurar a rede manualmente*.

2. Digite os dados da maneira que definiu anteriormente, como classe do IP a utilizar na rede, número IP do servidor, gateway etc. O próprio configurador sugere a numeração, caso concorde, clique em *Próximo*. Caso queira modificar algum item no futuro, não se preocupe, todos esses dados podem ser editados já com o sistema instalado.

1.5. Vídeo

As próximas etapas são referentes às configurações de vídeo, verifique, atentamente, a marca e o modelo de sua placa de vídeo e do seu monitor, então, siga os passos:

1. Na tela que aparece, se o sistema não conseguir detectar automaticamente sua placa de vídeo, basta clicar no item *Selecione a placa de vídeo manualmente* e escolha a marca e o modelo corretos da placa na lista abaixo, depois, é só pressionar o botão *Próximo*.

2. Da mesma maneira, se o sistema não encontrar a placa de vídeo automaticamente, basta selecionar a marca e o modelo corretos na lista. Caso não encontre, selecione genérico e a configuração mais próxima do seu monitor, por exemplo *Generic Non-Interlaced, 1024x768@60Hz, 800x600@72Hz*, para configurar corretamente verifique essas especificações no manual do monitor.

3. No quadro seguinte, marque o tamanho da tela e a profundidade de cores (número de cores). Para testar se o monitor, a placa

de vídeo e as configurações de cores são suportadas, clique em *Testar configuração*. Se aparecer uma tela pedindo a confirmação, clique em *OK*, caso contrário, tente uma configuração inferior e faça o teste novamente. Quando tudo estiver correto, clique em *Próximo*.

1.6. Criação de usuários

1. Na tela de configuração do usuário, deve-se criar a senha para o administrador do sistema (root) e especificar se outros usuários terão acesso ao sistema. Para criar a senha de root, basta digitá-la no primeiro campo e confirmá-la no espaço ao lado.

2. Os usuários são criados dentro do campo *Criação de usuários*, para isso, basta preencher todos os dados corretamente e confirmar a senha do usuário, depois, é só pressionar o botão *Criar usuário*. Crie quantos necessários e dê *Próximo*.

É aconselhável não haver muitos usuários além do root, não deixe que outros usuários, além de você, tenham acesso a essa máquina.

1.7. Finalizando a instalação

1. Na tela *Configuração do Loader*, não precisa alterar nada, somente se você preferir algum outro gerenciador de iniciação. O gerenciador, como o próprio nome diz, gerencia o início do sistema, é ele quem "escolhe" qual sistema será iniciado, caso haja mais de um instalado na mesma máquina. Deixe marcada a opção *Registro mestre de inicialização (MBR)*, a seguir, clique em *Próximo*.

2. Será pedida a criação de um disco de boot, não pule essa parte, pois esse disco é muito útil em caso de falhas no sistema ou em algum momento crítico. Insira o disquete no drive e clique em *Sim*. Não se esqueça de que o disco será formatado e servirá somente como disco de boot do seu sistema.

3. Espere a criação do disco, retire-o e identifique-o com uma etiqueta e guarde-o em um local seguro e de fácil acesso.

4. Pronto! O sistema foi instalado, retire os discos (CD, disquete) do seu micro e pressione o botão *Sair*, situado no canto inferior da tela, e espere que o micro seja iniciado.

2. Slackware 8

Particionando o disco com o FIPS.

2.1. Preparando o disco

Para instalar o sistema operacional em seu micro, você deve, em primeiro lugar, verificar se há espaço suficiente no disco e é recomendável que antes seja feito um backup de todos os dados importantes do computador. Caso já tenha o Windows instalado, proceda da seguinte maneira:

1. No Windows, clique no botão *Iniciar*, vá em *Programas*, *Acessórios*, *Ferramentas do sistema* e *Scandisk*, selecione o local no qual o sistema será instalado, marque a opção *Completo* e clique em *Iniciar*.

2. Após finalizar o *Scandisk*, será necessário utilizar o desfragmentador de disco, para isso, clique no botão *Iniciar*, vá *Programas*, *Acessórios*, *Ferramentas de sistema* e *Desfragmentador de disco*.

3. Selecione a unidade correta e clique em *Iniciar*. O processo é um pouco demorado, para que não ocorram problemas, desabilite o protetor de telas, caso este esteja ativado, e deixe o micro ocioso.

2.2. Dimensionando a partição

O Linux deverá ser instalado em uma partição diferente do Windows, para isso, você deverá criá-la da seguinte maneira:

1. Crie um disco de boot no Windows e, a seguir, baixe o arquivo do Fips (www.hackerinside.com.br/downloads/fips.exe) para o seu HD, de preferência para a raiz do drive C:. Reinicie o micro com o disco de boot, acesse o disco C: e execute o FIPS. Para executá-lo, basta digitar *fips* no DOS e pressionar a tecla *Enter*.

2. O programa verificará sua(s) unidade(s) de disco e mostrará uma tabela com as partições existentes. Utilize o cursor para dimensionar a sua nova partição e pressione a tecla *Enter*. É aconselhável deixar no mínimo 200 Mb livres.

3. O programa fará uma verificação da sua unidade e, a seguir, exibirá uma nova tabela de partição. Para aceitar as alterações, pressione a tecla *C*, depois, *Y*.

2.3. Boot a partir do CD-ROM

A instalação do Slackware é iniciada a partir do CD-ROM, a melhor maneira é iniciar o micro com o CD-ROM. Caso o CD-ROM não esteja iniciando automaticamente, configure o boot a partir do CD-ROM na configuração da Bios. Caso seu micro não suporte o boot via CD-ROM

ou por outro caso a instalação não esteja sendo iniciada automaticamente, você deve criar os discos de boot (disquetes) e, assim, instalar o Slackware.

2.4. A Instalação

Para isso, coloque o CD-ROM no drive e reinicie o computador. Logo no início, aparecerá uma tela preta com algumas informações e, por fim, os dizeres *boot:* na parte inferior da tela. Na maioria das máquinas, basta pressionar a tecla Enter que a instalação será iniciada, nesse caso, será carregado o kernel bare.i.

Caso você tenha algum dispositivo a mais em sua máquina, como drives não IDE ou outros não muito comuns, é necessário que seja digitado o kernel correto. Veja, a seguir, a lista dos kernels e o significado dos mais utilizados:

2.5. Kernels para dispositivos IDE (.i):

bare.i – Este é o kernel para ser utilizado na maioria dos PCs com controladoras IDE que também suporta IDE/ATAPI e drives de CD-ROM e DVD. A maioria dos drives está nesta categoria.

jfs.i – Uma versão do bare.i com suporte a arquivos de sistema IBM Journaled.

lowmem..i – Aconselhável para máquinas com menos de 8 Mb de RAM. Se com o kernel bare.i não funcionar corretamente, tente carregar com este.

old_cd.i – Versão do bare.i para máquinas com drives de CD-ROM mais antigos. Os drives suportados por este kernel são: Aztech CDA268-01[A], Orchid CD-3110, Okano/Wearnes CDD110, Conrad TXC, CyCDROM CD520, CR540, Sony CDU31/33a CD-ROM, Sony CDU531/535 CD-ROM, Philips/LMS cm206 CD-ROM, Goldstar R420, ISP16/MAD16/Mozart CD-ROM.

Pportide.i – Kernel com suporte a uma grande variedade de dispositivos de portas paralelas IDE. Também aceita dispositivos da HP, SyQuest, Imation, Avatar e outros.

usb.i – Este kernel é o mesmo que o bare.i, mas com suporte a alguns dispositivos USB, como máquinas com teclados USB.

2.6. Kernels para dispositivos SCSI (.s):

adaptec.s – Este kernel é compatível com a maioria das controladoras SCSI, incluindo os seguintes modelos:
AHA-1510, AHA-1520, AHA-1522, AHA-1740 e AHA-2825. Modelos AIC7xxx, incluindo 274x EISA, 284x VLB, 2902, 2910, 293x, 294x, 394x, 3985 e muitos outros dispositivos PCI e placas-mãe com controladoras SCSI da ADAPTEC. Este kernel também suporta todos os controladores RAID ADAPTEC I20 como também os cartões DPT SmartRaid V.

ibmmca.s – kernel para algumas máquinas IBM OS/2 e laptops. Compatível com a maioria das placas MCA SCSI, Ethernet e Token Ring.

raid.s – Suporte para algumas controladoras RAID SCSI e IDE, como:
3ware ATA-RAID controllers.
AMI MegaRAID 418, 428, 438, 466, 762, 490 e 467
Controladoras Compaq Smart Array
Controladoras Compaq Smart Array 5xxx
Highpoint 370 IDE RAID
Promisse Fasttrack (tm) IDE RAID
IBM ServeRAID
Mylex DAC960, AcceleRAID e controladoras eXtre RAID.

scsi.s – Suporte a controladoras SCSI, para as da ADAPTEC, u izar o adaptec.s. As controladoras compatíveis são:
AdvanSys, HP CD-R/RW e o Iomega Jaz Jet SCSI, AM53/79c974 PCI SCSI, BusLogic, EATA ISA/EISA/PCI (DPT e placas genéricas EATA/DMA), NCR53c0/53c400, Initio

91XXU (W), NCR53c406, NCR53c7, 8xx, SYM53C8 Version 2, Qlogic ISP e Qlogic QLA 1280.

Após selecionar o kernel correto, basta pressionar a tecla *Enter*. Pronto! Agora você estará no prompt do Linux, digite o nome do superusuário Root e pressione *Enter* novamente.

Root *(Enter)*.

Para iniciar a instalação, digite *Setup* e dê *Enter*.

Setup *(Enter)*.

2.7. Criando as partições Linux

Para que o Linux seja instalado, será necessário criar duas partições: a Swap, que é destinada para área de troca ou memória, e uma outra para os arquivos. Nesse caso, você utilizará o espaço vazio que já acertou, anteriormente, utilizando o fdisk do DOS ou o FIPS. Aqui você aprende como criar as partições do Linux.

O próximo item que aparece na instalação é o pedido de particionamento do disco, nele você deve escolher qual particionador utilizar, escolha o fdisk.

Para particionar seu disco, digite o fdisk e o caminho do HD a ser particionado. Veja os exemplos para cada HD:

fdisk /dev/hda (se o disco for o primeiro IDE)
fdisk /dev/hdb (se o disco for o segundo IDE)
fdisk /dev/sda (se o disco for o primeiro SCSI)
fdisk /dev/sdb (se o disco for o segundo SCSI)

Se preferir, é possível utilizar o cfdisk para criar as partições.

Ao iniciar o fdisk, será apresentado um prompt. Em primeiro lugar, visualize as partições existentes no seu disco, para isso, utilize o comando "p":

Command (m for help) : p

Aparecerá algo como:

Disk /dev/sda: 255 heads, 63 sectors, 1024 cylinders
Units = cylinders of 16065 * 512 bytes

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1	*	1	702	5638783+	4f	Win95 FAT32 (LBA)

Aqui pode-se ver que existe uma partição DOS (FAT32), que é iniciada no primeiro cilindro e vai até o cilindro 702. Então, como o disco tem 1024 cilindros, a faixa de 703 até 1024 está livre e pode ser utilizada para o Linux.

Se a partição FAT32 (Windows) estivesse utilizando o disco inteiro, você não teria como redimensioná-lo, somente se utilizasse o FIPS, como demonstrado anteriormente. Caso não tenha espaço livre no disco, utilize o FIPS e deixe um espaço livre para o Linux, aconselhável 3 GB e no mínimo 1 GB. Se não for mais utilizar o Windows nesse disco e quiser deletar a partição FAT (Windows), utilize o comando "d". Aparecerá uma pergunta, indique qual o número da partição a ser deletada, verifique o tamanho da partição e, então, quando estiver certo de que é a correta, apague-a.

O próximo passo será criar a partição primária, para isso, utilize o comando "n".

Command (m for help) : n
Command action
e extended
p primary partition (1-4)

Tecle "p" para criar a partição primária.

Partition number (1-4): 2

Nesta etapa, digite "2" se o DOS estiver utilizando a partição primária, caso vá instalar somente o Linux digite "1". O fdisk perguntará qual o cilindro em qual a partição será iniciada, como o particionador (fdisk) sabe qual o próximo cilindro disponível, então, aceite este valor. Agora será necessário escolher o tamanho da partição, você pode escolher

de duas maneiras: digitando o número do cilindro no qual a partição terminará ou, então, o tamanho ela. Escolha o tamanho, para isso, digite +tamanhoM, por exemplo +2500M, para que a partição tenha 2500 Mb ou 2.5 Gb. Veja como aparecerá na tela:

OBS.: Deixe por volta de 180 Mb livres, pois será necessário criar outra partição Linux.

First cylinder (703-1024) : 703

Last cylinder or +size or +sizeM or +sizeK (33-92) : +2500M

Pronto! A partição primária do Linux já está criada e com o tamanho de 2.5 Gb. Agora, como o Linux precisa de uma partição para área de troca (Swap), é preciso criá-la. Como a partição Swap será utilizada para "memória" e não para arquivos em si, ela terá um tamanho menor. O processo é o mesmo utilizado para a partição primária. Confira:

Command (m for help) : n

Command action

e extended

p primary partition (1-4)

Pressione a tecla "p" para selecionar a partição primária. Como a partição 1 está sendo utilizada para o Windows e a 2 para o Linux, a única escolha é a 3 para a partição Swap. Então, digite "3" e dê *Enter*.

Partition number (1-4) : 3

Como esta será a última partição a ser criada nesse HD, deve-se especificar o final do cilindro manualmente. Siga o exemplo:

First cylinder (999-1024): 999

Last cylinder or +size or +sizeM or +sizeK (999-1024) : 1024

Agora mude o tipo da partição para 82, que é o padrão para a partição Swap. Para isso, utilize o comando "t":

Command (m for help) : t

Partition number (1-4) : 3

Hex code (type L to list codes) : 82

Como as partições necessárias para a instalação do Linux foram criadas, basta salvar as alterações, mas antes confira se está tudo correto utilizando o comando "p":

Command (m for help) : p

Disk /dev/sda: 255 heads, 63 sectors, 92 cylinders

Units = cylinders of 16065 * 512 bytes

Device	Boot Start	End	Blocks	Id	System
/dev/sda1	1	702	5638783+	4f	Win95 FAT32 (LBA)
/dev/sda2	703	999	2385638	83	Linux
/dev/sda3	999	1024	200811	82	Linux Swap

Se tudo estiver correto, de acordo com os dados que você selecionou, utilize o comando "w" para gravar as alterações. Se desejar sair sem gravar as alterações, caso tenha feito algum erro, utilize o comando "q". É aconselhável que você reinicie o sistema caso tenha criado alguma partição estendida. Para isso, basta dar Ctrl+Alt+Del e reiniciar a instalação.

Capítulo 2

ESTEGANOGRAFIA

- Criptografia
- Criptoanálise

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

1. Esteganografia

A origem da esteganografia remonta a Grécia antiga e significa "escrita coberta". Sendo um dos métodos estudados pela criptologia, que basicamente funciona como uma maneira de camuflar a mensagem a ser passada, e não a torna totalmente ininteligível como a criptografia costuma fazer. Ao contrário da criptografia, que procura esconder a *informação* da mensagem, a esteganografia procura esconder a mensagem.

Antagonicamente à criptografia, que cifra as mensagens de modo a torná-las incompreensíveis, a esteganografia esconde as mensagens por artifícios, como, imagens ou um texto que tenha sentido, mas que sirva apenas para disfarçar o real conteúdo. Funciona da mesma forma que o *barn code*: mesclar a mensagem numa outra, em que apenas determinadas palavras devem ser lidas para descobrir o texto camuflado.

O primeiro uso confirmado da esteganografia está em "As Histórias" de Heródoto e remonta ao século V a.C.: um certo Histio, querendo fazer contato secreto com seu superior, o tirano Aristágoras de Mileto, escolheu um escravo fiel, raspou a cabeça dele e escreveu na pele a mensagem que queria enviar. Esperou que os cabelos crescessem e madou o escravo ao encontro de Aristágoras com a instrução de que deveriam raspar seus cabelos.

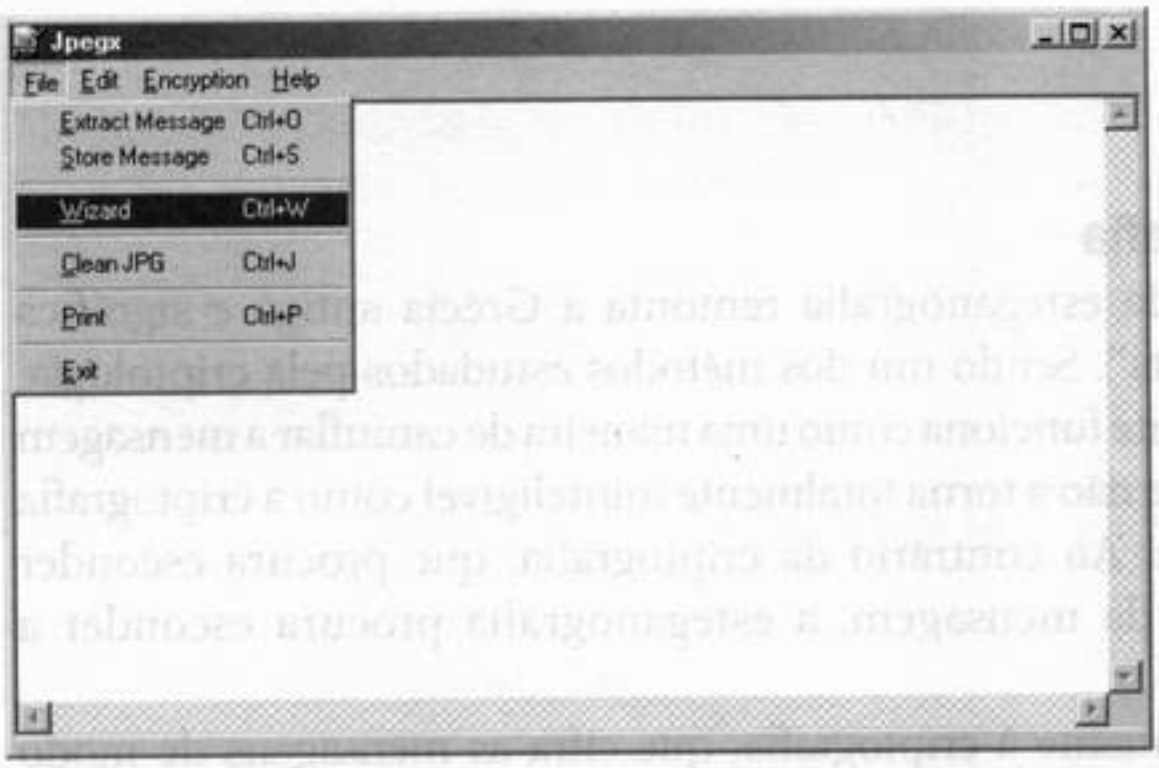
1.1. Jpegx

Atualmente, uma das maneiras mais usadas de esteganografia é por meio de programas que armazenam mensagens de texto em imagem. Funciona como uma troca de mensagens, porém por arquivos de imagens, assim se a imagem for interceptada por alguma pessoa não autorizada, ela não conseguiria ler a mensagem.

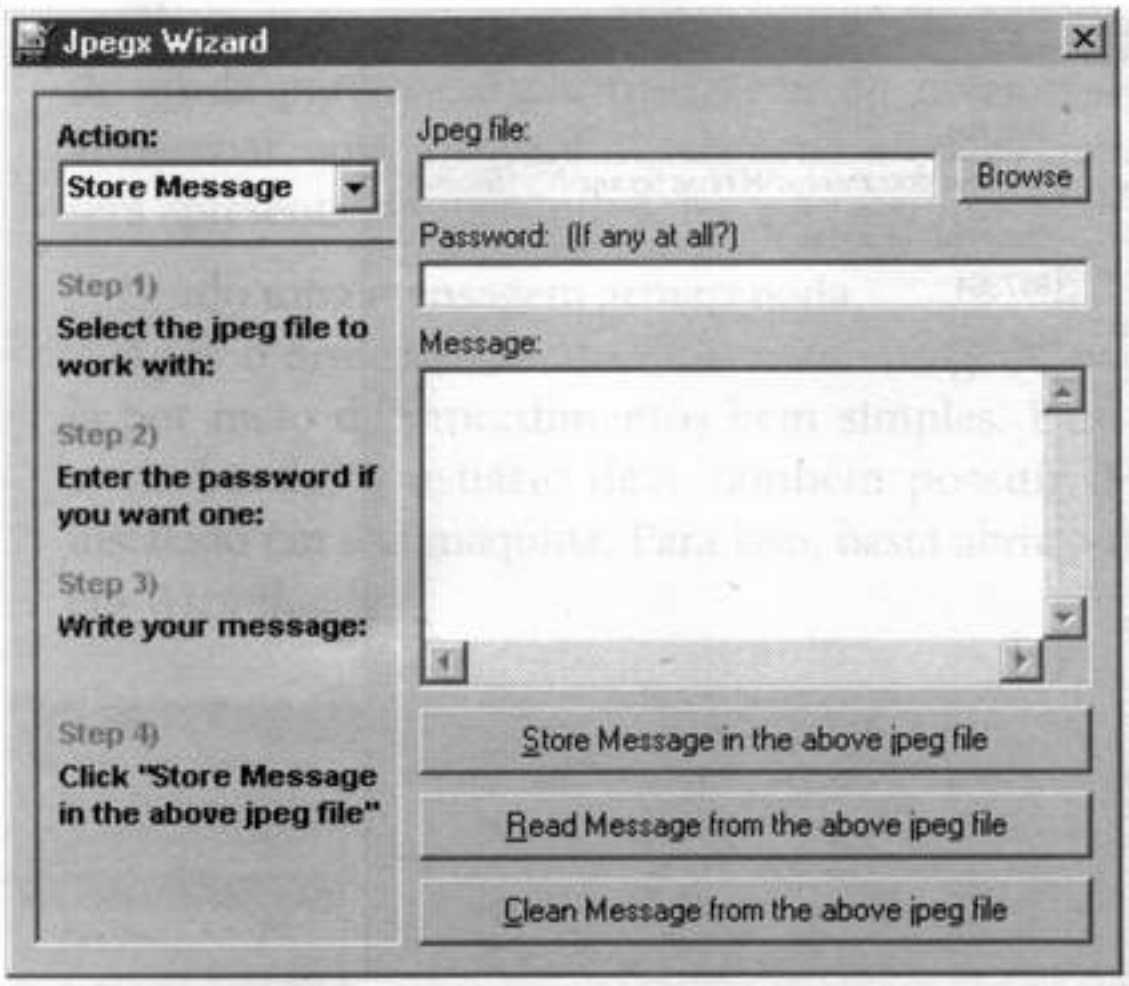
Armazenando uma mensagem

O programa Jpegx tem exatamente essa funcionalidade, ou seja, pode-se inserir mensagens de texto em arquivos de imagens. Veja a seguir como utilizá-lo.

Para iniciar, abra o menu *File* e clique em *Wizard*.

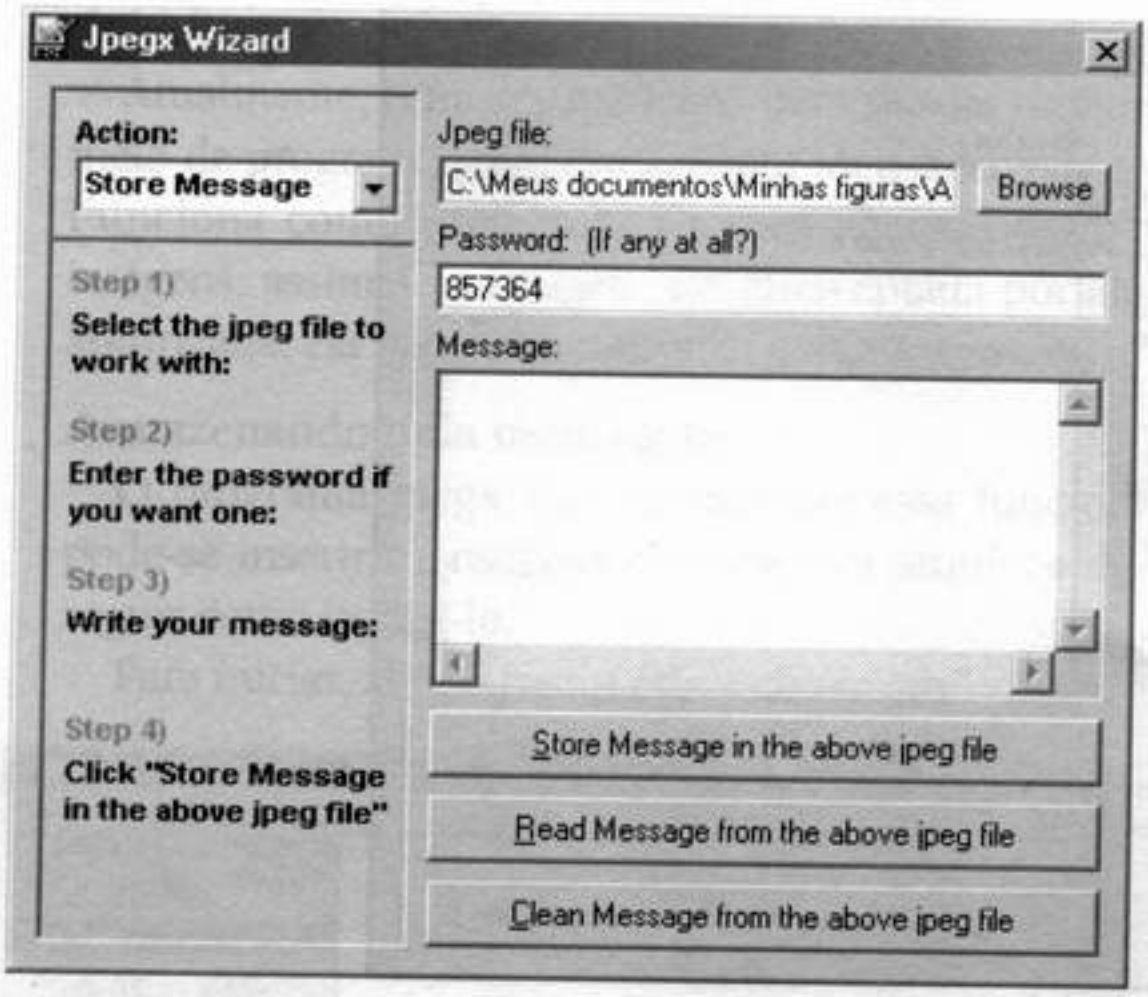


Nesse primeiro passo, vamos inserir um texto na imagem selecionada.

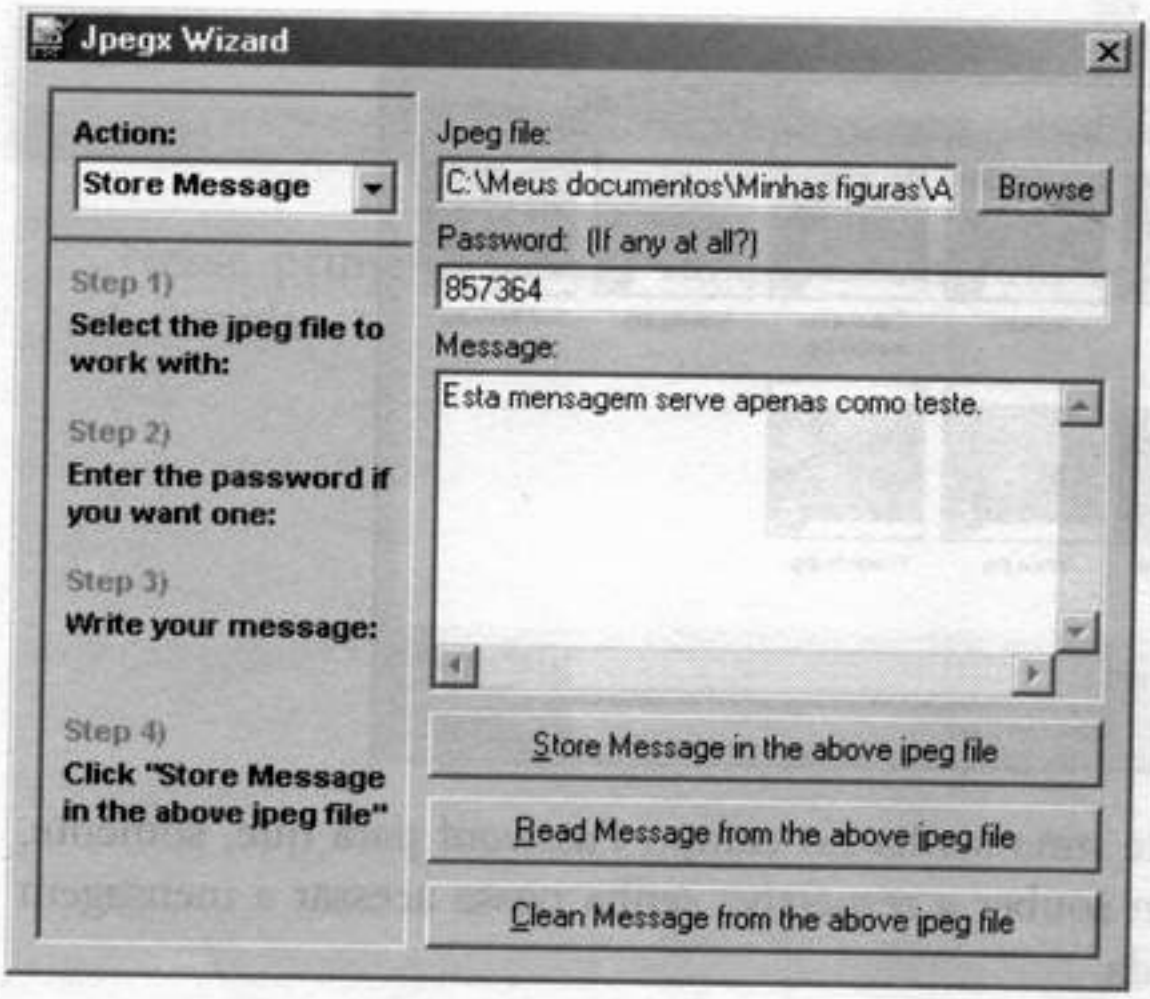


Podemos utilizar nesse programa arquivos no formato *jpg* e *bmp*. Selecione a imagem desejada, clicando em *Browse*. Na próxima janela, escolha a imagem desejada e, então, clique em *Abrir*.

Agora digite uma senha no campo *Password* para que, somente, quem também souber a respectiva senha possa acessar a mensagem esteganografada.



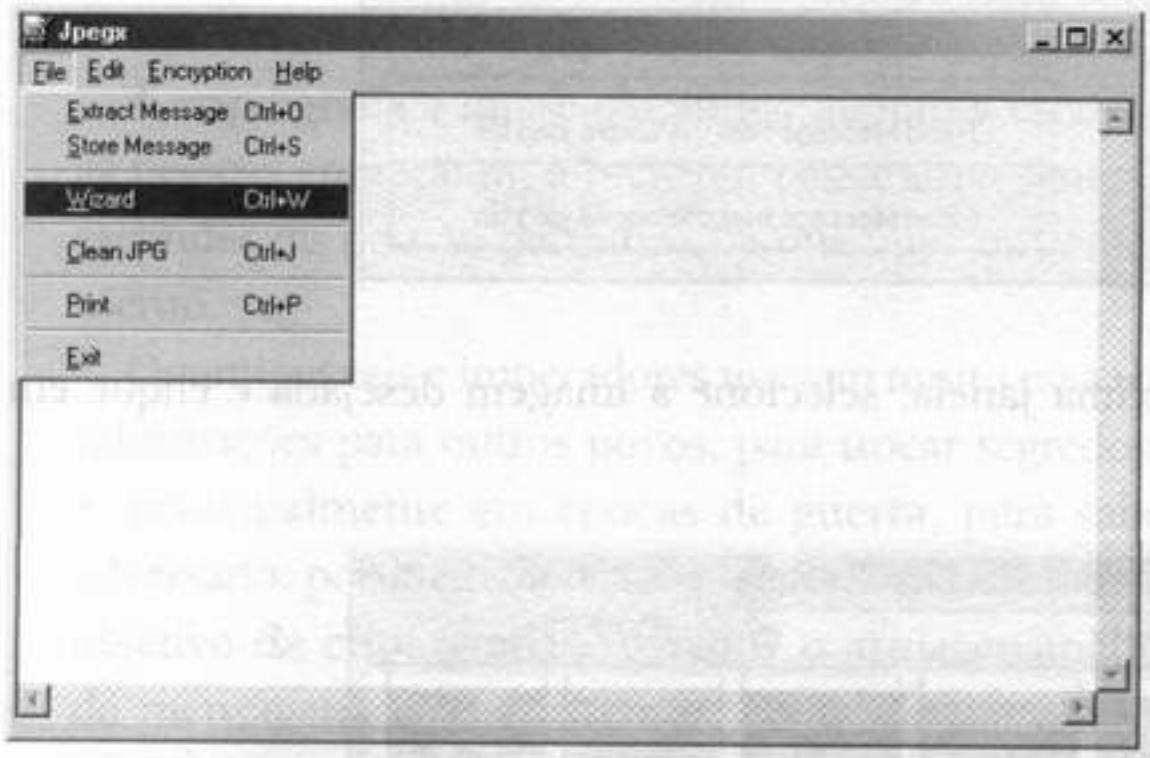
Digite, a seguir, a mensagem desejada, ela ficará armazenada junto da imagem que você selecionou, depois, clique no botão *Store Message in the above jpeg file*.



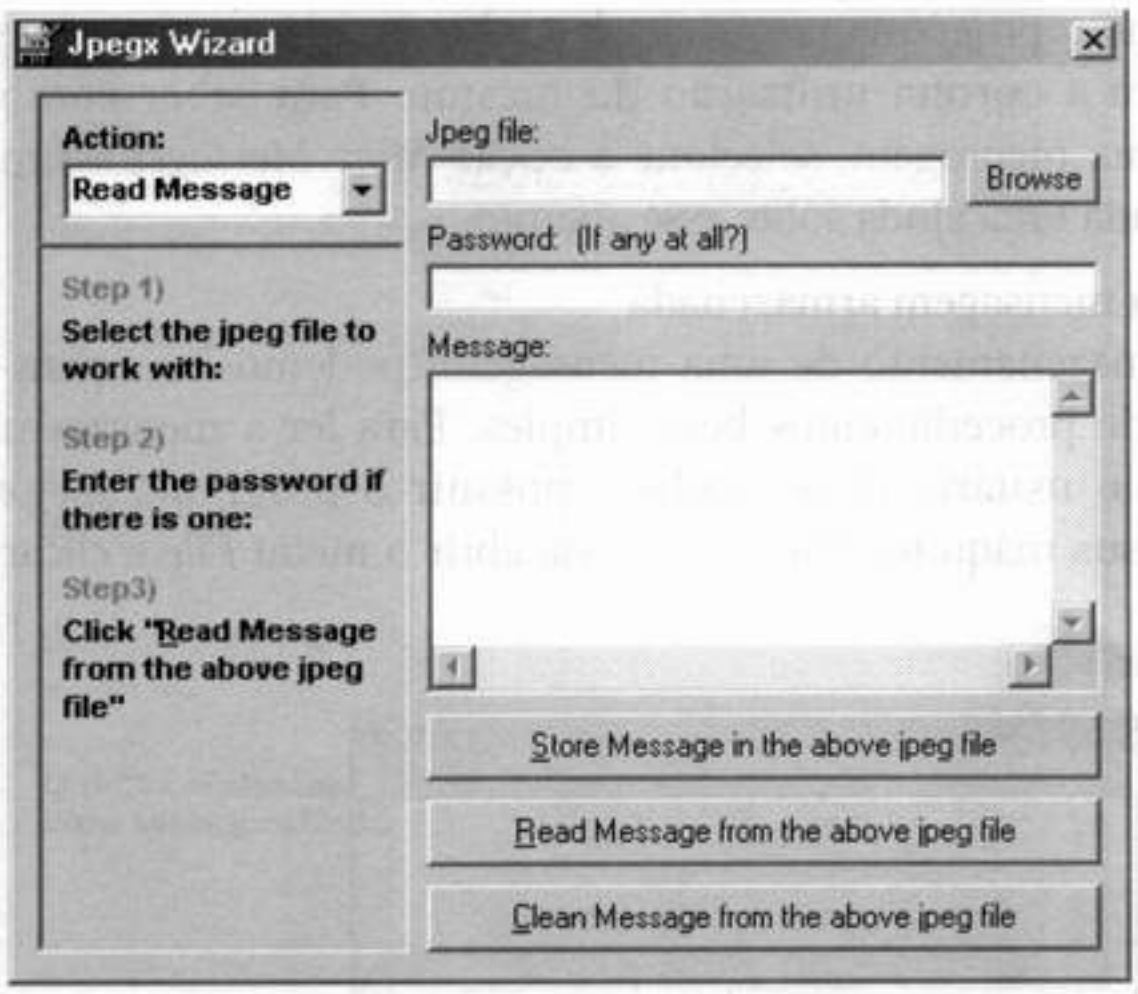
Observe que o programa possui, na lateral esquerda, uma espécie de ajuda para a correta utilização do mesmo. Para saber como armazenar uma mensagem, selecione a opção *Store Message*, assim será apresentada uma ajuda sobre esse assunto.

Lendo uma mensagem armazenada

Após o armazenamento de uma mensagem, podemos recuperá-la por meio de procedimentos bem simples. Para ler a mensagem armazenada, o usuário deve também possuir o programa *Jpegx* instalado em sua máquina. Para isso, basta abrir o menu *File* e clicar em *Wizard*.



Em seguida, selecione a imagem que está com o texto armazenado. Para isso, clique no botão *Browse*.



Nessa próxima janela, selecione a imagem desejada e clique em *Abrir*.

Agora digite, no campo *Password*, a senha que foi escolhida para ler o texto inserido na imagem. Em seguida, clique no botão *Read Message from the above jpeg file*. Assim o texto será exibido no campo *Message*.

1.2. Limpando uma mensagem de uma imagem

Para retirar uma mensagem de texto de um arquivo de imagem, basta prosseguir como nos passos anteriores, porém o botão a ser clicado é o *Clean Message from the above jpeg file*.

2. Conceitos de Criptografia

2.1. Introdução

A criptografia origina-se do grego: "kryptos", ou seja, secreto, e "grapho", escrita. A criptografia nada mais é do que escrever secretamente, comunicar-se de maneira que nenhuma outra pessoa, a não ser o remetente e o destinatário, possa decifrar a mensagem.

A criptografia é quase tão antiga quanto a escrita, pois, desde que as pessoas começaram a escrever, passaram a sentir a necessidade de esconder ou de não permitir que qualquer um entendesse o que foi escrito.

Os antigos reis e imperadores usavam muito essa técnica para enviar informações para outros povos, para trocar segredos com outros reis e, principalmente em épocas de guerra, para saber mais sobre o adversário, por meio da troca de segredos com os espiões. O principal objetivo da criptografia é garantir o armazenamento e a circulação de mensagens com segurança, tornando-as ininteligíveis para um adversário qualquer. E para tornar uma mensagem ininteligível, são usadas várias chaves e algoritmos. Uma chave é uma informação que o remetente e o destinatário possuem para permitir a encriptação e desencriptação do texto.

Um algoritmo são procedimentos, pré-definidos, usados para manipular a mensagem. Antigamente, os algoritmos eram bastante simples e fáceis de ser quebrados, sendo basicamente formados por substituição e permutação de letras ou palavras de uma mensagem. Atualmente, com o avanço nos estudos dos algoritmos e com o avanço da informática, os algoritmos puderam ser melhorados e tornados mais fortes. Os métodos criptográficos atuais podem ser considerados inquebráveis, ou praticamente, pois até um supercomputador levaria anos para decifrá-los.

2.2. Operações

Na criptografia, são usadas várias operações para manipular a mensagem, os bons algoritmos mesclam essas operações diversas vezes. As principais são:

Rotação – Consiste no deslocamento dos bits de uma variável para a esquerda ou para a direita. Podendo ser de dois modos:

Circular: O bit saído retorna do outro lado.

Não Circular: O bit saído é eliminado, sendo substituído pelo zero.

Permutação – A permutação consiste em embaralhar os elementos ou partes de um elemento. Um vetor é usado para alterar a ordem e, possivelmente, o número de elementos de um conjunto, mas sem alterar os seus valores.

Substituição Monoalfabética – Esse tipo de operação consiste em substituir uma letra pela outra, seguindo um padrão fixo. Cada letra (l) seria substituída por outra (l+ x), e, para desencriptar, seria l-x.

Substituição Polialfabética – São aqueles em que se tem a combinação ordenada de diversos sistemas monoalfabéticos. Ele adota uma chave (x), com *n* letras, e divide a mensagem em *n* blocos. A substituição polialfabética é muito mais complexa que a monoalfabética, mas ambas são inúteis (usando-as isoladamente), visto que qualquer computador pode quebrá-la facilmente.

2.3. Certificado Digital

O Certificado Digital é um par de chaves de criptografia vendidos para uma empresa por uma entidade certificadora, podemos citar a *Verisign* e a *Thawte*. Essas chaves são chamadas de Chave Privada e Chave Pública. O objetivo é simples, o que for criptografado pela chave privada deve, necessariamente, ser descriptografada pela chave pública. A chave pública qualquer pessoa pode obter. A privada fica

em poder de quem criptografa os dados. Isso garante, por exemplo, que a transação de pagamento do cliente será criptografada pelo banco com a chave privada e impressa no comprovante de pagamento pela internet como prova do pagamento. Para que um falsificador faça um comprovante, ele deverá saber como criptografar os dados e possuir a chave privada.

2.4. Sistema de chave pública (Pretty Good Privacy/PGP)

Um dos problemas de chave privada é a troca da chave, o remetente deve fazer com que o receptor tome conhecimento da chave. Se alguém mais tiver acesso à chave, essa pessoa poderá facilmente interceptar a mensagem e descriptografá-la. A troca da chave deve ser feita em segredo.

Esse problema foi resolvido com o sistema de chave pública. Nesse caso, o receptor gera duas chaves, a pública e a privada. A chave pública, que pode ser conhecida por qualquer pessoa, pode ser enviada por qualquer meio. O remetente criptografa a mensagem com a chave pública do receptor e a envia. Mas somente o receptor, com sua chave privada, poderá descriptografar a mensagem. Nem mesmo a chave pública pode ser usada para descriptografar a mensagem, apenas a privada.

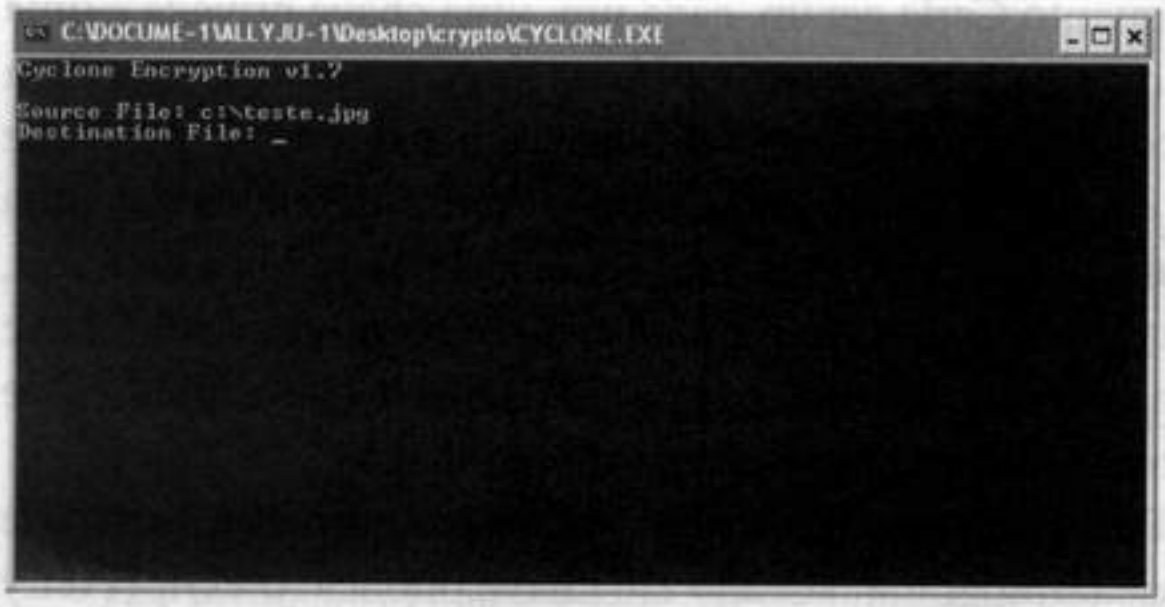
Por exemplo, André e Carla desejam trocar e-mail de forma segura. Tanto André quanto Carla geram, cada um, uma chave privada e uma pública. Os dois trocam as chaves públicas um com o outro e podem até mesmo colocar suas chaves públicas em páginas WWW que atuam como catálogos de chaves. Quando André deseja enviar uma mensagem para Carla, ele a criptografa com a chave pública de Carla, e somente ela poderá descriptografar a mensagem com sua chave privada. Obviamente, qualquer pessoa que saiba a chave pública de Carla pode enviar-lhe uma mensagem criptografada.

Em 1991, Phil Zimmerman tornou pública sua primeira versão de um software de criptografia baseado em chave pública, o PGP (Pretty Good Privacy). O PGP se tornou rapidamente popular, por ser um freeware (gratuito), e é usado largamente por Internautas. Para saber mais sobre o PGP, visite o site http://www.pgpi.com que oferece, além de FAQs, softwares PGP gratuitos para os mais variados sistemas operacionais, inclusive o Windows 95.

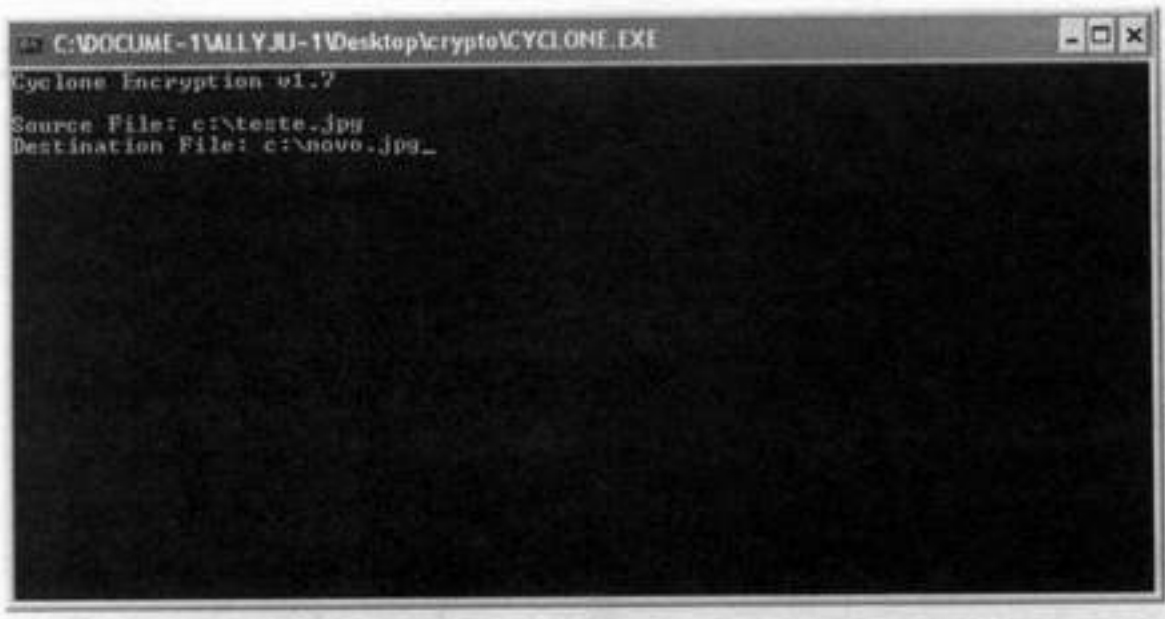
Existem diversos programas para criptografia, será apresentado o *Cyclone*, um software nacional, fácil de usar e todo em português. Acompahe, nos passos a seguir, como criptografar e descriptografar um arquivo:

Execute o arquivo *cyclone.exe*, uma tela do *MS-DOS* será aberta, digite o caminho completo do arquivo que deseja criptografar no campo *Source File* e, então, pressione a tecla *Enter*.

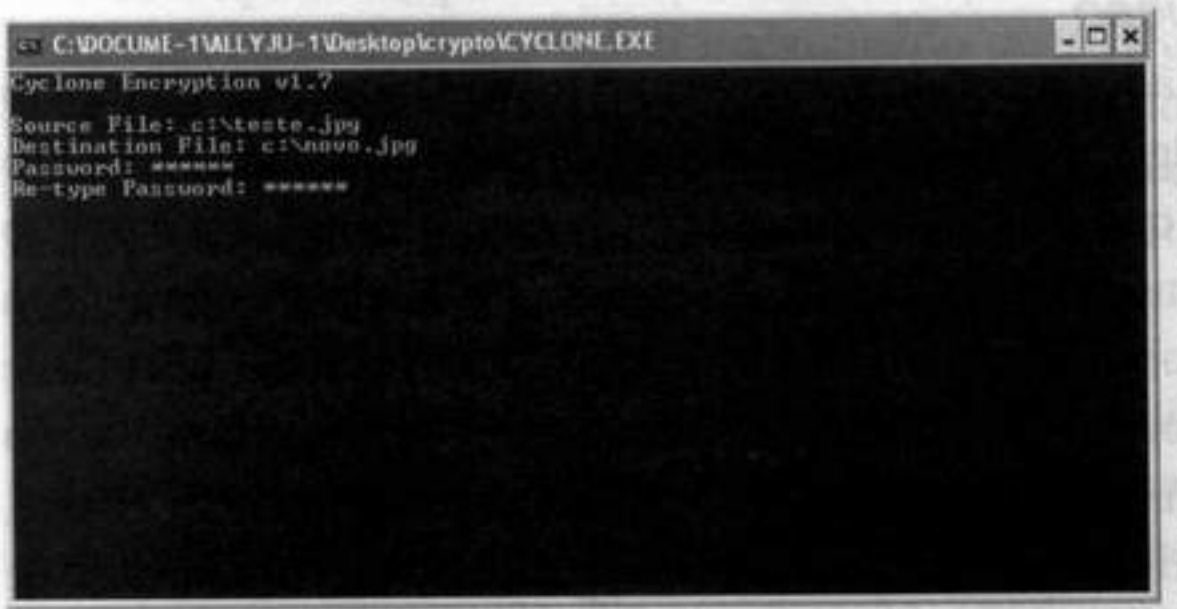
Como exemplo, vamos criptografar o arquivo teste.jpg (arquivo de imagem), mas lembrando o cyclone criptografa qualquer tipo de arquivo, poderia ser um arquivo do Word, Power Point, Note Pad etc.



No campo *Destination File*, digite o caminho completo de onde o arquivo criptografado será salvo. Nesse exemplo, o arquivo será salvo na raiz do C:\ com o mesmo nome e extensão *jpg*, feito isso, tecle Enter.

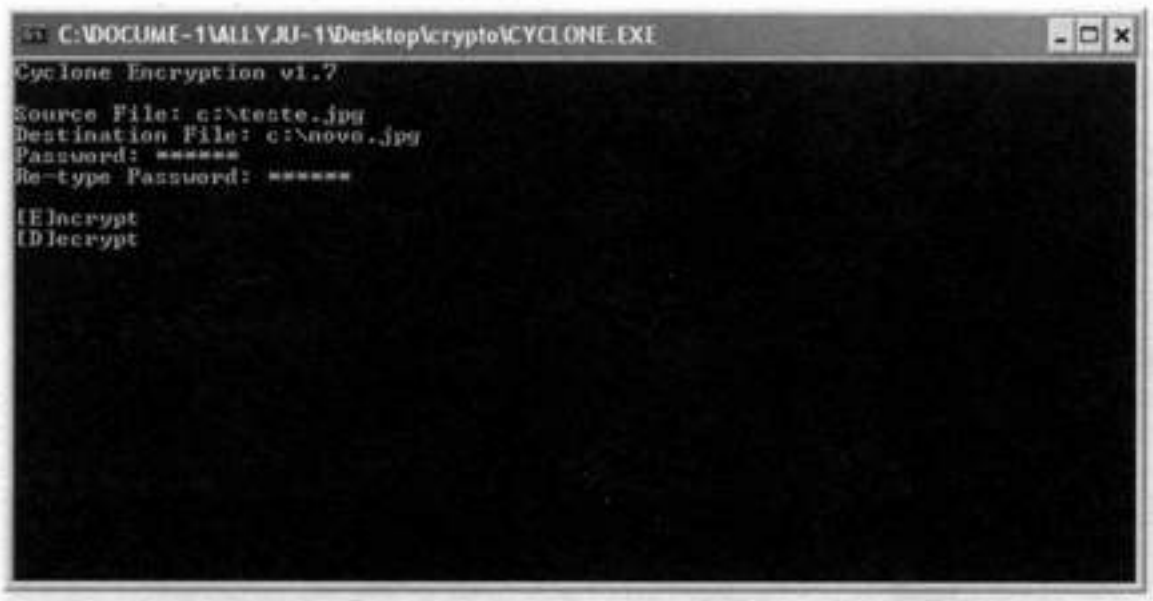


Na opção *Password*, digite uma senha para o arquivo, pressione *Enter* e a digite novamente em *Re-type Password*. Essa será a senha de criptografia do arquivo e, conseqüentemente, será utilizada para descriptografar o arquivo.



Feito todos os passos citados acima, pressione a tecla *E* se for criptografar ou *D* se estiver decriptografando.

OBS.: Você só pode descriptografar programas criptografados pelo programa crypto.



Esse programa passa arquivo a uma determinada pessoa sem que haja preocupação de violação do arquivo no trajeto.

3. Criptoanálise

3.1. Introdução

A criptoanálise consiste em estratégias matemáticas com o objetivo quebrar um algoritmo de criptografia. Como não há um meio matemático de se provar que esse algoritmo é ou não seguro, então, ele é seguro até que se consiga decodificá-lo. A segurança é válida até que alguém consiga descobrir um método de decodificação. A grande dificuldade que um criptoanalista encontra ao tentar quebrar um algoritmo está no número de chaves que este utiliza. Quanto maior o número de chaves, maior a dificuldade de se conseguir obter sucesso na criptoanálise de um determinado sistema. Um sistema que não se consegue quebrar é conhecido como sistema de segurança perfeita. Para se chegar per[illegible]le um sistema de segurança perfeito, é necessário que o número de chaves seja maior do que o tamanho do comprimento do texto legível e que a probabilidade de ocorrência de cada chave seja o mesmo. Um algoritmo que satisfaz essas condições é o *One-Time Pad*. Mas ele é inviá[illegible]le ser implementado, pois ainda não se sabe construir um gerador [illegible]ves realmente aleatória, o qual é necessário para que todas as chaves t[illegible]ham a mesma probabilidade de ocorrer.

3.2. Tipos de Ataque

3.2.1. Ataque por texto ilegível

Um ataque por texto ilegível ocorre quando algum criptoanalista consegue obter o texto legível simplesmente estudando o texto criptografado. Esse tipo de ataque consegue quebrar algoritmos baseados no método da monosubstituição (1 = 1+x, 2 = 2+x) e, atualmente, só serve para resolver problemas de desafios em revistas de palavra cruzadas. Usa-se, nesse tipo de ataque, a freqüência com que as letras ocorrem. Por exemplo, a letra "a" ocorre com mais freqüência na língua portuguesa, então, se no texto criptografado ocorrer mais a letra "b", pode-se deduzir que a letra "b" corresponde a letra "a".

3.2.2. Ataque por combinação

Esse tipo de ataque ocorre quando um criptoanalista consegue obter alguma parte do texto legível e alguma do texto ilegível. Com essas combinações, ele pode chegar a alguma conclusão do método criptográfico. Esse tipo de "ataque" é muito utilizado para resolver desafios de revistas de palavras cruzadas também.

3.2.3. Ataque por encriptação

Um criptoanalista, tendo acesso à chave de codificação, encripta um texto qualquer e utiliza o método da combinação para tentar descobrir algum texto encriptado. Ou então, pode-se utilizar uma espécie de comparação. Na comparação, encriptam-se vários textos aleatoriamente, comparando os textos encriptados. Vários "cracks" de senha utilizam essa técnica. Eles pegam um dicionário e encriptam cada palavra dele até encontrar algum que contenha o mesmo texto criptografado da senha desejada.

3.2.4. Conclusão

Esses são alguns dos métodos utilizados para se tentar descobrir alguma informação de um texto criptografado. Para se descobrir a chave utilizada, ou o algoritmo utilizado, há outros métodos de criptoanálise.

SSL

Primeiro vamos entender o conceito de *Sockets*, que na verdade são representações da conexão de um aplicativo com uma porta.

Com eles, podemos ter vários aplicativos conectados à mesma porta, cada um possuindo um Socket próprio. Os aplicativos, em sua grande maioria, abrem geralmente dois sockets, um Ativo e um Passivo. O ativo é usado para o envio de dados; o passivo, para o recebimento de dados. Geralmente, os *Sockets* são identificados pelo endereço IP da estação remota e o número da porta utilizada. Com a introdução do *Home Banking* e de transações comerciais na Internet, era necessária uma solução que não fragilizasse tanto o usuário, uma vez que os pacotes trafegados entre ele e o servidor podem ser facilmente lidos por qualquer um no caminho. Criou-se, então, o *SSL*. O conceito básico de *Secure Sockets Layer* e de transação criptografada, ou seja, seus dados são criptografados antes de saírem do computador e, ao chegarem do outro lado, são descriptografados. Acontece que essa criptografia utilizada, é considerada "fácil" de se quebrar, o problema é que nem todo mundo tem condição de quebrá-la, pois seria necessário um poder computacional razoável para tal.

Quanto aos riscos de se fazer compras na Internet, consideraremos um site no qual você envie o seu número do cartão de crédito sem criptografia alguma. Lógico que qualquer um pode pegar esse número, mas essa pessoa deve estar no lugar certo, na hora certa e pegar o pacote correto para possuir o número do seu cartão de crédito. Numa transação "segura", utilizando SSL, além de tudo já descrito, a pessoa ainda deve conseguir descriptografar o pacote, o que levaria um bom tempo para ser feito em um PC doméstico. Se o site onde você for comprar for muito visitado e possuir um movimento grande, fica mais difícil ainda ser você o "escolhido". Em resumo: "Compre na Internet, é rápido, fácil, cômodo e 'tecnicamente seguro'!" (Alberto Cozer).

CAPÍTULO 3

PESQUISA DE INFORMAÇÃO

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

Para invadir uma máquina ou servidor, é necessário o IP correspondente a essa máquina. Neste capítulo, serão apresentados alguns dos métodos usados por hackers para conseguir o ip de suas vítimas.

Descobrindo IP de um Website

Para invadir o servidor de determinado site, deve-se primeiro buscar seu endereço IP. Neste exemplo, descobriremos o IP do domínio *www.google.com.br*. Uma maneira mais fácil é acessar o serviço do site *www.netcraft.com* e anotar as informações que serão apresentadas. Logo após, acesse o netcraft, vá ao campo de texto abaixo de *Webserver Search*, digite o domínio que deseja obter as informações e clique em *Search*, a resposta obtida será a mostrada no quadro abaixo. No item *OS*, é informado o sistema operacional usado pelo servidor; no campo server, o servidor *Web* que está sendo usado; em *Last changed*, a última modificação realizada no servidor; em *IP address*, o tão desejado número IP.

Os Web Server and Hosting History for www.google.com.br				
OS	Server	Last changed	IP address	Netblock Owner
Linux	GWS/2.1	9-Oct-2003	216.239.41.99	Google Inc.
unknown	GWS/2.1	8-Oct-2003	216.239.59.99	Google Inc.
Linux	GWS/2.1	16-Sep-2003	216.239.59.99	Google Inc.
unknown	GWS/2.1	30-Aug-2003	216.239.59.99	Google Inc.
Linux	GWS/2.1	29-Aug-2003	216.239.53.99	Google Inc.
unknown	GWS/2.1	28-Aug-2003	216.239.59.99	Google Inc.
Linux	GWS/2.1	17-Aug-2003	216.239.41.99	Google Inc.
unknown	GWS/2.1	16-Aug-2003	216.239.59.99	Google Inc.
Linux	GWS/2.1	10-Aug-2003	216.239.57.99	Google Inc.
unknown	GWS/2.1	9-Aug-2003	216.239.59.104	Google Inc.

Descobrindo IPs em chats

Os chats, ou bate-papos, é um dos serviços mais utilizados na Internet, perdendo só para o próprio correio eletrônico, o e-mail. Como chat, podemos citar salas de bate-papo, instant messengers, IRC, entre outros. Aqui você entenderá como agem os hackers para conseguir chegar até o endereço IP.

Salas de bate-papo

Para esse método funcionar, é necessário que o hacker esteja conversando somente com a vítima. Se o invasor estiver trocando mensagens com mais alguém, normalmente ele pedirá para as pessoas não enviarem mais mensagens a ele. O primeiro passo é mandar algumas mensagens em seqüência para a vítima, feito isso, o invasor acessa o prompt do *MS-DOS* e, então, digita: *arp -a* (arp espaço -a). Como resposta, vão aparecer alguns endereços IP, geralmente iniciados com 200.xxx.xxx.xxx. O primeiro IP que aparece é o do próprio chat, e normalmente o segundo é o da vítima para qual foram enviadas as mensagens em seqüência. Se o invasor tiver alguma informação da vítima como provedora, por exemplo, pode-se confirmar se o IP obtido com o método acima é o da vítima, digitando no prompt do *MS-DOS* o comando *tracert* mais o número de IP obtido acima, basta prestar atenção que a provedora aparecerá nesse comando.

Pegando IP em salas que aceitam imagens

Para pegar IP em chats que aceitam imagens geralmente utiliza-se um servidor Web, aqui será apresentado o servidor web *Xitami*. Nesse caso, a máquina da pessoa funcionará como um servidor WEB, veja como utilizá-lo, seguindo os passos abaixo:

1. A primeira etapa é instalar o programa, depois, deve-se procurar um arquivo de imagem (preferível *gif* ou *jpg*). A seguir, é só inserir as imagens dentro da pasta *WebPages* dentro de *Xitami*.

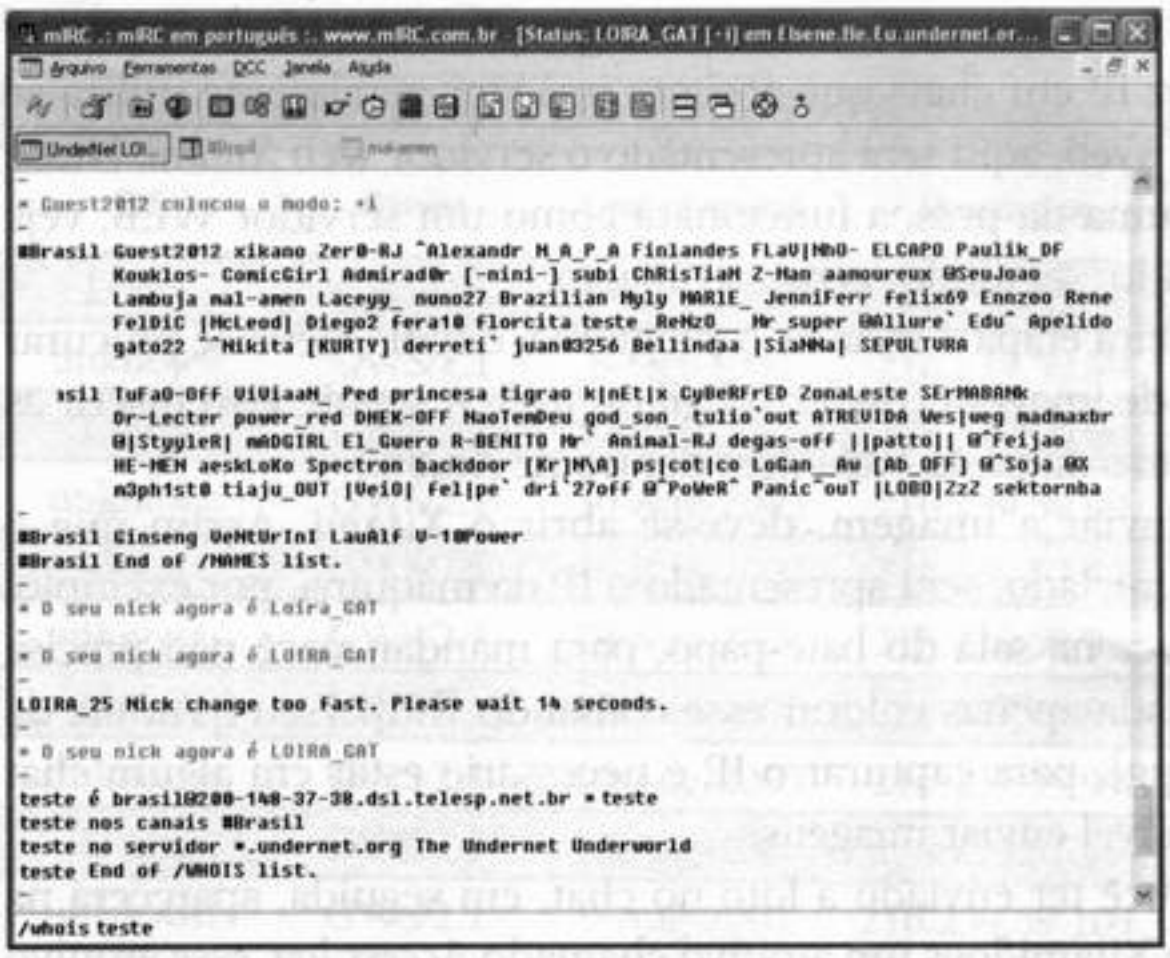
2. Para enviar a imagem, deve-se abrir o *Xitami*. Assim que o servidor for iniciado, será apresentado o IP da máquina, por exemplo, se você estiver na sala do bate-papo, para mandar, você não precisa fazer mais nada apenas colocar esse comando [http://seu ip/nome da foto.gif ou jpg], para capturar o IP, é necessário estar em algum chat que seja possível enviar imagens.

3. Após você ter enviado a foto no chat, em seguida, aparecerá na pasta raiz do Xitami/logs um arquivo chamado *Access.log*, esse arquivo (*Access.log*) aparece toda vez que um arquivo for enviado, nele vai conter o IP de todos da sala que acessarem este link.

IRC

Aqui será mostrado como é simples capturar IPs no *IRC*, veja como um hacker consegue seu objetivo em pouco tempo.

1. Execute um cliente de *IRC*, como o *mIRC*, acesse um servidor qualquer, depois, entre em uma sala. Dentro da sala, escolha a vítima, vá até a janela de status do servidor, mostrada na imagem abaixo, e digite no campo de comando o comando /whois o nickname da pessoa da qual você quer o ip. Por exemplo: Quero saber o ip do usuário teste. No campo de texto, digite o comando /whois teste. A resposta retornada é o IP da vítima. Nesse caso, o IP aparece logo após o sinal @ 200-148-37-38. Caso o IP esteja oculto (0), você pode tentar se conectar a outro servidor que não mascara o número.



Outra maneira é partir para a engenharia social, como veremos a seguir.

Descobrir IP por engenharia social

No IRC, para conseguir o *IP* de alguém no próprio *IRC*, dependendo do caso, é mais fácil do que utilizar ferramentas de busca por *IP*. A idéia é a seguinte, se você quer o *IP* de um homem, acesse com um nick feminino, puxe conversa com a vítima e peça para que ela solicite *DCC CHAT* chat para você. Pronto! O IP da pessoa aparecá na tela *status* quando ele te envia a solicitação de chat.

Essa é uma maneira de se conseguir o *IP* de alguém, é o modo mais utilizado por hackers, no *IRC*, basta o usuário abrir alguma conexão direta com o invasor para saber seu *IP*, nesse caso citamos um *DCC CHAT*, mas pode-se conseguir conexão direta pelo envio de imagens, arquivos etc.

Uma outra técnica que funciona em qualquer situação é você ganhar a confiança da vítima e pedir para que ela lhe envie um e-mail. Em um e-mail, é possível pegar as informações referentes ao servidor de envio e, em alguns casos, ao próprio IP da máquina.

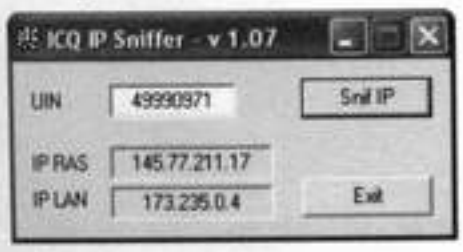
Aqui será apresentado como capturar o *IP* da vítima utilizando como cliente de e-mail o *Outlook express*, que é um dos clientes de e-

mail mais utilizados no *Windows*. Mas essa busca é válida em qualquer cliente de correio eletrônico, basta visualizar as propriedades da mensagem.

No Outlook, proceda da seguinte maneira: Clique, com o botão direito, sobre a mensagem e, a seguir, vá em *Propriedades* e *Detalhes*. Note que agora é possível visualizar um quadro parecido com a tela mostrada a seguir. Nesse caso, o *IP* da vítima fica na linha: *Received: from unknown (HELO chris) (christiane@xxxxx.xxxx.xxx@200.xxx.xx.xx)*, e, nesse caso, é 200.xxx.xx.xx, como podemos notar no final da linha.

Descobrindo um IP no icq 2000/2002

Para capturar um IP no icq 2000/2002, é necessário utilizar um sniffer, nesse caso, mostraremos no exemplo a utilização do *ICQ IP SNIFFER - v1.07*, que é uma das ferramentas preferidas para esse tipo de tarefa. Para iniciar, execute o *ICQ IP SNIFFER* e, no campo UIN, digite o UIN da vítima, depois, clique em *Snif IP*, no campo *IP RAS*, aparecerá o *IP* da vítima caso ela use a versão 2000 ou 2002 do *ICQ*.



O IP de uma máquina na mesma rede

Execute um programa de varredura de rede, como o *Shadowscan*, e clique na aba *Internet Scanner*, *Scanners*, depois, clique em *IP Scanner*, *IP Zone*, no campo *Starting IP*, coloque o primeiro *IP* da sua rede. Por exemplo, se seu *IP* é 192.168.1.11, coloque, no campo *Starting IP*, o *IP* 192.168.1.1 (primeiro *IP* da rede) e, no campo *Ending IP*, 192.168.1.255, assim o programa vai varrer toda sua rede. Para iniciar a varredura, clique em *Start scan*, agora, basta esperar o programa concluir a busca. Normalmente, os usuários colocam seus nomes em suas máquinas, se você quer o *IP* do usuário *DANIN*, basta você olhar o nome das maquinas na resposta retornada pelo scaneamento no campo *host*. Encontrado o nome, olhamos na mesma linha o campo IP, logo chegamos ao IP: 192.168.1.9. Não se esqueça de que isso só será válido se o invasor souber o nome da máquina que está buscando.

Capítulo 4

PROTEÇÃO

• Firewalls

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

1. Firewalls

Em redes de computadores, firewalls são barreiras interpostas entre a rede privada e a rede externa com a finalidade de evitar intrusos (ataques); ou seja, são mecanismos (dispositivos) de segurança que protegem os recursos de hardware e software da empresa dos perigos aos quais o sistema está exposto. Esses mecanismos de segurança são baseados em hardware e software e seguem a política de segurança estabelecida pela empresa.

Basicamente, um firewall trabalha junto a um roteador ou a uma máquina responsável pelo roteamento. Assim, ele examina cada pacote de rede determinando qual é sua origem e seu destino. Geralmente, o firewall é instalado em uma máquina separada do restante da rede corporativa, dessa maneira cria-se uma barreira entre a rede interna e a rede externa.

2. Tipos de Firewall

2.1. Firewalls baseados em filtragem de pacotes

Para implementar uma barreira de segurança em uma rede de computadores, é fundamental que se conheça os detalhes dos protocolos de comunicação utilizados. Na Internet, a atenção deve ser voltada aos protocolos *IP*, *TCP*, *ICMP* e *UDP*. Esses são os principais

protocolos na rede e no transporte (*Modelo OSI*) que são considerados e examinados ao se estabelecer regras de filtragem em uma filtragem de pacotes para a Internet. Esse mecanismo de filtragem em roteador possibilita que se controle o tipo de tráfego de rede que pode existir em qualquer segmento de rede; conseqüentemente, pode-se controlar o tipo de serviços que pode existir no segmento de rede. Serviços que comprometem a segurança da rede podem, portanto, ser restringidos. Com o exposto acima, fica evidente que a filtragem de pacotes não se encarrega de examinar nenhum protocolo de nível superior em transporte, como por exemplo, o nível de aplicação que fica como tarefa dos *application gateways* (servidores proxy). Portanto, qualquer falha de segurança na camada de aplicação não pode ser evitada utilizando somente uma filtragem de pacotes, utilizam-se dispositivos alocados especificamente para essa função.

Dentre os baseados em filtragem de pacotes, existem os roteadores, que também são chamados de firewalls por hardware. Geralmente, ligados às duas redes em questão: a privada e a pública. Possuem a vantagem de se obter uma melhor proteção do que os baseados em software, além de poderem proteger mais de um sistema de cada vez. Outro ponto positivo dos firewalls baseados em hardware é que eles não afetam a performance do sistema, pois são independentes do sistema operacional. A desvantagem destes é que é necessário alocar mais energia e espaço na sua rede de computadores, que já pode estar saturada, além de tenderem a ser soluções mais caras que dos baseados em software.

2.2. Firewalls baseados em aplicações

Os firewalls baseados em aplicações, trabalham como um intermediador nas comunicações entre duas redes, verificam as requisições provenientes de usuários remotos e bloqueiam ou não a sua utilização. O cliente e o servidor não conversam diretamente, o servidor proxy é intermediário da conexão e analisa de acordo com as regras definidas, a autorização para a conexão, permitindo ou bloqueando. Também chamados de *proxy servers*, eles podem filtrar pacotes na camada de aplicação do modelo OSI. Pacotes de entrada ou saída não podem acessar os serviços para o qual não haja proxy. Melhor explicando, esse tipo de firewall, que é configurado para ser um Web proxy, não permitirá nenhum ftp, gopher, telnet ou outro tipo de tráfego, porque ele examina

os pacotes na camada de aplicação e pode filtrar comandos específicos da aplicação, como http:post e get etc. Com isso, ele pode oferecer um alto grau de segurança, mas a um custo relativamente grande de desempenho, o que não ocorre com a filtragem de pacotes. Por exigir melhor desempenho do sistema, esse tipo de firewall é implementado em uma máquina em separado, cuja função primária é prover o serviço de proxy. Outro problema é que os firewalls não são transparentes aos usuários finais e requerem uma configuração manual para cada cliente.

3. Roteamento Dinâmico

Estabelecemos um roteamento dinâmico quando colocamos uma máquina entre duas ou mais sub-redes diferentes e quando necessário, há a livre passagem de pacotes entre elas. Vale lembrar que o roteamento só funcionará quando for feito entre sub-redes distintas. Não se pode colocar um roteador entre duas sub-redes iguais. O roteamento também é útil para diminuir o tráfego na rede como um todo, pois só deixa o pacote mudar de sub-rede se isso for realmente necessário. Para fazer o roteamento, o micro roteador deve possuir uma placa de rede configurada em cada sub-rede. Também deve-se informar em cada máquina quem será o micro responsável pelo roteamento. O nome técnico desse micro é *gateway*. No caso do esquema anterior, temos as seguintes situações:

Gateway para 10.0.0.1, 10.0.0.2 e 10.0.0.3: 10.0.0.10

Gateway para 172.20.0.1, 172.20.0.2 e 172.20.0.3: 172.20.0.10

É importante que, nos dois lados, todos os micros saibam quem é o seu gateway, pois, do contrário, os pacotes podem-se perder na ida ou na volta. Exemplo: A máquina 10.0.0.1 sabe que 10.0.0.10 é o seu gateway. A máquina 172.20.0.1 não sabe quem é o seu gateway. Um *ping* de 10.0.0.1 para 172.20.0.1 sairá de 10.0.0.1, passará por 10.0.0.10, seguirá por 172.20.0.10 e chegará em 172.20.0.1. Como o 172.20.0.1 não sabe quem é o seu gateway para a rede 10.0.0.0, não conseguirá responder. O ping vai morrer por *timeout*, acontecerá o *icmp echo request*, mas será impossível gerar o *icmp echo reply*.

Fazendo o roteamento dinâmico (Linux)

Para estabelecermos o roteamento dinâmico entre duas sub-redes, basta: inserir um micro com duas placas de rede entre as duas sub-redes, configurando cada placa de acordo com cada sub-rede; definir,

em cada máquina, de cada sub-rede, quem é o seu gateway; ativar o roteamento dinâmico via kernel.

Definindo o gateway

Para definirmos o gateway em cada cliente Linux, devemos editar o arquivo:/etc/sysconfig/network e inserir a linha: GATEWAY=ip_do_gateway. Em seguida, devemos reiniciar a rede:#/etc/rc.d/init.d/network restart.

Ativando o roteamento via kernel

O roteamento via kernel será ativado com o comando: #echo 1 > /proc/sys/net/ipv4/ip_forward

Esse roteamento será perdido se a rede (e, em conseqüência, a máquina) for reinicializada (#/etc/rc.d/init.d/network restart). Poderíamos inserir a regra no fim do arquivo /etc/rc.d/rc.local para que ela seja ativada a cada reinicialização do sistema. No entanto, um reinício da rede mataria o roteamento novamente. Uma forma de deixar a regra de roteamento permanentemente ativada, resistindo a qualquer tipo de reinicialização, seria a alteração do arquivo /etc/sysctl.conf:

net.ipv4.ip_forward = 1.

Os filtros Linux

O firewall, na maioria das vezes, atua como um roteamento dinâmico controlado. É uma atividade interna, uma propriedade, do kernel. São os seguintes os filtros existentes:

kernel 2.0.x: ipfwadm
kernel 2.2.x: ipchains
kernel 2.4.x: iptables

Devemos ressaltar que, se o ipchains estiver ativo, o iptables não funcionará. Assim, no Red Hat, torna-se necessário entrar no #setup e: habilitar o iptables e desabilitar o ipchains. Se a distribuição utilizada não possuir o comando #setup, utilize o comando #rmmod ipchains.

Como funciona um firewall

O FILTRO DE PACOTES do Linux funciona mediante regras estabelecidas. Todos os pacotes entram no kernel para serem analisados. As *chains* (correntes) são as situações possíveis dentro do kernel. Quando um pacote entra no kernel, este verifica o destino do pacote e decide qual *chain* tratará do pacote, isso se chama roteamento interno. Os

tipos de *chains* dependerão da tabela que se estiver utilizando no momento. Existem três tabelas possíveis:

1. *filter*: é a tabela default (padrão). Quando não especificarmos a tabela, a *filter* será utilizada. Refere-se às atividades normais de tráfego de dados, sem a ocorrência de *NAT*. Admite as *chains INPUT*, *OUTPUT* e *FORWARD*.

2. *NAT*: utilizada quando há *NAT*. Exemplo: Passagem de dados de uma rede privada para a Internet admite as *chains PREROUTING*, *OUTPUT* e *POSTROUTING*.

3. *mangle*: há referências de que ela é utilizada para alterações especiais em pacotes.

TABELAS

Tabela Filter

Vejamos o funcionamento da tabela *filter* (default) e as suas respectivas *chains*:

INPUT: utilizada quando o destino final é a própria máquina firewall.

OUTPUT: qualquer pacote gerado na máquina firewall e que deva sair para a rede será tratado pela chain *OUTPUT*.

FORWARD: qualquer pacote que atravessa o firewall, oriundo de uma máquina e direcionado a outra, será tratado pela chain *FORWARD*.

Regras de firewall

As regras (rules) de firewall geralmente são compostas assim:

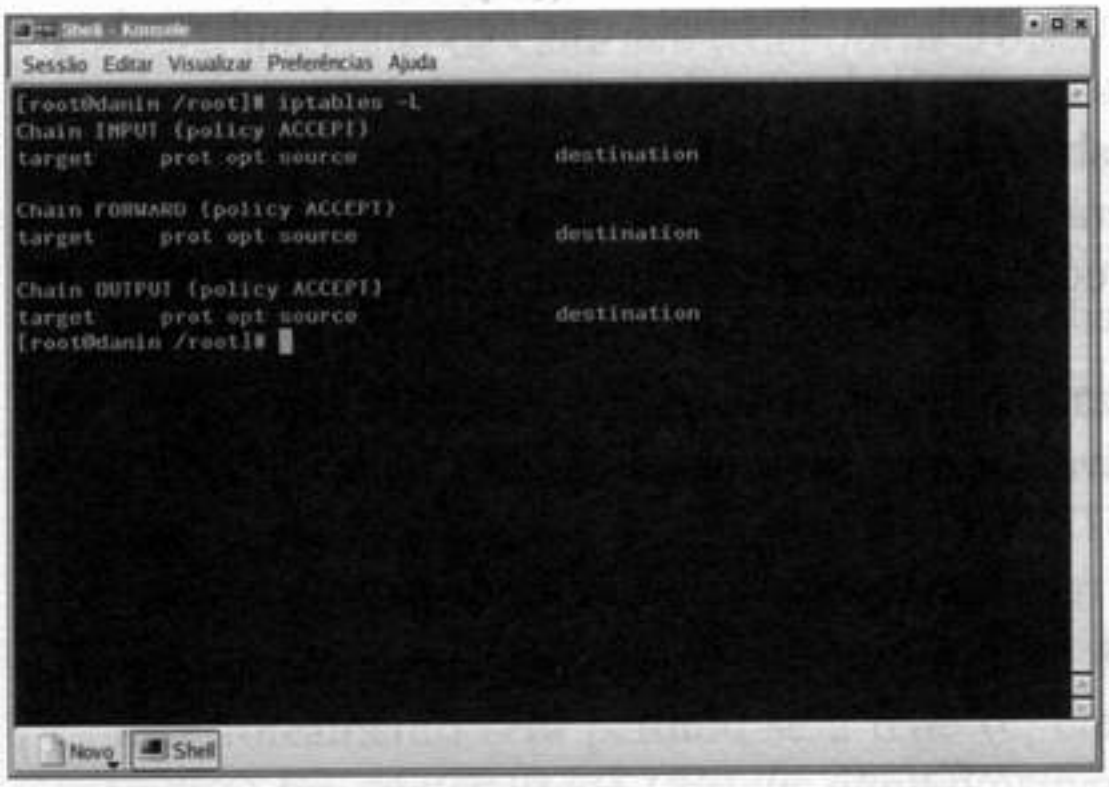
#iptables [-t tabela] [opção] [chain] [dados] -j [ação]

Existem outras possibilidades que fogem à sintaxe mostrada anteriormente. É o caso do comando #iptables -L, que mostra as regras em vigor.

Primeiramente, vamos listar as regras inseridas no firewall, para isso, utilize o seguinte comando #iptables -L.

E confira o resultado desse comando, que lista todas as regras existentes.

Observe que, com o #iptables, temos de inicialmente proibir todos os tipos de passagem pelo firewall. Assim, ao invés de iniciar com todas as portas fechadas (ou rotas), o Linux inicia com todas abertas. Então, o que devemos fazer é bloquear tudo no firewall e, em seguida, liberar gradativamente o que será necessário para nossa melhor segurança.

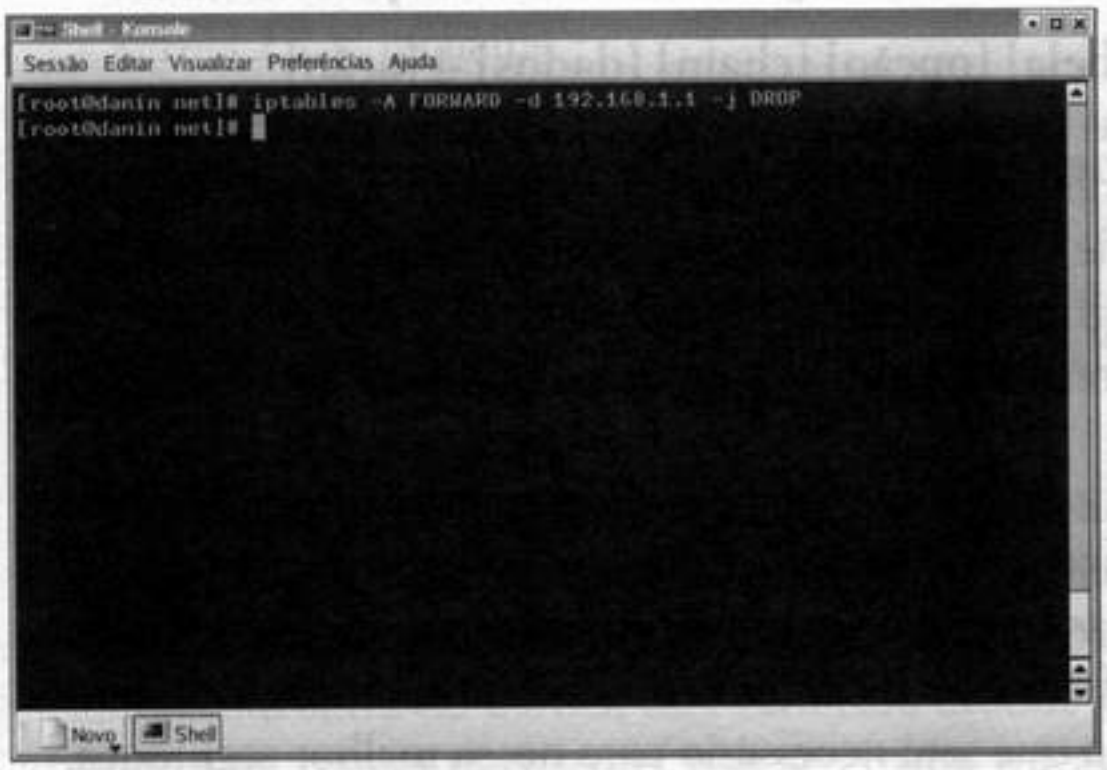


Isso significa que o nosso firewall ainda não possui nenhuma regra adicionada.

#iptables -A FORWARD -d 192.168.1.1 -j DROP

Agora, vamos adicionar uma regra que determina que todos os pacotes destinados à máquina 192.168.1.1 devem ser descartados. No caso:

tabela: filter
opção: -A
chain: FORWARD
dados: -d 192.168.1.1
ação: DROP.



Para confirmar a nova regra adicionada, use novamente o comanado #iptables -L e observe as mudanças.

```
[root@danin net]# iptables -A FORWARD -d 192.168.1.1 -j DROP
[root@danin net]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             192.168.1.1

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin net]#
```

A seguir, alguns comandos básicos para configuração de um firewall utilizando o iptables. Algumas palavras, que são parâmetros para o iptables, expressam por si só o que deve ser feito. FORWARD significa encaminhar, é um comando muito usado. DROP significa descartar, ou seja, impede a passagem de pacotes. ACCEPT já é o contrário, significa aceitar a passagem de pacotes.

#iptables -F

Apaga todas as regras sem alterar a política.

#iptables -P FORWARD DROP

Estabelece uma política de proibição inicial de passagem de pacotes entre sub-redes.

#iptables -A FORWARD -j DROP

Todos os pacotes oriundos de qualquer sub-rede e destinados a qualquer sub-rede deverão ser descartados.

#iptables -A FORWARD -j ACCEPT

Todos os pacotes oriundos de qualquer sub-rede e destinados a qualquer sub-rede deverão ser aceitos.

#iptables -A FORWARD -s 10.0.0.0/8 -d www.icq.com -j DROP

Os pacotes oriundos da sub-rede 10.0.0.0 (máscara 255.0.0.0) e destinados ao host www.icq.com deverão ser descartados. Nesse exem-

plo, estamos impedindo que um usário da nossa rede interna acessa o site em questão.

```
Sessão Editar Visualizar Preferências Ajuda
[root@danin net]# iptables -A FORWARD -s 10.0.0.0/8 -d www.icq.com -j DROP
[root@danin net]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             192.168.1.1
DROP       all  --  10.0.0.0/8           icqwww-m01.icq.aol.com
DROP       all  --  10.0.0.0/8           icqwwp-m01a.icq.aol.com

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin net]#
```

#iptables -A FORWARD -s 10.0.0.0/8 -d www.icq.com -j REJECT

Os pacotes oriundos da sub-rede 10.0.0.0 (máscara 255.0.0.0) e destinados ao host www.icq.com deverão ser descartados. Deverá ser enviado um ICMP avisando a origem.

```
Sessão Editar Visualizar Preferências Ajuda
[root@danin net]# iptables -A FORWARD -s 10.0.0.0/8 -d www.icq.com -j REJECT
[root@danin net]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             192.168.1.1
DROP       all  --  10.0.0.0/8           icqwww-m01.icq.aol.com
DROP       all  --  10.0.0.0/8           icqwwp-m01a.icq.aol.com
REJECT     all  --  10.0.0.0/8           icqwww-m01.icq.aol.comreject-with icmp-
port-unreachable
REJECT     all  --  10.0.0.0/8           icqwwp-m01a.icq.aol.comreject-with icmp
-port-unreachable

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin net]#
```

#iptables -A FORWARD -d www.icq.com -j DROP

Os pacotes oriundos de qualquer lugar e destinados ao host www.icq.com deverão ser descartados.

```
[root@danin net]# iptables -A FORWARD -d www.icq.com -j DROP
[root@danin net]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             192.168.1.1
DROP       all  --  10.0.0.0/8           icqwww-m01.icq.aol.com
DROP       all  --  10.0.0.0/8           icqwwp-m01a.icq.aol.com
REJECT     all  --  10.0.0.0/8           icqwww-m01.icq.aol.comreject-with icmp-
port-unreachable
REJECT     all  --  10.0.0.0/8           icqwwp-m01a.icq.aol.comreject-with icmp
-port-unreachable
DROP       all  --  anywhere             icqwwp-m01a.icq.aol.com
DROP       all  --  anywhere             icqwww-m01.icq.aol.com

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin net]#
```

#iptables -A FORWARD -d 10.0.0.0/8 -s www.icq.com -j DROP

Os pacotes destinados à sub-rede 10.0.0.0 (máscara 255.0.0.0) e oriundos do host www.icq.com deverão ser descartados.

```
[root@danin net]# iptables -A FORWARD -d 10.0.0.0/8 -s  www.icq.com -j DROP
[root@danin net]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             192.168.1.1
DROP       all  --  10.0.0.0/8           icqwww-m01.icq.aol.com
DROP       all  --  10.0.0.0/8           icqwwp-m01a.icq.aol.com
REJECT     all  --  10.0.0.0/8           icqwww-m01.icq.aol.comreject-with icmp-
port-unreachable
REJECT     all  --  10.0.0.0/8           icqwwp-m01a.icq.aol.comreject-with icmp
-port-unreachable
DROP       all  --  anywhere             icqwwp-m01a.icq.aol.com
DROP       all  --  anywhere             icqwww-m01.icq.aol.com
DROP       all  --  icqwww-m01.icq.aol.com  10.0.0.0/8
DROP       all  --  icqwwp-m01a.icq.aol.com  10.0.0.0/8

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin net]#
```

#iptables -A FORWARD -s www.icq.com -j DROP

Os pacotes oriundos do host www.icq.com e destinados a qualquer lugar deverão ser descartados.

```
Sessão Editar Visualizar Preferências Ajuda
[root@danin net]# iptables -A FORWARD -s  www.icq.com -j DROP
[root@danin net]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             192.168.1.1
DROP       all  --  10.0.0.0/8           icqwww-m01.icq.aol.com
DROP       all  --  10.0.0.0/8           icqwwp-m01a.icq.aol.com
REJECT     all  --  10.0.0.0/8           icqwww-m01.icq.aol.comreject-with icmp-
port-unreachable
REJECT     all  --  10.0.0.0/8           icqwwp-m01a.icq.aol.comreject-with icmp
-port-unreachable
DROP       all  --  anywhere             icqwwp-m01a.icq.aol.com
DROP       all  --  anywhere             icqwww-m01.icq.aol.com
DROP       all  --  icqwww-m01.icq.aol.com  10.0.0.0/8
DROP       all  --  icqwwp-m01a.icq.aol.com  10.0.0.0/8
DROP       all  --  icqwwp-m01a.icq.aol.com  anywhere
DROP       all  --  icqwww-m01.icq.aol.com  anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin net]#
Novo  Shell
```

#iptables -A FORWARD -s 200.221.20.0/24 -j DROP

Os pacotes oriundos da sub-rede 200.221.20.0 (máscara 255.255.255.0) e destinados a qualquer lugar deverão ser descartados. Com essa regra, estamos negando o acesso de uma determinada rede, assim podemos controlar nossas redes permitindo separá-las conforme a política de segurança da empresa.

```
Sessão Editar Visualizar Preferências Ajuda
[root@danin net]# iptables -A FORWARD -s 200.221.20.0/24 -j DROP
[root@danin net]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             192.168.1.1
DROP       all  --  10.0.0.0/8           icqwww-m01.icq.aol.com
DROP       all  --  10.0.0.0/8           icqwwp-m01a.icq.aol.com
REJECT     all  --  10.0.0.0/8           icqwww-m01.icq.aol.comreject-with icmp-por
t-unreachable
REJECT     all  --  10.0.0.0/8           icqwwp-m01a.icq.aol.comreject-with icmp-po
rt-unreachable
DROP       all  --  anywhere             icqwwp-m01a.icq.aol.com
DROP       all  --  anywhere             icqwww-m01.icq.aol.com
DROP       all  --  icqwww-m01.icq.aol.com  10.0.0.0/8
DROP       all  --  icqwwp-m01a.icq.aol.com  10.0.0.0/8
DROP       all  --  icqwwp-m01a.icq.aol.com  anywhere
DROP       all  --  icqwww-m01.icq.aol.com  anywhere
DROP       all  --  200-221-20-0.speedy.speedvol.com.br/24  anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin net]#
Novo  Shell
```

#iptables -A FORWARD -s 10.0.0.5 -p icmp -j DROP

Os pacotes icmp oriundos do host 10.0.0.5 e destinados a qualquer lugar deverão ser descartados.

```
[root@danin /root]# iptables -A FORWARD -s 10.0.0.5 -p icmp -j DROP
[root@danin /root]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             192.168.1.1
DROP       all  --  10.0.0.0/8           icqmm-m01.icq.aol.com
DROP       all  --  10.0.0.0/8           icqmp-m01a.icq.aol.com
REJECT     all  --  10.0.0.0/8           icqmm-m01.icq.aol.comreject-with icmp-por
t-unreachable
REJECT     all  --  10.0.0.0/8           icqmp-m01a.icq.aol.comreject-with icmp-po
rt-unreachable
DROP       all  --  anywhere             icqmp-m01a.icq.aol.com
DROP       all  --  anywhere             icqmm-m01.icq.aol.com
DROP       all  --  icqmm-m01.icq.aol.com  10.0.0.0/8
DROP       all  --  icqmp-m01a.icq.aol.com  10.0.0.0/8
DROP       all  --  icqmp-m01a.icq.aol.com  anywhere
DROP       all  --  icqmm-m01.icq.aol.com  anywhere
DROP       all  --  200-221-20-0.speedy.spnetuol.com.br/24  anywhere
DROP       icmp --  10.0.0.5             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin /root]#
```

#iptables -A FORWARD -i eth0 -j ACCEPT

Os pacotes que entrarem pela interface eth0 serão aceitos.

```
[root@danin /root]# iptables -A FORWARD -i eth0 -j ACCEPT
[root@danin /root]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             192.168.1.1
DROP       all  --  10.0.0.0/8           icqmm-m01.icq.aol.com
DROP       all  --  10.0.0.0/8           icqmp-m01a.icq.aol.com
REJECT     all  --  10.0.0.0/8           icqmm-m01.icq.aol.comreject-with icmp-por
t-unreachable
REJECT     all  --  10.0.0.0/8           icqmp-m01a.icq.aol.comreject-with icmp-po
rt-unreachable
DROP       all  --  anywhere             icqmp-m01a.icq.aol.com
DROP       all  --  anywhere             icqmm-m01.icq.aol.com
DROP       all  --  icqmm-m01.icq.aol.com  10.0.0.0/8
DROP       all  --  icqmp-m01a.icq.aol.com  10.0.0.0/8
DROP       all  --  icqmp-m01a.icq.aol.com  anywhere
DROP       all  --  icqmm-m01.icq.aol.com  anywhere
DROP       all  --  200-221-20-0.speedy.spnetuol.com.br/24  anywhere
DROP       icmp --  10.0.0.5             anywhere
ACCEPT     all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin /root]#
```

#iptables -A FORWARD -i ! eth0 -j ACCEPT

Os pacotes que entrarem por qualquer interface, exceto a eth0, serão aceitos.

```
Shell - Konsole
Sessão Editar Visualizar Preferências Ajuda
[root@danin /root]# iptables -A FORWARD -i ! eth0 -j ACCEPT
[root@danin /root]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             192.168.1.1
DROP       all  --  10.0.0.0/8           icqwww-m01.icq.aol.com
DROP       all  --  10.0.0.0/8           icqwwp-m01a.icq.aol.com
REJECT     all  --  10.0.0.0/8           icqwww-m01.icq.aol.comreject-with icmp-por
t-unreachable
REJECT     all  --  10.0.0.0/8           icqwwp-m01a.icq.aol.comreject-with icmp-po
rt-unreachable
DROP       all  --  anywhere             icqwwp-m01a.icq.aol.com
DROP       all  --  anywhere             icqwww-m01.icq.aol.com
DROP       all  --  icqwww-m01.icq.aol.com  10.0.0.0/8
DROP       all  --  icqwwp-m01a.icq.aol.com  10.0.0.0/8
DROP       all  --  icqwwp-m01a.icq.aol.com  anywhere
DROP       all  --  icqwww-m01.icq.aol.com  anywhere
DROP       all  --  200-221-20-0.speedy.speedusl.com.br/24  anywhere
DROP       icmp --  10.0.0.5             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin /root]#
Novo  Shell
```

#iptables -A FORWARD -s 10.0.0.5 -p tcp –sport 80 -j LOG

O tráfego de pacotes TCP oriundos da porta 80 do host 10.0.0.5 e destinados a qualquer lugar deverá ser gravado em log. No caso, /var/log/messages.

```
Shell - Konsole
Sessão Editar Visualizar Preferências Ajuda
[root@danin log]# iptables -A FORWARD -s 10.0.0.5 -p tcp --sport 80 -j LOG
[root@danin log]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             192.168.1.1
DROP       all  --  10.0.0.0/8           icqwww-m01.icq.aol.com
DROP       all  --  10.0.0.0/8           icqwwp-m01a.icq.aol.com
REJECT     all  --  10.0.0.0/8           icqwww-m01.icq.aol.comreject-with icmp-por
t-unreachable
REJECT     all  --  10.0.0.0/8           icqwwp-m01a.icq.aol.comreject-with icmp-po
rt-unreachable
DROP       all  --  anywhere             icqwwp-m01a.icq.aol.com
DROP       all  --  anywhere             icqwww-m01.icq.aol.com
DROP       all  --  icqwww-m01.icq.aol.com  10.0.0.0/8
DROP       all  --  icqwwp-m01a.icq.aol.com  10.0.0.0/8
DROP       all  --  icqwwp-m01a.icq.aol.com  anywhere
DROP       all  --  icqwww-m01.icq.aol.com  anywhere
DROP       all  --  200-221-20-0.speedy.speedusl.com.br/24  anywhere
DROP       icmp --  10.0.0.5             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
LOG        tcp  --  10.0.0.5             anywhere          tcp spt:www-http LOG le
vel warning

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin log]#
Novo  Shell
```

#iptables -A FORWARD -p tcp –dport 25 -j ACCEPT

Os pacotes TCP destinados à porta 25 de qualquer host deverão ser aceitos.

```
Sessão Editar Visualizar Preferências Ajuda
[root@danin log]# iptables -A FORWARD -p tcp --dport 25 -j ACCEPT
[root@danin log]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             192.168.1.1
DROP       all  --  10.0.0.0/8           icqmm-m01.icq.aol.com
DROP       all  --  10.0.0.0/8           icqmmp-m01a.icq.aol.com
REJECT     all  --  10.0.0.0/8           icqmm-m01.icq.aol.comreject-with icmp-por
t-unreachable
REJECT     all  --  10.0.0.0/8           icqmmp-m01a.icq.aol.comreject-with icmp-po
rt-unreachable
DROP       all  --  anywhere             icqmmp-m01a.icq.aol.com
DROP       all  --  anywhere             icqmm-m01.icq.aol.com
DROP       all  --  icqmm-m01.icq.aol.com  10.0.0.0/8
DROP       all  --  icqmmp-m01a.icq.aol.com  10.0.0.0/8
DROP       all  --  icqmmp-m01a.icq.aol.com  anywhere
DROP       all  --  icqmm-m01.icq.aol.com  anywhere
DROP       all  --  200-221-20-0.speedy.speedsul.com.br/24  anywhere
DROP       icmp --  10.0.0.5             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
LOG        tcp  --  10.0.0.5             anywhere           tcp spt:www-http LOG le
vel warning
ACCEPT     tcp  --  anywhere             anywhere           tcp dpt:smtp

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin log]#
Novo  Shell
```

```
Sessão Editar Visualizar Preferências Ajuda
[root@danin log]# iptables -A FORWARD -s 10.0.0.0/8 -d 172.20.0.0/16 -j ACCEPT
[root@danin log]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             192.168.1.1
DROP       all  --  10.0.0.0/8           icqmm-m01.icq.aol.com
DROP       all  --  10.0.0.0/8           icqmmp-m01a.icq.aol.com
REJECT     all  --  10.0.0.0/8           icqmm-m01.icq.aol.comreject-with icmp-por
t-unreachable
REJECT     all  --  10.0.0.0/8           icqmmp-m01a.icq.aol.comreject-with icmp-po
rt-unreachable
DROP       all  --  anywhere             icqmmp-m01a.icq.aol.com
DROP       all  --  anywhere             icqmm-m01.icq.aol.com
DROP       all  --  icqmm-m01.icq.aol.com  10.0.0.0/8
DROP       all  --  icqmmp-m01a.icq.aol.com  10.0.0.0/8
DROP       all  --  icqmmp-m01a.icq.aol.com  anywhere
DROP       all  --  icqmm-m01.icq.aol.com  anywhere
DROP       all  --  200-221-20-0.speedy.speedsul.com.br/24  anywhere
DROP       icmp --  10.0.0.5             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
LOG        tcp  --  10.0.0.5             anywhere           tcp spt:www-http LOG le
vel warning
ACCEPT     tcp  --  anywhere             anywhere           tcp dpt:smtp
ACCEPT     all  --  10.0.0.0/8           172.20.0.0/16

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin log]#
Novo  Shell
```

Regras de retorno

Para termos o total controle sobre as regras de nosso firewall, devemos prever o retorno. Assim, digamos que exista a seguinte situação:

#iptables -P FORWARD DROP

#iptables -A FORWARD -s 10.0.0.0/8 -d 172.20.0.0/16 -j ACCEPT.

Essas regras fecharam todo o FORWARD e, depois, abrimos da sub-rede 10.0.0.0 para a sub-rede 172.20.0.0. No entanto, não tornamos possível a resposta da sub-rede 172.20.0.0 para a sub-rede 10.0.0.0. O correto, então, seria:

#iptables -P FORWARD DROP

#iptables -A FORWARD -s 10.0.0.0/8 -d 172.20.0.0/16 -j ACCEPT

#iptables -A FORWARD -d 10.0.0.0/8 -s 172.20.0.0/16 -j ACCEPT

```
Shell - Konsole
Sessão  Editar  Visualizar  Preferências  Ajuda
[root@danin log]# iptables -P FORWARD DROP
[root@danin log]# iptables -A FORWARD -s 10.0.0.0/8 -d 172.20.0.0/16 -j ACCEPT
[root@danin log]# iptables -A FORWARD -d 10.0.0.0/8 -s 172.20.0.0/16 -j ACCEPT
[root@danin log]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
DROP       all  --  anywhere             192.168.1.1
DROP       all  --  10.0.0.0/8           icqmm-m01.icq.aol.com
DROP       all  --  10.0.0.0/8           icqmp-m01a.icq.aol.com
REJECT     all  --  10.0.0.0/8           icqmm-m01.icq.aol.comreject-with icmp-port
-unreachable
REJECT     all  --  10.0.0.0/8           icqmp-m01a.icq.aol.comreject-with icmp-por
t-unreachable
DROP       all  --  anywhere             icqmp-m01a.icq.aol.com
DROP       all  --  anywhere             icqmm-m01.icq.aol.com
DROP       all  --  icqmm-m01.icq.aol.com  10.0.0.0/8
DROP       all  --  icqmp-m01a.icq.aol.com  10.0.0.0/8
DROP       all  --  icqmp-m01a.icq.aol.com  anywhere
DROP       all  --  icqmm-m01.icq.aol.com  anywhere
DROP       all  --  200-221-20-0.speedy.speeduol.com.br/24  anywhere
DROP       icmp --  10.0.0.5             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
LOG        tcp  --  10.0.0.5             anywhere           tcp spt:www-http LOG lev
el warning
ACCEPT     tcp  --  anywhere             anywhere           tcp dpt:smtp
ACCEPT     all  --  10.0.0.0/8           172.20.0.0/16
ACCEPT     all  --  10.0.0.0/8           172.20.0.0/16
ACCEPT     all  --  172.20.0.0/16        10.0.0.0/8

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin log]#
```

Salvando e recuperando tudo

As regras iptables poderão ser salvas com o comando:

#iptables -save > arquivo

A recuperação poderá ser feita pelo comando:

#iptables -restore < arquivo

Um típico exemplo de carregamento de regras de iptables, após a inicialização do sistema, seria:

#echo 1 > /proc/sys/net/ipv4/ip_forward

#iptables-restore < /etc/firewall

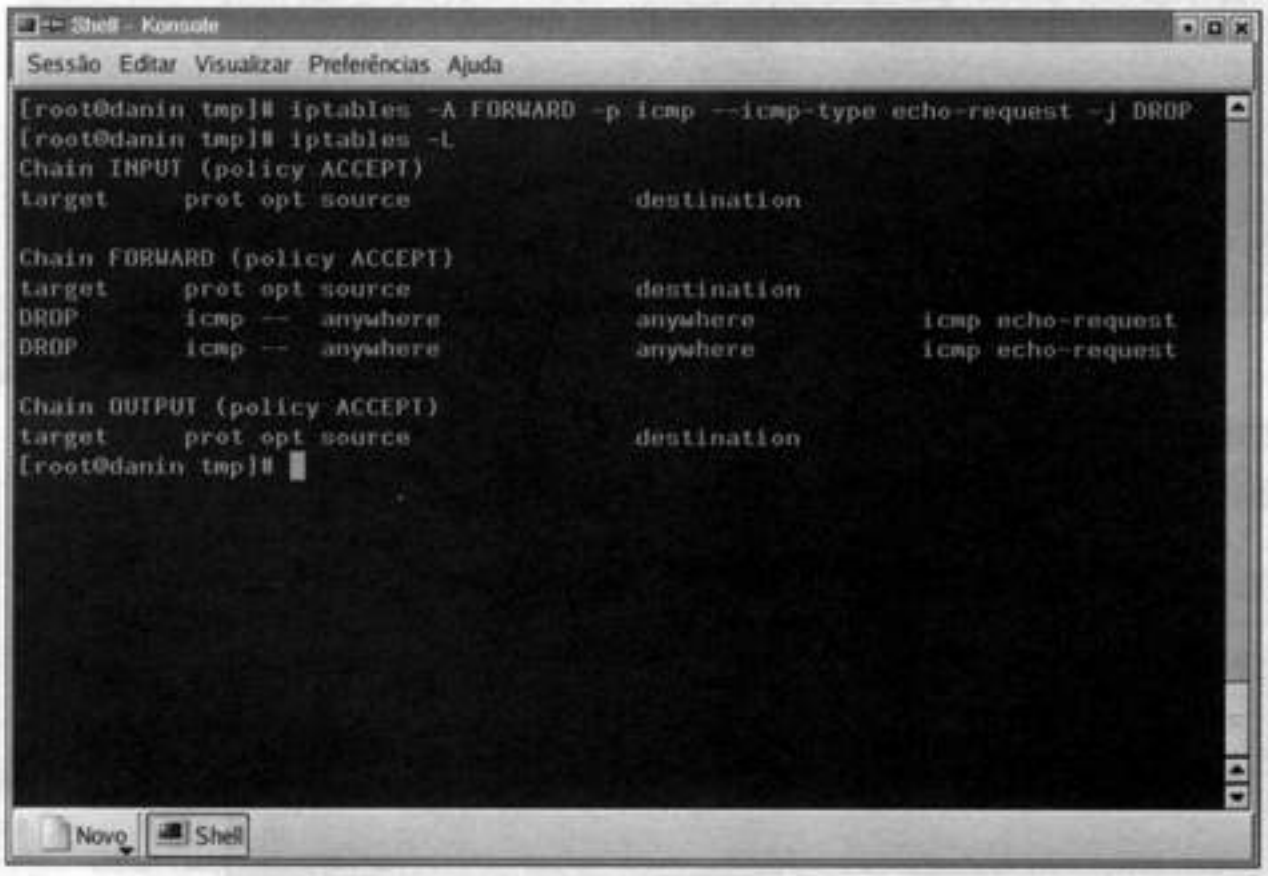
Isso pode ser inserido no fim do arquivo /etc/rc.d/rc.local.

Segurança Avançada

Existem maneiras específicas de se proteger contra-ataques de hacker, vamos agora dar alguns exemplos de regras que previnem alguns ataques comuns. Quando necessárias, devem ser as primeiras linhas do firewall. As mais importantes são:

Bloqueando Ping

#iptables -A FORWARD -p icmp --icmp-type echo-request -j DROP



Bloqueando Ping of Death

#iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT

```
Shell - Konsole
Sessão Editar Visualizar Preferências Ajuda
[root@danin tmp]# iptables -A FORWARD -p icmp --icmp-type echo-request -m limit
--limit 1/s -j ACCEPT
[root@danin tmp]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere            icmp echo-request
DROP       icmp --  anywhere             anywhere            icmp echo-request
ACCEPT     icmp --  anywhere             anywhere            icmp echo-request li
mit: avg 1/sec burst 5

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin tmp]#
Novo  Shell
```

Bloqueando ataques Syn-flood

#iptables -A FORWARD -p tcp -m limit --limit 1/s -j ACCEPT

```
Shell - Konsole
Sessão Editar Visualizar Preferências Ajuda
[root@danin tmp]# iptables -A FORWARD -p tcp -m limit --limit 1/s -j ACCEPT
[root@danin tmp]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere            icmp echo-request
DROP       icmp --  anywhere             anywhere            icmp echo-request
ACCEPT     icmp --  anywhere             anywhere            icmp echo-request li
mit: avg 1/sec burst 5
ACCEPT     tcp  --  anywhere             anywhere            limit: avg 1/sec bur
st 5

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin tmp]#
Novo  Shell
```

Bloqueando Port scanners

#iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST SYN -m limit --limit 1/s -j ACCEPT

```
Shell - Konsole
Sessão Editar Visualizar Preferências Ajuda
[root@danin /root]# iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST SYN -
m limit --limit 1/s -j ACCEPT
[root@danin /root]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp flags:FIN,SYN,RS
T,ACK/SYN limit: avg 1/sec burst 5

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@danin /root]#
Novo  Shell
```

Em todos os exemplos anteriores, adicionamos várias regras ao nosso firewall, porém, quando a máquina for reinicializada, perderemos todas as configurações. Temos duas opções nesse caso, uma delas é salvar o arquivo do firewall com o comando #iptables-save e, todas as vezes que ligarmos a máquina, teremos de recuperá-lo com o #iptables-restore. Ou, simplesmente, criamos um script que será executado junto com a inicialização da máquina, assim nossas regras estarão sempre funcionando. Para isso, dentro do diretório /etc/init.d/, crie um arquivo com o nome de "firewall" com o editor de textos "vi", executando os seguintes comandos:

#cd /etc/init.d
#vi firewall

```
Shell - Konsole
Sessão Editar Visualizar Preferências Ajuda
[root@danin /]# cd /etc/init.d
[root@danin init.d]# vi firewall
Novo  Shell
```

Digite todo o script como aqui descrito. Esse é apenas um exemplo com apenas algumas regras iniciais do nosso Firewall, com o passar do tempo, você adicionará as regras que lhe forem convenientes.

```
Shell - Konsole
Sessão Editar Visualizar Preferências Ajuda
#! /bin/sh
# descricao: Carregamento do Firewall
#
# chkconfig: 2345 80 30
# processname: iptables
# pidfile: /var/run/firewall.pid

. /etc/rc.d/init.d/functions
. /etc/sysconfig/network

if [ ${NETWORKING} = "no" ]
then
exit 0
fi

case "$1" in
  start)
      gprintf "Carregando as regras de Firewall do %s: " "Firewall"
      echo
      echo 1 > /proc/sys/net/ipv4/ip_forward

      /usr/sbin/iptables -t filter -P INPUT DROP
      /usr/sbin/iptables -t filter -A INPUT -j ACCEPT -i lo
      /usr/sbin/iptables -t filter -A FORWARD -j ACCEPT -m state \
--state ESTABLISHED, RELATED
      /usr/sbin/iptables -t filter -A INPUT -j ACCEPT -m state \
--state ESTABLISHED, RELATED
      /usr/sbin/iptables -t filter -A FORWARD -j ACCEPT -m state \
NEW -p tcp --dport http
      /usr/sbin/iptables -t filter -A FORWARD -j ACCEPT -m state \
NEW -p tcp --dport auth
      /usr/sbin/iptables -t filter -A FORWARD -j REJECT
      /usr/sbin/iptables -t nat -A POSTROUTING -j MASQUERADE -o ppp0
      /usr/sbin/iptables -t nat -A PREROUTING -j DNAT \
--to-dest 192.168.1.200 -i ppp0 -p tcp --dport 80

        ;;
"firewall" 56L, 1282C written                          1,1           Top
Novo  Shell
```

A seguir, o script na íntegra.

```
#! /bin/sh
# descricao: Carregamento do Firewall
#
# chkconfig: 2345 80 30
# processname: iptables
# pidfile: /var/run/firewall.pid

. /etc/rc.d/init.d/functions
. /etc/sysconfig/network

if [ ${NETWORKING} = "no" ]
then
exit 0
fi

case "$1" in
 start)
   gprintf "Carregando as regras de Firewall de %s: " "Firewall"
   echo
   echo 1 > /proc/sys/net/ipv4/ip_forward

   /usr/sbin/iptables -t filter -P INPUT DROP
   /usr/sbin/iptables -t filter -A INPUT -j ACCEPT -i lo
   /usr/sbin/iptables -t filter -A FORWARD -j ACCEPT -m state \
--state ESTABLISHED, RELATED
   /usr/sbin/iptables -t filter -A INPUT -j ACCEPT -m state \
--state ESTABLISHED, RELATED
   /usr/sbin/iptables -t filter -A FORWARD -j ACCEPT -m state \
NEW -p tcp --dport http
   /usr/sbin/iptables -t filter -A FORWARD -j ACCEPT -m state \
NEW -p tcp --dport auth
   /usr/sbin/iptables -t filter -A FORWARD -j REJECT
   /usr/sbin/iptables -t nat -A POSTROUTING -j MASQUERADE -
o ppp0
   /usr/sbin/iptables -t nat -A PREROUTING -j DNAT \
--to-dest 192.168.1.200 -i ppp0 -p tcp --dport 80
```

```
    ;;
stop)
gprintf "Interrompendo o Firewall de %s:" "Firewall"
echo
/usr/sbin/iptables -F
;;
*)
    gprintf "Uso: iptables (start|stop)"
    echo
;;
esac
exit 0
```

Capítulo 5

SENHAS

• Keylogger

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

A principal função de uma senha é guardar algo, por isso não deve ser escolhida de qualquer maneira, quanto mais fácil de ser descoberta, menos proteção terão seus dados. Neste capítulo, mostra-se como melhorar a segurança escolhendo senhas seguras e também mostra como, dependendo da senha, é fácil quebrá-la.

Senhas comuns e simples

Tratam-se daquelas senhas que qualquer um, sem muito esforço e com pouco conhecimento de informática, é capaz de quebrá-la. As senhas que dizemos serem fáceis de se quebrar são combinações utilizando nomes, datas, números, como placa de carro, telefone, documentos, e não é difícil alguém utilizar dados pessoais como senha. Aí mora o perigo! Uma pessoa mal-intencionada pode descobrir uma combinação em pouco tempo e, dependendo do que tiver acesso, pode atrapalhar muita coisa. Portanto, tente não utilizar senhas muito óbvias e guarde-as bem.

Nível de segurança

Nem todas as senhas têm o mesmo grau de importância, é muito comum a utilização de uma mesma senha em ambientes distintos. Imagine uma pessoa utilizar a mesma senha do banco para acessar um site de música ou mesmo e-mail. Muitas vezes deixa-se escapar esse tipo de informação, seja por digitar a senha em uma máquina que esteja com

um trojan, seja por digitar sem querer em uma tela errada. Uma vez que alguém saiba essa senha, pode-se tentar utilizá-la em outros ambientes que você utilize, como e-mail, acesso à sistema e mesmo uma conta bancária. Qual o problema? É simples: Se alguém descobrir a sua senha para um ambiente, terá em mãos a senha para todos os outros.

Não compartilhe

Não compartilhe com outras pessoas o nome de usuário e a senha de acesso a suas informações sensíveis. Mas, se por algum motivo isso for extremamente necessário, não envie os dados por e-mail, mesmo criptografados, também não os envie usando um telefone celular. Providencie, logo que possível, a troca da senha.

Métodos para criar senhas seguras

Usar os caracteres iniciais e finais: Uma forma de se criar uma senha longa e segura é você pensar em uma frase longa, e depois extrair o primeiro e último caractere de cada palavra. Exemplo: "ninguem acessa aqui" extraindo os caracteres iniciais e finais de cada palavra temos a seguinte senha: "nmaaai"

Somente os caracteres iniciais teríamos: "naa"

Somente os caracteres finais teríamos: "mai"

Caps Lock: Para se ter uma senha realmente segura é sugerido que a mesma seja composta de letras, números e ainda que as letras tenham uma combinação de maiúsculas e minúsculas. Alguns truques são usados para facilitar sua vida na hora de criar senhas desse tipo, todas as vogais maiúsculas e todas as consoantes minúsculas ou vice-versa.

Peguemos uma frase como exemplo: "hoje eu aprendi como criar senhas seguras com o hacker inside".

Siga a dica de pegar o primeiro e último caractere de todas palavras, conte todas elas e coloque no final de seus respectivos caracteres, o número de caracteres encontrados na mesma. Todas as vogais serão maiúsculas e todas consoantes minúsculas, seguindo o raciocínio, chegaríamos a seguinte senha:

he4eu2ai7co4cr5ss6ss7cm3o1hr6ie6

Claro, não exagere muito no tamanho das senhas, esse é somente um exemplo do que se pode fazer para criar uma boa senha. Tente utilizar de 8 a 12 caracteres.

Gerenciador de senhas: A profusão de senhas na internet e a dificuldade de lembrá-las e armazená-las com segurança abriram espaço para o surgimento de um novo tipo de aplicativo: o gerenciador de senhas. Dezenas dessas ferramentas podem ser encontradas em qualquer site de download na internet.

Um exemplo de senha gerada por um gerenciador de senhas é: "bl zNccm9Rp3rulEWMyv71rmxejRXcRNNi5hVvcitHtjzb1VfD7", essa senha possui 400 bits de criptografia, isso quer dizer que é praticamente impossível de se quebrar. Todas as nossas senhas deveriam ser iguais ou no mínimo parecidas com essa senha.

Como guardar: O aconselhado é memorizar as senhas e nunca registrá-las por escrito. Mas como a memória pode falhar, o mais seguro é anotá-las, mas obedecendo alguns critérios, como: anotar a senha de forma disfarçada, sem deixar claro que se trata de uma senha; outra forma é tentar escrevê-la de forma diferente do que realmente é, reordenando de uma maneira simples de lembrar depois. Caso contrário, se confundir com a ordem, sua senha tornará secreta até mesmo para você.

Para maior tranqüilidade, o melhor é colecionar esses dados em gerenciadores de senha.

Troca de senha periódica: Faça uma troca periódica de senhas mesmo que sua senha seja bastante robusta, pois, se algum Hacker estiver disposto a invadir seu micro, será só uma questão de tempo até ele quebrar sua senha. Uma troca freqüente de senha dificulta mais a invasão, já que o Hacker será constantemente obrigado a recomeçar do zero.

PGP

Quem quiser se aprofundar no estudo das senhas seguras acaba batendo nas portas da criptografia. Definida como a arte de proteger informações convertendo-as para um formato ilegível, a criptografia hoje é usada para proteger informações como dados de cartões de créditos, mensagens sigilosas de e-mail e documentos corporativos. Para essas tarefas, a ferramenta de criptografia mais conhecida é o Pretty Good Privacy (PGP), sistema desenvolvido pelo americano Philip Zimmerman. O PGP utiliza a chamada criptografia de chave pública, sistema que trabalha com duas chaves – uma que todos podem saber (a chave pública) e a outra, que só é

conhecida e usada pelo receptor de mensagens (a chave privada). O processo funciona assim: você, usuário do PGP, gera as duas chaves, a pública e a privada. A primeira você envia para todas as pessoas de quem espera receber mensagens. Essas pessoas usam essa chave pública para criptografar mensagens destinadas a você. Somente sua chave privada é capaz de decodificar os documentos. Assim, mesmo que as informações enviadas a você parem em outras mãos, não há possibilidade de alguém ter acesso a elas. Existem duas fontes para download do PGP. Americanos e Canadenses podem obtê-lo no site www.pgp.com, enquanto os residentes em outro países devem fazer o download da versão internacional em www.pgpi.org. Há versões do PGP para treze plataformas, entre as quais Windows, Unix, Mac e Palm OS.

Quebrando senhas: Uma das melhores e mais completa suíte de programas para a quebra de senhas é a da elcomsoft, que é a série Advanced, eles têm programas para a quebra de senha dos seguintes programas:

Arquivos compactados do tipo: ZIP/PkZip/WinZip, RAR/WinRAR, ACE/WinACE, ARJ/WinArj.

Programas da Microsoft: Word, Excel, Access, Outlook, PowerPoint, Project, Visio, VBA, Money, Mail, Schedule+, IE

Microsoft Word and Excel 97/2000

Corel WordPerfect Office: WordPerfect, QuattroPro, Paradox

Lotus SmartSuite (Organizer, WordPro, 1-2-3 and Approach)

Clientes de email (Microsoft Internet Mail And News, Eudora, TheBat!, Netscape Navigator/Communicator Mail, Pegasus mail, Calypso mail, FoxMail, Phoenix Mail, IncrediMail, @nyMail, QuickMail Pro, MailThem, Opera mail, Kaufman Mail Warrior, Becky! Internet Mail)

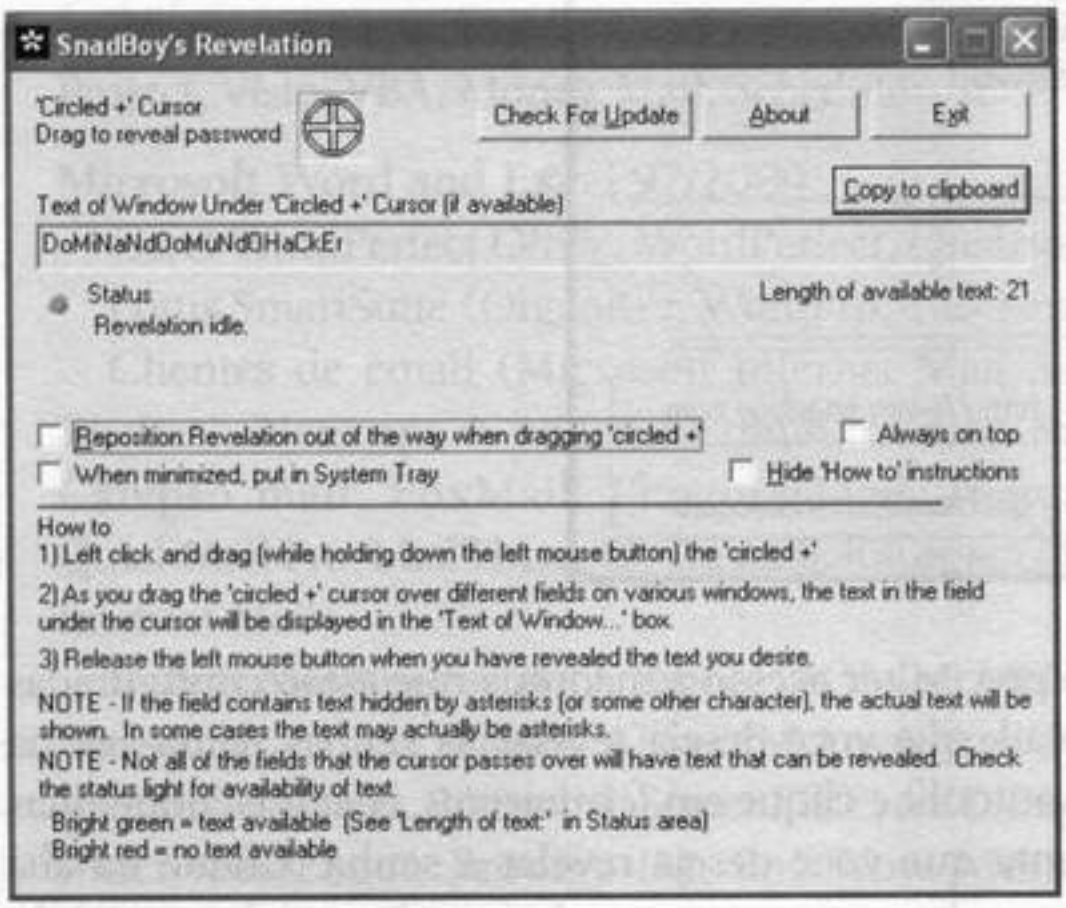
Instant Messengers (ICQ, Yahoo!, AOL IM, MSN Messenger, Excite Messenger, Odigo, Trillian, AT&T IM Anywhere, T-Online Messenger, Match Messenger, Praize IM, ScreenFIRE, ACD Express Comunicator, Imici Messenger, Prodigy IM, PowWow Messenger, Jabber IM, Kellster IM, PalTalk, Indiatimes messenger, Miranda, Tiscali, Ya.com Messenger, Rediff Bol, Sifty Buzz, Devil, Tencent QQ, &RQ, Ipswitch Instant Messenger, Eighth Wonder Catax, Simple Instant Messenger, Vista IM, GAIM, Global-IM).

Intuit Quicken, Quicken Lawyer and QuickBooks.

Você pode fazer o download da versão trial dos programas da elcomsoft acessando o site http://www.elcomsoft.com/, muitos hackers usam programas dessa empresa para descriptografar senhas dos softwares listados acima. Como a versão trial tem limitações, os Hackers costumam crackear esses programas usando sites como http://www.astalavista.box.sk, http://www.cracks.am/.

– **Senhas com máscaras**: Para pegar senhas de contas de email no Windows 95, 98, Me, 2000, NT ou XP, configuradas no Outlook, vamos usar o revelation, um programa usado para revelar máscaras usadas em campos do tipo senha.

Primeiro você precisa ter acesso à máquina que estão configuradas as contas de e-mail, que você deseja revelar as senhas. Uma vez na máquina, abra o outoolk e clique em *ferramentas*, *contas* e clique duas vezes sobre a conta que você deseja revelar a senha. Clique na aba *servidores*, feito isso, abra o programa *revelation*, clique sobre o círculo com uma cruz ao meio, mantenha o botão pressionado e passe a cruz sobre o campo que está a senha do *Outlook*, a senha será mostrada no campo *Text of Window Under 'Circled+' Cursor (if available)*.

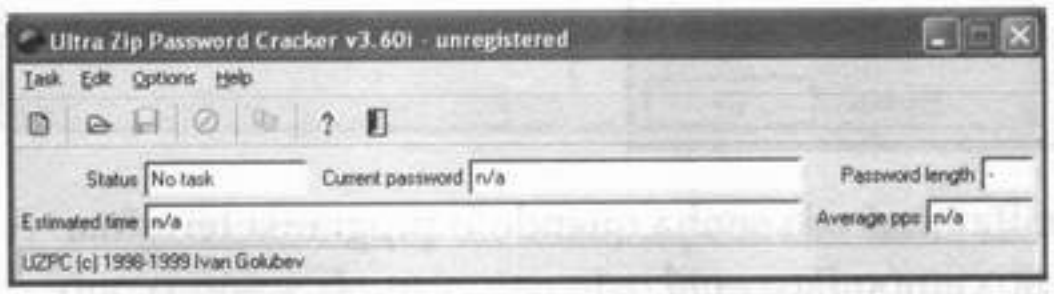


A senha dessa conta de E-mail é: DoMiNaNdOoMuNdOHaCkEr, como podemos ver esta não é uma senha muito fácil de ser quebrada por métodos como o brute force. É bom observarmos que o revelation

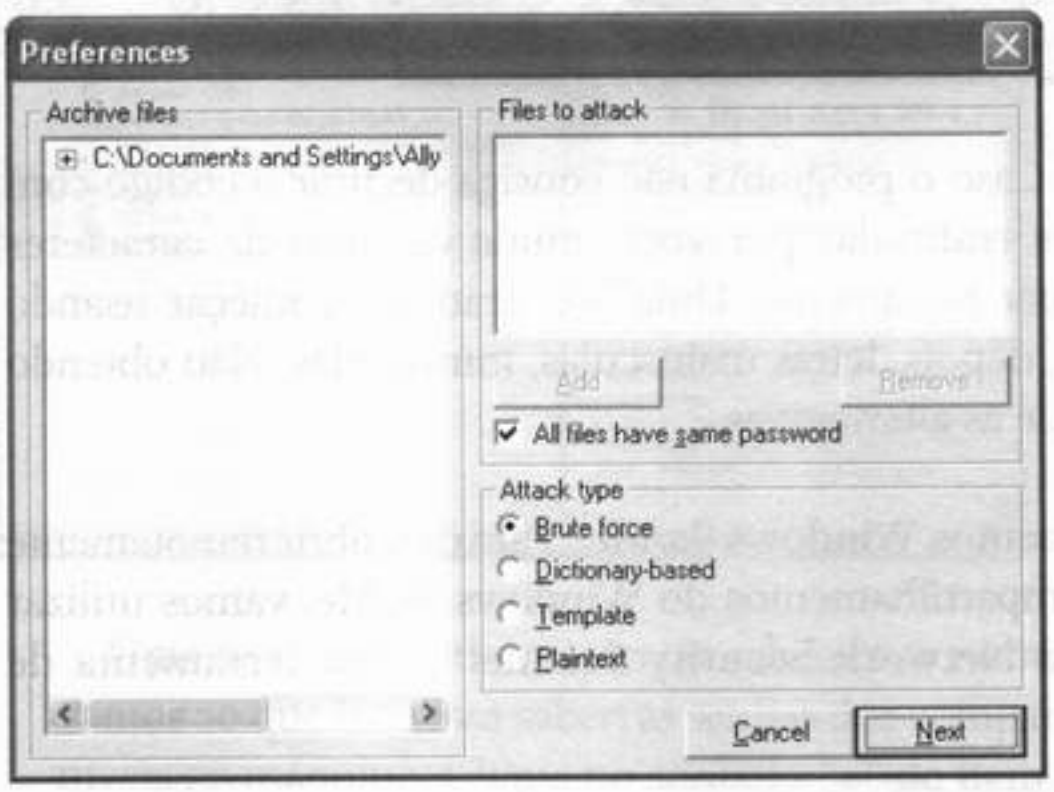
pode facilitar e muito nossa vida quando se trata de conseguirmos senhas cuja máquina esteja em nosso alcance, e a senha encontra-se com máscara de senha, como mostrado acima. Normalmente, quem possui conta no Hotmail configura o Outlook para ser seu cliente de e-mail, esse método revelaria a senha do Hotmail da pessoa sem nenhum problema.

– **Arquivos ZIP**: Para quebrar senhas de arquivos zip, vamos usar o Ultra Zip Password Cracker. Na sua versão não registrada, o máximo de caracteres que a senha pode ter é 5.

Primeiro execute o programa na tela mostrada abaixo, clique em task, new, selecione o arquivo zip que está com **senha** e clique em *Abrir*.

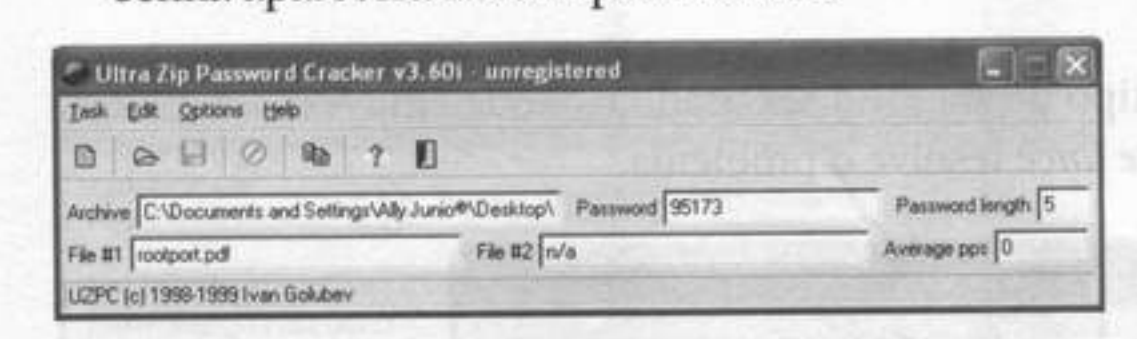


Selecione o tipo de ataque a ser usado e clique em *Next*, na maioria dos casos, *Brute force* resolve o problema.



Selecione os tipos de caracteres usados na senha, o tamanho mínimo e máximo da senha e clique em *Go*.

Aguarde o deciframento da senha quando o programa terminar. A senha aparecerá no campo *Password*.

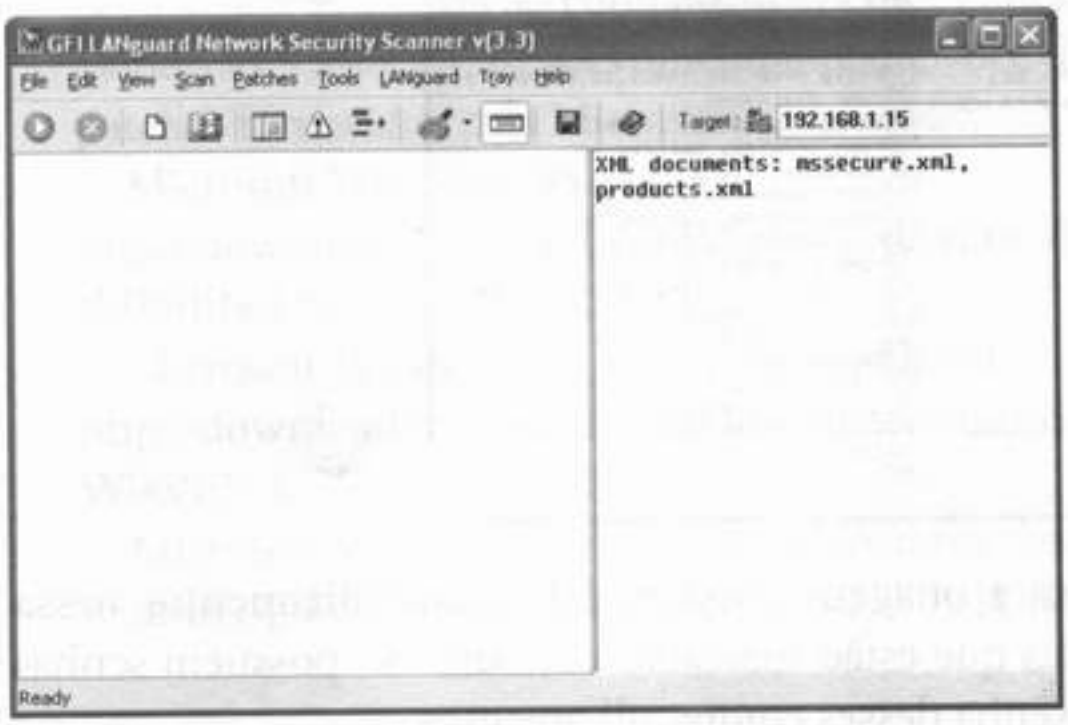


Observações: Caso o programa não consiga decifrar o código com as configurações realizadas por você, mude os tipos de caracteres usados para tentar novamente. Uma boa prática é começar usando somente dígitos, depois, letras maiúsculas, minúsculas. Não obtendo resultados, mescle as alternativas.

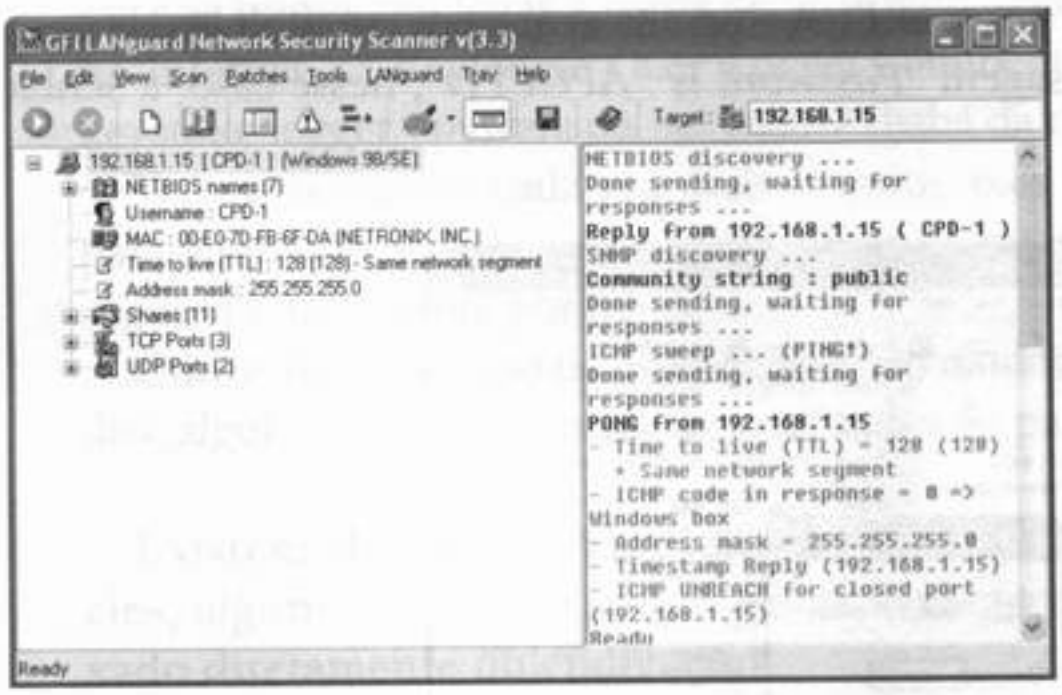
– **Compartilhamentos Windows 9x/Me** : Para descobrir remotamente senhas de compartilhamentos do Windows 9x/Me, vamos utilizar o "LANguard Network Security Scanner", uma ferramenta de auditoria.

Instale o programa, em seguida, execute-o e digite no campo "**Target:**" o número do IP da máquina que você pretende descobrir os recursos que estão sendo compartilhados. Supondo que a máquina-

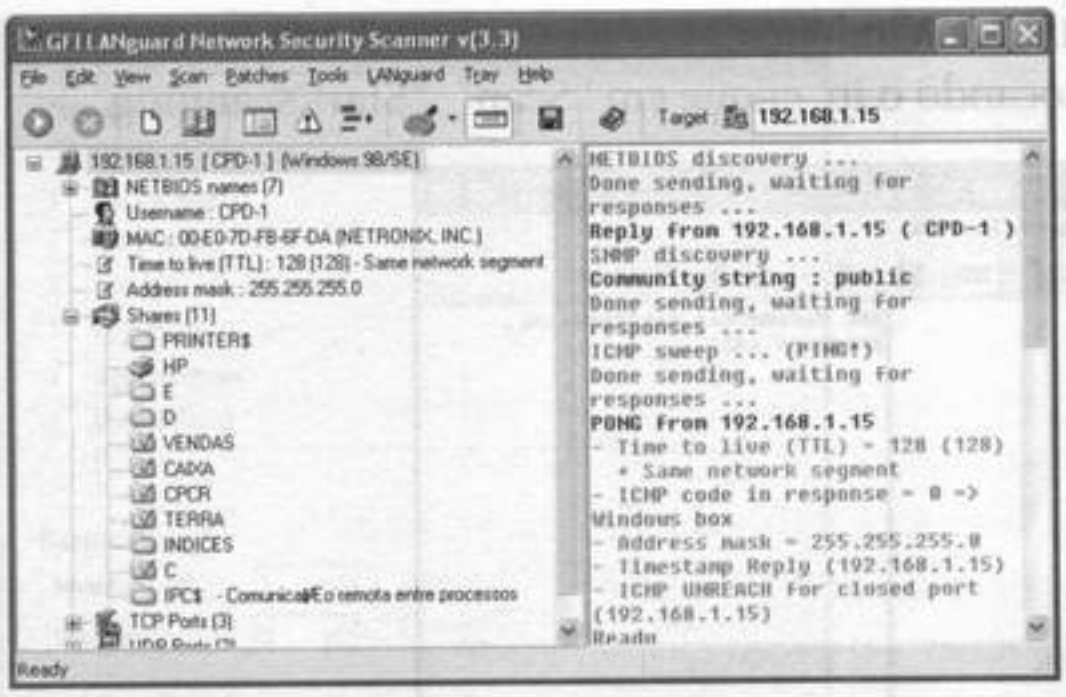
alvo seja uma estação Windows 98 SE com IP 192.168.1.15, digite: 192.168.1.15, colocando o ip, clique em "**Scan**", "**Start scanning**".



Após a execução do scan, a primeira linha do LANguard informa que o nome da máquina-alvo (Username) é "**CPD-1**" e que ela está rodando Windows 98/SE.

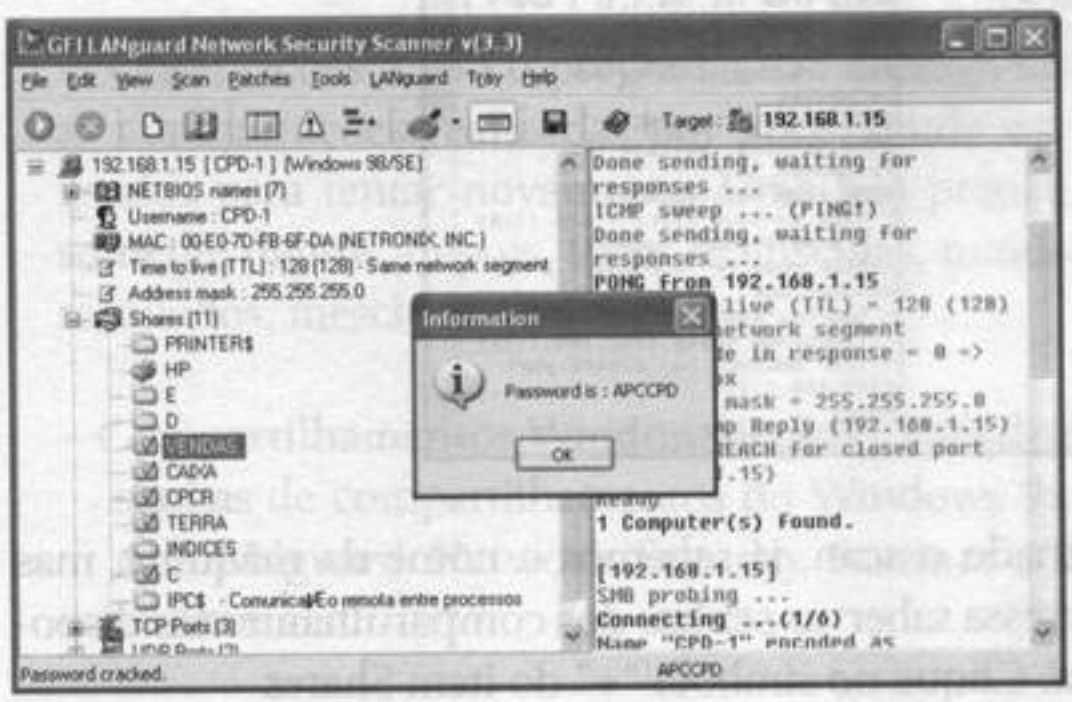


Uma vez terminado o scan, já sabemos o nome da máquina, mas vamos ao que interessa saber: as senhas dos compartilhamentos disponíveis na máquina. Clique no símbolo "+" do item Shares



De acordo com a imagem, existem 10 compartilhamentos nessa máquina, as pastas que estão marcadas com um "v" possuem senhas para descobrir a senha desses compartilhamentos.

Ex.: Para descobrir a senha do compartilhamento VENDAS, selecione-o clicando sobre o compartilhamento com o botão esquerdo, depois de selecionado, clique sobre a pasta com o botão direito e selecione a opção *"Crack password"*. A resposta aparecerá em uma janela com a seguinte mensagem *"Password is : APCCPD"*, nesse caso, a senha é *APCCPD*.



Solução para o problema: Para corrigir esse problema, a Microsoft liberou um patch que elimina uma vulnerabilidade de segurança

que permite a um usuário malicioso acessar arquivos compartilhados pelo Windows 95, 98, 98 Second Edition e Windows ME sem conhecer a senha associada ao compartilhamento. Para proteger seu sistema Windows 95/98/ME dessa vulnerabilidade, você deve instalar um dos patches fornecidos pela Microsoft:

Microsoft Windows 95
http://download.microsoft.com/download/win95/Update/11958/W95/EN-US/273991USA5.EXE

Microsoft Windows 98 and 98 Second Edition
http://download.microsoft.com/download/win98SE/Update/11958/W98/EN-US/273991USA8.EXE

Microsoft Windows Mehttp://download.microsoft.com/download/winme/Update/11958/WinMe/EN-US/273991USAM.EXE

Keylogger

Espionagem - Keylogger

O Keylogger é um software ou um hardware que captura as conversas e as transações feitas a partir de uma rede, seja ela local ou mesmo na Internet. O Keylogger (Key Logger) também é conhecido como keystoke logger, spyware ou net nanny (babá da net).

Vem-se tornando cada vez mais comum, pais instalam keyloggers para terem um melhor controle dos filhos na Internet, já que não conseguem estar sempre por perto.

Outros fãs desse tipo de espionagem são namorados, esposas, maridos, alguém querendo controlar as atitudes do parceiro na Internet.

Existem diversos keyloggers disponíveis na Internet, dentre eles, alguns freeware, como o *Home keylogger*, que pode ser baixado diretamente no endereço:

http://www.hackerinside.com.br/

Como utilizar o programa

Logo que o programa for instalado, será apresentado um ícone no System Tray (barra inferior do windows), isso significa que o programa está sendo executado e já está capturando tudo o que for digitado.

Para visualizar todo o conteúdo do log, basta clicar com o botão

esquerdo do mouse sobre o ícone e escolher a opção *View log*, será apresentada uma tela como esta:

```
Keylog.txt - Bloco de notas
Arquivo Editar Formatar Exibir Ajuda
<!--18.11.2003, 15:11.  User: "Administrador".  Window title:"Fator - Microsoft Internet Explorer"-->

<!--18.11.2003, 15:11.  User: "Administrador".  Window title:"Continuação do capitulo 05 - Microsoft office word 2003 Beta"-->

<!--18.11.2003, 15:11.  User: "Administrador".  Window title:"Home Key Logger - Quick Start - Microsoft Internet Explorer"-->

<!--18.11.2003, 15:11.  User: "Administrador".  Window title:"Continuação do capitulo 05 - Microsoft office word 2003 Beta"-->
sera apresentado um icone na

<!--18.11.2003, 15:11.  User: "Administrador".  Window title:"Home Key Logger - Quick Start - Microsoft Internet Explorer"-->
[

<!--18.11.2003, 15:11.  User: "Administrador".  Window title:"Continuação do capitulo 05 - Microsoft office word 2003 Beta"-->
[Backspace] [Backspace]o System tray

<!--18.11.2003, 15:11.  User: "Administrador".  Window title:"Home Key Logger - Quick Start - Microsoft Internet Explorer"-->

<!--18.11.2003, 15:11.  User: "Administrador".  Window title:"Continuação do capitulo 05 - Microsoft office word 2003 Beta"-->
[Backspace]T[Ctrl+s]

<!--18.11.2003, 15:11.  User: "Administrador".  Window title:"Home Key Logger - Quick Start - Microsoft Internet Explorer"-->

<!--18.11.2003, 15:11.  User: "Administrador".  Window title:"Continuação do capitulo 05 - Microsoft office word 2003 Beta"-->
. (barra inferior do windows)[Ctrl+s].

<!--18.11.2003, 15:11.  User: "Administrador".  Window title:"Home Key Logger - Quick Start - Microsoft Internet Explorer"-->

<!--18.11.2003, 15:11.  User: "Administrador".  Window title:"Continuação do capitulo 05 - Microsoft office word 2003 Beta"-->
[Backspace] isto significa que o programa esta sendo executado

<!--18.11.2003, 15:11.  User: "Administrador".  Window title:"Home Key Logger - Quick Start - Microsoft Internet Explorer"-->

<!--18.11.2003, 15:11.  User: "Administrador".  Window title:"Continuação do capitulo 05 - Microsoft office word 2003 Beta"-->
e ja esta capturando tudo que for digitado

<!--18.11.2003, 15:12.  User: "Administrador".  Window title:"Home Key Logger - Quick Start - Microsoft Internet Explorer"-->

<!--18.11.2003, 15:12.  User: "Administrador".  Window title:"Continuação do capitulo 05 - Microsoft office word 2003 Beta"-->
[Ctrl+s]

<!--18.11.2003, 15:12.  User: "Administrador".  Window title:"Home Key Logger - Quick Start - Microsoft Internet Explorer"-->

<!--18.11.2003, 15:12.  User: "Administrador".  Window title:"Continuação do capitulo 05 - Microsoft office word 2003 Beta"-->

<!--18.11.2003, 15:12.  User: "Administrador".  Window title:"Fator - Microsoft Internet Explorer"-->

<!--18.11.2003, 15:12.  User: "Administrador".  Window title:"Continuação do capitulo 05 - Microsoft office word 2003 Beta"-->
```

Mostrando data da entrada de dados, hora, nome do programa que foi executado e texto.

Para que o programa seja iniciado automaticamente, basta clicar com o botão esquerdo do mouse sobre ele e, então, escolher o item Autorun, para que o ícone seja ocultado, escolha *Hide icon*. Para que o ícone reapareça, basta pressionar juntas as teclas *CTRL ALT SHIFT* e *M*.

Capítulo 6

DESAFIO HACKER

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

Hackers Lab foi aberto oficialmente em julho de 1999, quando foi também colocado no ar seu web site com uma zona livre de hackeamento. Esta zona de hackeamento nada mais é que um servidor Linux pré-configurado com algumas falhas, falhas essas que podemos encontrar nos servidores que estão em pleno funcionamento.

O objetivo do jogo é chegar ao último nível que seria o *level 17*, você começa no *level 0*, e, de acordo com a sua evolução no JOGO, a senha do próximo nível vai sendo revelada. A idéia é que, por um jogo, o leitor possa aprender, na prática, técnicas de um hacker para invadir um sistema Linux, sendo que, com a evolução do jogo, todas as áreas do conhecimento serão exploradas como conhecimento avançado do sistema operacional Linux, domínio do funcionamento de protocolos de rede, conhecimento avançado de programação Linux, entre outras. Resumindo, ao final do jogo, teremos a certeza de que você se tornou um verdadeiro conhecedor das técnicas hackers. Tudo bem que você ainda não domine todas as áreas do conhecimento hacker, mas estará certo de que passamos para você uma base de conhecimento sólida. De agora em diante, o total domínio de todas as técnicas hackers para você é uma questão de tempo.

Começando o desafio: Para começar a jogar, a primeira coisa que você deve fazer é criar uma conta, assim, sempre que você avançar no

jogo, ele será salvo; sempre que você entrar com seu login e senha, aparecerá o problema no qual você parou.

Para criar uma conta, acesse o site www.hackerslab.org, vá a *Free Hacking Zone*, *Registration* e siga as instruções.

Prova 1

Seria uma boa se alguém tivesse instalado um backdoor nesse sistema, essa é a dica para passar para o próximo nível. Para iniciar, acesse por telnet o endereço:

drill.hackerslab.org

login: level0
password: guest

O Backdoor funciona como uma "entrada pelos fundos", ou seja, um programa que alguém faz quando está em um nível determinado, nesse caso, deve-se buscar por algum backdoor gerado a partir do nível 1 (level1) e que sirva para que aquele que executar esse programa passe a ter privilégios de nível1.

Pode-se dizer que, na maioria dos níveis, você encontrará a necessidade de procurar por programas com *suid*, ou seja, programas que, enquanto são executados, passem privilégios de um nível superior, é isso que se deve aproveitar, utilizar esses programas para que, quando estiverem em execução, iniciem outras aplicações para então abrir um novo *shell* e utilizar esses privilégios.

Para isso, utilizaremos nossa "arma" número 1, o comando *find*, que serve basicamente para localizar arquivos com determinadas características, nome, permissões etc.

Para saber mais sobre o comando *find*, basta digitar no terminal *find* e ler as instruções básicas do comando.

Digite no terminal o comando:

Find / -perm +4000 2>/dev/null

```
Telnet drill.hackerslab.org
[level00@drill level01$ find / -perm +4000 2>/dev/null
/dev/.hi
/dev/audio2
/usr/man/pt_BR/man8/today
/usr/bin/alert
/usr/bin/amos
/usr/bin/ps2
/usr/games/trojka
/usr/local/bin/ssh-signer2
/usr/local/bin/format
/usr/local/bin/bof
/usr/sbin/sendmail
/etc/bof
/etc/one
/bin/su
/lib/security/pam_auth.so
[level00@drill level01$
```

Bom, agora que já se sabe quais arquivos tem *suid*, mas ainda assim não temos muitas informações sobre eles, nesse caso então, deve-se usar o comando *ls* para obter mais detalhes. Como já encontramos os arquivos com o *find*, podemos mesclar o comando *find* (com o qual já conseguimos filtrar os arquivos que nos interessam) com o *ls*. Fazendo desta maneira:

ls -l `find / -perm +4000 2>/dev/null`

```
Telnet drill.hackerslab.org
[level00@drill level01$ ls -l `find / -perm +4000 2>/dev/null`
-rwsr-x---    1 root     wheel      14188 Mar  7  2000 /bin/su
-rwsr-x---    1 level1   level0     13500 Sep 12 11:05 /dev/.hi
-rwsr-x---    1 level18  level17     13785 Aug 27  2002 /dev/audio2
-rws--x---    1 level10  level9      13577 Jul 10  2001 /etc/bof
-rws--x---    1 level16  level15    964040 Jul  5  2001 /etc/one
-rwsr-x---    1 level6   level5      14386 Jul 10  2001 /lib/security/pam_auth.s
o
-rwsr-x---    1 level3   level2      13469 Jul  5  2001 /usr/bin/alert
-rwsr-x---    1 level2   level1      13987 Jul  5  2001 /usr/bin/amos
-rws--x---    1 level9   level8      15739 Jul  5  2001 /usr/bin/ps2
-rwsr-x---    1 level5   level4      30422 Jan 10  2003 /usr/games/trojka
-rws--x---    1 level17  level16    963825 Jul  5  2001 /usr/local/bin/format
-rws--x---    1 level12  level11     14705 Jul 10  2001 /usr/local/bin/bof
-rws--x--x    1 root     root      1768284 Mar 26  2003 /usr/local/bin/ssh-signe
r2
-rws--x---    1 level4   level3      13781 Oct 26  2002 /usr/man/pt_BR/man8/toda
y
-rwsr-s---    1 root     smmsp      559080 Apr 28  2003 /usr/sbin/sendmail
[level00@drill level01$
```

Para conseguir melhores resultados, também pode-se utilizar o comando:

find / -perm +4000 -user level1 -group level0 -exec ls -l {} \;

Tendo em conta que procuramos um *suid* que nos traga um arquivo com permissões do nível1 (você está no nível0), agora temos praticamente todos os arquivos com *suid* e a grande maioria teremos de executá-los para conseguir a passagem para o nível seguinte.

Nesse caso, só nos fixaremos no arquivo */bin/.hi*, que é o programa que buscávamos, assim que o arquivo for executado, você terá privilé-

gios do nível 1. Para verificar qual seu privilégio, digite, no terminal, o comando *whoami*.

Como pode-se ver, o servidor assume como nível 1 (*level1*), isso é porque você está executando um arquivo com privilégios do nível 1. Pronto, feito isso, é só executar a aplicação *pass*, assim você terá em mãos a senha (*password*) do nível 1.

A senha para o nível 1 é *newworld*.

Prova 2

Para acessar o nível 1, vá ao endereço *drill.hackerslab.org* por telnet e, então, digite as informações pedidas:

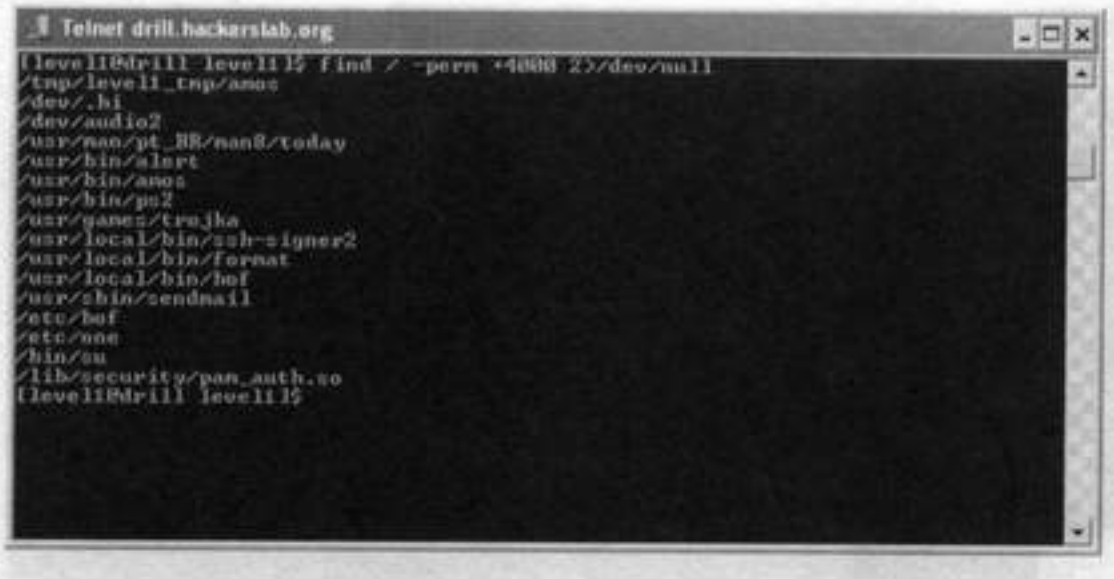
telnet drill.hackerslab.org
login:level1
password: newworld

Um estudante de computação, chamado Matthew está fazendo um trabalho sobre programação em C. Seu professor pediu para que, criasse um script que quando fosse digitado o endereço do arquivo, o programa mostra que tipo de diretório é.

Ele poderia conseguir isso com o utilitário *file* dos comandos Unix, entretanto, existe uma falha, aí é que você vai atuar para, então, conseguir passar para o próximo nível. Tente um dos 12 livros conhecidos como de menos importância dos profetas.

Nesse caso, funcionará como no nível anterior, o problema é um programa que alguém fez e você terá de tentar aproveitar para passar ao nível seguinte.

Assim, como já feito antes utilizando o comando *find* e forem encontrados diferentes arquivos com *suid*, agora deve-se fixar em um arquivo concreto.



Como pode-se ver, é um arquivo que pode ser executado no nível1, mas que tem privilégios do nível2 assim que ele for executado.

Seguindo a dica dada no início do jogo, pode-se verificar o arquivo *amos* que é o nome de um profeta.

Esse programa tem uma falha, é possível executar outra aplicação por meio do próprio arquivo.

Ao chamar o programa, coloque um ";" e a aplicação que você quiser executar. Com isso, será executado o que você quiser, como por exemplo, um shell com o programa *pass* para ver a senha do nível 2.

Vamos chamar o programa e um shell que dessa maneira será sempre melhor, a falha do arquivo vem seguramente devido a que o programa dentro dele mesmo faz uma chamada ao comando *ls* ou a algo parecido mas... fica a pergunta: como deve-se enganar o sistema?

O programa *amos* espera o caminho e o nome de um arquivo, dessa maneira, vamos chamar *;/bin/bash* para que, dentro do processo, seja chamado o shell com privilégios do nível2.

Pronto, agora só falta saber o ID (whoami) para ter certeza de que deu tudo certo, a seguir, dê o comando *pass* para passar de fase.

Agora é com você, tente passar para as próximas fases! No próximo fascículo, você encontrará a resolução dos 4 níveis seguintes. Vai encarar?

Expediente

Papel

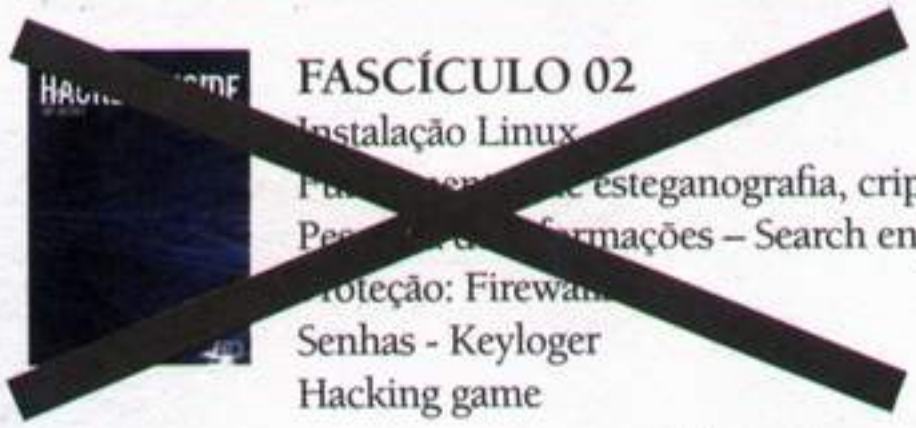
Capa: Triplex 250 g;
Miolo: Sulfite 70 g.

Tipografia

Berkeley (Adobe);
Helvetica (Adobe);
Downcome (www.misprintedtype.com).

EDITORA TERRA LTDA.
Av. Caiapó, 758 – Setor Santa Genoveva
CEP: 74672-400 – Goiânia-GO – Brasil
Tel: (62) 4005-9000 – Fax: (62) 207-1666
Televendas: (62) 4005-9090
e-mail: info@editoraterra.com.br

VOCÊ ACHA QUE JÁ APRENDEU TUDO? ESTÁ ENGANADO. ESTE É SÓ O BÁSICO QUE OS HACKERS PODEM FAZER COM UM SISTEMA. CONFIRA AS PRÓXIMAS EDIÇÕES!



FASCÍCULO 02
Instalação Linux
esteganografia, criptografia
mações – Search engines
oteção: Firewa
Senhas - Keyloger
Hacking game

E MAIS.... UM DESAFIO HACKER! VOCÊ TERÁ DE ACESSAR UM SISTEMA E DESCOBRIR SUAS FALHAS, AS PRIMEIRAS FASES EXPLICADAS PASSO A PASSO.

FASCÍCULO 03
Sniffing
Scripts
Anonimato, utilização do proxy
Tunneling
Antivírus
Hacking Games

MAIS DESAFIO HACKER... A BRINCADEIRA ESTÁ SÓ COMEÇANDO.

FASCÍCULO 04
Cookies: alterações de dados
Mapeamento de rede
DNS queries
PHP: falhas e exploits
Spoofing e Scanning
Hacking Games

DESAFIO HACKER – NÍVEL AVANÇADO

FASCÍCULO 05

TOP SECRET

ISBN: 85-7491-167-4
9 788574 911670 >